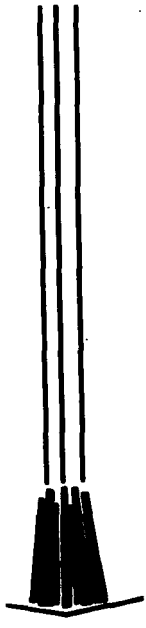
57
24.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"CAMPUS ARAGÓN"



SEGURIDAD INFORMATICA Y PLANES DE CONTINGENCIA EN CASOS DE DESASTRE

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A :

LILIA RODRIGUEZ MUÑOZ

ASESOR DE TESIS: ING. MA. GABRIELA GONZALEZ HDEZ.

MÉXICO 1997

AGRADECIMIENTOS

A mis padres:

Por el amor incondicional que siempre me han brindado y por enseñarme el camino a seguir.

A mi hijo Mario Alberto:

Con todo mi amor, gracias por permitirme conocer la alegría de ser madre.

A mis hermanos Alejandro, Sergio, Leticia, Héctor, Juan Alberto, Gerardo y Ricardo:

Por su apoyo en todos los aspectos de mi vida y por su ejemplo.

A mis sobrinos Alejandro, Yadira, Karen, Sergio, Paola, Jimena, Rubí, Carlos y Erick:

Por darme su cariño y alegría infantil.

A mis tías Maricela y Bertha:

Por su cariño y apoyo a lo largo de toda mi vida.

A mis amigos:

Por su amistad, la cual es uno de los tesoros más valiosos que poseo.

A mi familia en general:

Por estar siempre conmigo brindándome su cariño.

RECONOCIMIENTOS

Al Ing. Ma. Gabriela González Hernández

Por su tiempo y dedicación durante el desarrollo del presente trabajo de tesis.

A la Universidad Nacional Autónoma de México

Por brindarme la oportunidad de una formación profesional.

Al Instituto Mexicano del Petróleo

Por las facilidades otorgadas.

Al Ing. Cesar A. del Cid Orozco

Por su apoyo y ayuda.

INDICE

INDICE

PAG.

PAG.

OBJETIVO

OBJETIVO

En el presente trabajo se describen los diferentes conceptos relacionados con seguridad informática en general con el objetivo de enfátizar su importancia, así como la de desarrollar e implementar en centros de procesamiento un Plan de Contingencia en Casos de Desastre Informático, el cual está orientado a desarrollar medidas tanto preventivas como correctivas para salvaguardar la integridad de la información, del equipo de cómputo y asegurar la continuidad de las funciones informáticas prioritarias dentro de una empresa en caso de que ocurra un desastre, así como de volver a las condiciones operativas normales en el mínimo de tiempo posible.

INTRODUCCION

INTRODUCCIÓN

Actualmente, en la mayoría de las empresas es indispensable la utilización de sistemas informáticos para lograr un funcionamiento adecuado y competitivo, por lo que la información y los procesos para manejarla cobran vital importancia: Es por eso que a la seguridad e integridad de los datos, sistemas y equipo de cómputo debe dárseles la importancia que merecen.

El aumento de actividades efectuadas con sistemas informáticos es cada vez más común en todas la áreas de la vida cotidiana, sobre todo desde la aparición en el mercado de las computadoras personales. En el caso de las empresas, el que cada vez sean más los procesos controlados mediante sistemas informáticos, hace que se dependa en gran medida del apoyo que el área de sistemas proporciona. Un contratiempo en sus sistemas de información puede traer consecuencias graves y poner en riesgo la continuidad de las operaciones de una empresa. La automatización en el manejo de información permite tomar decisiones de alto nivel oportunamente, lo cual le da un valor inapreciable como uno de los activos principales de las empresas, de ahí la importancia de proteger lo más posible la información y los bienes que ésta representa.

Existen incontables riesgos que ponen en peligro tanto a la información como al equipo informático. La magnitud de las consecuencias de afrontar un desastre debido a estos riesgos varía dependiendo de las causas y de la intensidad del mismo, por lo que las pérdidas tanto de información como de equipo pueden ser parciales e incluso totales. Por ello, las medidas de seguridad deben ser observadas por cualquier usuario de computadoras, independientemente del tipo de equipo de computo o sistema que se emplee, ya que si bien la pérdida puede no catalogarse como un desastre informático, siempre resulta molesto sufrir cualquier contratiempo.

Se debe tener presente que no todos los riesgos de desastre pueden ser eliminados por completo, pero si es posible tomar medidas preventivas y correctivas enfocadas a evitarlos o a reducir lo más posible su probabilidad de ocurrencia, así como de minimizar los efectos del desastre en caso de que éste ocurra. Para lograrlo, es necesario estudiar y controlar en la medida que sea posible las causas y efectos que se pudieran presentar.

Anteriormente, los esfuerzos encaminados a la seguridad informática se enfocaban primordialmente a prevenir y controlar contingencias en centros de cómputo, ya que en ellos se encontraba concentrada la mayor parte de la información de procesamiento y el equipo de cómputo de las empresas; pero la situación a cambiado, si bien es cierto que los centros de

cómputo siguen vigentes, la tendencia a la utilización de microcomputadoras y redes de éstas es cada vez mayor. Pero independientemente de cual sea la infraestructura utilizada, es igualmente importante su seguridad, ya que el valor y la importancia tanto de la información como del equipo informático es indiscutible en cualquier caso.

Un desastre informático puede ser causado por factores humanos, naturales o accidentales; los primeros pueden ser provocados por descuidos o acciones mal intencionadas (incendios, pérdida de datos, robo, etc.) ya sea por parte del personal de la propia empresa o individuos externos; los segundos pueden ocurrir por daños provocados por fenómenos naturales (terremotos, inundaciones, huracanes, etc.), mientras que los accidentes pueden deberse a fallas en los equipos y/o instalaciones.

Las medidas de seguridad que deben tomarse varían dependiendo del tipo de instalación informática con que se cuente. Por ello, en el presente trabajo se describen los conceptos de seguridad en computadoras personales, en sistemas de redes y en general en cualquier centro de cómputo.

Hoy en día, una de las principales causas de daños a la información se debe a los llamados virus informáticos. Este tipo de riesgo presenta una situación muy particular, ya que se autoreproducen, y esto, aunado a la aparición continúa de nuevos tipos de virus y a la falta de precauciones por parte de los usuarios, a hecho que su proliferación no pueda ser eliminada. El daño que provoca un virus informático varía dependiendo del tipo del mismo, puede ir desde lo chusco hasta daños severos a la información e incluso en algunos casos hasta al equipo de cómputo. Debido a lo anterior, se considero un capítulo del presente trabajo para explicar con más detalle sobre sus causas, efectos y medidas de seguridad.

En el caso de los centros de cómputo, las medidas y acciones que se tomen deben formalizarse dentro de un Plan de Contingencias en caso de Desastre Informático (PCDI), enfocado a las necesidades específicas de cada empresa. La elaboración de dicho plan debe realizarse en forma responsable y consciente de su importancia, ya que en caso de que ocurra un desastre puede ser el factor clave que permita la continuidad de las funciones de la empresa en forma adecuada.

CAPITULO 1

RIESGOS, DESASTRES INFORMATICOS Y MEDIDAS PREVENTIVAS

1.1. INFORMACIÓN Y RIESGOS INFORMATICOS

1.1.1. VALOR DE LA INFORMACION Y DATOS

La generación de grandes bloques de información se elevó rápidamente a partir de la aparición de la imprenta de tipos móviles alrededor del año 1500, lo cual propicio que la información fuese cobrando cada vez mayor importancia.

Al hacer su aparición las computadoras digitales hacia el año de 1950, su rapidez, flexibilidad y poder analítico hizo que la producción de información se elevará repentinamente, impulsando la era de ésta. Nos encontramos dentro de una Segunda Revolución Industrial, causada por el impacto del acelerado avance tecnológico de los últimos años, en donde la economía se basa en la producción, administración y utilización de la información.

Debido a la transcendencia que ha cobrado la información, debe ser considerada como un recurso de igual importancia que el personal, las instalaciones o el capital de cualquier empresa.

La información tiene varias características: precisión, importancia, forma, fuente, completitud, oportunidad y VALOR. Cualquier alteración en alguno de los atributos anteriores afecta el valor de la información.

El valor económico que se asigna a la información es relativo, ya que depende de quien lo obtiene o utiliza. Por lo general, el valor se da en función a la cantidad de conocimiento que contiene, más que a la cantidad de información en si. En algunas ocasiones la información es sinónimo de poder para quien la posee.

INFORMACION Y DATOS

Aunque la información y los datos están íntimamente relacionados, no significan lo mismo. Para poder determinar cuales son las diferencias entre ambos, se presentan a continuación algunos conceptos al respecto:

INFORMACION

Es un conjunto de datos con un valor real o percibido por el usuario. La información es el resultado de efectuar procedimientos en base al conocimiento que se tiene de los datos con el objeto de darles significado, propósito y utilidad, proporcionando bases para apoyar la toma de decisiones o resolver algún problema dentro de una organización.
La información puede ser interna o externa, dependiendo si es originada dentro o fuera de la empresa.

DATOS

Los datos pueden ser números, letras o símbolos. Su valor depende del uso que se les de, ya que por si mismos no tienen ningún significado; cuando son procesados para proporcionar algún conocimiento útil (resultados, conocimientos, etc.), se transforman en información.
El almacenamiento de datos es importante cuando son útiles para las actividades de una empresa en un periodo de tiempo largo.

De los conceptos anteriores, podemos concluir que la diferencia básica entre datos e información, es que mientras que ésta última siempre es relevante, los primeros pueden no serlo en un momento dado.

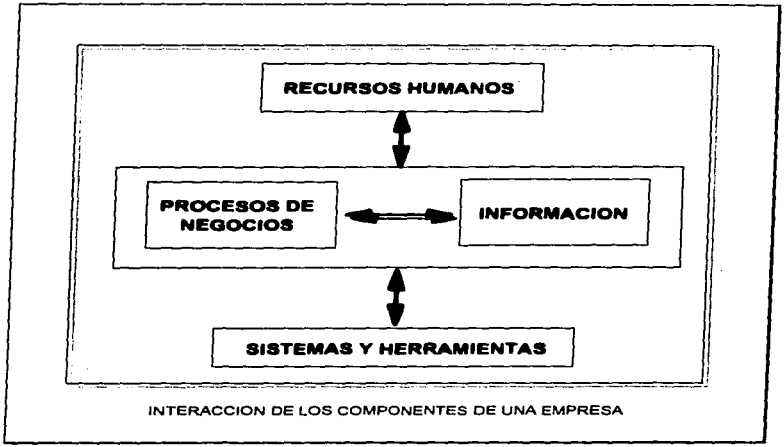
También cabe hacer la observación que la conceptualización de la información es relativamente subjetiva, ya que puede depender de criterios o puntos de vista específicos, y en determinado momento lo que para alguien representa información, para otra pueden ser sólo datos.

1.1.2. SISTEMAS DE INFORMACION BASADOS EN COMPUTADORA

SISTEMA

Un sistema es un conjunto de elementos interrelacionados cuyo objetivo común es apoyar los requerimientos de una organización, incluyendo las operaciones rutinarias, la comunicación de los datos e informes, la administración de actividades y la toma de decisiones.

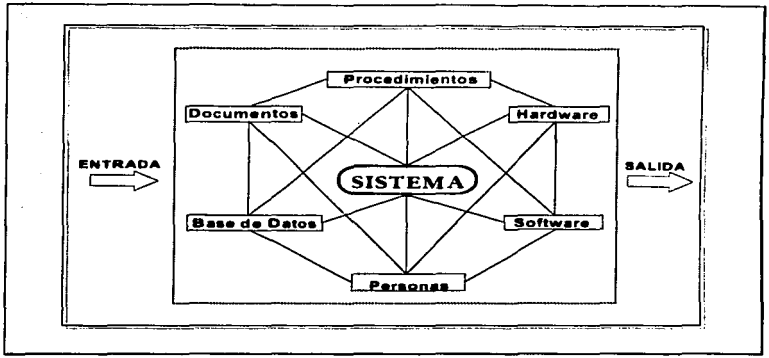
Los elementos que conforman un sistema son: sus componentes, el medio ambiente que lo rodea, sus fronteras y las entradas y salidas. Una empresa es en sí un sistema, donde la información es vital para su existencia.



INTERACCION DE LOS COMPONENTES DE UNA EMPRESA

Un sistema de información basado en computadora es un conjunto de elementos organizados para realizar algún método, procedimiento o control mediante el procesamiento de información. Un sistema de éste tipo se justifica cuando la capacidad de procesamiento de una empresa mejora en relación al funcionamiento con el sistema convencional.

Los elementos que constituyen un sistema de información basado en computadora son: software, hardware, personas, bases de datos, documentación y procedimientos.



- SOFTWARE
  Programas, estructuras de datos y documentación relacionada que se emplea para desarrollar el método, procedimiento o control requerido.

- HARDWARE
  Dispositivos electrónicos (CPU, memoria, etc.) que dan la capacidad de cómputo y dispositivos electromecánicos que proporcionan las funciones del exterior (sensores, motores, etc.)

- BASES DE DATOS
  Conjunto de información organizada, la cual se manipula mediante el software.

- PERSONAS
  Usuarios y operadores tanto del software como del hardware.

- DOCUMENTACION
  Manuales en donde se describe la operación y/o uso del sistema.

- PROCEDIMIENTOS
  Definen el empleo específico de cada elemento del sistema.

1.1.3. RIESGOS INFORMATICOS

Desde un punto de vista informático, un riesgo es cualesquiera circunstancia de cualquier naturaleza u origen que representa una amenaza para la integridad de la información o de las instalaciones. Existen diversos factores de riesgo, entre los que se encuentran los siguientes:

UBICACION DEL AREA INFORMATICA.

El medio ambiente es un factor fundamental para determinar a los tipos de riesgo a que puede estar expuesta un área informática. Algunos de los factores a considerar son los siguientes:

- ◊ Si el área en donde se encuentra el equipo de cómputo es visible a la calle, es más alto el riesgo de que sufra atentados de cualquier tipo.
- ◊ Si se encuentra ubicada en alguna zona en donde se manejen materiales inflamables, corre el riesgo de que se pueda suscitar un incendio.
- ◊ Se tiene que determinar si es susceptible de ataques por bandas o maleantes.
- ◊ Se debe saber si las instalaciones fueron diseñadas tomando en cuenta los factores del medio ambiente que puedan causar daños al equipo.

ACCESO AL AREA INFORMATICA.

La inversión empleada en bienes informáticos (tanto de software como de hardware) puede verse afectada si es dañada ya sea con o sin intención. Por ello, el acceso de personas tanto de la propia empresa como externo debe ser controlado. Entre los aspectos a considerar en este punto están:

- ◊ Si hay vigilantes que lleven un control del acceso al área.
- ◊ Si el personal autorizado puede identificarse fácilmente de los que no pertenecen al área.
- ◊ Conocer los métodos que se utilizan para restringir el acceso.
- ◊ Establecer si sólo gente autorizada tiene acceso al área.

- ◊ Conocer las medidas que se toman en caso de que alguien no autorizado entre al área.

- ◊ Si la vigilancia se realiza sólo en horas laborables o continuamente.

- ◊ Si el personal de limpieza conoce lo delicado y costoso que es el equipo de cómputo.

- ◊ Si a personas externas con autorización se les pide corroborar su identidad y si se lleva un control de sus entradas y salidas. También se debe saber cuales son las restricciones que se les aplican a fin de evitar robo de información, sabotaje, etc.

PERSONAL AUTORIZADO.

- ◊ Verificar que el personal sea de absoluta confianza, y que las contrataciones no se realicen sin conocer los antecedentes delictivos.

- ◊ Asegurarse de que no existe alguien del personal descontento, ya que esto podría originar un daño intencional a instalaciones o sistemas.

- ◊ Determinar si la empresa considera que existe un riesgo en este punto y si se toman en cuenta estas medidas de seguridad.

- ◊ Si no se cuenta con un control de acceso de personas, se corre el riesgo de que pueda ocurrir un sabotaje, robo de información y/o equipo, etc.

CAPACITACION AL PERSONAL.

- ◊ Conscientizar al personal de la importancia de mantener la seguridad física del área informática y capacitarlos para evitar daños al equipo por descuido o mala operación.

- ◊ Capacitar a los empleados para actuar en caso de emergencia. Si el personal desconoce que hacer ante cualquier tipo de siniestro, pueden aumentar las pérdidas tanto económicas como humanas.

- ◊ Es importante que se lleven a cabo simulacros para casos de emergencia, ya que en este tipo de situaciones la teoría no es suficiente.

EMERGENCIA POR FALTA DE ENERGIA ELECTRICA.

- ◊ Cuando las actividades que se realizan en el equipo informático son vitales para la operatividad de la empresa, es importante contar con un sistema de energía eléctrica de emergencia. Para las PC's, se puede instalar fuentes de energía ininterrumpida para respaldar en caso de falta de electricidad.

- ◊ Conocer si el servicio eléctrico de la red pública puede influir en la seguridad.

- ◊ Los tableros de control deben encontrarse en un lugar accesible en las salidas del área.

- ◊ Los cables eléctricos deben encontrarse protegidos contra agua, para que no resulten dañados en caso de encharcamiento o goteras.

AIRE ACONDICIONADO.

En caso de que las instalaciones cuenten con aire acondicionado, existen algunos riesgos que deben ser tomados en cuenta:

- ◊ En caso de tener un centro de cómputo, es conveniente que la sala de cómputo tenga su sistema de aire acondicionado independiente debido a que sus requerimientos de temperatura y humedad son diferentes al resto del centro. Con lo anterior se evita que un incendio se origine en los ductos del aire acondicionado.

- ◊ El aire acondicionado debe desconectarse cuando se interrumpa la energía eléctrica en el tablero general, ya que éste podría avivar el fuego en caso de incendio.

RIESGOS DE DAÑOS POR AGUA

- ◊ Es importante saber en donde se localizan las tuberías de agua y si representan un riesgo para las instalaciones.

- ◊ Cuando se trata de un centro de cómputo ubicado en el sótano, es necesario que se tenga una bomba para poder desalojar en caso de encharcamientos o inundación.

- ◊ Si se tiene piso falso, el drenaje debe ser el adecuado, ya que de lo contrario podría provocarse un corto circuito en el cableado.

ABUSO COMPUTACIONAL

Los usuarios son la amenaza más grande a las organizaciones, ya que generalmente si un usuario obra de mala fe, los daños causados por éste pueden ser mayores a los de un ataque externo. Según el National Center for Computer Crime Data de los Angeles, Cal., cerca del 70% de los casos reportados se deben a usuarios autorizados. El Bank Administration Institute calculó, que tan solo en 1986, los fraudes por computadora a bancos en EU ascendieron a 1 billón de dólares, con una tendencia a incrementarse cada año. El motivo de éste tipo de ataques varía desde obtención de un beneficio personal, hasta una venganza.

OTROS RIESGOS

- ◊ Desastres naturales: sismos o terremotos, lluvia e inundaciones, huracanes, etc.
- ◊ Interrupción de las comunicaciones.
- ◊ Pérdida de información por errores humanos.
- ◊ Incumplimiento de proveedores.
- ◊ Contagio de virus informáticos.
- ◊ Fallas en el software o hardware, etc.

1.2. DESASTRES INFORMATICOS

1.2.1. DEFINICION DE DESASTRE INFORMATICO

Un desastre informático es cualquier evento que interrumpe o afecta la operación normal de un sistema por un período de tiempo significativo, causando interrupción en las actividades de una empresa, pérdida de funcionalidad en los procedimientos, daño a instalaciones, datos y archivos. El alcance y la severidad de los posibles desastres varían ampliamente y pueden calificarse en base a el tiempo de interrupción y los factores afectados. Las causas de un desastre informático pueden ser por riesgos propios de la naturaleza, accidente o factores humanos.

1.2.2. CLASIFICACION DE LOS DESASTRES

Existen diferentes causas de desastres:

FACTORES HUMANOS:

- Robos
- Error de operación
- Vandalismo
- Huelgas
- Pérdida de personal
- Infecciones de virus
- Disturbios civiles
- Guerras
- Terrorismo
- Incendios

FENOMENOS NATURALES:

- Terremotos
- Inundaciones
- Huracanes
- Tormentas o descargas eléctricas
- Roedores e insectos
- Incendios
- Epidemias, plagas
- Sequías
- Temperaturas extremas

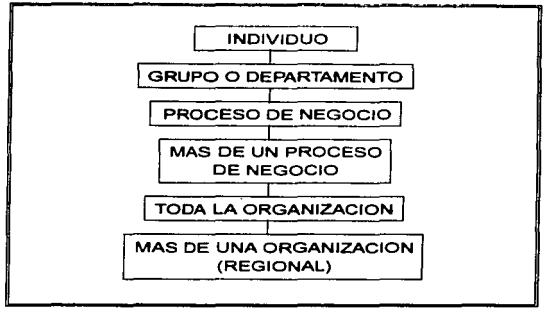
ACCIDENTALES:

- Falta de energía eléctrica
- Radiaciones
- Defectos o fallas estructurales
- Interrupción de servicios
- Fallas en el sistema de aire acondicionado
- Cortos circuitos
- Fallas en las comunicaciones
- Medio ambiente

FACTORES DE SOFTWARE/HARDWARE:

- Fallas en los sistemas operativos
- Errores de programación
- Pérdida de las bases de datos
- etc.

Es posible jerarquizar los desastres en base a lo que afecten:



También, dependiendo del daño o grado de destrucción que provoquen, los desastres se pueden agrupar en categorías, entre las más comunes se encuentran las siguientes:

Destrucción masiva

Se tiene una destrucción total del área informática. Los sistemas no pueden seguirse procesando. Existen daños tanto al software y al hardware como a las comunicaciones. La causa puede ser temblor, incendio, inundación o por una explosión mayor por bomba.

Daños mayores

Existen imposibilidad para continuar con el procesamiento de la información, al grado de requerirse un sitio alterno para recuperar y levantar la información.

Este grado de daños puede deberse a temblor, explosión, edificio colapsado, inundación parcial, fuego parcial, vandalismo o sabotaje.

Destrucción parcial y/o temporal

Se tiene una interrupción en el procesamiento por pérdida de elementos clave, pero no se tiene una destrucción física.

Las causas pueden ser huracanes, caminos de acceso bloqueados, interrupción de energía eléctrica, incendio menor, vandalismo, sabotaje, caída de enlaces durante la transmisión de datos, interrupción en los servicios de comunicaciones, fugas de gas, huelgas, o puede deberse a alguna afectación al edificio en donde se encuentran las instalaciones informáticas.

Daño o interrupción menor

En este caso el procesamiento de información se ve interrumpido temporalmente y no se presenta destrucción de software o de hardware.

Puede deberse a fallas en el hardware, errores de operación, daño en los archivos o en bases de datos, fallas en el sistema operativo, negligencia de usurarios, etc.

1.2.3. CASOS REALES DE DESASTRES INFORMATICOS

Entre algunos casos de desastres informáticos reales relevantes, se pueden mencionar los siguientes:

En 1988 se incendio la central telefónica Hinsdale Illinois, resultando afectados alrededor de 500,000 usuarios. Esta misma compañía se vio envuelta en otro desastre en 1990, cuando fueron cortados sus cables de fibra óptica.

En 1985, durante los sismo de México, resultaron afectadas muchas empresas, ya que extensas áreas estuvieron incomunicadas, el servicio Lada estuvo interrumpido y varios centros de cómputo completos y redes de comunicación resultaron considerablemente dañados.

Durante el sismo en San Francisco en 1989, la energía eléctrica estuvo interrumpida por periodos prolongados y las centrales telefónicas resultaron seriamente afectadas.

En enero de 1991, empleados de AT&T cortaron accidentalmente un cable de fibra óptica que daba servicio de larga distancia al 40% de la ciudad de Nueva York; como el centro de operaciones de la empresa no había sido notificado sobre dicho trabajo, las computadoras no se habían programado para dar prioridad a la transmisión de datos para el control de tráfico aéreo. Como consecuencia, hubo pérdida en los radares de rango amplio de los tres aeropuertos principales de la ciudad durante más de hora y media.

El 26 de febrero de 1993, en el Word Trade Center de Nueva York ocurrió una explosión a consecuencia de un ataque terrorista. En el edificio se encontraban más de 900 negocios, varios de ellos eran compañías con centros de procesamiento informático. Las instalaciones fueron reabiertas hasta abril de ese mismo año; quienes contaban con un plan de recuperación pudieron continuar operando en sitios alternos durante ese tiempo.

1.3. RIESGOS A LA SALUD DE LOS USUARIOS

1.3.1. RIESGOS DE DAÑOS A LA SALUD ASOCIADOS AL USO DE COMPUTADORAS

Existen diferentes riesgos que pueden ocasionar daños a la salud de los usuarios de computadoras. Los problemas que se presentan se asocian al empleo de monitores, al medio ambiente de trabajo y a los hábitos del usuario al utilizar el equipo.

Las personas que están expuestas a tener alteraciones a la salud asociadas al uso de computadoras, son aquellas que trabajan con el equipo durante períodos de tiempo prolongados (cuando menos 26 horas a la semana), y los riesgos que tienen son los siguientes:

- PROBLEMAS EN EL SISTEMA ESQUELETO-MUSCULAR
- PROBLEMAS DE VISION
- ESTRESS
- RIESGOS PARA LA REPRODUCCION

los daños y causas que pueden llegar a presentarse en cada una de ellas se describen a continuación:

PROBLEMAS EN EL SISTEMA ESQUELETO-MUSCULAR.

Es común que los usuarios de computadora permanezcan largos períodos de tiempo en posiciones inadecuadas; como consecuencia, se comienza con problemas en el sistema Esqueleto-Muscular, tales como:

- Desordenes en músculos, tendones y ligamentos, especialmente en espalda, cuello, hombros y región lumbar.
- Dolores de cabeza.
- Tensión e inflamación en muñecas, manos, cuello, espalda, brazos y piernas.

Los daños ocasionados pueden variar desde leves molestias hasta problemas severos, incluso incapacidad total. Las principales causas de que se presenten estos tipos daños a la salud son:

- Permanecer sentados en posición incorrecta durante largos períodos de tiempo.
- Utilizar muebles mal diseñados.
- Movimientos repetidos constantemente en el teclado, mouse y dispositivos.

PROBLEMAS DE VISION.

Al hacer uso de las computadoras, se tiene que trabajar muy cerca de los monitores de éstas, lo que ocasiona problemas en el sistema ocular:

- Tensión en los ojos
- Irritación en los ojos
- Fatiga visual y visión borrosa
- Dolores de Cabeza

Los motivos de que se presenten este tipo de molestias están relacionados al uso de monitores y su efecto sobre los músculos de los ojos:

- El observar objetos o figuras a corta distancia fatiga los músculos CILIARES, que son los encargados de cambiar la forma del lente para que el ojo pueda enfocar.

- Al ver objetos brillantes alternados con obscuros se tensionan los músculos del IRIS, cuya función es ajustar el tamaño de la pupila dependiendo de la intensidad de la luz.

- El constante movimiento de los ojos entre pantalla y documentos provoca que los músculos OCULOMOTORES se fatiguen, ya que son los encargados de mover los ojos hacia los lados, arriba o abajo.

Las causas que pueden agudizarlos son las siguientes:

- Mal diseño de monitores (caracteres o pantallas pequeñas).
- Parpadeo en el monitor (por mal estado o ajuste erróneo).
- Mala iluminación del área de trabajo (excesiva, reflejos, etc.).

ESTRESS.

El estress es un mecanismo de respuesta natural del organismo ante demandas adicionales de energía para lapsos cortos de tiempo. Si se prolonga este estado durante períodos largos o ininterrumpidos, se crean problemas de salud, incluso la muerte, ya que se asocia el estress con paros cardiacos.

El estress en usuarios de computadoras es el más alto según el NIOSH (National Institute of Occuppational Safety Health), y tienen el doble de incidencia de paros cardiacos que otros grupos de trabajadores. Los síntomas que se pueden presentar debido al estress son:

- Irritabilidad.
- Depresión y debilidad.
- Vulnerabilidad a las enfermedades.
- Insomnio.
- Presión arterial alta.
- Incapacidad de relajarse sin TV, alcohol o drogas.
- Sensación de fatiga con facilidad.
- Dolores de cabeza.
- Falta de apetito.
- Ulcera.
- Irregularidades menstruales en mujeres.
- Tensión muscular.

Existen varias causas que provocan el estress:

- Trabajo repetitivo y bajo presión.
- Estaciones de trabajo mal diseñadas (muebles y sillas mal diseñadas, mala iluminación).
- Condiciones ambientales inadecuadas (ruido, mala ventilación, etc.).
- Fijar la vista al monitor durante mucho tiempo.
- Organización deficiente y desarrollo incorrecto del trabajo.

RIESGOS PARA LA REPRODUCCION.

Aunque todavía no se ha comprobado totalmente, se ha observado que existe una relación entre el uso de computadoras y problemas durante el embarazo, incluyendo abortos.

La incidencia de abortos y defectos de nacimiento es mayor entre mujeres que trabajan más de veinte horas a la semana con computadoras. Se han efectuado investigaciones que sugieren que los factores que influyen en este tipo de problema son los monitores (debido a la radiación electromagnética), el estress, el ambiente y los hábitos higiénicos en el trabajo.

Los monitores emiten diferentes tipos de radiación electromagnética:

- Luz visible.
- Luz ultravioleta.
- Radio frecuencia.
- Radiación de muy baja frecuencia.
- Rayos X.

Son las radiaciones de muy baja frecuencia hacia donde se están enfocando las investigaciones. Anteriormente no se creía que la exposición a este tipo de radiación afectará a los humanos, pero actualmente se tienen pruebas de que la radiación electromagnética vlf y elf producen efectos nocivos, aunque aún no se han determinado con claridad. Las radiaciones de muy baja frecuencia están asociadas a campos eléctricos y magnéticos y se producen en un rango muy amplio de frecuencia, desde frecuencias altas (**Rayos X**) hasta muy bajas (**vlf y elf**). A frecuencias altas corresponden niveles altos de energía. Para los diferentes tipos de radiación, la alta frecuencia está relacionada a un mayor potencial de riesgo.

1.3.2. MEDIDAS PARA PREVENIR DAÑOS A LA SALUD DE USUARIOS

Una vez que se conocen los posibles daños y las causas de estos para los usuarios, se deben tener en cuenta las medidas preventivas adecuadas para minimizar los efectos nocivos que puedan presentarse por utilizar computadoras. A continuación se mencionan cuales serían las acciones a tomar para cada riesgo:

SISTEMA ESQUELETO-MUSCULAR.

Las medidas a tomar están orientadas e evitar problemas de salud en el sistema Esqueleto-Muscular:

- Silla y Mesa ergonómicas.
  La ergonomía significa adaptabilidad, es decir, que un mueble ergonómico es aquel que puede ajustarse a las necesidades de cada usuario. Es importante que la silla este bien diseñada y que la Mesa pueda ajustarse para el monitor que se utilice.
- Soporte acojinado y desmontable para las muñecas.
- Soporte para documentos.
- Teclado que se pueda acercar o alejar de la pantalla.
- Espacio suficiente entre rodillas y mesa.
- Suficiente espacio para todo el equipo.
- Soporte de descanso para pies.
- Blindaje contra el ruido de impresora.
- Recesos durante la jornada.

VISION

- Recesos por períodos de quince minutos por cada tres horas de trabajo en la computadora, durante los cuales pueden realizarse actividades laborales que no requieran el empleo de la misma.
- Tomar un leve receso cada diez minutos para observar objetos distantes durante algunos segundos.
- Los monitores deben estar diseñados con las características siguientes:
  - Caracteres grandes y nítidos.
  - Control de contraste y brillo sin parpadeos.
  - Pantalla con inclinación ajustable.
  - Teclado independiente.
  - Pantalla antirreflejante.
- Iluminación adecuada, evitando que la luz exterior incida sobre la pantalla o los ojos del usuario. La luz ambiental debe ser la mitad de intensa que la que se requiere para papel y de preferencia que el usuario pueda ajustarla.
- Emplear lentes especiales.

- Ejercicios de relajación para los ojos, como moverlos hacia arriba y abajo, de izquierda a derecha, en círculos y hacia los extremos inferiores y superiores; también se puede colocar el dedo índice a unos cuantos centímetros e irlo alejando sin dejar de enfocarlo y luego regresarlo lentamente, cerrar los ojos, descansar y relajarse por unos cuantos minutos.
- Utilizar pantallas protectoras especiales para monitores de computadoras.

ESTRESS

El estress es un problema individual, por lo que requiere soluciones de tipo personal, tales como caminar, hacer ejercicio, practicar técnicas de respiración y de relajación, tomar sesiones motivacionales, etc.

Dichas soluciones funcionan en forma parcial y temporalmente, sin embargo, conforme se adquiere conciencia del problema, se detecta que la mejor solución es adecuar el espacio y las condiciones de trabajo.

RIESGOS PARA LA REPRODUCCION

- Adquisición por parte de las empresas de la mejor tecnología del mercado.
- Empleo de filtros o dispositivos para aminorar la radiación.
- Iluminación adecuada para evitar reflejos en la pantalla del monitor.
- Empleo de lugares de trabajo ergonómicos.
- Tomar recesos después de tres horas de trabajar con monitores o programar el trabajo para que no se tenga que permanecer mas de cuatro horas diarias en ellos.
- Reubicar parcialmente a las mujeres embarazadas a áreas donde no se requiera el uso constante de la computadora.
- La radiación electromagnética se puede disminuir empleando algún tipo de blindaje o utilizando tecnología avanzada que produzca menos cantidad de radiación o en menor intensidad.
- Tratar de disminuir el estress mediante el mejoramiento de las condiciones de trabajo.

1.4. MEDIDAS DE PREVENTIVAS

El valor de los bienes informáticos tanto hardware como software es alto, por lo que se deben tomar medidas que salvaguarden su integridad. Además, un ambiente de seguridad entre el personal y los clientes comunica una imagen de solidez y profesionalismo.

1.4.1. MEDIDAS PARA PREVENIR DESASTRES

Si bien es imposible evitar en su totalidad que ocurra algún desastre, si podemos disminuir el riesgo de que se presente. Para ello, es conveniente tomar algunas medidas preventivas, tal como las que se mencionan a continuación.

- Medidas para evitar que se llegue a producir un incendio.
  Debe instalarse, de acuerdo con las necesidades y características de la empresa, equipos o sistemas contraincendio. Debe restringirse el fumar dentro del área.

- Instalar unidades de respaldos, no breacks o fuentes emergentes de energía, para evitar perdida de información debido a interrupción de electricidad.

- Control de acceso a las instalaciones de la empresa.
  Debe implementarse un sistema de vigilancia de acuerdo a las necesidades y características de la empresa. El acceso al área informática debe ser restringido.

- Medidas para la seguridad física de instalaciones y edificios.
  Para lo cual los centros de datos o las instalaciones en donde se ubican las áreas informáticas deben estar en apego a las normas de construcción correspondientes (de tal forma que puedan soportar terremotos, bombas, inundaciones y otros elementos de la naturaleza)

- Tomar medidas preventivas para que no se produzcan inundaciones dentro de las instalaciones de la empresa, tal como evitar que el área informática sea instalada en sótanos.

- Medidas de seguridad contra ataques terroristas.
  Debe instruirse al personal de la empresa a actuar en caso de que se detecte algún acto terrorista:

- Si una persona es testigo de que se está cometiendo un atentado, debe guardar la calma, procurando no involucrarse ni impedirlo y dando aviso con toda discreción al encargado de seguridad.

- Como medida preventiva, se debe reportar a cualquier persona sospechosa.

- Si se detecta algún objeto extraño o inusual en su área de trabajo, no moverlo, no tocarlo, no acercarse ni tratarlo de abrir (portafolios sin dueño, maletas abandonadas, sobres muy abultados, vehículos mal estacionados, etc.), y reportarlo al personal de seguridad.

- Ubicación adecuada del centro de trabajo.
  Las instalaciones deben encontrarse localizadas lejos de fuentes de amenazas a su alrededor.

- Ubicación adecuada del área informática.

  Debe ubicarse en un lugar poco transitado dentro del centro de trabajo.

  En planta baja de preferencia.

  Evitar que sea instalarla cerca de fuentes de generación magnética.

- Acatar las políticas de respaldo de información establecidas, con información actualizada y depurada. Los respaldos pueden ser en cintas, discos flexibles, cartuchos, microfichas o discos ópticos.

- Efectuar auditorías periódicas a los respaldos a fin de asegurarse que la información sea reciente, completa y confiable.

- Para evitar errores humanos no intencionados, se debe capacitar a al personal y proporcionar a los usuarios los procedimientos de arranque, respaldo y apagado del equipo.

- Capacitar al personal en la operaciones de emergencia y mantener todos los manuales de operación actualizados.

- Instalaciones de seguridad para almacenaje de registros y datos importantes, archivos maestros y documentación legal.
  El almacenamiento se debe llevar a cabo en algún lugar remoto de acuerdo a las normas de protección. También es conveniente contar con bóvedas de seguridad.

- Proporcionar mantenimiento a los sistemas, tanto de software como de hardware.

- Evitar la piratería del software para reducir la incidencia de virus informáticos.

- Instalaciones adecuadas para equipo de cómputo.
  Estas deben evitar vibración, electricidad estática, radiación electromagnética, radar, humo, polvo, sustancias contaminantes, humedad y temperatura inadecuadas, etc.

- Implementar un programa continuo de limpieza y obediencia a las normas de seguridad
  Establecer reglas para evitar que el personal coma o fume dentro del área informática, manteniendo el orden y limpieza dentro de la misma. Se pueden efectuar auditorías sorpresa para determinar si existen anomalías o violaciones a las normas implantadas.

- Instalación de escaleras de emergencia.
  En caso de edificios altos, es idóneo que las escaleras de emergencia cuenten con las siguientes características: el cubo en donde se encuentren construido con material incombustible resistente al fuego por lo menos durante el periodo estimado de desalojo, que cuente con iluminación de emergencia y ventilación al exterior; que las puertas de acceso sean resistentes al fuego y los escalones deben ser de material antiderrapante. También es conveniente que cuente con rociadores de agua.

- Efectuar una revisión periódica en las líneas de comunicación para evitar problemas con la transmisión de datos.

- Asegurar el equipo e infraestructura informática y estar pendientes de que las primas estén actualizadas. Es conveniente conocer los procedimientos para el cobro de las mismas, contar con un inventario de toda la infraestructura instalada y tener toda la documentación vigente.

- Seguridad en las Telecomunicaciones
  La intercepción de información y los daños físicos son de las principales amenazas a la seguridad en las redes de cómputo. Algunas mediadas de seguridad son el encriptamiento, enrutamiento diverso, marcado automático (dial back), etc.

1.4.1.1. SISTEMAS DE VIGILANCIA

El sistema de vigilancia implementado varía dependiendo de las características de cada empresa, tomándose en consideración los siguientes puntos:

- ◊ El personal encargado de vigilancia debe reportar a sus superiores cualquier anomalía detectada, de preferencia por escrito.
- ◊ Revisar diariamente que los extintores se encuentren en su sitio y en buen estado. Cualquier anomalía en los equipos o en los sistemas contraincendio debe ser reportada.
- ◊ El personal de vigilancia debe exigir la identificación de todo aquel que ingrese a las instalaciones de la empresa.
- ◊ Capacitar al personal de vigilancia, a los encargados en caso emergencia y a los sustitutos de éstos en el uso del equipo contraincendio. De ser posible, enseñar a todo el personal a utilizar los extintores.
- ◊ Verificar diariamente que los accesos a escaleras y puertas de emergencia se encuentren libres de obstrucciones.
- ◊ La identificación y ubicación de los encargados debe ser conocida por todo el personal.
- ◊ Cortar el suministro de energía eléctrica cuando no haya personal laborando.
- ◊ Si es posible, tener un teléfono exclusivo para emergencias.
- ◊ Tener a la mano los números telefónicos de emergencia y su secuencia de llamadas.
- ◊ Además del personal de vigilancia, contar con cámaras de control de circuito cerrado, sensores, etc., que no afecten la infraestructura del inmueble.
- ◊ Instalación de sistemas biométricos para acceso a áreas de alta seguridad (tales como patrón de huellas digitales, geometría de la mano, "scaneo" retinal, verificación de voz y dinámica de firma)

1.4.1.2. SISTEMAS CONTRAINCENDIO

SISTEMAS HIDRAULICOS

En caso de contar con sistemas fijos contraincendio a base de agua (rociadores, hidratantes, red contraincendio, válvulas, etc.), estos tienen que encontrarse en condiciones de uso inmediato, para ello, deben efectuarse las siguientes verificaciones:

- ◊ Checar diariamente que por lo menos una de las bombas (en caso de contar con más) funcione adecuadamente.
- ◊ Comprobar los niveles de combustible, aceite, agua, y carga de batería de los motores que accionan las bombas de agua.
- ◊ Llevar a cabo mantenimiento preventivo a las bombas en base a un programa establecido previamente.

Los sistemas contraincendio a base de agua, son boquillas obturadas por un fusible que se rompe cuando se registran temperaturas de 68°, permitiendo la salida de agua y formando una cortina que combate el fuego.

SISTEMAS FIJOS DE BIOXIDO DE CARBONO (CO2)

Este tipo de sistemas cuentan con detectores termoneumáticos, los cuales envían una señal al elevarse la temperatura, a su vez, ésta provoca la descarga de los cilindros de bióxido de carbono por las espreas, mismas que deben encontrarse estratégicamente colocadas.
Al escucharse la alarma de este tipo de sistemas, el personal debe evacuar inmediatamente el área, ya que éste agente extintor (CO2) puede provocar asfixia al aspirarlo.

SISTEMAS FIJOS DE GAS HALON 1301

Los sistemas contraincendio en base a gas halón cuentan con detectores de ionización, los cuales son sumamente sensibles; cuando detectan humo envían una señal que provoca que sean descargados los tanques contenedores del gas, distribuyendo éste por medio de boquillas instaladas en toda el área a proteger.

1.4.1.3. SISTEMAS ELECTRICOS

Se pueden tomar algunas medidas preventivas con el objeto de evitar problemas con el sistema eléctrico, tales como:

- ◊ Probar mensualmente los circuitos de alimentación de emergencia, a fin de garantizar el suministro de energía eléctrica.
- ◊ Analizar las cargas eléctricas para evitar sobrecargar los circuitos.
- ◊ Supervisar y efectuar mantenimiento a la red eléctrica cuando ésta así lo requiera.
- ◊ Restringir el acceso a los circuitos e interruptores eléctricos.
- ◊ Mantener en condiciones óptimas tanto el alumbrado normal como el de emergencia.
- ◊ Si se cuenta con planta eléctrica de emergencia, verificar que el nivel de combustible de los motores de combustión que la alimentan sea adecuado, y checar sus cargadores de baterías.

1.4.1.4. OTROS SISTEMAS DE PREVENCION

En ocasiones, las empresas cuentan con algún otro sistema adicional a los antes mencionados, entre algunos de los cuales podemos mencionar los siguientes:

- ◊ Sistemas de detección de humo. Se le debe revisar y efectuar mantenimiento periódico.
- ◊ En caso de contar con elevadores, mantenerlos en condiciones adecuadas de operación, realizando regularmente pruebas para garantizar su confiabilidad.
- ◊ Elaborar procedimientos de emergencia adecuados a las condiciones particulares de cada empresa.
- ◊ Si existe sistema de aire acondicionado, calefacción y ventilación, estos deben encontrarse en condiciones de operación de acuerdo a los requerimientos y necesidades del personal. Además, deben ser revisados, reparados y probados para determinar su eficiencia y confiabilidad de acuerdo a las normas y/o procedimientos establecidos.
- ◊ Las telecomunicaciones representan hoy en día un factor fundamental en el buen funcionamiento de las áreas informáticas, es por ello que deben tomarse medidas para prevenir cualquier contingencia derivada de este tipo de sistemas, efectuándose mantenimiento a todos los sistemas de comunicación y orientando a los usuarios sobre la correcta utilización de los equipos de comunicación disponibles a fin de garantizar su adecuado funcionamiento.

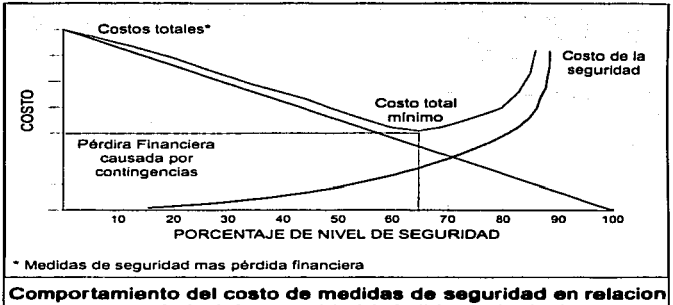
1.4.2. MEDIDAS PREVENTIVAS PARA EL PERSONAL

Es necesario que el personal conozca y respete las medidas de seguridad implementadas, tales como:

- No correr en pasillos y escaleras.
- No fumar en donde así se especifique.
- No tirar cigarros o cerillos encendidos en los cestos de basura.
- No utilizar parrillas eléctricas portátiles ni calefactores.
- Evitar el uso de extensiones eléctricas.
- Evitar conectar demasiados aparatos a una sola toma de corriente para no sobrecargar los circuitos eléctricos.
- Desconectar los aparatos eléctricos cuando no se utilicen.
- No utilizar ni almacenar líquidos inflamables; en donde su uso sea imprescindible, deben almacenarse en lugares diseñados exclusivamente para ello.
- Conocer el uso y ubicación de los extintores.
- Informar cualquier anomalía en los equipos de extinción.
- Reportar al encargado de seguridad si se detecta algún olor a gasolina, humo, etc.

1.4.3. IMPLEMENTACION DE MEDIDAS DE SEGURIDAD

El dinero que se invierta en medidas de seguridad debe ser proporcional al valor de los sistemas que protejan. Como es lógico, entre mayor seguridad se desee, mas elevado resultará el costo. Implementar demasiadas medidas puede no justificarse, por ello, debe buscarse el equilibrio al resguardar los sistemas vitales tanto como resulte justificable. A continuación se muestra una gráfica en donde puede observarse el equilibrio deseable entre el costo que implica la implementación de medidas de seguridad y la pérdida económica que se evita con las mismas:



Comportamiento del costo de medidas de seguridad en relacion con el nivel de seguridad (pérdidas evitadas)

como puede observarse, un 100% de seguridad resulta demasiado costoso y por consecuencia, de difícil justificación. Debido a que las medidas de seguridad conllevan un costo tangible y un beneficio generalmente intangible, la meta es lograr un equilibrio óptimo.

CAPITULO 2

SEGURIDAD EN COMPUTADORAS PERSONALES

2.1. ANTECEDENTES

El rápido avance tecnológico con que se han desarrollado las computadoras personales (llamadas comúnmente PC's por sus siglas en inglés), su disponibilidad, la creciente comunicación a través de líneas telefónicas entre los distintos tipos existentes, la creación de grandes redes que las interconectan, así como el desarrollo de software diverso para prácticamente todas las áreas y a todos los niveles, ha provocado que el empleo de estas valiosas herramientas de trabajo sea muy común, tanto en las empresas como en escuelas y hogares.

Las ventajas de trabajar en una computadora personal conlleva ciertos riesgos, tanto para el software como para el hardware de la misma. La información almacenada en los discos duros de las computadoras personales se encuentra expuesta a ciertos riesgos en los que ésta puede resultar dañada, eliminada o alterada, ya sea accidental o intencionalmente; lo mismo puede ocurrir a información de los discos flexibles, solo que éstos, al no ser una parte "fija" del equipo, tienen un manejo diferente, por lo que sus riesgos también difieren. En cuanto a la integridad física de la computadora personal, también se encuentra expuesta a ciertos riesgos, tales como robo o daño de partes (disco duro, monitor, etc.) o de todo el equipo.

La información manejada en una computadora personal depende del tipo de usuario que la utilice (empleado, investigador, estudiante, programador, etc.), pero independientemente de quien la emplee, el valor de la información y del equipo es importante para todos ellos, por lo que se deben tomar ciertas medidas de seguridad a fin de salvaguardarlos.

En el presente capítulo se describen algunas maneras de proteger a las computadoras personales de las acciones llevadas a cabo con la intención de dañar, sustraer o alterar la información contenidas en ellas.

En términos de seguridad de los sistemas de computación (incluyendo su información correspondiente) cabe destacar que no deben considerarse aquellos casos que tomados como riesgos suelen preocuparnos sin poder hacer algo al respecto, tales como terremotos, incendios, inundaciones, etc.

Las computadoras personales, orientadas generalmente al uso "casero" han sido consideradas para fines de seguridad de poco interés, sin embargo, debido a la proliferación de los medios para interconectar a éste tipo de equipos, se ha manifestado en el mundo de la computación la introducción de los virus como un problema de seguridad para todos.

Con el fin de entender la problemática de la seguridad en una computadora personal, se han dividido para su descripción tres temas principales: tipos de riesgos, causas de pérdida de información y protección de la misma.

2.2. TIPOS DE RIESGOS

Aquí se consideran aquellas partes de interés que amenacen con provocar un serio problema en la seguridad de la información, haciendo mención de su efecto en los casos en que los equipos se operen en grandes compañías, en empresas medianas o en el hogar.

Entre los riesgos a los cuales se encuentra expuesta la información contenida en computadoras personales, se pueden mencionar los siguientes:

- ◊ DAÑO INTENCIONAL
  El resultado de conservar información en una computadora, puede llegar a ser desastroso cuando se le provoca daño (que por lo general se realiza en pocos segundos) a través de muchos de los medios que la misma computadora proporciona. Un ejemplo de ello es cuando con intención se formatea el disco duro de una PC, causando una pérdida irreversible de la información, la cual puede representar el trabajo de muchos meses.

- ◊ DAÑO ACCIDENTAL
  Este riesgo se corre sobre todo cuando son usuarios inexpertos los que manipulan la información, misma a la que pueden ocasionar daños accidentalmente.

- ◊ INFECCIONES VIRALES
  La aparición de virus informáticos es también un problema que representa una seria amenaza tanto para la información como para la integridad física de la PC. La infección puede realizarse intencionalmente o por descuido.

- ◊ ROBO MATERIAL
  La substracción de bienes tangibles empleando equipo de computación se ha ido incrementado debido a la adaptación de la misma tecnología de sistemas de información para violar la información contenida como documentos de valor ó transacciones bancarias. Este tipo de amenazas suele aparecer en empresas medianas o grandes en las que se interactua con transacciones de tipo bancario.

◊ ROBO DE INFORMACION CONFIDENCIAL
El hecho de contar con información valiosa en computadoras personales, puede ser una razón por la cual se substrae ésta con el propósito de molestar, amenazar, chantajear o hasta robarla.

◊ ESPIONAJE INDUSTRIAL
La búsqueda de información a nivel de empresas y entre competidores, suele ser una forma de pérdida de información con el fin de lograr metas y perjuicios de tipo industrial. Generalmente ocurre cuando personal substrae la información de las computadoras personales de la empresa.

◊ ROBO DE SECRETOS DE GOBIERNO
La substracción de información de proyectos clasificados como "secretos" han sido vulnerados cuando las computadoras personales están como estaciones de trabajo y conectadas a una gran red que permite la intercomunicación.

Cabe mencionar que de los tipos de riesgos antes expuestos se aplican a diferentes usuarios de computadoras personales. Su evaluación permitirá observar a cual potencialmente están más expuestos y tomar las medidas preventivas apropiadas para cada caso.

2.3. PERDIDA DE INFORMACION

Existen diversas formas en perder información; una vez que se ha identificado el tipo de riesgo al que se encuentra expuesto, es necesario conocer también la forma en que pudiese presentarse:

- ROBO DE MEDIOS

  La forma más fácil de robar información es substrayendo discos, cintas o información impresa. Por ello, es importante asegurarse de que los medios de conservación de información sean guardados en lugares seguros.

- COMPUTADORAS SIN SUPERVISION

  Si no se realiza la supervisión de las computadoras en uso, es muy probable que la pérdida de información o su alteración sea un problema común, dado que cualquier persona tiene acceso a ella.

- INSERTANDO UN DISCO

  El uso de la unidad de discos para cargar información o programas puede inducir a la infección de virus que pueden provocar daños en el sistema.
  También por éste medio pueden efectuarse copias no autorizadas de la información contenida en el disco duro, o incluso de otras computadoras personales si se trata de una red.

- COMUNICACIONES POR MODEM

  Las computadoras conectadas en forma permanente mediante modems pueden ser atacadas desde el exterior. Se pueden infectar los equipos debido a la comunicación con terceros.

- COMUNICACIONES EN REDES

  El acceso al disco duro de la computadora personal es posible al estar conectado en red, por lo que es posible que una persona sustraiga información desde otra computadora. Igualmente, los virus pueden diseminarse con gran rapidez por las redes.

La medida básica para tener seguridad para la información, es el de realizar un respaldo de la misma. Un respaldo diario limita la pérdida del trabajo realizado a un solo día. También, en caso de presentarse daño o pérdida de archivos, éstos pueden ser restaurados desde el respaldo correspondiente. La siguiente medida a considerar es proteger la computadora personal contra infecciones de virus informáticos (ver capitulo 4)

2.4. MEDIDAS DE PROTECCION DE INFORMACION

Una forma preventiva de evitar problemas de pérdida y/o alteración de la información, se logra con el uso de varios dispositivos de hardware o software diseñados para proteger computadoras personales.

Los controles de acceso al sistema se emplean para limitar el acceso a las computadoras, entre dichos controles se pueden mencionar:

- ✓ La forma más sencilla para proteger la información es evitar que personas no autorizadas se acerquen a la computadora personal.

- ✓ A través de software, permitir el acceso solo a directorios o archivos específicos. También puede restringirse el acceso para que únicamente pueda utilizarse determinado drive sin tener acceso al disco duro del equipo. Los programas de seguridad actuales y que cumplen con su objetivo, son de bajo costo. Ejemplo de ellos son: Acces Control Software, Security Guardian, Protec, Watchdog, etc.

- ✓ Otra forma de proteger la información es limitando el acceso a la computadora personal mediante el uso de contraseñas (passwords) de entrada al sistema, manteniéndolo en secreto; no escribirlo ni ponerlo en la computadora o en el cajón del escritorio. Este método es débil pero funcional en muchas situaciones, sin embargo, es altamente vulnerable por gente experta.

- ✓ El control del acceso mediante hardware está ganado adeptos y es la forma más segura de limitar el acceso. Va desde lo simple a lo más complicado y costoso. La forma más sencilla de hardware de control de acceso son las cerraduras. Se utilizan generalmente para bloquear o desactivar el teclado. Sin embargo, su uso ha sido debilitado por la fabricación de "clones" que desmerecieron la continuidad de su utilización.

- ✓ También puede protegerse el equipo utilizando fichas de acceso para entrar al equipo, las cuales son dispositivos para ser insertados en algún tipo de lector antes de que el usuario pueda registrarse en una PC. Se combinan normalmente con contraseñas, haciendo el sistema más seguro. En muchas computadoras personales se usan fichas en forma de llaves o de tarjeta de crédito.

- ✓ Otra manera efectiva de controlar el acceso al equipo es utilizando candados (pastillas), estos son dispositivos que se conectan al puerto paralelo de la computadora, a partir del cual se verifica su existencia y el control de acceso. Su uso está dirigido actualmente a la protección de software de alto costo debido a su venta limitada. Ejemplo de ellos son: Glenco Enginnering, Protech, Rainbow Technologies, etc.

Además de los controles de acceso, deben tomarse otras medidas para prevenir daños a la información, tales como las que a continuación se mencionan:

- ➢ Apagar el equipo cuando no se utilice, ya que de lo contrario puede ser accesado por algún intruso que dañe o altere la información.
- ➢ Los discos e información impresa deben guardarse bajo llave
- ➢ Los respaldos de información vital deben guardarse en un lugar seguro lejos de los originales y del área de trabajo.
- ➢ Tener siempre bien identificada la información almacenada mediante etiquetas.
- ➢ No emplear ni hacer software ilegal.
- ➢ No comentar sobre información confidencial o delicada en sitios públicos como elevadores, cafeterías o restaurantes.
- ➢ Formatear los discos flexibles cuando se reciclen para prevenir el contagio de algún virus informático.

Se sabe que la seguridad de la información es un problema difícil y que el riesgo más grande no es el que proviene de los virus, o de espías industriales o equipos compartidos, sino el que proviene de fallas en el equipo y excusas de parte del usuario. Un sistema lógico de respaldo de información y de almacenamiento protegen contra estos problemas.

Es importante, antes de preparar un plan de seguridad, estudiar con cuidado los requerimientos de protección y contra qué o quien se va a proteger. En cuestión de virus, basta con tomar precauciones básicas y algún software económico. La mayoría de los usuarios y las empresas no necesitan ir más lejos.

Finalmente, se debe recordar que ningún sistema es perfecto, en el fondo, cada sistema depende de la buena voluntad de los seres humanos. Por ello, aquella frase tan común y tan cierta: 'no puede usted simplemente utilizar tecnología en un problema de seguridad. La seguridad es un problema humano'.

2.5. MEDIDAS PARA PREVENIR DAÑOS AL HARDWARE

Para evitar daños en el hardware de una computadora personal, es útil tomar las precauciones siguientes:

- ✓ Emplear cubiertas especiales para proteger el equipo (monitor, teclado, UCP o CPU, impresora, etc.).
- ✓ Mantener limpia el área de trabajo.
- ✓ No fumar, comer o beber cerca del equipo.
- ✓ Dar mantenimiento preventivo aproximadamente cada seis meses.
- ✓ Los discos flexibles deben guardarse en lugares adecuados y seguros.
- ✓ No exponer los discos flexibles a fuentes magnéticas que puedan dañarlos.
- ✓ Respetar las indicaciones del fabricante en el manejo del equipo y discos flexibles.
- ✓ Evitar el empleo de discos flexibles de dudosa procedencia o software 'pirata', ya que podrían estar contaminados con algún virus informático que fuera capaz de dañar el hardware de la computadora.
- ✓ Contar con software antivirus confiable y actualizado.
- ✓ Verificar los discos flexibles propios antes y después de utilizarlos en otras computadoras personales.

- ✓ Realizar con oportunidad el mantenimiento correctivo a los dispositivos que así lo requieran.

- ✓ Emplear reguladores confiables para evitar variaciones en la corriente eléctrica que pudieran dañar el equipo.

- ✓ Utilizar UPS (Uninterrupted Power System) cuando la importancia del equipo o de la información lo ameriten.

- ✓ Mantener alejados los aparatos eléctricos de la computadora y de los medios de almacenamiento (disco, cintas, etc.)

- ✓ Evitar que personas inexpertas usen el equipo sin supervisión. En el caso se tener un programa de entrenamiento, debe realizarse en equipos cuya información en disco duro no sea de vital importancia, o de preferencia en computadoras personales que no tengan disco duro ni estén conectadas en red.

- ✓ En el caso de las empresas:
  - Evitar que personas ajenas tengan acceso a las computadoras personales de la mismas.
  - Para evitar infecciones por virus, debe prohibirse a los empleados la introducción de programas ajenos a la organización, incluyendo juegos.
  - Capacitar al personal en el uso adecuado del equipo.
  - Informar al personal sobre las normas de seguridad vigentes y mantenerlos actualizados al respecto.

- ✓ Realizar respaldos en forma periódica de los archivos y sistemas de información vitales. Debe tenerse en cuenta que en ocasiones la pérdida de información es consecuencia del daño en dispositivos de almacenamiento por desgaste de los mismos y no por accidentes o errores humanos.

- ✓ El usuario no debe tratar de arreglar ninguna falla en el hardware del equipo, ya que puede ocasionar un daño mayor. Cualquier revisión, reparación o mantenimiento debe siempre llevarse a cabo por un técnico calificado.

2.6. SOFTWARE AUXILIAR PARA COMPUTADORA PERSONALES

Con el objeto de evitar y/o aminorar la pérdida de información y daños en computadoras personales, existe en el mercado software enfocado a proporcionar seguridad; también ésta aquel diseñado con el objeto de recuperar información dañada o borrada,. En los siguientes puntos se proporcionan nombres y proveedores de este tipo de software.

2.6.1. SOFTWARE DE SEGURIDAD

Este tipo de software sirve para que los usuarios de computadoras personales cuenten con un medio de protección adicional a las medidas básicas de seguridad mencionadas en el presente capítulo. A continuación se proporciona una relación* del software de éste tipo disponible en el mercado:

NOMBRE	PROVEEDOR
Citadel	Computer Security Corporation
Crypto	Basic Data System
Datasafe	AZ-Tech Software
Encrypt	Bourbaki, Inc.
MailSafe	RSA Data Security
Codename Password	DTI
PC/Dacs	Pyramid Development
PC Security	Systems Consulting, Inc.
Protec	Sophco
Secure	Winterhalter
Watchdog	Fisher International
X-Lock Safe Data	Info Safe Corporation

* Los datos fueron tomados del Apéndice II del libro 'Seguridad de la información en sistemas de Cómputo" de Luis A. Rodríguez

2.6.2. SOFTWARE DE RECUPERACIÓN DE INFORMACION

Cuando se llega a dañar o borrar información en la computadora personal, en ocasiones es posible recuperarla utilizando software elaborado para tal fin. A continuación se proporciona una lista* con algunos programas de éste tipo:

NOMBRE	PROVEEDOR
Autoback	Mectel International Inc.
Backpak	California Software Products, Inc.
Backup	Software Integration, Inc.
Bookmark	Intellisoft International
Counterpart	Technology Brokers International
Mace Utilities	Paul Mace Software Inc.
Norton Utilities	Peter Norton Utilities
Sy-Stor	System Corporation
Take Two Manager	United Software Security, Inc.
Utilities	Brown Bag Software

* Los datos fueron tomados del Apéndice II del libro 'Seguridad de la información en sistemas de Cómputo" de Luis A. Rodríguez

CAPITULO 3

SEGURIDAD EN REDES

3.1. ANTECEDENTES

A raíz de la aparición de las primeras redes de cómputo a principios de los 80's, el tema de la seguridad en éstas a sido muy controvertido, ya que una de las preocupaciones mas grandes entre los usuarios es la confidencialidad de su información. Un obstáculo para el uso de las redes era que no se consideraban lo suficientemente confiables, ya que la información se encontraba en un medio al que tienen acceso muchos usuarios.

La preocupación respecto a la seguridad de las redes aumentó conforme se dio el crecimiento de éstas y de las facilidades para interconectarse hacia cualquier red del mundo, ya que se hace cada vez mayor el número de personas que pueden acceder a la INTERRED (red compuesta por un conjunto de redes menores), con lo que el temor a que la información pueda ser vista, dañada o contaminada por virus se a incrementado. Debido a ello, los fabricantes de sistemas operativos para redes y de software de administración de estas, han desarrollado mecanismos que ofrezcan al usuario la seguridad que requieran, tales como el software antivirus, las llaves de protección (llave pública y llave privada), derechos específicos a cada usuario y los sistemas de respaldo.

La introducción de nuevas tecnologías acarrea la necesidad de adoptar nuevos métodos de seguridad. El ambiente cliente/servidor y la inclinación a usar el ciberespacio, conllevan la creación de medidas de seguridad nuevas que no eran necesarias en los ambientes no distribuidos, ya que en ellos el acceso a la información es más controlable. En el caso de los sistemas distribuidos, la información se maneja a través de una red, lo que la hace susceptible a ser observada o incluso interceptada. Por ello, el reto ahora es tener un alto grado de seguridad y protección con la mayor transparencia de estos mecanismos de control para los usuarios autorizados.

3.2. CONCEPTOS DE REDES

3.2.1. DEFINICION DE RED

Una red es una interconexión de sistemas de computadoras, canales y dispositivos de comunicación con el fin de compartir recursos e intercambiar información y servicios. Para que esto sea posible, es necesario el empleo de software para coordinar el acceso a los diferentes dispositivos ubicados en áreas geográficas diversas.

3.2.2. ELEMENTOS DE UNA RED

✧ ESTACIONES DE TRABAJO (work stations)

Las estaciones de trabajo son generalmente, sistemas inteligentes conectadas al servidor a través de una tarjeta de conexión de red y el cableado respectivo.
Para conectarse lógicamente con el servidor, se emplean archivos especiales de arranque de la red, los cuales se crean al momento de la instalación dependiendo del tipo de estación de trabajo y de la tarjeta de red usada en cada una de ellas.
Las estaciones de trabajo se encargan de procesar sus propias tareas, a diferencia de las terminales "tontas", en donde ésta es efectuada por el servidor de la red.

✧ SERVIDOR

Un servidor de red es una computadora empleada para administrar el sistema de archivos de la red; controla las comunicaciones y efectúa otras funciones. Un servidor puede ser dedicado (toda su capacidad se usa para efectuar los procesos de la red) o no dedicado (solamente parte de sus recursos son para la red y otra parte es para que se emplee como estación de trabajo)

✧ TARJETAS DE INTERFACE (NIC)

Permiten conectar el cableado entre servidores y estaciones de trabajo. Existen diversos tipos de tarjetas para soportar diferentes tipos de cables y topologías de red.
Las tarjetas contienen la circuitería que suministran los protocolos e instrucciones necesarios para cada tipo de red. También tienen varios interruptores y conmutadores (jumpers) que permiten seleccionar distintas interrupciones de hardware, direcciones de E/S y otras características que permiten que las tarjetas sean compatibles con el equipo en el que se instalan.

✧ CABLEADO O METODO DE ENLACE

Se utiliza para interconectar a los componentes de la red, una vez que se han colocado el servidor, las estaciones de trabajo y las tarjetas de red. El tipo de cable depende de varios factores, pero debe asegurarse que éste y la tarjetas sean compatibles. Entre los tipos de cable más comunes se encuentran los siguientes:

- **Par trenzado apantallado**
  Esta formado por dos hilos de cobre trenzados, aislados de manera independiente y trenzados entre sí, cubiertos por una capa externa aislante. Entre sus ventajas pueden mencionarse las siguientes:
  - Tecnología ampliamente estudiada.
  - Instalación fácil y rápida que no requiere habilidades especiales.
  - Emisión mínima de señales al exterior.
  - Tiene cierta inmunidad contra interferencias, modulación cruzada y corrosión.

- **Cable coaxial**
  Es un hilo conductor de cobre envuelto por una malla trenzada plana que hace las funciones de tierra; tiene una capa gruesa de material aislante entre le hilo y la malla, además, todo lo anterior está protegido por una gruesa cubierta externa. Existen dos espesores: el grueso para distancias largas y el fino para puntos cercanos. Entre sus ventajas se encuentran:
  - Tecnología ampliamente estudiada.
  - Soporta comunicaciones en banda ancha y en banda base.
  - Sirve para varias señales, incluyendo voz, video y datos.
  - Su instalación es sencilla.

- **Fibra óptica**
  El cable tiene dos núcleos ópticos, uno interno y otro externo, los cuales refractan la luz de manera diferente. La fibra está encapsulada en un cable protector. Esta tecnología es cara pero permite transmisión de información a gran velocidad y sin distorsión en las líneas. La señal se transmite a través de luz, por lo que las posibilidades de interferencias eléctricas o emisión de señal son muy pocas. Entre sus ventajas se pueden mencionar las siguientes:
  - Velocidad de transmisión alta.
  - No emite señales eléctricas o magnéticas, lo cual repercute en seguridad.
  - Es inmune a interferencias y modulación cruzada.
  - En algunas instalaciones puede resultar más económica que el uso de cable coaxial.
  - Soporta distancias largas.
  - Se usa en enlaces punto a punto.
  - Bajos requerimientos de energía.

- **Par trenzado telefónico o Twisted Pair**
  Es flexible y de bajo costo, fácil de instalar. Es el mismo tipo que el cable de las instalaciones telefónicas, por lo que en ocasiones los cables de las redes telefónicas pueden aprovecharse para efectuar la conexión de la red.

Este tipo de cableado tiene la desventaja de que su ancho de banda es estrecho y no puede soportar velocidades de transmisión altas. No se recomienda su uso en distancias de más de 500 metros.

- **Transmisión Inalámbrica**
  En las redes pueden utilizarse medios de comunicación inalámbricos como conexiones microondas o satélite:

  Microondas
  - Son ondas de radio concentradas a una frecuencia específica.
  - Los sistemas están limitados a línea vista, por lo que la existencia de agua o vapor provoca atenuación.

  Vía Satélite
  - Cubre gran parte de la superficie terrestre (un tercio, aproximadamente) y puede accesarse en lugares remotos.
  - El costo de las transmisiones no depende de la distancia.
  - Proporciona confiabilidad y disponibilidad elevadas.
  - Su implementación es rápida.

Cada tipo de cableado o método de enlace tienen sus ventajas y desventajas. Algunos son susceptibles a interferencias, mientras que otros no pueden ser utilizados por razones de seguridad (como el radio, por ejemplo). La velocidad y la extensión del tendido son otros factores a considerar.

✧ DISPOSITIVOS DE CONECTIVIDAD

- **Repetidores (Repeaters)**
  Se emplean para enlazar las redes físicamente. Reciben información a través de un medio de comunicación y transmiten por otro sin emplear ningún buffer.
  Son muy usados en las redes locales y en otros medios de comunicación como telefonía, fibra óptica, microondas, etc. Tiene las características siguientes:
  - Se emplean para extender la longitud del cableado.
  - Las fallas son fáciles de detectar.
  - Amplían y retransmiten todas las señales, incluyendo las colisiones en las redes locales.
  - No contienen software, por lo que su costo es bajo.
  - Solo pueden conectar a redes iguales.
  - No puede haber dos repetidores entre nodo y nodo.

- **Puentes (Bridges)**
  Un puente (bridge) es un dispositivo que permite conecta una red a otra, o a otro sistema a nivel enlace de datos. A partir de un bridge se forma una red nueva, en donde el acceso a los recursos de los servidores de ambas redes es transparente para el usuario. Entre sus características se pueden mencionar:

  - Si falla la red, evita que se deshabiliten las comunicaciones.
  - Las redes homogéneas pueden conectarse por diferentes vías (teléfono, satélite, etc.).
  - Son útiles para la administración de la seguridad, ya que pueden reportar el número de veces que un usuario intento accesar información confidencial.

- **Compuertas (Gateways)**
  Una compuerta (gateway) es un enlace de comunicación de una red local con sistemas mayores, uniendo sistemas operativos diferentes.

- **Ruteadores (Routers)**
  Permiten el enlace de dos o más redes con protocolos similares. Entre sus características están las siguientes:
  - Analizan la información para enviarla a otra red por la ruta mas adecuada.
  - Pueden encontrar rutas alternas en caso de fallas.
  - Balancean las cargas de las redes cuando existen saturaciones.
  - Procesan aproximadamente 2000 pps.

- **Puentes/Ruteadores (Brouters)**
  Son una combinación de los puentes y los ruteadores con lo mejor de ambos.

✧ SISTEMA OPERATIVO LOCAL

✧ SISTEMA OPERATIVO DE RED

✧ APLICACIONES

✧ PROTOCOLO DE COMUNICACIONES
  Establece las directrices que determinan cómo y cuándo una estación de trabajo puede accesar al cable y enviar información.

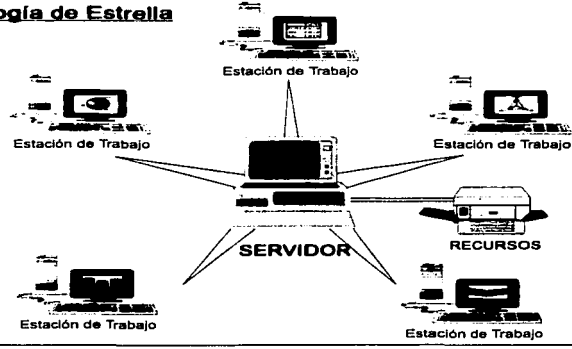
3.2.3. TOPOLOGIAS

Una topología de red es la forma de distribución del cableado para la conexión del servidor con cada una de las estaciones de trabajo. Existen varias posibles configuraciones, la mejor ésta determinada por las necesidades propias de cada sistema. Entre las más comunes se encuentran las siguientes:

TOPOLOGIA EN ESTRELLA

Se emplea un dispositivo como punto de conexión de todos los cables que salen de las estaciones de trabajo. Dicho dispositivo puede ser uno especial de conexión o el propio servidor.

Topología de Estrella



Ventajas:

- ✓ El diagnóstico de los problemas en la red es fácil debido a que las estaciones de trabajo se comunican a través del equipo central.
- ✓ Los fallos en los nodos se detectan fácilmente.
- ✓ La colisión entre datos no es posible debido a que cada estación de trabajo tiene su propio cable.
- ✓ La ampliación del sistema es sencilla.

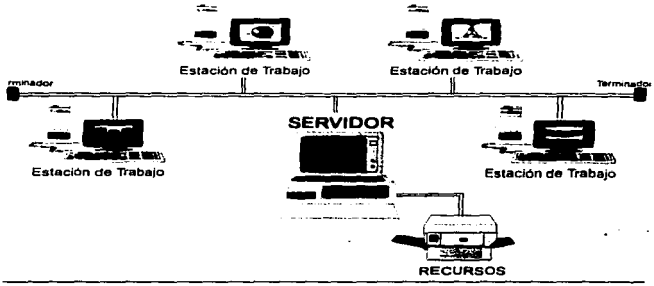
Desventajas:

- × En grandes instalaciones, la acumulación de cables en la unidad central crean una situación susceptible a errores de gestión.
- × Pueden necesitarse cantidades muy grandes de cable, lo cual resulta muy costoso.
- × Requieren un servidor dedicado.

TOPOLOGIA DE BUS LINEAL

El servidor y todas las estaciones de trabajo se conectan a un cable general central. Todos los nodos comparten el cable y en los extremos de éste se requieren unos acopladores (terminadores).

Topología en Bus



Ventajas:

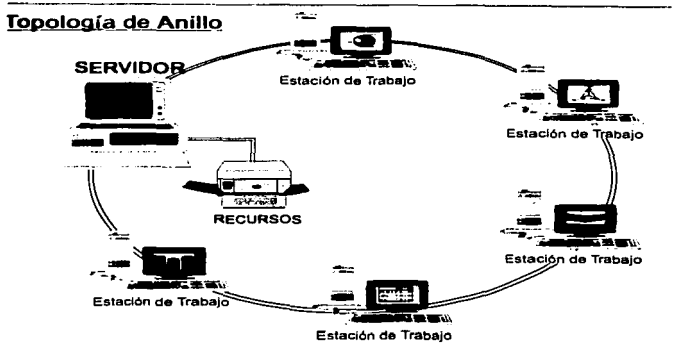
- ✓ Utiliza poca cantidad de cable.
- ✓ Es fácil de instalar el cableado.

Desventajas:

- × Es difícil aislar los problemas de cableado y determinar en que estación de trabajo o segmento de cable está el origen.
- × La desconexión en alguna parte provoca la caída del sistema.

TOPOLOGIA EN ANILLO

En este tipo de configuración las señales viajan en una sola dirección a lo largo del cable, el cual forma un círculo. Los datos transmitidos tienen asignada una dirección específica para cada estación de trabajo.



Ventajas:

- ✓ Pueden abarcarse distancias largas.
- ✓ El costo del cableado no es alto.

Desventajas:

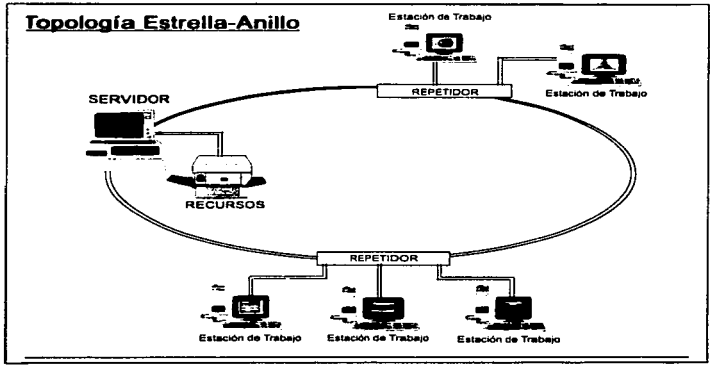
- × El cableado es complicado debido a que tiene que cerrarse sobre si mismo.
- × Una rotura en alguna parte del cable provoca la caída del sistema.

TOPOLOGIA COMBINADA ESTRELLA/BUS

En esta configuración un multiplexor de señal ocupa el lugar del dispositivo central. El cableado puede tomar la topología de estrella o bus lineal, lo cual facilita el cableado en edificios que tienen grupos de trabajo separados por distancias considerables. Ofrece gran flexibilidad para configurar la distribución del cableado y adaptarla a cualquier necesidad.

TOPOLOGIA COMBINADA ESTRELLA/ANILLO

En esta topología se pasa un "testigo" de comunicaciones alrededor de un conector central. Las estaciones de trabajo se extienden a partir de dicho conector para aumentar las distancias permitidas.



3.2.4. CLASIFICACION DE LAS REDES

Las redes se clasifican por su distribución geográfica en locales, de área metropolitana, de área amplia y de área muy amplia:

REDES DE AREA LOCAL ó LAN (Local Area Network)

Este tipo de redes están ubicadas en una área geográfica restringida (de 0.1 a 25 Km. aproximadamente) en donde las computadoras están conectadas directamente a la red. Generalmente manejan altas velocidades de transmisión sobre distancias cortas: Token-Ring (4 ó 16 Mbps), Ethernet (3 ó 10 Mbps), FDDI (100 Mbps).

Es común que en éste tipo de redes se compartan los periféricos costosos, tales como impresoras láser, graficadores, etc. Entre sus características básicas se encuentran:

- Los equipos que la conforman deben estar enlazados por algún medio físico, generalmente cable.
- Debe asignarse por lo menos un equipo de la red para compartir recursos hacia los demás equipos (servidor de la red).
- Los equipos que la conforman deben encontrarse cerca físicamente.

Las redes LAN se pueden adaptar fácilmente a cualquier necesidad; puede conectarse cualquier número de usuarios y correr cualquier tipo de aplicación a un costo/beneficio excelente. Esto se debe a que las LAN's se ensamblan con componentes de bajo costo y modulares (PC), además de que pueden seleccionarse individualmente o crecer conforme a las necesidades de los usuarios. Otra ventaja es los estándares de software que hay para este tipo de red.

REDES DE AREA METROPOLITANA ó MAN (Metropolitan Area Network)

Este tipo de redes se encuentra delimitada geográficamente por el tamaño de las ciudades. Emplean una infraestructura basada en fibra óptica.

Casi siempre se utilizan topología bus y anillo. Entre los servicios que proporcionan las MAN se encuentran los siguientes:

- ◊ Interconexión entre redes locales (backbone)
- ◊ Transmisión de imágenes, gráficas y voz digitalizados
- ◊ Transmisión de video comprimido
- ◊ Transmisión masiva de datos

REDES DE AREA AMPLIA o WAN (Wide Area Network)

Este tipo de redes pueden ser muy grandes; frecuentemente las computadoras requieren de equipos de conexión remota como modems, redes telefónicas públicas, etc. Las WAN pueden formarse por mainframes, minicomputadoras o microcomputadoras. Este tipo de redes manejan generalmente velocidades de transmisión mas bajas que las LAN's, ya que van de 10 a 64 Kbps hasta los 1.54 Mbps. Existen dos tipos de WAN's:

- ◊ REDES PUBLICAS (Public Networks)
  Rentan algún servicio de comunicaciones o de cómputo (como por ejemplo TELEPAC)
- ◊ REDES PRIVADAS (Private Networks)
  Se crean por una empresa o corporativo para su uso interno (por ejemplo, PEMEX, redes bancarias, etc.)

REDES DE AREA MUY AMPLIA (Very Large Area Network)

Son una extensión de las WAN y su cobertura puede llegar a abarcar varios países utilizando las comunicaciones por satélite.

3.3. FUNDAMENTOS DE SEGURIDAD EN REDES

En una red, la integridad de los datos, del equipo y su funcionamiento es fundamental, lo que hace que la seguridad de la red tenga vital importancia. Los niveles de seguridad que se pueden implementar van desde restricciones de hardware y de software, hasta de personas o zonas.

En el área de redes informáticas, la seguridad esta basada en los cuatro requerimientos siguientes:

- Confidencialidad
- Integridad
- Disponibilidad
- Uso legitimo

✓ **CONFIDENCIALIDAD**
La información no debe ser accesada por personas no autorizadas.

✓ **INTEGRIDAD**
Los datos deben ser consistentes, por lo que se tienen que evitar creaciones, alteraciones o eliminaciones no autorizadas.

✓ **DISPONIBILIDAD**
La información debe poder ser empleada en cualquier momento que se le necesite.

✓ **USO LEGITIMO**
El uso de los recursos debe ser por personas autorizadas y su empleo debe ser el adecuado. Para ello, se requiere que el administrador de la red establezca políticas y medidas de seguridad.

3.4. ANALISIS DE RIESGOS EN REDES

Existen muchos factores que pueden ser motivo de fallas en un sistema de red, por lo que se debe llevar a cabo un análisis de riesgos enfocado a las diferentes partes que lo integran y que pueden encontrarse susceptibles de un daño:

- Estaciones de Trabajo
- Redes LAN, MAN y WAN
- Sistemas operativos
- Dispositivos de interconectividad
- Manejadores de Bases de Datos
- Bases de datos y archivos
- Aplicaciones
- Usuarios

En el análisis se deben considerar tanto los riesgos particulares de cada elemento como aquellos que pudieran ocasionar daños masivos.

Es común que las empresas que cuentan con una red no cuenten con políticas y procedimientos de seguridad, de ahí que aproximadamente el 75% de las violaciones en redes provienen del propio personal que utiliza diariamente los dispositivos de la misma. Lo anterior conlleva grandes riesgos, tal como la proliferación de virus, los cuales pueden llegar a modificar los datos o alterar el funcionamiento del sistema.

Entre los riesgos más comunes se pueden mencionar los siguientes:

- Errores de los usuarios
- Errores por parte de los operadores
- Errores de administración
- Errores en los datos
- Errores en el sistema
- Errores de comunicación
- Infecciones virales

Una planeación en la administración de la red y un plan de seguridad puede evitar o minimizar estos riesgos.

3.5. FACTORES DE SEGURIDAD A CONSIDERAR

En los sistemas de redes, la seguridad es difícil debido al aumento de equipos que interactúan actualmente, haciendo compleja la localización de los accesos, lo cual expone la integridad de los datos, del equipo y su funcionamiento. Por ello, es conveniente tomar en cuenta los siguientes factores:

- ✓ La seguridad debe ser un objetivo estratégico para la empresa.
- ✓ Debe involucrarse a todo el personal en las medidas de seguridad, concientizando a los usuarios sobre la importancia las mismas.
- ✓ Es necesario contar con procedimientos de seguridad con un alto nivel de confiabilidad.
- ✓ Los accesos al sistema deben ser restringidos y controlados.
- ✓ Las claves de acceso no deben permanecer sin modificarse por períodos prolongados.
- ✓ Se debe dar seguimiento cuando ocurran violaciones de seguridad.
- ✓ Los productos que sean vulnerables o que se puedan eliminar o ser sustituidos deben ser evitados.
- ✓ Se debe prohibir el acceso a la red a personal no investigado o a quienes hayan reincidido en violaciones de seguridad.

3.5.1. NIVELES DE SEGURIDAD

Los niveles de seguridad se emplean para proteger los sistemas de administración de redes:

SEGURIDAD FISICA
Se refiere a salvaguardar la integridad física de los servidores y dispositivos con información importante en un lugar seguro.

AUTENTICACION DE USUARIOS

Consiste en la implementación de medidas para controlar el acceso a los diferentes recursos del sistema a través de claves de acceso. Existen ya algunas tecnologías avanzadas como el empleo de tarjetas magnéticas o reconocimiento de voz.

PRIVILEGIOS

Se refiere a los límites de accesos y permisos de lectura, escritura y modificación que deben de tener asignados los usuarios o grupos de ellos de acuerdo a sus actividades dentro de una empresa. El único que debe tener libre acceso a todo el sistema es el administrador del mismo.

ENCRIPCION

Se emplea cuando se requiere que la información no pueda ser "manipulada" por algún intruso durante su transmisión. Para ello, se utiliza algún método de encripción (como el software Mac PGP).

BITACORAS DE ACCESO

En las bitácoras pueden ser registradas todas las actividades de un usuario, a fin de poder detectar cuales archivos a utilizado y si existe algún intento de acceso no autorizado.

3.5.2. SERVICIOS DE SEGURIDAD

Existen cuatro tipos de servicios de seguridad:

1. SERVICIOS DE AUTENTICACION

   Este servicio se emplea para conocer la identidad del usuario por medio de la autenticación, llevando un conteo de las violaciones de acceso al sistema; se aplica cuando el usuario se identifica al momento de conectase. Todos los demás servicios dependen de éste.

2. SERVICIOS DE CONTROL DE ACCESO

   Este servicio está enfocado a mantener los fundamentos de la seguridad (confidencialidad, integridad, disponibilidad y uso legítimo). Para ello, impide el acceso a cualquier recurso del sistema de usuarios no autorizados.

3. SERVICIOS DE CONFIDENCIALIDAD

Este servicio se enfoca a impedir que la información sea expuesta a personas u organizaciones no autorizadas.

4. SERVICIOS PARA LA INTEGRIDAD DE LOS DATOS

Este tipo de servicios actúan como protectores de la información ante las amenazas a que pueda estar expuesta cuando es alterada inconsistentemente durante la adición, eliminación, modificación, etc.

3.5.3. PAREDES DE FUEGO O FIREWALLS

Las paredes de fuego o firewalls informáticas, son una herramienta para impedir el acceso no autorizado en conexiones de redes privadas a Internet, mediante el filtrado de paquetes, puertas de acceso por hardware (circuit gateway) y por software(application gateways) que proporcionan mayor seguridad que la que se tiene mediante las contraseñas. Las firewalls impiden que una persona externa pueda, por ejemplo, obtener archivos vía FTP (File Transfer Protocol).

Creadas en los 80's ante la necesidad de las empresas de contar con nuevas herramientas para evitar accesos no autorizados, las modelos más modernos bloquean el tráfico que trata de entrar a la red pero permite el libre tráfico al exterior. Sin embargo, una firewall no protege a la red contra virus, ya que hay miles de ellos y de formas muy variadas como para poder filtrarlos.

TIPOS DE PAREDES DE FUEGO

Las paredes de fuego o firewalls se clasifican dependiendo de sus componentes principales, aunque en la práctica se crean combinando los tres tipos:

1. BARRERAS INTERRED

Se emplean para dividir una red en grupos que no pueden ser accesados si no tienen los derechos correspondientes.

Este tipo de barrera se forma colocando estratégicamente los ruteadores y gateways dentro de los límites del área a proteger. Tienen la ventaja de ser baratas y poder controlar el tráfico, pero tienen la desventaja de que pueden ser penetradas con relativa facilidad.

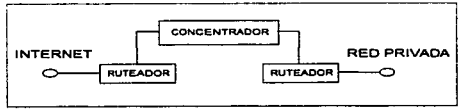
2. FIREWALLS BASADAS EN RUTEADORES

Se emplea un ruteador (generalmente asociado a un concentrador (host) especialmente configurado) para aislar el punto de enlace entre el exterior y la red.

Se forman mediante la configuración de dispositivos para direccionar datos de la red hacia el exterior y permitir el ruteo solo de determinado tipo de datos hacia ella; ésta comunicación en ambas direcciones impide un alto nivel de seguridad, por lo que se le agrega otro ruteador y un host especialmente configurado entre ambos, el cual funciona como puerta de acceso, con lo que se tienen dos variaciones de éste tipo de firewalls: configuración de bastión y la de diodo.

Configuración de Bastión

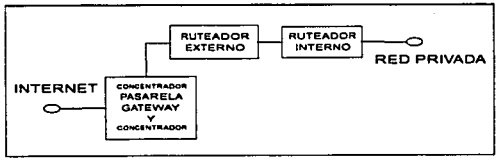
Se forma con dos ruteadores con un concentrador (configurado para proteger a la red) entre ambos:



PARED DE BASTION

Configuración de Diodo

Se forma por un concentrador y dos ruteadores entre los que se permite el tráfico interno de la red y se impide el externo:



PARED DE DIODO

La desventaja de este tipo de firewalls es que, como se necesita por lo menos un tráfico hacia dentro de la red, se emplea el protocolo FTP, por lo cual los intrusos pueden copiar archivos hacia la red protegida.

3. FIREWALLS BASADAS EN SOFTWARE

Se basan en aplicaciones conocidas como servidores proxy (llamadas también de aplicación de pasarela), las cuales sirven de mediador entre Internet y la red a proteger. Muchos proxies contienen autenticación extra o dispositivos de acceso adicionales; como dependen del protocolo empleado, pueden desarrollar mecanismos de seguridad específicos para cada protocolo (por ejemplo, para que FTP permita recepciones pero impida salidas).

El tipo de pared a elegir depende de las necesidades específicas y de las políticas de seguridad de cada empresa. Algunas consideraciones al implementar firewalls son las siguientes:

- La protección tiene sus costos asociados, es decir, a mayor protección, mayor costo.
- Los ruteadores deben programarse con los equipos desconectados y a través de una terminal, nunca vía telnet.
- Los ruteadores y los gateways host deben ubicarse en áreas con acceso controlado.
- La configuración de las firewalls debe ser de manera que no se indique su presencia a los posibles intrusos.
- Es conveniente realizar pruebas para tratar de violar la seguridad de la red.

3.5.4. PROCEDIMIENTOS DE RESPALDO EN REDES

El respaldo de la información es de vital importancia, ya que para una empresa podría llegar a ser catastrófico si su información llegara a perderse o dañarse.

La empresa norteamericana Cheyene Software, realizó un estudio en el que se determinó que cada 20 Mb de información dañada representaba una pérdida aproximada de 15 mil dólares en el área de mercadotecnia, 20 mil dólares en la financiera y 40 mil dólares en las de investigación y desarrollo. Estas cifras dan una idea de lo importante que es contar con un respaldo de la información, ya que la pérdida de ésta puede llevar a una empresa incluso a la quiebra.

Para saber cual información es la que debe respaldarse, deben considerarse los siguientes puntos:

- Identificar la información crítica para la empresa, es decir, aquella que es vital para su funcionamiento.

- Conocer cual información está en red y cual es su ubicación geográfica.

- Identificar como está distribuida la información y sobre cuantos equipos se encuentra.

- Determinar la cantidad de información que se tiene y la frecuencia con que debe ser respaldada. Para ello, debe tenerse en cuenta el dinamismo de la información y su importancia.

El proceso de respaldo de redes debe especificar la configuración mínima de la red que se necesita para que las aplicaciones críticas puedan ser soportadas. Entre los puntos a considerar se encuentran los siguientes:

- Diagrama de la red

- Controladores de comunicaciones
  - Tipo
  - Configuración

- Características de la línea
  - Tipo
  - Velocidad
  - Dispositivos remotos
  - Protocolos de comunicación

- Modems
  - Tipo
  - Proveedores

Cuando se requiera la activación del respaldo de la red, se requieren los procedimientos para la activación de la red y los procedimientos de supervisión que muestren que ésta es operacional.

CONSIDERACIONES SOBRE RESPALDOS

- Deben realizarse dos copias de seguridad en conjuntos de discos o cintas totalmente independientes. Estos respaldos deben actualizarse alternadamente, de forma que si uno de ellos se daña, puede utilizarse el otro.

- Debe tenerse presente que entre menor sea el intervalo de tiempo entre los respaldos, menor será la cantidad de información que deba volverse a introducir para que el sistema se restablezca a como se encontraba antes de producirse el problema.

- Una copia del respaldo debe ser guardada en un sitio externo seguro, a fin de salvaguardar la información en caso de que ocurriese algún daño mayor en las instalaciones en donde se encuentra instalada la red.

- Se debe realizar una copia de seguridad maestra con todo el sistema a intervalos regulares.

- Si el sistema lo permite, se puede optimizar el tiempo de respaldo actualizando solo los archivos nuevos y los modificados.

- Asegurarse de respaldar también los archivos ocultos.

- Se tiene que poder identificar plenamente la fecha exacta en la que se llevo a cabo el respaldo.

- El empleo de cintas para respaldar es una opción buena, ya que debido a la capacidad del disco duro del servidor, se necesitaría una gran cantidad de discos para realizar un respaldo adecuado.

- El uso de discos ópticos es más recomendable para volcados de información (un volcado es el respaldo de archivos de datos que ya no se utilizan pero se deben guardar), ya que la escritura en ellos es más lenta que en cita pero tienen un período de almacenamiento de varios años.

3.6. ADMINISTRACION DE LA SEGURIDAD

El objetivo de la administración de la seguridad en una red, es implementar todas medidas de protección posibles en forma ordenada y previamente analizada.

3.6.1. MECANISMOS DE SEGURIDAD

Entre los mecanismos de seguridad con que se cuentan para ello se pueden mencionar los siguientes:

✧ IDENTIFICACION DE LA RED

Es imprescindible contar con la identificación de la red, es decir, la especificación de su configuración:

- Diagrama de configuración
- Características de los equipos de la red
- Características de las líneas (tipo, velocidad, dispositivos remotos, protocolos, etc.)
- Modems (tipo, proveedor)

✧ SOFTWARE ANTIVIRUS.

Los virus informáticos son muy comunes en nuestros días, y conforme aparecen nuevos virus se desarrollan nuevos antivirus. Aunque todos los antivirus tienen sus pros y contras, aquellos que residen en memoria y pueden detectar el virus antes de que ataque son los más recomendables.
Existen varias versiones de software antivirus: para monousuarios, computadoras en red, servidores, etc. Lo recomendable es contar con protección contra virus en todas las computadoras de la empresa estén o no conectadas a la red, así como checar todos los discos flexibles que se utilicen en las mismas.

✧ CLAVES DE ACCESO

A fin de contar con una protección para que solo usuarios autorizados puedan utilizar una red, se establecen claves de acceso diversas para diferentes niveles de protección.

Inicialmente, el procedimiento que se tenía en los sistemas de red era el siguiente: Cuando la red tenía varias estaciones de trabajo conectadas a un servidor central, cada usuario tenía una cuenta de acceso, la cual era única, y cuya función era la de permitir al usuario el acceso al servidor; asociada a dicha cuenta existía un password que solo era conocido por el usuario. Cuando el usuario proporcionaba su cuenta de acceso y su password, el sistema verificaba que dicha cuenta existiera y que el password fuera correcto, en cuyo caso se permitía el acceso a la red. Este procedimiento tiene la desventaja de que una vez que se ha autorizado el acceso a la red, no se vuelven a verificar durante la sesión de trabajo las claves proporcionadas.

Actualmente se valida constantemente la vigencia y autenticidad de la cuenta y del password de la siguiente manera: al proporcionar el usuario su cuenta de acceso y su password, se aplica a estos dos valores un algoritmo del cual se obtiene un dato llamado ***"llave privada"***, la cual se envía al servidor para su validación; si es correcta, el sistema combina el valor de la llave privada con un valor que el proporciona, formándose así una ***"llave única"***. Cuando el sistema permite el acceso del usuario a la red, le envía esa llave única, misma que deberá acompañar cualquier petición del usuario, verificándose ésta por el servidor cada vez a fin de checar que sea la misma que el usuario dio al inicio de la sesión de trabajo.

✧ DERECHOS ESPECIFICOS A CADA USUARIO.

Una vez que el usuario accesa la red, tiene restricciones a determinados privilegios (de lectura y/o escritura), los cuales se otorgan por cuenta y sobre archivos y directorios.
Antes de instalar una red, en conjunto con el usuario el administrador debe diseñar con detalle el esquema de seguridad a seguir, el cual debe considerar las normas de seguridad establecidas.

✧ SISTEMAS DE RESPALDO

Es relativamente común que un usuario autorizado y con los privilegios adecuados, borre información por equivocación. Por ello, otra medida de seguridad es proteger los datos para posteriormente poder recuperar la mayor parte de la información.

Existen sistemas que permiten respaldar la información de todos los equipos desde un solo punto; en otros se puede realizar el respaldo conforme a estadísticas, de tal forma que la información es resguardada solo cuando fue modificada después del último respaldo. Los mejores sistemas de respaldo son aquellos que permiten respaldar tanto los datos como los esquemas de seguridad como son los privilegios que cada usuario tiene asignados, de tal forma que si se llegará a dañar un servidor se tenga algún medio para restablecerlo.

Para que la administración de la seguridad de la red sea adecuada, los mecanismos de seguridad previamente descritos deben implementarse ordenadamente y previo análisis de la red. La secuencia que se recomienda es la siguiente:

1. Identificación de la información confidencial y de aquella que pueda compartirse.

2. Identificar los puntos desde los cuales se accesa a la red. Este punto es de la estación de trabajo al servidor en una red local, pero en una interred estos puntos se incrementan debido a que los usuarios pueden tener acceso al servidor o al mainframe o a ambos (usuarios que estén físicamente dentro de la empresa) y usuarios móviles que la accesan por medio de modems u otros medios de acceso remoto.

3. Determinar que software y/o hardware será instalado en cada punto de acceso a la red para garantizar éste solo a usuarios autorizados. También se debe establecer la periodicidad de los respaldos, así como que información contendrán estos.

4. Es importante saber si las medidas de seguridad adoptadas cumplen su objetivo correctamente, para ello, pueden elaborarse bitácoras en las que se registren la frecuencia en que se presentan los accesos no autorizados y establecer mediante las estadísticas que tan segura es la red.

3.6.2. SUPERVISOR DE SEGURIDAD

La seguridad de la red puede asignarse a una persona, la cual fungiría como supervisor de seguridad, cuyas características y actividades serían las siguientes:

- ⇨ Evaluar los riesgos y en base a ellos elaborar planes de seguridad.
- ⇨ Participación en las acciones a realizar cuando se presentan violaciones a las medidas de seguridad.
- ⇨ Colaborar durante la planeación de la administración de la red.
- ⇨ Supervisar la compra de hardware y software.
- ⇨ Elaborar un plan de capacitación para el personal que trabaje a su cargo.
- ⇨ Mantener contacto con otros supervisores de administración de redes y de seguridad, consultores y proveedores.
- ⇨ Conocer bien la empresa y sus clientes.
- ⇨ Conocer el impacto de seguridad en la empresa.
- ⇨ Tener conocimientos sobre herramientas y técnicas de administración de la seguridad.

El supervisor de seguridad debe ser apoyado en sus actividades por un grupo formado por personal capacitado en el área de seguridad.

3.6.3. EJEMPLO DE ADMINISTRACION DE LA SEGURIDAD: SISTEMA AIX/6000

➢ CUENTAS DE USUARIO

- A cada usuario le es asignado un nombre, una identificador (ID del usuario) y una contraseña únicos, dependiendo de la prioridad o nivel que éste tenga en la empresa.
- La propiedad de los archivos es dada por el ID del usuario.
- El usuario que genera los archivos es normalmente el propietario, pero el propio usuario o el administrador (superusuario) puede transferir dicha propiedad a otro usuario.

La seguridad del sistema se sustenta en las identificaciones únicas asignadas a cada usuario; cuando éste entra al sistema por medio de un login, su ID de usuario se usa para validar todos los requerimientos de acceso a los archivos.

3.6.2. SUPERVISOR DE SEGURIDAD

La seguridad de la red puede asignarse a una persona, la cual fungiría como supervisor de seguridad, cuyas características y actividades serían las siguientes:

- ⇨ Evaluar los riesgos y en base a ellos elaborar planes de seguridad.
- ⇨ Participación en las acciones a realizar cuando se presentan violaciones a las medidas de seguridad.
- ⇨ Colaborar durante la planeación de la administración de la red.
- ⇨ Supervisar la compra de hardware y software.
- ⇨ Elaborar un plan de capacitación para el personal que trabaje a su cargo.
- ⇨ Mantener contacto con otros supervisores de administración de redes y de seguridad, consultores y proveedores.
- ⇨ Conocer bien la empresa y sus clientes.
- ⇨ Conocer el impacto de seguridad en la empresa.
- ⇨ Tener conocimientos sobre herramientas y técnicas de administración de la seguridad.

El supervisor de seguridad debe ser apoyado en sus actividades por un grupo formado por personal capacitado en el área de seguridad.

3.6.3. EJEMPLO DE ADMINISTRACION DE LA SEGURIDAD: SISTEMA AIX/6000

➢ CUENTAS DE USUARIO

- A cada usuario le es asignado un nombre, una identificador (ID del usuario) y una contraseña únicos, dependiendo de la prioridad o nivel que éste tenga en la empresa.
- La propiedad de los archivos es dada por el ID del usuario.
- El usuario que genera los archivos es normalmente el propietario, pero el propio usuario o el administrador (superusuario) puede transferir dicha propiedad a otro usuario.

La seguridad del sistema se sustenta en las identificaciones únicas asignadas a cada usuario; cuando éste entra al sistema por medio de un login, su ID de usuario se usa para validar todos los requerimientos de acceso a los archivos.

➢ GRUPOS

Se crean grupos de usuarios para aquellos que requieran accesar los mismos archivos. El identificador de grupo (ID de grupo) proporciona un nivel extra de propiedad sobre los archivos, ya que el nombre del grupo y su ID son únicos, además de que este último es asignado a un archivo cuando se crea.

Un usuario puede formar parte de uno o más grupos. La creación de grupos para organizar y diferenciar usuarios en la red forma parte de la administración del sistema. Crear demasiados grupos puede dificultar demasiado la administración. Se tienen diferentes tipos de grupos:

- Grupos de administradores
  Son usuarios de al red que tienen permisos para desarrollar algunas tareas no permitidas a los usuarios ordinarios.

- Grupos de usuarios comunes
  Son usuarios que requieren compartir archivos sobre el sistema, como por ejemplo, un grupo de un mismo proyecto.

- Grupos extras
  Este tipo de grupos son definidos con privilegios limitados y específicos de administración sobre el sistema; se utilizan para controlar determinados subsistemas. Por ejemplo, el grupo *Security*, cuya función es el manejo de contraseñas y control de límites.

➢ CONTROL DE ACCESO

- El acceso a logins privilegiados debe limitarse.
- El administrador del sistema debe ser el único que pueda cambiar la contraseña de root.
- Deben asignarse contraseñas diferentes de root para diferentes máquinas.
- Los administradores del sistema deben accesar como usuarios comunes y luego cambiarse al root en lugar de conectarse directamente.
- La trayectoria (path) empleada por root debe ser revisada periódicamente.
- La contraseña de root debe ser limitada, de preferencia a un solo administrador.
- Debido a que los cambios a root pueden ser rastreados, deberá llevarse un registro de los logins exitosos y los rechazados en el sistema.

➢ REGISTROS DE SEGURIDAD

- Los intentos de entrada a root son registrados en un archivo de texto que puede ser visto (archivo sulog). La información que tiene es la fecha, hora, nombre del sistema y nombre del login, así como si fué o no exitoso el acceso.

- Cada que un usuario se conecta exitosamente al sistema o realiza un intento y falla (contraseña incorrecta), el programa login lo registra.

➢ PERMISOS DE ACCESO A ARCHIVOS Y/O SUBDIRECTORIOS

- Archivos
  - Acceso de solo lectura
  - Acceso para escritura y/o lectura
  - Ejecución solo con el UID del propietario
  - Ejecución solo con el GID del grupo propietario
  - Permiso para ejecución del archivo

- Directorios
  - Permiso para listar el contenido del directorio
  - Permiso para crear y borrar archivos del directorio
  - Acceso al directorio
  - Eliminación de un archivo sólo por el UID propietario o el GID propietario

➢ ARCHIVOS DE SEGURIDAD

La seguridad del sobre el sistema está controlada por archivos, los cuales son empleados para contener atributos de usuario y control de acceso:

- Validación de usuarios (ID, grupo primario, directorio hogar y shell del login)
- Validación de grupos (ID de grupo, miembros)
- Contraseñas de usuarios (contraseñas encriptadas e información de actualización de usuarios)
- Restricciones de las contraseñas (atributos extendidos para los usuarios)
- Límites para los usuarios (límites de recursos para los procesos de los usuarios)
- Valores de login (intentos de login, listas de programas válidos de login (shells), etc.)

➢ POLITICAS DE SEGURIDAD

- Identificar los diferentes grupos de usuarios y los datos que requieren accesar.
- Los grupos deben organizarse dependiendo del tipo de trabajo a realizar.
- Se tiene que organizar la propiedad de los datos para que cumplan con la estructura del grupo.

3.7. MEDIDAS DE SEGURIDAD

Los sistemas y medidas de seguridad se deben adoptar de acuerdo al tamaño y características de la red, por lo que es importante el análisis de ésta antes de cualquier implementación. También debe ser evaluada la compatibilidad entre las herramientas de seguridad de los equipos, así como su nivel de confiabilidad, la cual debe ser similar en todos ellos.

3.7.1. MEDIDAS DE PROTECCION Y DE SEGURIDAD

MEDIDAS DE PROTECCION

Existen dos tipos de protección en redes: protección física y protección lógica:

PROTECCION FISICA

Seguridad del lugar físico en donde se encuentra ubicada la red. Seguridad del equipo, las telecomunicaciones y los usuarios. Entre las medidas a tomarse se encuentran:

- Control de los accesos de los usuarios al equipo
- Evitar el uso de drives en las estaciones de trabajo para eliminar contagio de virus o robo de información
- Hacer firmar a los usuarios un documento comprometiéndolos a mantener las medidas de seguridad estipuladas por la empresa.
- Los servidores deben encontrarse en áreas de acceso restringido.
- El cableado y los sistemas de interconectividad deben estar protegidos.

PROTECCION LOGICA

Esta debe efectuarse desde la planeación y diseño de la red, incluyéndose:

- Claves de acceso
- Códigos de acceso
- Definición cerrada de grupos de usuarios
- Técnicas de encriptamiento
- etc.

MEDIDAS DE SEGURIDAD

Las medidas de seguridad se dividen principalmente en dos categorías:

Seguridad en las comunicaciones
Están enfocadas a proteger la información durante la comunicación de un sistema a otro.

Seguridad en los sistemas
Esta enfocada a salvaguardar la información dentro de un sistema informático, incluyendo subcategorías de seguridad, como la del sistema operativo, bases de datos, etc.

3.7.2. METODOS DE SEGURIDAD

CRIPTOGRAFIA ESTANDAR O DES (Data Encryption Standard)

Este método se emplea para transferir información; está limitado debido a que para efectuarse emplea muchos recursos (para encriptar 64 bits de información necesita 64 bits de llave, 56 de los cuales son para encriptar y los demás para detección de errores).

MARCAJE AUTOMATICO (Dial Back)

Este método es empleado en redes públicas conmutadas, por lo que se efectúa a través de una línea telefónica. En el dial back el receptor se desconecta al recibir una señal; luego verifica la existencia y validación de la contraseña, y si es correcta, hace la llamada de regreso.

PREVENCION DE ANALISIS DE FLUJO DE TRAFICO

Este método se usa para proteger la información durante las transmisiones. Para ello, se rellenan los espacios de tiempo entre transmisiones y se encriptan ambas comunicaciones. Tiene la desventaja de que ocasiona cuellos de botella porque el sistema ocupa el tiempo cuando no se está transmitiendo información, lo que lo hace muy costoso.

3.7.3. MEDIDAS PREVENTIVAS EN REDES LAN

Entre las medidas preventivas en redes locales pueden señalarse las siguientes:

- ✓ Evitar que exista un punto potencial de falla, como podría ser el centro de la topología estrella.
- ✓ Contar con la cantidad adecuada de ruteadores, bridges y switches.
- ✓ Emplear ductos alternos.
- ✓ Redundancia en medios coaxial, fibra, inalámbrica.
- ✓ Verificar que el cableado este dentro de las normas establecidas.
- ✓ Probar vías alternas.

3.7.4. MEDIDAS PREVENTIVAS EN REDES MAN Y WAN

- ✓ Contar con el equipo adecuado de ruteadores, multiplexores, bridges y switches.
- ✓ Redundancia en nodos y rutas: malla.
- ✓ Redundancia en medios: VSAT, fibra óptica, microondas, RDI.
- ✓ Redundancia en carriers.

CAPITULO 4

VIRUS INFORMATICOS

4.1. ANTECEDENTES

Los virus informáticos son segmentos de código que afectan a sistemas de aplicación u otros componentes del sistema.

Uno de los primeros casos sonados de una infección informática, ocurrió en noviembre de 1988, cuando dos importantes redes norteamericanas fueron atacadas por un virus que en unas cuantas horas se extendió a cientos de computadoras, impidiendo por espacio de dos días a más de 6000 usuarios el uso de las mismas, algunas de las cuales se encontraban en universidades, instalaciones militares de la NASA y centros privados. Este suceso alarmó a muchos usuarios, sobre todo aquellos de los sectores financiero y comercial, ya que puso de manifiesto la vulnerabilidad de los sistemas informáticos.

Los virus pueden atacar los sectores de "boot", los componentes del sistema operativo, los dispositivos de drive y cualquier aplicación (procesadores de palabras, bases de datos, etc.).

Los virus pueden transmitirse a través de redes locales, cuando se accesan tableros de información y por medio de conexiones remotas de computadora a computadora. En cuanto a las computadoras personales, lo más común es que las infecciones se lleven a cabo por la compartición de discos flexibles entre usuarios de las mismas.

Existen algunos factores que dificultan la eliminación de virus en los sistemas informáticos: la mayoría de los virus no muestran señales de su presencia inmediatamente después del contagio, ya que infectan al host de manera que las funciones de este no cambian, por lo que un programa infectado puede seguir operando normalmente sin mostrar sintomatología o alguna anormalidad durante días, semanas, meses e incluso años; sin embargo, durante ese tiempo el virus contamina a otros programas del sistema operativo y a discos empleados en la computadora afectada. Una vez que el virus se activa, los efectos de este pueden ser notados; estos pueden variar desde un simple mensaje inofensivo hasta causar daño parcial o total de la información almacenada, dependiendo del código de cada virus. La manifestación de un virus puede depender de varios factores:

- Tiempo de permanencia del virus en el sistema.
- Cantidad de infecciones llevada a cabo.
- Las veces que se a ejecutado el programa host infectado.
- Un día y hora específicos.

Existen dos tipos de infección: los llamados Caballos de Troya y los Gusanos. Los primeros son programas que parecen legítimos pero contienen código que daña a otros programas o datos; por sus parte, los gusanos son programas que utilizan el software de una red y de las instalación de comunicaciones para reproducirse y pasar de sistema en sistema, realizando actividades de procesamiento o colocan virus. La diferencia entre ambos es que los virus afectan a otros programas y los gusanos no lo hacen, siendo éstos últimos más difíciles de crear, y por lo tanto, menos comunes.

4.2. CARACTERISTICAS DE LOS VIRUS

Existen muchos tipos, cada uno de ellos con características diversas, tales como la forma en que se expanden y su alcance destructivo. Además, cada virus presenta diversas variedades. Todo ello hace que la proliferación de los virus informáticos se encuentre alrededor de todo el mundo.

4.2.1. CLASIFICACION DE LOS VIRUS.

VIRUS QUE INFECTAN EL BOOT.

Este tipo de virus atacan los sectores "boot" de los discos duros y de los discos flexibles, tomando el control del sistema cuando estos son ejecutados al inicio de cada sesión de trabajo, por lo que siempre toman el control. El virus actúa de tal forma que mediante el monitoreo del sistema se adueña del software, efectuando interrupciones en éste para realizar copias de si mismo en discos insertados en los drives. Es por ello que cuando un disco flexible se emplea en un equipo contaminado, el virus se transfiere al sector 0 e infecta el siguiente sistema ejecutado desde dicho disco; por consiguiente, para que un disco contaminado afecte a su vez a otro equipo, se requiere que se efectúe una ejecución desde el disco flexible en el drive de dicho equipo.

Este tipo de virus son los primeros programas que se ejecutan durante cualquier sesión de trabajo debido al lugar en donde se alojan. Como programas residentes pueden superar arranques en caliente (Ctrl+Alt+Del) y contaminar discos de arranque no infectados; también es posible que alteren la lista de directorios mostrando los tamaños correctos de los archivos cuando en realidad estos ya han sido modificados por el virus debido al código añadido.

Existen dos maneras en que un virus ataca; una de ellas el alterando un segmento de código y la otra es reemplazándolo totalmente. Algunos virus del sector "boot" reemplazan completamente el sector por una copia de si mismos, convirtiéndose así en el nuevo programa "boot" del sistema, mientras que otros atacan un sistema existente. Esta última contaminación es menos grave que la primera porque los virus tienen que duplicar las funciones del sistema que estén reemplazando.

VIRUS INFECTORES AL PROCESADOR DE ORDENES.

Este tipo de virus infectan shells de órdenes centrales como el command.com. Permanecen residentes durante toda la sesión de trabajo y tienen la capacidad de supervisar y controlar casi todas las interacciones entre usuarios y computadora, esto es, cuando se ejecuta una orden primero buscan e infectan otros procesadores de órdenes y luego realizan las funciones normales de la orden original.

VIRUS QUE HACEN INFECCIONES AL SISTEMA.

Este tipo de virus infecta al sistema operativo (atacando por lo menos a uno de sus módulos) o a un driver del sistema. Toman el control después de que el sistema operativo inicia y permanecen activados; cuando detectan que se insertó un disco flexible, el virus se copia a si mismo dentro de los archivos del sistema de éste.

VIRUS DE PROPOSITO GENERAL.

Este tipo de virus es el que tiene mayor difusión, puede infectar cualquier programa de aplicación, ya que si bien generalmente no pueden infectar archivos de bajo nivel de sistemas operativos, si pueden infectar cualquier archivo ejecutable. Toman el control cuando se accesa alguna aplicación que se encuentra infectada; una vez con el control, buscan en el sistema host adicionales en el disco duro o en los discos flexibles presentes para atacar a los nuevos hosts. Después de que realizan la infección, tienen el control sobre el programa de aplicación.

VIRUS MULTIPROPOSITO.

Son virus diseñados de forma tal que combinan algunas o todas las características de los tipos de virus ya mencionados. Este tipo de virus es una combinación muy potente, adaptable y fatal de tecnologías, ya que puede causar estragos de todas las áreas de los sistemas de archivos del usuario.

VIRUS QUE INFECTAN A ARCHIVOS ESPECIFICOS.

Este tipo de virus están diseñados para atacar solamente a un número fijo y a un tipo especifico de archivos.

VIRUS RESIDENTES EN MEMORIA.

Gran cantidad de virus tienen la característica de que quedan residentes en memoria, pero a diferencia de los archivos residentes cuyo objetivo es tener un acceso rápido, estos atacan inmediatamente y permanecen activos a lo largo de las sesiones de cálculo.

4.2.2. METODOS DE INFECCION MAS COMUNES.

Los virus informáticos tienen varias formas de reproducirse. Los métodos de infección más comunes son los siguientes:

AGREGACIÓN.
El virus se reproduce agregando su código vírico al extremo final de los archivos ejecutables, los cuales son modificados para que al ser ejecutados el control del programa se pase primero al código vírico agregado.

INSERCION.
Este tipo de virus coloca su código vírico directamente en el código no utilizado y de segmentos de programas ejecutables, esto es, que el código del virus se encuentra dentro de los archivos ejecutables de destino en lugar de agregados al final.

SUSTITUCION.
En este caso, el virus ataca el sistema en que residen los archivos ejecutables y no a estos en si. Para ello, se escribe sobre los archivos a infectar, borrando y sustituyendo el código del programa por el código vírico.

REORIENTACION.
Este tipo de virus se ubican en una o más posiciones físicas de los discos: áreas de partición, sectores marcados como dañados o como archivos ordinarios ocultos. Este tipo de infección, en combinación con la de sustitución hacen que los virus con estas características puedan ser tan pequeños de tamaño que sean fáciles de ocultar dentro de limitados espacios no usados de programas. La ventaja de una infección de este tipo, es que una vez detectada puede ser quitada con facilidad.

4.2.3. SINTOMATOLOGIA

Cuando en la computadora se detecta algo anormal, puede tratarse de una infección por virus. Entre algunos de los síntomas que pueden presentarse se encuentran los siguientes:

- El equipo no se inicializa normalmente.
- El texto de algún archivo se encuentra alterado.
- Aparición en la pantalla de desplegados, imágenes o gráficas extrañas.
- Sonidos fuera de lo habitual.
- El Tamaño de los archivos cambia.
- La computadora envía mensajes de error en software que no se habían presentado.
- La memoria disponible disminuye.
- Aparecen inexplicablemente nuevos archivos y/o directorios.
- Se tienen problemas en las comunicaciones o al imprimir.
- El reloj del sistema tiene cambios inexplicables.
- Se presentan sectores dañados en los discos flexibles o un número extremadamente elevado de sectores defectuosos en disco duro.

4.2.4. TECNICAS DE OCULTAMIENTO DE LOS VIRUS

Los creadores de virus informáticos han diseñado varias formas de evitar su detección. Entre las principales técnicas de ocultamiento pueden mencionarse las siguientes:

- Creación de virus de tamaño pequeño. Esta técnica consiste en que el virus ocupe poco espacio para que su detección visual se dificulte.
- Encriptación del código, esto es, se lleva a cabo modificando el código del virus de acuerdo a cierta regla que cambia el significado de las instrucciones.
- Desarrollo de virus poliformáticos. El código del virus es alterado en su secuencia en forma "limitada" una decena de veces.
- Creación de virus mutantes, desarrollando para ello gran variedad de estos para impedir su detección.
- Alteración de rutinas del sistema operativo y/o BIOS de la computadora.
- Generación de código que detecte si existe algún antivirus en el sistema para evadirlo o incluso dañarlo.
- Combinación de las técnicas antes mencionadas.

4.2.5. ALCANCE DE UNA INFECCION POR VIRUS

Habiendo tanta variedad de virus, es lógico suponer que también hay gran cantidad de resultados de un contagio, así como la gravedad del mismo. A continuación se mencionan algunos de tipos más conocidos:

- ◊ Virus que bloquean algunos componentes del sistema, por lo regular los buffers, de forma que se no permite la E/S de la información de los discos, lo cual puede llegar a confundirse con una falla de hardware.

- ◊ Existen virus que pueden dañar el equipo físicamente. Se conocen hasta ahora dos tipos de daños ocasionados por virus: a monitores y a las cabezas de lectura/escritura de los discos, provocando con esto último el daño irreparable a los discos que se lleguen a emplear.

- ◊ Virus que en cuanto se efectúa la infección proceden a borrar información, ya sea de programas o de archivos de usuario, efectuando el daño sin previo aviso. Tanto el disco duro como cualquier medio magnético puede ser afectado.

- ◊ Existen virus que son diseñados por los fabricantes de software para evitar la piratería. Este tipo de virus infecta únicamente a copias obtenidas ilegalmente; generalmente se manifiesta destruyendo los programas y archivos relacionados con el sistema en cuestión.

- ◊ Algunos virus marcan sectores como dañados cada vez que se ejecuta el programa infectado, siendo que en realidad dichos sectores se encuentran sin daño alguno. Este tipo de infección trae como consecuencia que se vaya disminuyendo la capacidad de almacenamiento en los discos.

- ◊ Virus revisan la información contenida en el disco al que infectaron y no actúan hasta que la capacidad de este excede el 50%.

- ◊ También existen virus que son diseñados por personal de una empresa con el fin de sabotear a la misma. Generalmente se instalan de forma anónima y con fines de venganza, por lo que su alcance de destrucción puede variar dependiendo de las intenciones y habilidad de su creador.

- ◊ Existen también algunos virus que luego de borrar la información envían un mensaje al usuario, por lo que se les conoce como los burlones, o los descarados, cuando el mensaje incluye los datos del autor.

- ◊ Algunos virus son controlados por la empresa, se diseñan para efectuar una supervisión de los empleados que realizan copias no autorizadas de software.

- ◊ Virus que provocan daños al sistema operativo, ocasionando una caída total del sistema.

- ◊ Algunos virus son inofensivos, solo envía algún saludo, felicitación o mensaje en el monitor.

4.3. DESASTRES INFORMATICOS POR VIRUS

4.3.1. PROBLEMATICA

Según John McAfee, presidente de Computer Virus Industry Asociation, una vez activado, un virus puede extenderse de forma increíble, ya que son tan persistentes como un resfriado común, expandiéndose rápidamente, lo que hace muy difícil su exterminación. Un ejemplo de ello es un virus que viajó desde Pakistán a EU infectando a cerca de 100,000 computadoras, causando daños incalculables a la información en ellas almacenada.

La utilización de programas antivirales no siempre es efectiva, ya que puede ser que el virus no sea detectado o no puede ser removido por el antivirus empleado debido ya sea a que el programa antiviral no es una versión reciente o a que el virus sea nuevo en el mercado y aún no se haya desarrollado la vacuna correspondiente.

Desafortunadamente, en México no se ésta haciendo mucho respecto a tomar medidas de seguridad para evitar infecciones por virus. Si bien es cierto que existen representantes legales y exclusivos de las más acreditadas firmas de software y hardware, sus funciones han ido encaminadas al apoyo de sus ventas, pues se han aprovechado de la confusión al respecto para -con justa razón-, efectuar campañas contra la piratería. Invierten en aulas y capacitación de su personal para diseñar, vender e impartir asesorías y cursos, pero no en investigar acerca del virus computacional para proteger a sus clientes.

Muchas de las organizaciones no se encuentran preparadas para afrontar adecuadamente las consecuencias de un ataque viral. Generalmente los programas de seguridad de la información son implementados solo hasta después de que ocurre un desastre. En la mayoría de las empresas hay cada día más conciencia del problema, pero no saben que hacer al respecto, ya que si bien se trata de un problema de tecnología, también lo es de administración.

4.3.2. DESASTRES POR VIRUS

Existen muchos casos importantes de desastres por virus, por ejemplo, en 1988 Internet fue infectada; en ese entonces la red contaba con alrededor de 85,000 computadoras entre universidades, agencias de gobierno y centros de investigación. El impacto de ésta contaminación (que fue medido en cuanto a horas-hombre pérdidas, tiempo de equipo y costo por la eliminación del virus) se estimó en casi 100 millones de dólares.

Otro ejemplo es el de USPA&IRA Inc., una empresa de seguridad de Texas, en la cual, en 1985 un operador detectó que la mitad de los registros correspondientes a las ventas habían desaparecido; como consecuencia, alrededor de 400 ventas no podrían ser pagadas. Se procedió a recuperar los registros con los respaldos disponibles, pero al hacerlo se detectó que en el código se habían colocado "bombas de tiempo" que infectaron por completo el sistema de la computadora, ya que se reprodujeron a si mismas y destruyeron áreas de memoria. En la investigación se descubrió al responsable: un empleado que se desempeñaba como programador y oficial de seguridad de computadoras, quien molesto porque recién había sido despedido colocó el virus en el sistema. La empresa llevó el caso a la corte y ésta, tres años después, declaró culpable al ex-empleado de felonía en 3er. Grado, sentenciándolo a 7 años de prisión y a pagar 11,800 dólares por daños a la empresa. Después de lo sucedido, la empresa tuvo que revisar y aumentar sus medidas de seguridad.

El último ejemplo muestra la vulnerabilidad de las empresas si llegan a fallar sus sistemas informáticos, los cuales a su vez son indispensables para las operaciones de las mismas.

4.3.3. PROBLEMAS ATRIBUIBLES A UNA INFECCION VIRAL

En ocasiones, pueden presentarse problemas en el equipo informático que pueden ser causados por virus, pero no siempre es así. A continuación se mencionan algunas fallas de este tipo, así como su probable causa:

- La pantalla del monitor se pone en blanco a la mitad de un proceso.
  El monitor puede tener alguna falla; también es probable que exista algún problema en los cables o conexiones.

- Bloqueo del teclado.
  Puede deberse a que el cable del teclado a la CPU no se encuentre bien conectado, a que el conector este dañado o un falso contacto en el cable o en la(s) tecla(s) presumiblemente bloqueada(s).

- Se despliega en pantalla el mensaje "Sector NOT found".
  Generalmente es porque se encuentra dañado físicamente algún sector o en la FAT del disco que se está tratando de accesar.

- No efectúa una copia de archivos a un directorio específico.
  Puede deberse a un error u omisión del usuario en la especificación de las trayectorias destino.

- Se generan múltiples directorios con archivos iguales.
  Esto puede presentarse cuando por equivocación el usuario crea directorios con caracteres extraños y luego, al no poder accesarlo crea otro con el nombre correcto.

- Eliminación de archivos sin que el usuario lo haya especificado.
  Puede ser que por el uso continuo que se hace del disco, los apuntadores a la FAT sean borrados o modificados accidentalmente.

- Se presenta un error de paridad.
  Ocurre cuando se produce una falla en la RAM.

- Errores en el controlador de disco, lee esporádicamente.
  Este tipo de errores puede presentarse debido a una falla real en el controlador, o bien, si se trata de discos flexibles, puede ser que el drive no se encuentra correctamente alineado.

- Modificaciones en algún archivo de trabajo.
  Puede tratarse de algún que el usuario cometió al manejar el paquete. Por ejemplo, si se selecciona por equivocación o desconocimiento alguna opción que afecte de alguna forma la información.

- El sistema operativo no puede ser cargado.
  Si se trata de una carga desde drive, puede deberse a que el disco flexible con el sistema operativo se encuentra dañado o hay daño en el sector de boot del mismo.

- Aparición de algún texto extraño en la pantalla.
  Puede deberse a fallas en el controlador de video.

- Fallas en la ejecución de algún sistema, paquete o archivo.
  No debe descartarse probables fallas de diseño en el programa, o bien a falta de conocimiento del usuario en la operación del mismo.

4.4. MEDIDAS PREVENTIVAS Y CORRECTIVAS

4.4.1. MEDIDAS PARA PREVENIR INFECCIONES

Las medidas a tomar para evitar infecciones por virus en los equipos de una empresa, depende de las características de ésta y de sus necesidades particulares. Sin embargo, existen ciertas medidas generales que deben ser observadas:

- Prohibir al personal el uso de copias no autorizadas, realizando auditorias sin previo aviso a los usuarios para verificar el cumplimiento de esta norma, además de llevar un control del software contenido en cada equipo

- Llevar un control del acceso de los bienes informáticos, es decir, que solo usuarios autorizados puedan utilizarlos.

- Contar con programas antivirus instalados en todos los equipos y capacitar a todos los usuarios en su utilización. De preferencia se recomienda que este tipo de programas sean ejecutados al inicio y al final de cada sesión de trabajo, a fin de detectar con oportunidad cualquier infección.

- Mantener los discos originales de sistemas, lenguajes y paquetería a buen resguardo y utilizar una copia de seguridad.

- Destinar un equipo sin información vital y fuera de la red para la carga y prueba de discos de sistemas de demostración, obsequiados en exposiciones, prestados, etc.

- Proteger contra escritura aquellos discos flexibles cuyo contenido no debe ser alterado, así como asignarle atributos de Read Only (sólo lectura) a los archivos en disco duro que no se desee modificar o borrar accidentalmente.

- Los programas desarrollados deben ser revisados y aprobados por personal autorizado.

- Estar atento a los mensajes enviados por el equipo al encenderlo, con el objeto de verificar que el sistema operativo sea cargado correctamente.

- Crear claves de acceso a los sistemas solo para usuarios autorizados. Dichas claves no deben formarse con fechas de cumpleaños, nombres de esposas (os) e hijos o con cualesquiera otro dato que sea fácil de descubrir.

- Contar con sistemas que impidan el acceso a gente no autorizada vía modem conocidos como "respaldo de llamada", en los cuales la computadora primero llamaría a ellos, y si se trata de un número de teléfono no autorizado, la computadora no funciona.

- Utilización de controles lógicos, los cuales van más allá de prevenir la entrada a los sistemas de gente no autorizada mediante claves de acceso; actúan en el monitor indicando quien está en el sistema y que está haciendo. Este tipo de controles normalmente requieren que el usuario indique que está realizando y porqué, la computadora graba toda la información e indica situaciones anormales, tal como el acceso al sistema a las 4 a.m. De preferencia, se instalan sistemas que permitan a los usuarios accesar solamente la parte del sistema que requieran sus funciones.

- Es conveniente nombrar un administrador de la seguridad, el cual debe ser una persona responsable; su función sería la de administrar y asegurarse de que las medidas de seguridad se están llevando a cabo, así como de que sean implementados los controles de seguridad apropiados.

4.4.2. PROGRAMAS ANTIVIRUS

Así como existen gran cantidad de virus, se han desarrollado otro tanto de programas antivirales, sin embargo, estos pueden dividirse en las siguientes tres categorías:

- Preventores de infecciones
- Detectores de infecciones
- Identificadores de infecciones

ANTIVIRUS ORIENTADOS A PREVENIR INFECCIONES

Los programas antivirus de este tipo, tienen la característica de detener la reproducción viral genérica y preservan los virus de infecciones iniciales en el sistema. Generalmente no son diseñados para virus individuales, por lo que pueden proteger contra casi toda clase de virus. Estos programas residen en memoria y supervisan todas las actividades del sistema, efectuando un análisis de las características propias de una contaminación por virus; también llevan a cabo un monitoreo de todos los programas que han entrado o salido de la memoria y revisan todos los aspectos del sistema operativo, sobre todo los comandos de servicio.

En general, todos los programas antivirus preventores de infecciones funcionan basándose en la detección de un intento de algún virus por introducirse al sistema, esto es, cuando un virus está tratando de contaminar un archivo ejecutable (el boot, el sistema operativo o un programa de aplicación); cuando esto ocurre, el antivirus detiene el sistema antes de que el virus se reproduzca y envía un mensaje de advertencia al usuario para que éste proceda a eliminar el virus.

La manera en que el antivirus diferencia un acceso viral a alguno proveniente de una aplicación o base de datos, es que en éste último nunca existe un intento de escribirse sobre si mismo, a menos que se le reemplace por otra versión. Sin embargo, existen funciones en algunos sistemas que activan este tipo de antivirus produciéndose así una "falsa alarma"; la cantidad de falsas alarmas depende en gran medida de la calidad del programa antivirus que se utilice.

Una desventaja de los antivirus preventores es que no protegen al sector de boot de una infección. Esto es debido a que cuanto se lleva a cabo la contaminación el sistema a sido reinicializado, por lo que hasta ese momento el programa antivirus no ha sido cargado.

También es importante mencionar que aunque difíciles y tardados de desarrollar, es posible la creación de virus que pueden engañar al antivirus usando mecanismos de infección diseñados para evadir las detecciones, para ello, suscriben de manera directa el hardware controlador de los mecanismos de almacenamiento o utilizando los llamados de E/S que evitan la función de chequeo antiviral.

ANTIVIRUS DISEÑADOS PARA LA DETECCION DE INFECCIONES

Este tipo de programas antivirales trabajan bajo la consideración de que las infecciones son detectadas inmediatamente después de que ocurren, mediante la localización de los rastros que deja el virus, los cuales consisten en cambios en el sistema provocados por el virus durante la infección. Estos antivirus generalmente tienen la capacidad para identificar el área específica del sistema en que se produjo la infección. Además, tienen como característica común a los programas antivirus de prevención que detectan géneros de infecciones antes que infecciones individuales, aunque estos son más confiables y sirven para atacar cualquier clase de virus.

Los antivirus detectores de infecciones tienen dos formas de actuar: por vacunación o por una técnica instantánea:

POR VACUNACION

En esta forma el antivirus trabaja modificando los programas para añadir un mecanismo de prueba en cada programa, el cual es activado cada vez que el programa es ejecutado. Dicho mecanismo de prueba utiliza alguna técnica matemática o algorítmica para ver si se ha modificado la secuencia de instrucciones del programa en cuestión, en cuyo caso envía un mensaje al usuario para advertirlo de la infección.

La desventaja de la vacunación es que existen programas críticos para la computadora que difícilmente pueden ser vacunados. Tal es el caso del sector de boot, el cual es desplazado en su totalidad por el virus por lo que aunque sea vacunado no funciona correctamente después de una infección, y en el caso de que funcionara, el mecanismo de prueba no detectaría el virus debido a que el virus mueve el segmento de boot pero no lo modifica en otros aspectos. Otra desventaja de la vacunación es que como se efectúa después de ocurrida la infección, el virus tiene la oportunidad de activarse o propagarse antes de que la vacuna actué.

A pesar de las desventajas antes mencionadas, los programas antivirales basados en la vacunación sí proporcionan cierto grado de protección, que aunque parcial, siempre es mejor contar con él a no contar con ninguna protección.

POR PROGRAMAS INSTANTANEOS

Esta forma es mejor a la de vacunación. Los programas instantáneos actúan transportando toda la información del sistema al tiempo de instalación inicial, ejecutando luego en intervalos regulares una rutina cuya función es verificar el estado normal del sistema con el original instantáneo; en caso de que se detecte alguna infección, se identifica el área afectada y se envía un mensaje al usuario notificándoselo.

Una de las ventajas de los programas instantáneos es que pueden verificar todas las partes del sistema, por lo que se pueden detectar infecciones en el sector de boot, en el sistema operativo y virus genéricos. Otra ventaja de esta forma de trabajar de los antivirus es que el archivo y el programa comparado pueden mantenerse en off-line, es decir, fuera de la computadora, de tal forma que no pueden ser violados.

La desventaja de esta forma es el tiempo que emplea en realizar las verificaciones del sistema interno, pero actualmente se están diseñando nuevas técnicas para acelerar este proceso, sin embargo, aunque el riesgo de que ocurra es bajo, debe tomarse en cuenta que un virus puede activarse o reproducirse entre un chequeo y otro si se cumplen las condiciones para ello.

Las rutinas para verificar si existe alguna infección pueden ejecutarse cuando el usuario así lo desee, o en la mayoría de los antivirus de este tipo, corridas automáticamente, generalmente al encenderse la computadora.

ANTIVIRUS PARA IDENTIFICACIÓN DE INFECCIONES

Este tipo de programas antivirales son empleados cuando la ya se presentó una infección e incluso el virus a presentado actividad. Generalmente tienen la capacidad de eliminar el virus, de tal forma que el sistema recupere su operación normal anterior a la contaminación. Su forma de trabajar se basa en la búsqueda de rastros específicos de virus en todo el sistema, monitoreándolo para localizar un segmento particular de código viral o alguno de sus rastros característicos; al encontrarlo lo desactivan y eliminan.

Este tipo de programas antivirus tiene la desventaja de que para poder detectar y eliminar un virus, los diseñadores deben conocer antes la forma en que éste funciona, por lo que el proceso puede llevar varios meses desde el virus hace su aparición hasta la obtención de un producto comercial final. Sin embargo, estos antivirus pueden limpiar gran cantidad de discos infectados en forma automática, lo que los hace más efectivos y costeables que cualquier método manual, sobre todo para empresas grandes.

Aunque los programas antivirus pueden ayudar en un momento dado, no existe ninguno que sea absolutamente seguro, por lo que siempre es necesario tomar medidas de prevención como respaldar la información.

CAPITULO 5

PLANES DE CONTINGENCIA CONTRA DESASTRES INFORMATICOS (PCDI)

Un Plan de contingencias es un medio en el cual se identifican y asignan prioridades en las aplicaciones criticas de una empresa, se diseñan y llevan a cabo medidas de seguridad para minimizar las pérdidas en el caso de que ocurra un desastre. También puede definirse como un proceso continuo de planeación, desarrollo, prueba e implementación de procedimientos que aseguran la adecuada disponibilidad de las funciones vitales de una empresa.

La realización de un plan de contingencias debe ser considerado como un proyecto prioritario dentro de las empresas que basan actividades importantes dentro de las mismas en sistemas informáticos, ya que la pérdida de información y/o equipo puede resultar sumamente costosa si no se cuentan con las medidas preventivas y correctivas adecuadas.

En un PCDI se debe identificar y asignar prioridades a las aplicaciones informáticas existentes, así como detectar cuales de ellas son críticas, es decir, señalar cuales son las más importantes o estratégicas para la operatividad de la empresa. También se tienen que diseñar y poner en práctica las medidas de seguridad adecuadas para minimizar los costos por pérdidas y el tiempo de recuperación a la normalidad de funciones en caso de desastre.

Para ello, debe asignarse la elaboración de un PLAN DE CONTINGENCIA CONTRA DESASTRES INFORMATICOS a una persona sumamente capaz y conocedora del manejo del área informática, ya que no es una tarea fácil, pues la organización y definición de la planeación es en si complicada. El apoyo que los directivos brinden es de suma importancia, ya que la persona encargada de la elaboración del plan debe disponer de un horario adecuado para poder realizar procedimientos, inventarios y selección de personal capacitado para efectuar las actividades requeridas para una pronta recuperación en caso de desastre, incluso ante la posibilidad de requerirse la movilización hacia un sitio alterno garantizado.

5.1. OBJETIVOS DEL PLAN

Un PCDI debe proporcionar los recursos y procedimientos para manejar situaciones de emergencia, de operación provisional, etapas de recuperación y regreso a la normalidad en caso de un desastre, especialmente en cuanto a infraestructura informática se refiere. Sus objetivos principales son:

- Minimizar el tiempo de caída.
- Permitir la continuidad de las operaciones de la empresa lo más pronto posible a un nivel costo-efectivo.

- Reducir al mínimo la posibilidad de que ocurra algún desastre que pueda interrumpir o alterar las actividades de la empresa.
- Minimizar el daño en caso de que un desastre llegará a ocurrir.
- Contar con procedimientos para poder actuar de inmediato y en forma adecuada ante la ocurrencia de un desastre.
- Recuperación de los sistemas y actividades criticas para la empresa en los tiempos especificados por la gerencia.
- Evitar sanciones legales por incumplimiento.
- Volver a las condiciones de operación normales.
- Prevenir la pérdida total de información de la empresa.
- Proteger la vida humana.
- Detectar riesgos de forma más efectiva.

5.2. DESARROLLO DE UN PCDI

5.2.1. FACTORES A CONSIDERAR AL DESARROLLAR UN PCDI

El tiempo que se requiere para desarrollar un PDCI varía dependiendo del tamaño del centro de datos.

Al elaborar un Plan de contingencias, existen varios factores que deben ser tomados en cuenta para que contemple la situación particular de cada empresa:

- DEPENDENCIA INFORMATICA DE LA EMPRESA.
  Existen empresas que dependen en gran medida de sus sistemas informáticos, por lo que fallas en los mismos podrían ocasionar grandes pérdidas.

- NUMERO DE EMPLEADOS.
  Entre más empleados se tenga, es mayor la inversión en bienes y recursos necesarios para que estos realicen sus actividades, por lo que el control de los mismos también debe incrementarse.

- UBICACION DEL CENTRO DE COMPUTO.
  Es importante considerar el área en que se encuentra ubicado el Centro de Cómputo, ya que el medio ambiente que lo rodea es fundamental en los riesgos potenciales que pueda tener (clima, accidentes geográficos, índices de vandalismo, si está cercano a industrias que laboren con materiales peligrosos, etc.)

- EXPERIENCIA INFORMATICA DE LA EMPRESA.
  Se debe tomar en cuenta la experiencia de la empresa en el campo de la computación, ya que cuando una empresa recién inicia actividades en el área informática, normalmente se carecen de los conocimientos y la experiencia necesarios para manejar el equipo y sistemas adecuadamente, lo que incrementa el riesgo de que se presente alguna anomalía.

- DISPONIBILIDAD DE RECURSOS.
  Se debe asegurar que se cuenta con todos los recursos necesarios para que el equipo y sistemas funcionen correctamente.

- CAPACITACION AL PERSONAL.
  Debe determinarse si el personal cuenta con la capacitación adecuada, ya que para evitar fallas humanas por desconocimiento, el personal debe ser capacitado en la utilización de los sistemas y del equipo.

- MANTENIMIENTO AL PLAN DE CONTINGENCIAS.
  Dentro del desarrollo de un PCDI debe considerarse su mantenimiento, ya que las medidas de seguridad tomadas pueden deteriorarse o volverse obsoletas por los cambios que se efectúen en la empresa.

- ALCANCES DE PROTECCION

- TIEMPO DESEADO DE RECUPERACION

- PRESUPUESTO

5.2.2. PREMISAS DE UN PCDI

El éxito de un PCDI depende en gran medida de la difusión que se lleve a cabo, por lo que no sólo debe informarse a ejecutivos y usuarios de su existencia, sino también necesitan conocer el significado específico de una interrupción y la serie de acciones que se derivarán de ello.

Confusión y objetivos no definidos son las causas principales para que un PLAN DE RECUPERACIÓN DE DESASTRE no pueda llegar a ser concretado.

Se sugiere desarrollar una lista con las premisas del plan como se muestra a continuación:

- El peor caso de interrupción.
  Diseñar el PCDI para manejar una destrucción total de los datos. Esto debería también permitir la recuperación en el peor punto de interrupción.

- Interrupción menor.
  El plan, aunque diseñado para el peor caso debe ser suficientemente para soportar recuperación de interrupciones menores.

- Nivel de Detalle.
  El plan debe prever los detalles suficientes para permitir que el personal capacitado pueda recuperar los procesos de cómputo.

- Sitio o sitios alternativos.
  Un caso extremo de interrupción hace necesario contar con uno o más sitios remotos para efectos de recuperación.

- Daños al centro de datos solamente.
  Aunque las funciones del usuario está concentrada en un solo centro de datos, un plan debe asumir que posiblemente las funciones de los usuarios también se verán afectadas por el impacto de una interrupción. Restablecer las funciones de los usuarios deberá ser contemplado en planes separados.

- Almacenaje en un lugar alterno.
  Guardar la información en un lugar remoto que contiene los recursos para efectuar la recuperación.
  El propósito es contar con un sitio, ya sea reconstruido o nuevo permanente para el procesamiento de datos, el cual cumpla con las especificaciones requeridas para correr sistemas críticos y no críticos al nivel que existía antes del desastre. El sitio alterno puede ser un lugar de respaldo vacío (cold-site) que cuente con las instalaciones adecuadas de electricidad, aire acondicionado, sistemas contraincendio, equipo de comunicaciones, etc. para recibir al equipo de respaldo, incluyendo al rehabilitado y transportado desde el sitio afectado.
  Es importante contar con los croquis y diagramas de conexión, distribución de equipos, cableado de servicios, etc.

5.2.3. ESTRATEGIAS DE RECUPERACION

Existen varias opciones para poder efectuar la recuperación de la información:

- RECUPERACION EN UN SITO ALTERNO
  Esta opción requiere la duplicidad de la infraestructura y cubrimiento redundante de personal.

- RECUPERACION CORPORATIVA
  Se utiliza el apoyo de otra empresa que cuente con una infraestructura informática compatible.

- DEGRADACION
  En esta opción la duplicidad es limitada, lo cual permite únicamente una recuperación degradada de la información.

- RECUPERACION COMERCIAL
  Se contratan los servicios de una empresa especializada en recuperación.

- RECUPERACION INTERNA
  En este tipo de recuperación se eliminan los procesos y servicios en la recuperación.

- RECUPERACION COMBINADA
  Esta opción es una combinación de las formas de recuperación antes descritas.

5.2.4. ANALISIS DE INFORMACION

Para elaborar un PCDI es necesario efectuar un análisis adecuado de la información, ya que ésta es la base del funcionamiento de cualquier empresa. Por ello deben considerarse los siguientes puntos:

- Evaluar cuales sistemas son obligatorios y cuales necesarios o deseables.
- Efectuar un análisis de las probabilidades de que ocurra cada tipo de desastre.
- Analizar aplicaciones y sitios contra los objetivos del plan. Para ello, se deben determinar los requerimientos por aplicación/recurso, así como definir prioridades y tiempos de recuperación.

- Efectuar un inventario de recursos y procesos:
  - Elaborar una lista detallada del software, hardware, comunicaciones, proveedores, empleados, teléfonos y organizaciones.
  - Equipo de energía eléctrica y aire acondicionado, instalaciones, etc.
  - Funciones y espacios necesarios.
  - Servicios de emergencia.
  - Aplicaciones.
  - Etc.

Para elaborar el análisis mencionado, se utilizan las metodologías que se describen en los puntos siguientes.

5.2.4.1. ANALISIS DE RIESGOS

El análisis de riesgos tiene como objetivo minimizar la probabilidad de que ocurra un evento que ocasione daños a los bienes informáticos, proporcionando medidas de seguridad para que los costos se reduzcan en caso de que llegará a ocurrir un desastre

Al realizar un análisis de riesgos se pretende determinar los riesgos a los que se encuentran expuestos los bienes informáticos, la pérdida económica en caso de que ocurrieran y el costo de implantar medidas de seguridad; éste último debe ser menor a las posibles pérdidas para que se justifique su implantación.

Un análisis de riesgos debe contemplar los siguientes aspectos:

⇒ Efectuar un análisis del tiempo y los recursos con que cuenta la empresa y de aquellos que se requieren para enfrentar los riesgos de un desastre.
⇒ Análisis de las consecuencias de no contar con un plan para enfrentar una contingencia.
⇒ Evaluar las pérdidas probables y determinar los costos de reposición y reparación.
⇒ Las áreas de riesgo son fundamentalmente tres: las instalaciones donde se lleva a cabo el procesamiento, la información y las comunicaciones. Es conveniente hacer un inventario de sus activos.
⇒ Efectuar un análisis de las amenazas potenciales, calculando la probabilidad de que lleguen a ocurrir.
⇒ Identificar los puntos débiles y las amenazas y vulnerabilidad de los mismos.

⇒ Evaluar las medidas de seguridad ya existentes y determinar si es necesario incrementarlas, considerando los costos y beneficios esperados.
⇒ Reconocer las prioridades de los servicios del área contra los beneficios de estos a la empresa.
⇒ Realizar una estimación de las pérdidas por cada tipo de evento.

En ocasiones es difícil determinar la probabilidad de que ocurra un desastre, ya que ésta depende del conocimiento que se tenga del fenómeno en particular. Cuando un evento se produce con relativa frecuencia, se puede utilizar ésta para estimar la probabilidad de ocurrencia, pero generalmente los desastres causados por fenómenos naturales no ocurren frecuentemente.

Aunque casi siempre son los eventos con menor probabilidad de ocurrencia los que producen daños más considerables, debe tomarse en cuenta el costo acumulado de aquellos eventos de menor importancia pero mayor frecuencia.

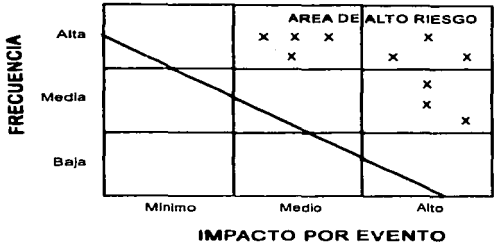
ANALISIS DE IMPACTO

Consiste en efectuar un análisis de los riesgos existentes, a fin de determinar cuales son aquellas amenazas que pueden provocar consecuencias más graves para la empresa.

Para poder analizar el impacto de los riesgos, se elabora un cuadro llamado "matriz de amenazas", en donde se enumeran y describen los posibles riesgos, daños y frecuencia de ocurrencia:

# Amenaza	Descripción	Impacto por Evento			Frecuencia		
		Alto	Medio	Bajo	Alta	Media	Baja

a continuación, se elabora un cuadro frecuencia vs impacto:



Cuando para un evento ya se ha determinado su probabilidad de ocurrencia en un período específico, debe calcularse la pérdida acumulada en ese período. Con ello puede calcularse la pérdida estimada para el riesgo analizado:

$$PE = PO * PA$$

Donde:

PE = Pérdida estimada
PO = Probabilidad de ocurrencia
PA = Pérdida acumulada

Para estimar la pérdida involucrando varios riesgos, solamente se efectúa la sumatoria correspondiente:

$$PE_T = \sum_{i=1}^{n} PO_i * Pa_i$$

Al efectuar los cálculos anteriores, deben considerarse los siguientes aspectos:

- ◊ Costos involucrados (reparación, reemplazo, instalación, servicio, etc.)
- ◊ Pérdida de ganancias y oportunidades
- ◊ Costo del tiempo laboral perdido a causa de la interrupción del procesamiento
- ◊ Deterioro de la imagen de la empresa.

El análisis de riesgos descrito es cuantitativo, ya que proporciona información precisa de todas las pérdidas probables. También existen técnicas para efectuar un análisis cualitativo, con las cuales se obtiene la pérdida probable debida a un evento en forma relativa y sin llegar a la cuantificación.

En el análisis cuantitativo se identifican todas las áreas expuestas a riesgos, pero pueden resultar caros y requerir de mucho tiempo y recursos, mientras que el cualitativo involucra solamente un conjunto básico de controles en base a experiencias previas, con lo que se ahorra tiempo y recursos pero pueden omitirse áreas expuestas que no se consideren como fuentes de posibles riesgos.

Ambos enfoques tienen ventajas y desventajas, por lo que el más adecuado dependerá de las necesidades de cada empresa. En general, cuando se tienen pocas medidas de protección, se puede optar por un análisis cualitativo, mientras que si la empresa cuenta con medidas de seguridad y protección de información sofisticadas, requiere un análisis cuantitativo en áreas de riesgo.

5.2.4.2. ACTIVIDADES Y SISTEMAS CRITICOS

Para poder determinar las actividades y los sistemas críticos de una empresa, deben considerarse los siguientes aspectos:

- Realizar un inventario de los sistemas en operación.

- Determinar cuales actividades de la empresa son fundamentales para que ésta sea rentable. Para ello, puede establecerse un esquema de clasificación de los sistemas en operación, determinando si son críticos, necesarios, no tan críticos o de importancia menor. Para definir la criticabilidad, se puede hacer una evaluación de riesgos considerando los siguientes factores:

  - ⇨ Daños a la Base de datos
  - ⇨ Penalizaciones gubernamentales
  - ⇨ Implicaciones legales por requerimientos de accionistas o por acuerdos contractuales
  - ⇨ Impacto en el personal
  - ⇨ Pérdida de servicios a clientes

- Utilizar métodos de análisis de riesgos respaldados con información obtenida de entrevistas con los altos mandos de la empresa y con los usuarios. Dicha información será empleada para determinar la estrategia de protección y también para el diseño del programa de respaldo y restauración.

- Normalmente, un PCDI debe incluir únicamente a los sistemas críticos, pero si se desea, puede incluirse en él alguna actividad no crítica que interese su recuperación en caso de ocurrir de que se presente una contingencia.

- Es necesario que se especifique cuales son los tipos de desastre contemplados en el PCDI y a qué nivel de destrucción es posible la protección y recuperación. Para ello, se necesitan definir los escenarios críticos a considerar dentro del plan.

Es importante recalcar que para aquellos escenarios y sistemas no considerados en el plan, no se tienen ninguna seguridad de que puedan ser recuperados en caso de que llegara a ocurrir un desastre.

5.2.4.3. VENTANA DE TIEMPO DE VULNERABILIDAD

La Ventana de Tiempo de Vulnerabilidad (VTV) es el lapso de tiempo máximo que debe pasar para retornar a la normalidad de las operaciones de la empresa, de manera que el estado de estas sea lo mas aproximado al existente antes de que ocurriera la contingencia y antes de que este produzca perdidas significativas.

El concepto de la ventana de tiempo de vulnerabilidad es importante para el diseño de un plan de contingencias.

La VTV debe ser determinada y clasificada para cada actividad o sistema critico. Para estimar el tiempo se utilizan las entrevistas a los usuarios, considerando los rangos de clasificación de VTV siguientes:

TIEMPO DE INTERRUPCION (horas)	CLASIFICACION DE VTV
0 -1	Hipercrítica
2 - 6	Muy crítica
7 - 12	Crítica
13 - 48	Criticalidad normal
Más de 48	Menos crítica

IMPACTO DEL DESASTRE VTV

NIVEL DE IMPACTO EN OPERACIONES CRITICAS	VTV EN CUADROS DE TIEMPO
1. Crítica y mayor	Recuperación en minutos
2. Grave y mayor	Recuperación en 4 a 6 horas
3. mayor	Recuperación en 24 a 36 horas
4. Significativo	Recuperación en X días
5. Limitado o menor	Recuperación en Y días
6. Inconveniente	Recuperación en Y semanas
7. No notable	En un tiempo conveniente después de la recuperación

VTV PARA CADA SISTEMA:

ACTIVIDAD CRITICA	SISTEMA QUE SOPORTA LA ACTIVIDAD CRITICA	VTV (horas)	USUARIO Y COMENTARIOS

5.2.4.4. ESCENARIOS DE DESASTRE

Un escenario es la representación de probables eventos en un futuro, esto es, una visualización anticipada de determinadas situaciones que pueden llegar a ocurrir en base a las condiciones actuales prevalecientes.

En los planes de contingencia, un escenario permite disponer de una medio para evaluar el impacto físico y financiero que puede ocurrir a las actividades vitales de una empresa si éste llegase a presentarse. En este sentido, puede hacerse la diferenciación los objetivos de un escenario de desastre y los de un análisis de riesgos, ya que el primero es una visualización de un evento y el segundo se enfoca a las pérdidas potenciales que pudieran ser el resultado de desastres visualizados en el desarrollo de un escenario, es decir, que al desarrollar escenarios de desastre, se tiene otro recurso para realizar el análisis de riesgo.

El desarrollo de un escenario de desastre permite tener una clave de la naturaleza y el alcance de una contingencia y del plan de recuperación. En la siguiente tabla se mencionan algunos escenarios, sus amenazas y algunas estrategias que pudieran implementarse para disminuir el riesgo:

ESCENARIOS	AMENAZA: FUEGO	SISMO	BOMBA	ERRORES DE OPERACION	PERDIDA DE ENERGIA	ESTRATEGIAS
Destrucción total del centro de cómputo	X	X	X			* Ubicación adecuada del centro de cómputo * Tipo de construcción
Contingencia de incendio	X				X	* Sistemas contraincendio * No fumar en el área * Mantenimiento a las instalaciones eléctricas
Mala operación del equipo				X		* Acceso restringido al centro de cómputo
Pérdida de información				X		* Procedimientos de respaldo y bóvedas de seguridad
Destrucción masiva de la base de datos	X	X	X	X	X	* Equipos de energía ininterrumpida * Plantas de energía de emergencia

Ejemplo del desarrollo de un escenario de contingencia

Area dañada:

8vo. piso, edificio principal de la oficinas generales de la empresa Productos Universales, S.A., incluyendo la información del departamento de sistemas.

"Durante la noche del sábado 22 de abril de 1997, un fuego masivo dio inicio en el 6to. piso de las oficinas generales, propagándose cuatro pisos arriba en el edificio de un total de 12 pisos localizado en el área del centro de la ciudad. Las alarmas se activaron y se alertó al personal de seguridad, así como al departamento de Bomberos, los cuales se encontraban laborando en su totalidad en otro siniestro por lo que demoraron 25 minutos en arribar. Cuando el fuego fue controlado, se llevo a cabo el recuento de los daños, encontrándose la siguiente situación:

1. Daños masivos en los pisos 6 a 9.

2. Destrucción total de las oficinas administrativas y la central de servicios, lo que incluye teléfonos, central de contactos, archivo, centro de almacenaje de datos, microfilms, contratos, etc.

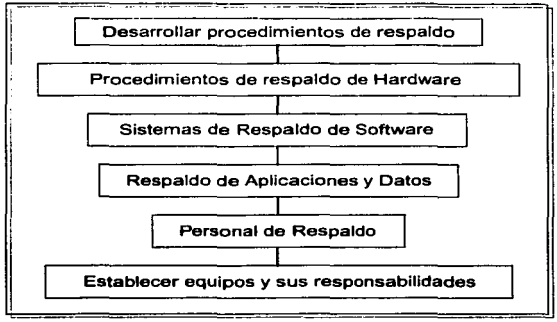
3. Destrucción grave del departamento de procesamiento de datos, el área de control de datos y las unidades de entrada, sistemas de facturación y servicio a clientes, los cuales representaban el 50% del total de actividades de procesamiento de la compañía.

4. El agua utilizada para extinguir el incendio causó inundación de dos pies de alto, afectando los pisos y causando daños a la información almacenada y al suministro de servicios, incluyendo la energía eléctrica.

5. La seguridad del edificio y la reglas ambientales demandan una operación de seguridad y limpieza minuciosa, estimando que se tomará 2 semanas antes de que los empleados puedan regresar.

5.2.5. PROCEDIMIENTOS DE RESPALDO

El propósito de definir procedimientos de respaldo es el de salvaguardar la información de las funciones vitales de la empresa. A continuación se presenta el diagrama de flujo para procedimientos de respaldo:



⇨ **Procedimientos de respaldo de hardware**

Se debe especificar cual es la configuración de hardware mínima requerida para procesar las aplicaciones críticas. La documentación de ésta información es de gran utilidad cuando se necesita reconstruir o reestructurar los procesos.

⇨ **Sistemas de respaldo de software**

El software debe ser respaldado basándose en la frecuencia de cambios realizados. Los respaldos deben almacenarse en un sitio remoto (off-site) y estar disponibles en todo momento. Algunos ejemplos del software a considerar son:

- Sistemas operativos.
- Subsistemas.

- Bases de datos/comunicaciones.
- Usuarios privilegiados y claves de acceso (passwords).
- Data sets como procedimientos de arranque.
- Procedimientos para restaurar el software.
- Manuales.

⇨ **Respaldo de aplicaciones/datos**

La frecuencia de respaldo de las aplicaciones dependerá de los ciclos del negocio y del número de modificaciones hechas a las mismas. Los respaldos deben ser guardados off-site y estar siempre disponibles. Entre las aplicaciones que deben tomarse en cuenta están:

- Bases de datos.
- Módulos de carga y códigos fuente.
- Archivos batch.
- Archivos y procedimientos para restaurar la información.
- Documentación.
- Identificaciones privilegiadas y claves de acceso (passwords).
- Formas especiales de impresión.

Es importante que la información sea respaldada por duplicado y almacenada por separado, para que en caso de dañarse o si ocurre una contingencia pueda recurrirse al duplicado y agilizar la restauración.

⇨ **Personal de respaldo**

Se debe tener personal que respalde a aquel que no se encuentre disponible. Para ello, puede elaborarse una lista basada en la identificación de:

- Actividades requeridas para ejecutar el plan de recuperación.
- Conocimientos para realizar ciertas actividades.
- Personal de soporte primario y secundario.

⇨ **Establecer equipos y sus responsabilidades**

Una vez definidas las actividades y el personal, se deben formar grupos de trabajo con responsabilidades bien definidas para antes, durante y después de un desastre.

5.2.6. ALCANCES DE UN PCDI

El PCDI incluye los procedimientos y acciones relativas al proceso de planeación de contingencias antes, durante y después del desastre, así como a su documentación formal (manuales, instructivos, procedimientos, rutas de evacuación, etc.).

También pretende establecer medidas de control para evitar pérdidas financieras y de bienes o recursos a consecuencia de una contingencia, así como definir mecanismos para asegurar la recuperación de la organización pronta y adecuadamente.

Dentro de un PCDI debe considerarse toda la infraestructura informática, así como también a los usuarios y clientes. Los alcances del plan dependen de varios factores:

- ◊ Tipos de desastre considerados
- ◊ Areas a proteger
- ◊ Aplicaciones criticas a recuperar prioritariamente
- ◊ Magnitud del desastre
- ◊ Coberturas de servicios contemplados
- ◊ Tiempos de recuperación clasificados :
  - 24 hrs, servicios con prioridad A
  - 7 días, servicios con prioridad B
  - 20 días, servicios con prioridad C

5.2.7. RESPONSABLES DEL PLAN

Es responsabilidad del gerente de sistemas el contar con un plan adecuado, así como de supervisar que una vez implementado sea cumplido por todas las personas involucradas. La elaboración de dicho plan puede ser asignada a otra persona, siempre y cuando cuente con los conocimientos adecuados para ello, la cual fungirá como coordinador del proyecto, pero siempre bajo la supervisión del gerente, ya que éste será el enlace entre directivos de la empresa , PCDI y usuarios.

Los ejecutivos del área de sistemas son los adecuados para desarrollar los PLANES DE DESASTRE, ya que generalmente tienen amplia experiencia con las funciones de servicio de la empresa, y pueden determinar la prioridad de la aplicación de una recuperación en caso de desastre con una exactitud aceptable. Sin embargo, debe considerarse al usuario como parte esencial en la elaboración del plan, ya que es quien conoce mejor el manejo de la información y las prioridades de los servicios de la computadora, por lo que puede identificar adecuadamente cuales son las operaciones criticas (las más importantes dentro del funcionamiento de la empresa), así como el tiempo para su recuperación.

Además, el usuario debe revisar los procedimientos para los que se utiliza el procesador central, a fin de que éste pueda ser relocalizado en un sitio alterno.

Un minucioso plan de recuperación de desastres debe ser observado desde dos perspectivas. Por un lado, el gerente debe nombrar un responsable para desarrollo e implementación del PDCI y por otro uno para lo referente a mantenimiento (el cual debe ser continuo). El responsable de desarrollo debe preferentemente tener experiencia con sistemas de aplicación grandes y de la mayoría de los sistemas existentes, ya que será la conexión entre los directivos y los usuarios: también tiene que conocer acerca del procesamiento de datos, comunicaciones, operación del software, hardware y aplicaciones de sistemas, a fin de definir prioridades en las aplicaciones a recuperar. Un 75% de su tiempo dedicado al proyecto del PCDI es adecuado. En cuanto al responsable de mantenimiento, puede ser un analista o programador con capacidad administrativa, ya que debe conocer a la perfección los requerimientos administrativos del plan. Este responsable debe trabajar bajo la supervisión del coordinador del proyecto.

5.3. PLAN DE TRABAJO PARA EL DESARROLLO DE UN PCDI

Los procedimientos generales del plan de trabajo para la elaboración de un PCDI son los siguientes:

1. Definir los objetivos del plan y las metas que se desean lograr con el mismo.

2. Elaborar una lista que contenga todas las funciones que involucrará el plan, tales como:

- Asignación del coordinador del plan
- Relación del personal que deberá ser entrevistado o consultado
- Determinar cual es la información que se requiere y especificar en donde puede obtenerse.
- Determinar la función especifica de cada uno de las personas del grupo de trabajo.
- Definir cual es la prioridad en las actividades a realizar, así como la secuencia en que han de realizarse.

3. Para poder contar con un apoyo gráfico de tiempos y actividades, se puede realizar un diagrama de "Grant" o uno de "Pert" para mostrar la organización del plan.

   Por un lado, el diagrama de "Grant" contempla actividades, secuencia de éstas y el tiempo asignado para realizar cada una de ellas; mientras que el de "Pert" muestra además la interdependencia existente entre las actividades, el tiempo crítico mínimo para realizarlas y especifica aquellas tareas que pueden efectuarse paralelamente, por lo que éste último tipo de gráfica es más recomendable de utilizar en el plan.

4. Determinar los límites de tiempo para llevar a cabo cada actividad y lograr su meta.

5. Especificar cual documentación se empleará para llevar un control de los acontecimientos, así como de los resultados del plan en cada etapa del mismo. La documentación debe contener los siguientes aspectos:

   - Políticas de la empresa con respecto a la continuidad en las operaciones de la misma y de recuperación en caso de que ocurriera un desastre.
   - Objetivo del plan respecto a la continuidad de operaciones de la empresa.
   - Plantear los posibles escenarios de desastre y las premisas clave para cada uno de ellos.
   - Especificar cuales serán los planteamientos con respecto a seguridad.
   - Definir cual es el período critico de vulnerabilidad.
   - Especificar los escenarios de desastre aprobados por los altos mandos de la empresa.
   - Documentar los pasos a seguir en caso de que se declare una contingencia, tales como:

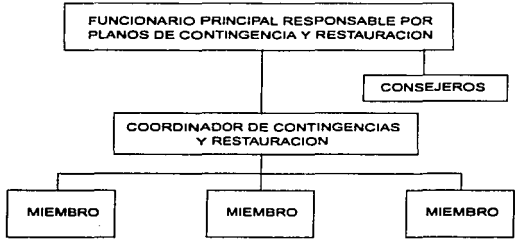
- Procedimientos que se llevarán a cabo para analizar y declarar una contingencia.
- Definir como se efectúa la clasificación de las emergencias y desastres.
- Relación de funcionarios de la empresa que deben ser notificados en caso de presentarse una contingencia.
- Forma en que se avisará al personal involucrado en el plan sobre la contingencia.
- Procedimientos que deberán realizarse ante las entidades externas que brindan a la empresa sus servicios (como proveedores).
- Lista de los servicios de emergencia, tales como policía, hospitales, bomberos, etc.

- Especificación de los sistemas y actividades críticas para la continuidad en las actividades de la empresa.
- Determinar cuales son los recursos disponibles para hacer frente a una contingencia y para poder mantener operando los sistemas críticos para la empresa.
- Relación de los elementos que deben ser respaldados para que sea posible la recuperación y restablecimiento de las operaciones de la empresa.
- Lista a detalle de la configuración del hardware en que se llevan a cabo los respaldos.
- Relación detallada de programas a respaldar.
- Relación de los archivos y/o sistemas que deben ser respaldados off-site, es decir, en un lugar remoto a la empresa.
- Lista de los manuales a respaldar.
- Relación del equipo de oficina requerido para efectuar el respaldo.
- Especificaciones de las unidades de entrada de datos.
- Relación de las actividades de emergencia que se necesitan poner en operación en caso de presentarse una contingencia.
- Procedimientos de seguridad durante la contingencia y la evacuación del personal.
- Definir como se llevará a cabo la notificación para que se efectúe el respaldo "en caliente" por el personal asignado para ello dentro del plan.
- Relación para llevar un control del personal autorizado para recibir copias del Plan de Contingencia (o alguna sección). También debe contarse con una relación de la ubicación de las copias para tener acceso a ellas en caso de contingencia.
- Relación del hardware y software con el que se cuenta en el lugar remoto de respaldo.
- Relación de los elementos que deben encontrarse respaldados para que sea posible la recuperación y restablecimiento de las operaciones de la empresa.

5.4. IMPLANTACION Y MANTENIMIENTO DE UN PCDI

5.4.1. ESTRUCTURA DE ORGANIZACION PARA LA IMPLANTACION

A continuación, se muestra un diagrama en el que se puede observar la estructura general de organización para un plan de contingencias:



La estructura de organización del personal involucrado en el plan de recuperación se divide en dos grupos:

1. El grupo de control
2. Grupos especializados

GRUPO DE CONTROL

Entre las funciones de recuperación, se debe instalar un centro de control para que todas las actividades sean canalizadas por un área. Para ello, se forma un grupo de control, el cual es el encargado de llevar a cabo la coordinación del plan durante la contingencia y la restauración. El personal que lo integra debe ser, de preferencia, el siguiente:

- ⇨ Ejecutivos con poder de decisión.
- ⇨ Algunos líderes de grupo.
- ⇨ Personal de recursos humanos, seguridad, fianzas.
- ⇨ Personal encargado seguros.
- ⇨ Personal de servicios administrativos, relaciones públicas, transportes, auditoría.

El grupo de control debe contar con un Centro de Control, mismo que debe reunir las siguientes características:

- ☞ Fácil de localizar.
- ☞ Ubicación estratégica.
- ☞ Que cuente con múltiples vías de comunicación: teléfonos, radios, celular, etc.
- ☞ Contar con suficiente equipo, mobiliario y suministros.
- ☞ Contar con copia actualizada del Plan, tanto en papel como en algún medio magnético.

Además, el grupo de control debe tener un coordinador general, el cual es el responsable de mantener la continuidad de las funciones informáticas, así como de la organización de los grupos de trabajo (el coordinador tiene la obligación de mantener informados a los altos mandos de todos los inconvenientes y progresos de la aplicación del plan, para en caso de no tener los resultados esperados se tomen medidas de redireccionamiento). Entre sus funciones se encuentran:

- Encabezar las reuniones del grupo de control
- Administrar y promover el plan
- Probar y dar mantenimiento al plan para que se encuentre actualizado
- Coordinarse con los líderes de grupo internos y externos
- Ir personalmente a revisar el o los sitios alternos
- Dar continuidad al plan

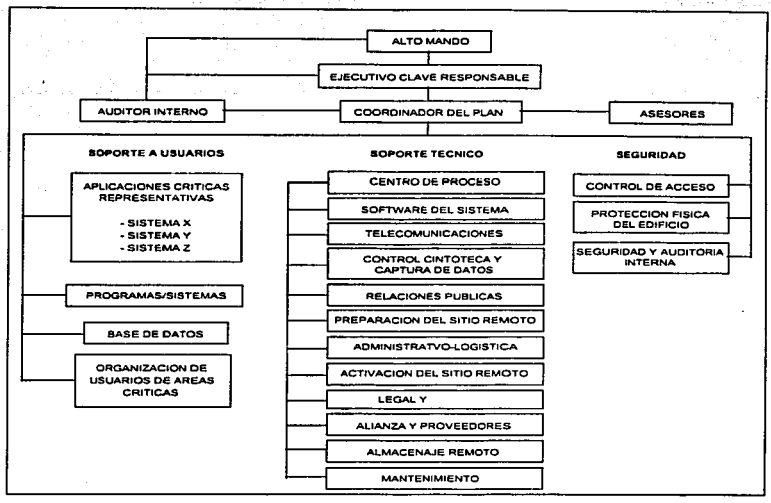
GRUPOS ESPECIALIZADOS

Estos grupos deben estar formados por personal capacitado, ya que son los responsables de realizar la restauración de las operaciones.

El número de grupos, tanto en tamaño como en responsabilidades, varían de acuerdo a la complejidad de la instalación y a la organización de la empresa. Una organización grande y compleja puede requerir la asignación de varios equipos, mientras que una pequeña puede necesitar solo uno; el objetivo es que el o los grupos realicen las actividades asignadas. Entre los grupos que pueden formarse se encuentran los siguientes:

- ◊ Grupo de emergencia inmediatamente después de que ocurre un desastre.
- ◊ Grupo de seguridad y auditoría interna.
- ◊ Grupo encargado del centro de procesamiento de datos.
- ◊ Grupo responsable de preparación del nuevo sitio de operaciones (off-site o sitio alterno).
- ◊ Grupo administrativo - logístico.
- ◊ Grupo responsable de las telecomunicaciones.
- ◊ Grupo encargado de salvaguardar las bases de datos.
- ◊ Grupo encargado del software (sistemas y programas).
- ◊ Grupos de sistemas que representen aplicaciones críticas.
- ◊ Grupo encargado de la restauración y reacondicionamiento del sitio afectado.
- ◊ Grupo responsable de Relaciones públicas.
- ◊ Grupo legal y de seguros.
- ◊ Grupo de mantenimiento (electricidad, aire acondicionado, etc.).
- ◊ Grupo encargado de organizar a los usuarios de áreas críticas.
- ◊ Grupo de alianza y proveedores.
- ◊ Grupo encargado del software del sistema - sistemas operativos.
- ◊ Grupo de control de cintoteca y captura de datos.
- ◊ Grupo de almacenaje remoto.

Por lo tanto, la estructura organizacional para contingencias, considerando los grupos especializados sería la siguiente:



A manera de ejemplo, entre las actividades que pudiesen asignarse a algunos de estos grupos especializados se encuentran las siguientes:

Grupo de telecomunicaciones

- Establecer la comunicación de datos.
- Asegurar la existencia de líneas, terminales y modems.
- Efectuar pruebas en línea.

Grupo responsable del sitio alterno (off-site)

- Preparar las instalaciones para recibir equipo eléctrico, teléfonos, muebles, etc.
- Supervisar instalaciones de hardware, líneas, teléfono, etc.
- Desarrollar procedimientos de seguridad en el sitio alterno.
- Proveer de los servicios necesarios al sitio alterno.

Grupo administrativo - logístico

- Proveer transportación tanto para el equipo como para el personal
- Reconectar las líneas telefónicas
- Distribuir mapas y dirección del sitio alterno
- Encargarse de lo referente a hospedaje, servicio médico, etc.
- Contratar personal temporal
- Administrar los gastos y pagos de eventos
- Desarrollar métodos de contacto en caso de un desastre potencial

Grupo de restauración y reacondicionamiento del sitio afectado

- Determinar la seguridad física en el sitio dañado
- Coordinar y efectuar trámites con la policía, bomberos, etc.
- Dictaminar si el área afectada puede ser reutilizada
- Recuperación de equipo no dañado

Grupo de software del sistema

- Determinar el tipo de requerimientos del sistema operativo, como librerías y utilerías
- Coordinar pruebas de software
- Informar al equipo encargado de hardware sobre el software que depende de algún dispositivo.

A continuación, se muestra un formato que puede ser empleado para llevar un control en cada grupo de sus requerimientos y responsabilidades:

Nombre del Grupo:
Líder del grupo:
Nombre del miembro:
Conocimientos requeridos:
RESPONSABILIDADES
ANTES del desastre
DURANTE el desastre
DESPUES del desastre

También es conveniente contar con un registro de los miembros que conforman los grupos especializados; para ello, pueden utilizarse los siguientes formatos de organización:

CARTA DE ORGANIZACION - GRUPOS ESPECIALIZADOS

COORDINADOR GENERAL:		SUSTITUTO:		
TITULO	**NOMBRE**	**DEPARTAMENTO**	**TELEFONO**	
			OFICINA	**HOGAR**
1. Coordinador de Planeación de Contingencias				
2. Alto mando - Ejecutivo clave				
3. Grupo de Emergencia				
4. Grupo seg. y autditoria interna				
5. Grupo de Centro de proceso				
6. Gpo. responsaible del sitio alterno				
7. Grupo Admvo-logístico				
8. Grupo de Telecomunicaciones				
9. Grupo de Bases de Datos				
10. Grupo de Sistemas/Programación				
11. Grupo de Aplicaciones críticas				
12. Gpo. restauración y reacond.del sitio afectado				
13. Grupo de relaciones públicas				
14. Gpo. Legal y de Seguros				
15. Grupo de mantenimiento				
16. Gpo. de organizacion de área críticas				
17. Gpo. de alianza y proveedores				
18. Gpo. de software del sistema				
19. Gpo. control de cintoteca y captura de datos				
20. Grupo de almacenaje remoto				

Nombre del Grupo:			
Lider del grupo:			
Miembro	**Tel.**	**Sustituto**	**Tel.**

5.4.2. RECUPERACION EN CASO DE DESASTRE INFORMATICO

El plan de recuperación es un documento en el que se definen los recursos necesarios y los pasos a seguir para permitir a la empresa la restauración de sus procesos en un lapso de tiempo razonable, minimizando el impacto y costo de un desastre.

Al declararse una emergencia, se deben tener presentes los objetivos primordiales de los procedimiento implementados para ese momento:

- Manejar la fase de emergencia de forma mas ordenada posible.
- Minimizar el daño a valores, recursos y personal.
- Proporcionar el medio ambiente para la recuperación.

Para ello, se deben llevar a cabo las medidas y procedimientos de emergencias elaborados en el PCDI, hasta la declaración de fin de la contingencia; si ésta no amérita la activación de los procedimientos generales, puede considerarse:

- Realizar cambios en el calendario de trabajo o ajustes al mismo.

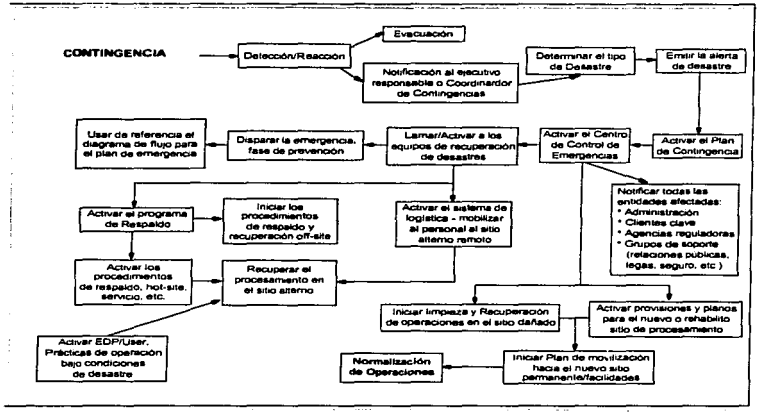
- Contratación de servicios externos para que realicen las actividades que no pueden ser demoradas o de clientes importantes.

5.4.2.1. MEDIDAS Y PROCEDIMIENTOS EN CASO DE CONTINGENCIA

Entre las medidas y procedimientos a desarrollar al declararse una emergencia se encuentran:

- Clasificación de emergencias.
- Notificación por parte del coordinador general a los altos mandos de la empresa.
- Procedimientos de notificación internos y externos (grupos especializados, personal, prensa, grupos de auxilio externos, etc.).
- Procedimientos de evacuación del personal y retiro de archivos y otros elementos críticos.
- Declaración del tipo de emergencia y puesta en marcha de los procedimientos inmediatos.
- Clausura del sito afectado.
- Notificación a los grupos de recuperación.

- Puesta en marcha del programa de evaluación de daños y recuperación de equipos y otros recursos reutilizables.
- Notificación y activación del sito de procesamiento de respaldo (Hot-site o Backup site).
- Activación de los procedimientos de recuperación de respaldos.
- Restauración del sitio afectado o activación del sitio de respaldo.
- Declaración del fin de la emergencia.
- Elaboración de un reporte de la emergencia, su cronología y como se manejo.



Mientras se restauran los servicios informáticos, si es posible, se busca un modo de operación alterno. Para ello, los pasos a seguir deben desarrollarse de acuerdo a lo siguiente:

- Reorganizar los grupos de usuarios y procesamiento de datos para realizar las actividades de los sistemas críticos prioritarios.

- Si es posible que se opere manualmente, deben desarrollarse procedimientos para asegurar que ésta forma de operar sea eficaz para la transición del momento temporal a la recuperación del procesamiento informático.

- Los servicios externos de asesoría y respaldo pueden utilizarse de otro centro de trabajo siempre y cuando tenga las mismas características del que se encuentra interrumpido temporalmente. En éste caso se deben considerar los siguientes puntos:

  ⇒ Tomar en cuenta las prioridades del centro alterno en cuanto a tiempos, espacios y actividades que puedan afectar el personal que se envíe a él.
  ⇒ Considerar loas ajustes a las prácticas de seguridad y las facilidades para el procesamiento en condiciones difíciles.
  ⇒ Tener presente las facilidades de transportación en la situación momentánea.

EVALUACION DE DAÑOS

Al efectuar la evaluación de los daños, se deben considerar los siguientes aspectos:

- Personal afectado.
- Recursos de hardware.
- Archivos clave.
- Sistemas críticos más afectados.
- Afectación de los recursos que se trasladarán al sitio remoto (en caso de haberse requerido).
- Servicios auxiliares disponibles (medio ambiente, aire, humedad, energía eléctrica, etc.).
- Servicio de comunicaciones.
- Documentación y manuales de instrucciones.

La elaboración del reporte de daños debe ser clara, directa y precisa e indicar la prioridad en las aplicaciones críticas, considerando en él aspectos como los siguientes:

- Los elementos dañados, especificando si es posible su reconstrucción o si es necesario reemplazarlos.
- Evaluación de las situaciones más serias.
- Aspectos que requieren prioridad, con comentarios que permitan tomar decisiones inmediatas.

RESUMEN DE ACTIVIDADES Y SISTEMAS CRITICOS

Es de gran utilidad elaborar un resumen de medidas que permitan la continuidad de operaciones en las actividades y sistemas críticos; el resumen debe contener las acciones a llevar a cabo en base al tipo de desastre/escenario que se presente. Para ello, debe hacerse una clasificación de escenarios de desastre para después relacionarlos con la acción específica a efectuar; también debe especificarse la ubicación de las instrucciones para tomar acción en el manual de documentación del plan. Lo anterior puede hacerse en base al siguiente formato - *ejemplo:*

TIPO DE DESASTRE/Escenario #	ACCION	REFERENCIA EN MANUAL
1.Pérdida total de la base de datos	Plan de acción No. ___	Sección ___ , página ___
2. Daño mayor en edificio y oficinas	Plan de acción No. ___	Sección ___ , página ___
3. Pérdida del centro de cómputo por:		
a. Incendio (causa eléctrica)	Plan de acción No. ___	Sección ___ , página ___
b. Explosión o Bomba	Plan de acción No. ___	Sección ___ , página ___
c. Inundación	Plan de acción No. ___	Sección ___ , página ___
4. Fallas de software	Plan de acción No. ___	Sección ___ , página ___
5. Etc.		

5.4.2.2. PRUEBAS AL PLAN

El objetivo de probar el plan de contingencias es el de verificar que los procedimientos a seguir en caso de ocurrir un desastre funcionen de acuerdo a la planeado con los grupos de trabajo responsable de la recuperación. Los parámetros de prueba, los objetivos y los criterios de medición deberán ser previamente establecidos.

Realizar simulacros ayuda a corregir detalles que no pueden apreciarse cuando se desarrollan de manera rutinaria las actividades. Además, el entrenamiento que se proporciona al personal permite que éste efectúe con mas seguridad y presión las acciones encomendadas.

Entre algunas de las pruebas que se deben llevar a cabo se pueden mencionar la siguientes:

- Activación de los grupos especializados
- Checar la documentación del plan
- Verificar el levantamiento de los sistemas críticos fuera del centro de proceso
- Simulacro de emergencia y evacuación
- Checar el traslado de información al sitio remoto
- Si se cuenta con planta de emergencia, verificar que funcione adecuadamente
- Calendarización de las pruebas
- Comparación de los respaldos con los originales
- Probar los respaldos
- Procedimientos de recuperación
- Restauración de sistemas

Los problemas encontrados deben documentarse y el plan debe ser actualizado conforme al resultado de las pruebas.

5.4.2.3. ACCIONES Y TIEMPO DE RECUPERACION

El tiempo es un factor fundamental durante la activación de procesos de recuperación, por ello, las acciones a ejecutar deben llevarse a cabo en el mínimo de tiempo requerido. A continuación, se presenta un ejemplo de las acciones a tomar después de que a ocurrido un desastre:

CONTINGENCIA	
Tiempo transcurrido (horas)	**Acciones**
1 a 6	• Evaluar daños. • Activar el centro de control. • Notificación a los altos mandos de la empresa. • Aviso al sitio alterno . • Tener disponible el respaldo. • Activar los grupos especializados de recuperación. • Inicio del traslado de suministros al sitio alterno.
6 a 12	• Notificación a los usuarios involucrados en la recuperación. • En caso de requerirse, establecer las necesidades de hardware. • Ordenar el equipo y suministros necesarios. • Movilización hacia el sitio alterno de la documentación y cintas.

12 a 24	• Transportación de todos los sistemas que se encontraban operando.
	• Establecer la operatividad en el sitio alterno:
	  • Levantar el sistema operativo.
	  • Pruebas al nuevo equipo.
	  • Restauración del respaldo de archivos.
	  • Restauración de bases de datos.
	• Pruebas para verificar la integridad de la información.

24	• Recuperación del material y documentación reutilizable. • Restauración e instalación de sistemas críticos. • Arranque de los sistemas críticos.

5.4.3. MANTENIMIENTO AL PCDI

Para que el plan sea efectivo al momento de requerirse, es necesario que una vez implementado se le de un mantenimiento continuo. Siempre que se incorpore un nuevo elemento, ya sea de hardware o de software, se tiene que adecuar al plan, a la capacitación y a los procedimientos.

Para el mantenimiento debe asignarse un responsable, el será supervisado por el coordinador general del Grupo de Control (GC), el cual tiene las siguientes funciones:

- ⇒ Estándarizar la documentación.
- ⇒ Llevar el control de las versiones y distribución de éstas.
- ⇒ Mantener una seguridad elevada en el contenido del plan.

El plan debe poder ser revisado en cualquier momento, siendo conveniente elaborar un calendario de revisiones y modificaciones al plan. Es importante que todos los resultados de las revisiones sean documentados y empleados para al actualización del plan. Entre algunos de los puntos que deben ser tomados en cuenta al efectuar la revisión se encuentran los siguientes:

- ☞ Cambios de personal.
- ☞ Cambios de prioridades.
- ☞ Modificaciones de hardware y software.
- ☞ Cambios en las organizaciones de los clientes.
- ☞ Resultados de las pruebas al plan.
- ☞ Cambios legales.
- ☞ Nuevas aplicaciones críticas.
- ☞ Cambios relacionados a las aseguradoras.
- ☞ Nuevos controles de seguridad.
- ☞ Adquisición de equipo nuevo.
- ☞ Cambios en la empresa.
- ☞ Nuevos dispositivos de control para el medio ambiente.
- ☞ Aumento en la complejidad de las aplicaciones.
- ☞ etc.

Todas las copias del plan deben actualizarse periódicamente y destruir las anteriores versiones, incluidas las ubicadas en sitios externos.

5.4.4. OBJECIONES AL PCDI

Existen diversas razones - y a diferentes niveles -, que impiden el desarrollo de un Plan de Contingencias contra Desastres Informáticos:

ALTOS MANDOS

- No entienden el problema o su concepto les es confuso.
- A pesar de la importancia de la información, ésta no se considera como un activo.
- La elaboración de un plan interfiere con las labores normales.

GERENCIA MEDIA

- No se quiere contraer un compromiso.
- No se desean mas controles.
- El desarrollo del plan no produce ingresos, sino al contrario, requiere inversión de recursos.

USUARIOS

- No existe conciencia sobre la situación.
- Existe resistencia al cambio.
- El plan puede interferir con el trabajo cotidiano.
- No saben cuales serían sus responsabilidades.

RECURSOS

- Se requiere de una persona de tiempo completo.
- Es costoso para algo que puede no utilizarse.
- Es difícil mantenerlo actualizado.

CULTURA

- Creer que nunca va a ocurrirnos a nosotros.
- No saber cual es la mejor solución.
- En ocasiones se piensa que todo esta prevenido aunque no se cuente con procedimientos de emergencia.

EL COORDINADOR DEL PLAN

- En ocasiones se frustra debido a que no tiene experiencia en trabajos políticos o no sabe como moverse en la organización, además de que en ocasiones puede ser que no tenga autoridad.

5.5. JUSTIFICACION DE UN PCDI

Se necesita interacción entre el coordinador del proyecto y la comunidad de usuarios porque los requerimientos de recuperación de los usuarios debe ser justificada para que se apruebe su financiamiento dentro de la estrategia de recuperación. El BIA (Business Impact Analysis - Análisis de Impactos en Negocios) tiene rangos de aplicaciones de sistemas de recuperación por pérdida de evaluación financiera e impactos operacionales, por lo que se debe contar con servicios de NO INTERRUPCIÓN (No Breaks). El rango de la red se justifica al recobrar cuadros de tiempo, ajustando para cada aplicación.

Los efectos que buscan reducirse mediante la implantación de un Plan de Contingencia son los siguientes:

Pérdida financiera.
Se reduce al tomar medidas para el control físico de la información y del equipo informático.

Vulnerabilidad.
Se deben adoptar medidas que reduzcan la posibilidad de perder información estratégica por errores operacionales, así como tomar las medidas necesarias para afrontar una interrupción en las operaciones.

Pérdida de Flexibilidad.
Se busca que las aplicaciones puedan ser adaptadas fácilmente a los cambios provocados por la dinámica de la empresa, para ello se requiere usar métodos adecuados de desarrollo de aplicaciones y controles de las mismas.

Responsabilidad Legal.
Tomando las medidas de seguridad adecuadas, se disminuye la posibilidad de un manejo inadecuado de la información de la empresa, sobre todo de aquella en la que existe responsabilidad por parte de funcionarios de la misma.

Invasión de Privacidad.
Se debe proteger la información confidencial y personal controlando el acceso a la misma.

Interrupción Temporal de las Operaciones.
Se debe contar con procedimientos adecuados para afrontar interrupciones temporales en aplicaciones o en el equipo de cómputo.

5.5.1. CUADRO DE TIEMPO

El cuadro de tiempo de recuperación representa la línea de tiempo crítica desde el punto de vista de una interrupción contra el punto del sistema de aplicación y tiene que estar actualizado siempre. Se establecen los cuadros de tiempo de recuperación en base de cada proyecto. El equipo a cargo de desarrollar el PCDI debe entrevistar a los usuarios activos para obtener una estimación acerca del periodo de tiempo máximo posible de recuperación. Típicamente, el cuadro de tiempo es un punto independiente de cualquier pérdida financiera e impacto operacional que llega a ser inaceptable para la empresa, como un bien o un usuario individual.

Mientras se lleva a cabo el BIA, el coordinador necesita estar consciente de los costos que conlleva el mantenimiento del Plan de respaldo; necesita comprender una de las tendencias básicas en la planeación: lo corto del cuadro de tiempo especificado en la recuperación de la aplicación más crítica.

El más alto costo es el de mantener un plan: recíprocamente, un tiempo prolongado de recuperación disminuye el costo. Mientras ésta tendencia no es absoluta, esto tiende a ser un principio confiable, por lo que los entrevistadores del BIA deberían buscar el más largo período de tiempo para una posible recuperación con cada usuario con conocimiento de los costos de mantenimiento para que puedan ser reducidos. Una alternativa para lograr prolongar el tiempo de recuperación es el de explorar los procedimientos alternos para el usuario.

5.5.2. IMPACTO ECONOMICO DE UN DESASTRE Y ASPECTOS LEGALES

El no contar con un PCDI que permita la continuidad en las operaciones de la empresa, puede traer problemas legales, ya que es posible caer en faltas administrativas y de carácter contractual por incumplimiento. Por ello, es importante que el plan pueda aplicarse en el momento requerido y con margen de seguridad en su funcionamiento aceptable, de tal manera que minimice la problemática y evite grandes repercusiones en las demás actividades de la empresa.

En el caso de empresas públicas, los servidores de éstas están obligados por ley a salvaguardar los bienes que tienen a su cargo propiedad de la nación; en caso de incurrir en actividades u omisiones en el desempeño de sus funciones que afecten a éstas, se hacen acreedores a sanciones de acuerdo con el código penal para el distrito federal (capítulo II, artículo 214, párrafo V).

CONCLUSIONES

CONCLUSIONES

Si bien los equipos más complejos y el procesamiento de grandes volúmenes de información se lleva a cabo en empresas o instituciones, el valor de la información y de los bienes informáticos es importante para todos los usuarios, independientemente si se trata de un programador, un estudiante, un empleado, un investigador o un profesionista independiente; de ahí la importancia de adquirir una cultura en seguridad informática a todos los niveles, ya que desafortunadamente en México no existe una conciencia real de la importancia de tomar medidas para proteger tanto la información como los equipos donde se lleva a cabo el procesamiento. Es común creer que tener respaldada la información es suficiente protección, sin embargo, si no se tiene donde procesarla en caso de que los equipos fallen o se dañen, ésta no podrá ser empleada.

La seguridad informática es un factor fundamental de cualquier empresa moderna,que utilice equipo de cómputo para procesar su información. Por ello, es importante que se determinen políticas y se implementen mecanismos de seguridad por medio de los cuales se garantice la integridad de los recursos informáticos, lo cual permitirá a su vez la continuidad en las operaciones de la empresa y lograr los objetivos de la misma.

Las medidas de seguridad varían dependiendo de las necesidades particulares de cada usuario y/o empresa, por lo que éstas deben adecuarse e implantarse de forma lógica de acuerdo a las condiciones específicas. Así, las medidas de seguridad en computadoras personales varía si ésta se encuentra conectada a una red o no; en el caso de redes, las medidas dependerán de las características de ésta (si es local, que tipo de sistema operativo emplea, etc.); para los centro de cómputo, deben emplearse procedimientos más sofisticados, tales como la elaboración de un plan de contingencias elaborado en base a las características y necesidades del mismo.

La importancia de una administración de una red con niveles de seguridad adecuados o el implementar un PCDI es que con ello se asegura la permanencia de la empresa, pero es necesario que ésta siempre cuente con el apoyo de los altos mandos. Todo proceso requiere inversión de tiempo y dinero, pero vale la pena no arriesgar la información, sobre todo cuando de ésta depende en gran medida una organización.

GLOSARIO DE TERMINOS

GLOSARIO DE TERMINOS

ACCIDENTE
Un suceso repentino que puede o no ser consecuencia de una emergencia y que provoca lesiones al personal y/o daños a las instalaciones; además interfiere o afecta el proceso de una actividad productiva.

AMENAZA
Estar expuesto a un peligro.

DISPOSITIVOS DE ENTRADA/SALIDA
Los componentes que introducen datos o instrucciones a la CPU son dispositivos de ***entrada*** (teclado, discos, etc.); mientras que aquellos que reciben los resultados son los de ***salida*** (impresoras, discos, graficadores, etc.).

EMERGENCIA
Toda aquella situación que puede ocasionar daños al personal o afectar físicamente las instalaciones. Ejemplos: incendios, sismos, explosiones, actos terroristas, etc.

GATEWAY
Host que tiene múltiples tarjetas adaptadoras de red. Este puede ser una computadora dedicada a proporcionar la función de ruteo de datos entre redes.

HARDWARE
Es el equipo FÍSICO en el que se lleva a cabo el procesamiento de datos de los sistemas informáticos. La configuración de un equipo de cómputo esta formada por la Unidad Central de Proceso (CPU por sus siglas en ingles) y los dispositivos de entrada y salida.

HOST
Computadora unida a una red que tiene una dirección TCP/IP. Cada Host tiene un nombre único (para los usuarios) y dirección (para el software) para poder ser identificado en redes interconectadas.

INFORMACION
Datos lógicamente asociados, los cuales se requieren para el manejo u operación de los procesos de negocio.

INTERRED
Red informática formada por un conjunto de redes menores.

MACROCOMPUTADORA
Sistema de cómputo de tamaño grande, también conocidos como MAINFRAMES. Se caracterizan por tener gran velocidad de procesamiento y capacidad de almacenamiento. Las macrocomputadoras se emplean cuando se requiere manejar grandes volúmenes de información o cuando se necesita gran velocidad de procesamiento.

MICROCOMPUTADORA
Sistema de cómputo de tamaño pequeño, comúnmente conocido como Computadora Personal o PC (Personal Computer), cuyo componente principal es el ***microprocesador***, que es el que realiza los cálculos. La tecnología de las PC's a avanzado rápidamente en los últimos años, a tal grado, que actualmente tienen mayor capacidad de procesamiento que los sistemas grandes de hace poco tiempo.
Hoy en día, la tendencia en las empresas es a utilizar microcomputadoras y/o redes de éstas combinadas con equipos más grandes.

MINICOMPUTADORA.
Sistema de cómputo de tamaño mediano más rápido y con mayor capacidad de almacenamiento que una microcomputadora. Las minicomputadoras se utilizan principalmente para control de procesos industriales. Su empleo va en decremento por que la capacidad de las PC's es cada vez mayor aunado a la baja de costos de equipos mayores.

PROCEDIMIENTO O SUBRUTINA
Es un conjunto de instrucciones que indica a la computadora los procedimientos u operaciones que debe llevar a cabo.

PROGRAMA INFORMATICO
Es un conjunto de instrucciones u ordenes para manipular los datos con el objeto de obtener resultados específicos.

PROTOCOLO
Conjunto de reglas que describen los mecanismos y estructuras de datos involucradas.

RIESGO
Peligro, que puede o no suceder un daño.

SECTOR DE BOOT
Area del disco del sistema en donde se almacenan los programas de las órdenes de arranque.

SEGURIDAD
Conjunto de leyes, normas y procedimientos y de los entes que los aplican, que tiene por objeto proteger contra determinados riesgos (accidentes, enfermedades, desastres, etc.)

SISMO
Un sismo o terremoto se produce por el sacudimiento repentino de la corteza terrestre en una gran extensión, lo cual produce movimientos en el terreno, leves o bruscos, y en una o varias direcciones. Este fenómeno se presenta por los desprendimientos o fracturas de grandes masas de rocas, por acción volcánica o por desplome o hundimiento de cavidades subterráneas. Existen dos escalas de medición de la intensidad de los sismos: la Mercalli y Richter.

SUBSISTEMA
Es un sistema, que a su vez, forma parte de un sistema mayor, pero que se encuentra dedicado a una sola aplicación.

UNIDAD CENTRAL DE PROCESO (CPU)
Se divide en tres partes: la Unidad de Control (su función es examinar y ejecutar los programas); la Unidad Aritmético-Lógica (encargada de efectuar las operaciones de cálculo como sumas, restas, etc., y las comparaciones); y la memoria principal (en ella se almacenan los datos procesados en la unidad aritmético-lógica).

BIBLIOGRAFIA

BIBLIOGRAFIA

1. Revista Byte, México, año 9 No. 90
pág. 22, Julio de 1995

2. Conferencia "Disaster Recovery"
Word Trade Center, Cd. de México
Julio 1995

3. Desarrollo de un Plan de Contingencia.
Javier F Kuong
Contingency Planning & Recovery Institute and Management Advisory Services & Publications
1992

4. Reglamento para el Control de Emergencias y Accidentes en el Centro Administrativo de Petróleos Mexicanos
RE.03.0.01
Gerencia de Seguridad e Higiene Industrial Institucional. Pemex
Agosto, 1990

5. Plan de Contingencias
Gerencia de Informática y Sistemas, Pemex Exploración-Producción
Marzo de 1994

6. Revista "Informática"
No. 146

7. Revista "RED"
Año V, Nov/95, No.62

8. Gaceta IMP
Págs. 14 y 15
Año Vi, No. 5

9. Virus Informáticos
José Ramón Gallardo
Facultad de Ingeniería, UNAM

10. Boletín informático.
No. 189
Mat. Héctor Elías Alvarado
Págs. 9-11
Petróleos Mexicanos

11. Boletín informático.
Sep-Oct/91
Lic. Sergio A. Pulido
Pág. 7
Petróleos Mexicanos

12. Revista Informática
No. 147
El virus: la plaga de la computadora
Págs. 24-32

13. Manuales y documentación de antivirus informáticos
Agosto de 1993
Pemex, SPMP-GDT

14. Planeación de la Recuperación
IBM de México
Servicios de Recuperación

15. Plan de Recuperación de operaciones
Elsa Piñones / Carlos Ludewig
Seguridad de Información y Planes de Recuperación
IBM de Venezuela, S. A.

16. Disaster Backup/Planning Presentation
Wayne P. Lambert
Sperry-Eagan, Mn.

17. Contingency and Disaster Planning and Disaster Recovery
Laurence W. Olson
Unisys, Chicago, Il.

18. AIX/6000 Administración del Sistema
Manual del estudiante
IBM

19. Novell Netware
Manual de referencia

20. Ingeniería de Software, un enfoque práctico
Roger S. Pressman
2a. edición
Editorial McGrawHill

21. Seguridad de la información en sistemas de cómputo
Luis Angel Rodríguez
Ventura Ediciones S.A. de C.V.