7
29

Universidad Nacional Autónoma de México

FACULTAD DE CONTADURIA Y ADMINISTRACION

SEGURIDAD INFORMATICA

SEMINARIO DE INVESTIGACION INFORMATICA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

P R E S E N T A N :

LOURDES YOLANDA FLORES SALGADO

OLIVIA GUZMAN GONZALEZ

ASESOR DEL SEMINARIO:

LIC. MA. CONCEPCION CAMARGO FAJARDO

MEXICO, D.F. 1996

TESIS CON
FALLA DE ORIGEN

AGRADECIMIENTOS

A Dios:

Por ser mi luz, mi camino y mi guía. Lo más importante de mi existencia.

A mis padres:

Por todo el ejemplo, amor y apoyo que me han brindado. Por tantos sacrificios para lograr hacer de mi la persona que soy. Los Amo.

A mis hermanos:

Guille: Por ser una excelente hermana mayor. Por tu buen ejemplo y por esa linda familia que has formado y que constituye un aliciente en mi vida.

Luis: Se que es difícil convivir con alguien tan opuesto a uno. Pero a pesar de todas las diferencias yo también te quiero.

A Armando:

Por lo que significas en mi vida. Por compartir tus sueños, alegrías y tristezas. Por tus consejos y regaños. Por tu gran amistad y tu cariño incondicional. Pero sobre todo por dejarme ser también yo parte de tu vida. T-137i-1.

A Oli:

Por todo lo que hemos compartido. Por tu amistad. Por este gran esfuerzo que significa tanto para ambas.

A la UNAM

Por todo lo que me ha brindado. Tanto profesional como personalmente.

Al Departamento de Supercómputo de la DGSCA, así como al Laboratorio de Visualización y Area de Seguridad por todos los recursos y facilidades que me dieron para realizar esta tesis.

Yolanda

AGRADECIMIENTOS

A mis Papás:

Con especial y profundo agradecimiento por sus esfuerzos y sacrificios que espero recompensarles infinitamente.

A mis Hermanos:

Que me han apoyado de manera incondicional hoy y siempre. Y a tí Karina que aún con lo ocurrido siempre estarás en mi corazón.

A Javier:

Con todo mi cariño, gracias por compartir momentos tan especiales y apoyarme siempre.

A Yolanda:

Agradecerte Yola por mostrarte siempre conmigo como una verdadera amiga. Por todos estos años que llevamos juntas.

A la UNAM:

Y muy en particular a la Facultad, así como a los profesores que participaron en mi formación como profesional.

Olivia

CONTENIDO

INTRODUCCION

CAPITULO I

LA INFORMACION

CAPITULO II

RIESGOS Y AMENAZAS RELACIONADOS CON LA PROTECCION DE LA INFORMACION

CAPITULO III

SEGURIDAD DE LA INFORMACION

CAPITULO IV

SEGURIDAD EN REDES Y TELECOMUNICACIONES

CAPITULO V

PLAN DE CONTINGENCIA

CONCLUSIONES

INTRODUCCION

Durante la última década, las computadoras han producido en nuestra sociedad un impacto de enormes consecuencias. Lo cierto es que estas herramientas han revolucionado y multiplicado la productividad y eficacia del trabajo, tanto para las empresas como para los usuarios individuales.

Día a día, infinidad de usuarios acuden a las computadoras para atender sus necesidades privadas o comerciales, y esta tendencia se acentúa a medida que las empresas y los usuarios van descubriendo estos medios.

La información que se almacena dentro de las computadoras es un recurso esencial que en algunos casos se constituye como estratégico y debe mantenerse de forma confidencial, libre de cualquier corrupción, a salvo de robos, sabotaje y disponible en el momento que sea necesaria, ya que la pérdida o divulgación de ésta puede poner en riesgo los negocios, el bienestar de la sociedad e incluso la vida.

Es por eso que uno de los problemas más grandes a los que se enfrenta la sociedad actual en la utilización de computadoras, es la seguridad de la información.

El entorno de la informática ha tratado el punto y se ha dado origen al surgimiento de una terminología especializada.

Existen gran cantidad de conceptos involucrados que hacen que aquellas personas que no están familiarizadas con el tema se pierdan dentro de él. Lo anterior se debe a que el problema es multifacetico e

involuera aspectos de carácter físico y de programación, característicos de software y hardware, así como aspectos humanos y operacionales, además se hace más complicado por el hecho de que la seguridad de la información esta relacionada con la pérdida de privacidad a que se enfrenta la sociedad al existir elementos tecnológicos que hacen posible tener acceso a ella aún cuando esto no sea permitido.

Como resultado de esta problemática surge la inquietud de desarrollar ésta tesis de Seguridad Informática con el objetivo de proporcionar un panorama *básico* y *general* de los aspectos que se consideran como introductorios al estudio de la seguridad en computo, sin enfocarlo a un ambiente específico de trabajo, de manera que proporcione la acumulación ordenada de conocimientos que sirvan como cimientos para un estudio más detallado de los temas que aquí se tratan.

CAPITULO I

LA INFORMACION

1.1 DEFINICION DE LA INFORMACION

La información se define como "Todo aquello que permite adquirir cualquier tipo de conocimiento; por tanto, existirá información cuando se da a conocer algo que se desconoce".[1]

Los datos pueden considerarse como "simbolos que describen un objeto, condición o situación. Son el conjunto básico de hechos referentes a una persona, cosa o transacción".[2] Incluyen cosas como tamaño, cantidad, descripción, volumen, tasa, nombre o lugar. Cuando los datos son tratados o procesados (ordenados, clasificados, sumados, etc.), constituyen información.

La diferencia básica entre datos e información consiste en que los datos no son útiles o significativos como tales, sino hasta que son correlacionados con otros datos, procesados y convertidos en una forma útil llamada información.

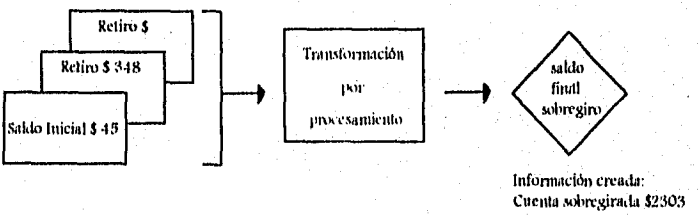

Figura 1.1

La distinción entre información y datos es importante por que existe una diferencia entre los dos conceptos desde el punto de vista de la informática por dos razones: Primero permite establecer por separado las necesidades de información de los gerentes y las exigencias de diseño de la base de datos; Segundo permite suministrar a los gerentes información, no datos.

La relevancia es un factor clave para distinguir entre datos e información. No todos los datos o hechos pueden ser relevantes en un momento dado. De hecho, algunos datos nunca pueden ser relevantes en relación con un suceso, la información afecta las actividades para la toma de decisiones.

La información es, entonces, conocimientos relevantes basados en los datos a los cuales, mediante un procesamiento, se les ha dado significado, propósito, utilidad y respaldan el proceso de toma de decisiones en una organización.

El valor de la información en un mensaje se relaciona con el valor que agrega a la información total o al cuerpo de conocimiento. Es decir, el punto central está en el valor incremental de la información en un mensaje; la ganancia económica adicional que se puede lograr por valerse de dicha información.

El valor no depende de que tanta información contenga el mensaje, sino de su relación con la cantidad de conocimiento previamente recopilada y almacenada.

Una manera de medir el valor de la información consiste en evaluar la utilidad obtenida al tomar una decisión cuando se presentan condiciones de incertidumbre y restarla a la utilidad que

se conseguiría si se conociera el futuro. Es por ello que volviendo a su definición, se dice que la información existe cuando se da a conocer algo que se desconoce.

Sin embargo para que la información sea tratada es necesario transmitirla y para que exista dicha transmisión es necesario el proceso de comunicación.

"La comunicación es la transmisión de información con significado desde un lugar (el emisor, la fuente o el origen) hasta un segundo lugar (el receptor o destinatario)".[3]

El proceso de comunicación consta de los siguientes factores (ver fig.1.2):

1) *Emisor*: Es la fuente que da inicio al proceso de comunicación. Contiene un conjunto de signos o mensajes.

2) *Codificador*: Convierte el mensaje en señales apropiadas para ser transmitidas por el medio.

3) *Medio o Canal*: Vehículo a través del cual se envía o difunde el mensaje.

4) *Decodificador*: Actúa sobre las señales para extraer el mensaje y convertirlo a una forma que pueda ser utilizada por el receptor.

5) *Receptor*: Es el que recibe el mensaje.

6) *Ruido*: Son todos los hechos o señales externas que interfieren con el proceso de comunicación.

7) *Mensaje*: Signo o secuencia de signos que provienen de un repertorio de signos comunes al emisor y al receptor.[3]

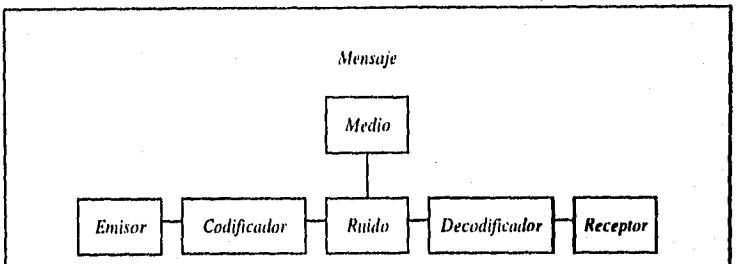

Figura 1.2 Modelo de Comunicación

Cuando un mensaje sale de la fuente de información, se desplaza hacia un transmisor o emisor que lo transforma en una señal que puede ser enviada a través del canal hasta el receptor. Este proceso se conoce como *codificación*, el mensaje es formulado de nuevo en una forma que pueda transmitirse al receptor designado para ese sistema.

En la comunicación humana, por ejemplo, el órgano de la voz es el codificador; convierte los mensajes recibidos del cerebro (la fuente de información) en palabras. El canal lleva el mensaje codificado al receptor. Entonces ocurre la decodificación, el receptor convierte nuevamente la señal en un mensaje para ser utilizado en el destino.

En las computadoras, los datos se traducen en señales electrónicas procesables por las máquinas en la entrada, y de señales electrónicas a símbolos y caracteres que pueden ser entendidos por el usuario, en la salida.

En el proceso de comunicación pueden esperarse algunas complicaciones como es el *ruido* en el canal. El ruido o perturbación son distorsiones, como de sonido o forma, errores en la transmisión. Ahora, cuando mayor sea la cantidad de ruido en la transmisión, tanto mayor será la probabilidad de que el receptor no reciba el mensaje en la forma en que se transmitió.

El ruido desempeña un papel trascendental en los sistemas de información utilizados por la gerencia. En estos sistemas, es importante proporcionar suficiente información para que el usuario detecte y trabaje el problema con facilidad, y un elemento clave en esta tarea es la redundancia.

La redundancia es "... la repetición de parte o todo un mensaje para evitar el ruido (distorsión ó errores de transmisión). " [4]

La mayor parte de la comunicación es redundante para asegurarse de enviar una información completa.

Uno de los ejemplos más sencillos y frecuentes de redundancia lo encontramos en la correspondencia, en los contratos o en los documentos crediticios que presentan un número o cantidad y luego traen el número escrito con letras dentro de paréntesis como:

$3,000.00 (TRES MIL PESOS 00/100 M.N.)

1.2 ATRIBUTOS DE LA INFORMACION

La información para que sea útil debe tener atributos esenciales, tanto en elementos individuales como en su conjunto (ver tabla 1.1). Los Atributos de la Información son características que tienen significado para el usuario de cada elemento de la información. Es decir, cada elemento individual informativo puede ser descrito con respecto a exactitud, forma, frecuencia, extensión o alcance y temporalidad o posición en el tiempo.

Tabla 1.1 Atributos de un elemento de la información

Exactitud	La información es cierta o falsa, exacta o inexacta. La pregunta crucial es: La información representa la situación o el estado como realmente es. La información inexacta pueda ser tratada por el usuario como si fuera exacta.
Forma	Las distintas clases de la forma son: cualitativa y cuantitativa, numérica y gráfica, impresa y visualizada, resumida y detallada. Por lo común, la selección de una u otra de las formas alternas depende del caso o situación.
Frecuencia	La frecuencia es la medida de que tan a menudo se requiere, se recaba o se produce.
Extensión	El alcance de la información define su campo de acción. Alguna información puede cubrir una amplia área de interés. Otra puede tener una esfera de acción muy reducida. El uso determina el alcance necesario.
Origen	La información se puede originar desde fuentes en la organización o fuera de ella.
Temporalidad	La información puede estar orientada hacia el pasado, hacia los sucesos actuales, o hacia las actividades y sucesos futuros.
Relevancia	La información es relevante si es necesaria para una situación particular. La información que se tiene " por si acaso" no es relevante.
Completitud	Una información completa proporciona al usuario todo lo que necesita saber acerca de una situación particular

Exactitud

La información puede ser cierta o falsa, exacta o inexacta (aunque puede haber matices entre estos dos extremos). " Exacto" y "Verdadero" describen si la información representa una situación, nivel o estado de un hecho o suceso exactamente como es.

La información inexacta es el resultado de equivocaciones, que pudieron haber ocurrido durante la compilación, procesamiento o preparación de un informe. A veces un usuario puede tomar una información inexacta como correcta. Esto no hace que la información sea verdadera, pero mientras que tal persona la considere como correcta y la utilice para cierto fin, constituye *información para esa persona.*

Forma

La forma es la estructura real de la información, incluyendo el medio de presentación. El criterio de diferenciación más comúnmente utilizado es el que existe entre formas cuantitativas y formas cualitativas.

La información cuantitativa dice que tanto de un elemento o de un hecho en particular ha sido medido. Desde luego, la información cuantitativa se usa mucho en los negocios y en la administración. Este tipo de información también puede ser categorizada como numérica o gráfica. La información numérica está constituida obviamente por números y la gráfica por diagramas o ilustraciones.

La información cualitativa sirve para describir una situación o un hecho en términos de ciertas características no medibles.

Frecuencia

La frecuencia de la información es la medida de cuán a menudo se le requiere, reúne o produce. Se puede originar periódica o esporádicamente, dependiendo de las necesidades del usuario. Es importante ya que repercute en su valor. La información que aparece con excesiva frecuencia tiende a producir interferencia, ruido o distracción, además de sobrecargar al receptor.

Alcance

Este concepto es la amplitud de acción de los acontecimientos, lugares, personas y cosas que representa la información. Por ejemplo, un amplio alcance de una información sobre ventas puede referirse a todas las zonas de ventas de una compañía que tiene negocios en La Republica Mexicana. Un alcance reducido puede comprender únicamente una región de una compañía o una parte de su territorio.

Origen

El origen de la información es la fuente de la que ésta se recibe, recopila o produce. La información interna se origina dentro de una organización, y la externa, desde fuera de ella por ejemplo del gobierno o de las organizaciones de negocios.

Temporalidad

La información puede estar orientada hacia el pasado (información histórica), hacia situaciones presentes o hacia sucesos y actividades futuros. La información histórica proporciona una perspectiva de lo que ocurrió en épocas anteriores.

Con frecuencia las compañías examinan la información histórica para analizar si las utilidades, gastos, ventas, número de empleados y otros elementos del presente han aumentado, disminuido o permanecido en los mismos niveles comparándolos con el pasado.

La información sobre el futuro ayuda a las organizaciones a planear las demandas y los requisitos de operación en años venideros.

Relevancia

La información es relevante si una persona la necesita en una situación particular de toma de decisiones o de resolución de un problema. Es una parte necesaria de los recursos utilizados en la selección de un curso de acción. Lo importante es su aplicabilidad a la situación presente.

Completitud

La completitud se refiere a que, si un conjunto determinado de información indica al usuario todo lo que necesita saber en relación con una situación en particular, entonces se dice que es completo.

Por otra parte, si un informe deja a una persona con muchas preguntas sin responder, es un conjunto incompleto de información.

Validez

Grado en que la información representa lo que pretende representar.

Finalidad

La información debe tener un objetivo específico al momento de transmitirla, para no ser considerada como un conjunto de hechos aislados. Tales objetivos pueden ir desde simplemente informar, hasta evaluar, convencer, planear, organizar, crear nuevos conceptos, detectar y resolver problemas, tomar decisiones, etc.

Actualidad

Consiste en la oportunidad de la información al momento de ser utilizada.

Claridad

Grado en que la información esta libre de ambigüedad.

Densidad

Es la cantidad de información presente en un informe o mensaje. Un informe puede contener muchas hojas pero con poca cantidad de información, mientras que un esquema o cuadro sinóptico en forma condensada puede representar gran cantidad de información.

Redundancia

La redundancia como ya se había mencionado, significa repetición o exceso de información transmitida. En algunos casos se utiliza para asegurar el envío de un mensaje completo, evitando ruido o distorción de la información.

1.3 TIPOS DE INFORMACION

Los directores de organizaciones necesitan dos tipos de información: información contable e información administrativa. Desde luego, no se debe concluir que una sea más importante que la otra; ambas son esenciales.

a) Información Contable

La información de tipo contable se origina en las áreas de contabilidad financiera y administrativa. En las áreas de contabilidad financiera se centra específicamente en la identificación y los reportes de ingresos y estados financieros. Los estados de resultados y de posición financiera o balance general, se elaboran para cumplir con este objetivo.

Por otra parte la contabilidad administrativa se enfoca a los costos en la operación de la empresa, por ejemplo en los asuntos de costos de personal, gastos de operación y distribución de los gastos generales.

Luego entonces, la información administrativa la consideramos como un subproducto del proceso de contabilidad, esto se debe a que los primeros sistemas de procesamiento de transacciones generalmente se establecieron para realizar labores de contabilidad, por consiguiente es de suma importancia en toda empresa.

b) Información Administrativa

La información administrativa se divide en siete tipos necesarios para la administración de más alto nivel. Observe la figura 1.3

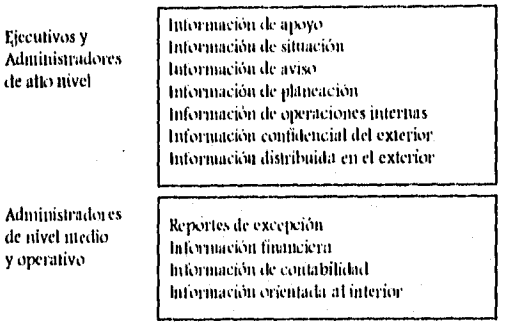

Figura 1.3

a) Información de apoyo

Este tipo de información mantiene informados a los administradores en relación con situaciones actuales o niveles de logros; así, permite saber qué rendimiento se ha alcanzado y si va de acuerdo con las expectativas generales en una área de interés. Por ejemplo información del volumen de ventas del día anterior.

b) Información de situación

A la información de situación también se le llama información de avance; y mantiene a los administradores al tanto de los problemas presentes y de las crisis, así como de los avances reportados con el fin de aprovechar las oportunidades que pueden perderse si no se actúa de inmediato. Por ejemplo el progreso en la investigación y desarrollo destinados a lanzar un nuevo producto para satisfacer un mercado naciente.

c) Información de advertencia

Esta información señala que están ocurriendo cambios, ya sea en forma de oportunidades que se presentan, o bien presagios de problemas futuros que afectarían el éxito de la empresa, de sus productos o de servicios, y su viabilidad a largo plazo.

d) Información de planeación

Se refiere a la descripción de los principales desarrollos y programas que deben iniciarse en un futuro; incluyendo las hipótesis en las cuales se basan los planes o los desarrollos anticipados esenciales para la realización de los planes establecidos.

e) Información de operaciones internas

Se refiere a los indicadores clave de cómo la organización o las personas se están desempeñando; también es útil para presentar

informes sobre la salud general de una organización, empresa subsidiaria, división o producto. Las áreas en las que los rendimientos reales no concuerdan con las expectativas se reportan como excepciones.

f) Información confidencial del exterior

Informes, rumores y opiniones respecto a las actividades en el entorno de la organización; incluye una gama amplia de áreas como cambios en la industria y en las estrategias de los competidores, movimientos en el mercado financiero, y transformaciones o fluctuaciones político-económicas.

g) Información difundida en el exterior

Es información que un ejecutivo principal desea revisar antes que sea transmitida a los accionistas o a los medios de comunicación.

1.4 FUENTES DE INFORMACION

Es particularmente importante hacer notar que la información proviene de muchas fuentes, sin embargo hemos optado por clasificarla en dos fuentes importantes que son Información primaria e Información secundaria. ver tabla 1.2

Fuentes de Información primaria

Cuando la información necesaria no existe en ningún lugar conocido o accesible, debe buscarse directamente. La información primaria puede obtenerse por observación, experimentación, encuesta, o por valoración subjetiva.

El costo de esta información es elevado debido a la cantidad de recursos, incluido el tiempo, que se utilizan para obtenerla. Generalmente esta información es muy valiosa y debe mantenerse en forma confidencial ya que si otra compañía logra obtenerla, obtendrá beneficios extras ya que no tendría que invertir los mismos recursos por ella.

Fuente Primaria	Ventajas	Desventajas
Observación	Conocimiento de primera mano. Evita respuestas distorsionadas	La observación puede no ser exacta. La observación puede afectar lo que se observa
Experimento	Control sobre las variables de interés	Diseño del experimento puede no ser representativo
Encuesta	Modo eficiente de llegar a grandes grupos de personas	Diseño del cuestionario. Tamaño de la encuesta
Estimación subjetiva	Información de los expertos. Puede ser la única manera de obtener alguna información	La respuesta puede no ser confiable

Fuente Secundaria	Ventajas	Desventajas
Información de la propia compañía	Es específica para la situación. Ya existe. Relativamente poco costosa	Puede no ser oportuna. Puede no estar integrada. Adecuadamente o en forma útil
Información conseguida de fuentes externas.	No puede obtenerse de otro modo	Es costosa de adquirir
Publicaciones	De bajo costo	Puede tener deformación
Organización del gobierno	Imparcial. Un gran volumen de datos	Puede no estar en forma utilizable

Tabla 1.2

Observación

A través de la observación de acontecimientos relacionados se puede obtener respuestas parciales a un problema en particular, y entonces los datos obtenidos así pueden procesarse para producir información acerca de un problema. La principal ventaja de utilizar la observación para extraer información es que proporciona conocimientos de primera mano respecto a los problemas, procesos, o actividades de interés. Este método evita distorsiones en las respuestas que se pueden encontrar cuando se utilizan otros métodos para recabar información primaria.

Experimentación

En ocasiones es adecuado incluir fuentes de información en experimentos controlados como personas, máquinas, y equipo, etc. Con este método, el experimentador puede ejercer gran control sobre la fuente, definiendo un entorno y manipulando las variables pertinentes para determinar el impacto sobre un problema en particular. El diseño del experimento es en extremo importante para determinar la confiabilidad de la información adquirida.

Encuestas

Las encuestas es uno de los métodos más comunes para conseguir información primaria, ya que este método permite llegar a gran número de fuentes de información. El contenido de las encuestas son preguntas adecuadas y seleccionadas cuidadosamente para obtener resultados significativos.

Valoración subjetiva

La valoración subjetiva es un método para obtener información de expertos, siendo los expertos jefes de división o de departamento dentro de una compañía, o consultores externos y funcionarios de asociaciones profesionales.

La valoración subjetiva, puede combinarse con la información objetiva de la que ya se dispone con introspección o intuición basada en la experiencia personal en un campo determinado.

Fuentes de información secundaria

Los usuarios de la información intentan utilizar fuentes secundarias siempre que sea factible para evitar los problemas de tiempo y de gastos que a menudo se encuentran al adquirir información primaria.

La información secundaria esta constituida por información interna de la propia compañía, información conseguida de fuentes externas, publicaciones y agencias del gobierno.

Información en la propia compañía

Es la información potencialmente más valiosa, para los gerentes o para quienes han de resolver problemas, tal vez sea la de la propia compañía donde se labora. Los reportes emitidos en forma regular o irregular por varios departamentos a menudo suministran gran cantidad de conocimientos.

Información conseguida de fuentes externas

La información conseguida de fuentes externas es posible adquirirla de compañías especializadas en el ramo. En esta categoría se incluyen agencias de investigación y empresas que llevan a cabo encuestas de la opinión publica.

Publicaciones

Existe gran número de publicaciones comerciales, industriales, de gobierno y profesionales en el campo de los negocios están disponibles gracias a la subscripción, uso de bibliotecas, o pedidos especiales. Estas fuentes generalmente intentan ser objetivas, pero el usuario no puede suponer que lo hayan logrado en todos los casos.

Organismos del gobierno

Las agencias gubernamentales recopilan enormes volúmenes de información sobre una amplia variedad de temas. Existe información de cálculos demográficos, el producto nacional bruto proyectado, el ingreso total per capita, entre otros.

1.5 INFORMACION Y TOMA DE DECISIONES

Hasta este momento hemos hablado de temas acerca de la información, datos, atributos, fuentes de información. Sin embargo es importante hablar del porqué la información juega un papel importante en las organizaciones.

Toda organización en su funcionamiento se enfrenta a problemas que deben ser resueltos por los directivos, pero no hay que considerar la palabra problema como algo malo necesariamente, si bien puede tratarse de una situación adversa, también puede serlo una situación agradable pero inesperada o desconocida.

Así por ejemplo, un problema para una empresa podría ser que uno de sus productos rebase en ventas lo que se había planeado.

"La resolución de problemas es la actividad de responder satisfactoriamente ante un problema, que incluye cuatro pasos básicos:

a) Entender un problema
b) Evaluar alternativas de solución
c) Implantar la mejor solución
d) Seguir hasta estar seguros que la solución funciona".[5]

Podemos considerar a una situación de *toma de decisiones*, como aquella en la cual un individuo, en un contexto determinado, se enfrenta cuando menos con dos posibles opciones en donde existen cuando menos dos posibles resultados de cada una de ellas, y cada opción puede producir más de un resultado con cierta eficiencia.

El proceso de toma de decisiones incluye cuatro etapas o fases: objetivos, información, predicción y evaluación. (ver figura 1.4).

Figura 1.4

Los objetivos son los elementos que nos indican hacia dónde queremos ir o hacia dónde nos debe llevar la decisión de que se trata. Estos objetivos deben ser cuantificables, claros y reales, a fin de que puedan ser comparados directamente con los resultados obtenidos y poder así corregir en caso de desviaciones.

Al hablar de información, nos referimos a los elementos que nos permiten conocer la situación actual y estimar la futura, relacionada con la decisión que debemos tomar.

Las predicciones en la etapa del proceso de decisión se refiere al procedimiento que nos permite pronosticar o definir cuáles serían las

posibles opciones por seguir y los probables efectos sobre factores como costos y utilidades, organización y personal de la empresa.

Después de obtener las predicciones, con base en la información disponible, se analizan considerando los objetivos fijados; con esto evaluamos las opciones y, gracias a esta evaluación, podemos decidir en forma objetiva cuál de ellas es la más conveniente.

En las organizaciones los directivos tomarán muchas decisiones durante el proceso de solucionar un problema. Sin embargo para que una solución sea la correcta, requiere de una serie de decisiones adecuadas. Observe la figura 1.5. que es información que ayuda a los directivos a tomar decisiones para resolver problemas.

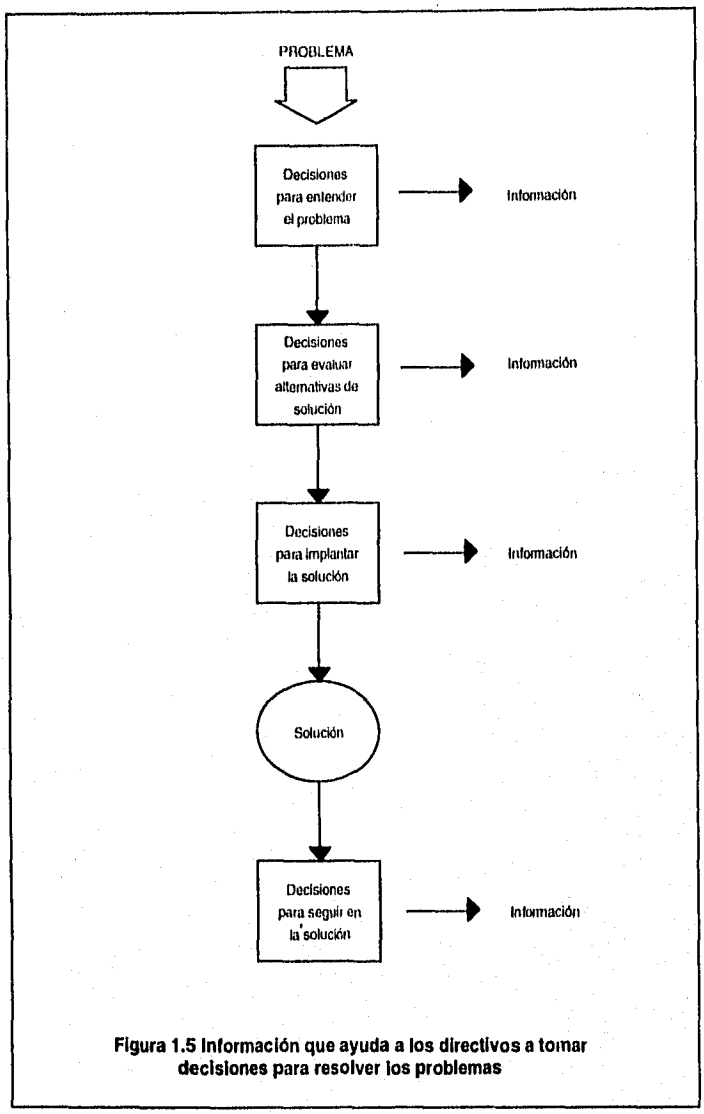

Figura 1.5 Información que ayuda a los directivos a tomar decisiones para resolver los problemas

1.6 IMPORTANCIA DE LA INFORMACION

El desarrollo histórico del hombre está fundamentado en el manejo de la información. El crecimiento de las sociedades, la utilización de nueva tecnología y el crecimiento y complejidad de los sistemas ha dado como resultado que la mayor parte de la información de que dispone actualmente el género humano haya sido producida en los últimos decenios.

Es tan grande la cantidad de datos que se genera al año que resulta extremadamente difícil entenderlos, analizarlos y más aún usarlos.

La información es requerida en todas las áreas; desde las compañías de ferrocarriles hasta las granjas, pasando por las fábricas y llegando hasta la bolsa de valores; provocando cambios significativos en la manera en que se vive, se organiza, se hacen las guerras y se formulan políticas.

Las sociedades modernas se han transformado en sociedades de información, en las cuales el número de empleados dedicados al procesamiento de información ha rebasado al número de empleados dedicados al sector industrial, debido principalmente a la enorme escala de actividades de los administradores, directivos o gerentes derivada del gran dinamismo de los mercados consecuencia de la expansión de los negocios y la demanda de mejores productos

Basta para tener una idea de esto dar una mirada al mundo que rodea al empresario de los tiempos actuales:

El ejecutivo moderno debe en un momento dado estudiar las interacciones de su organización con los gobiernos tanto nacionales como internacionales, los sindicatos, las asociaciones patronales, juntas de conciliación, grupos de consumidores, intereses regionales, bolsas de valores, la prensa del mundo de las finanzas, la competencia, accionistas, empleados, clientes, acreedores, etc., así como mantenerse enterado de los cambios tecnológicos, sociológicos y legales, para lo cual requiere gran cantidad de información y un enorme flujo de datos de manera que le sea posible tener los elementos necesarios para tomar decisiones cada vez más precisas y con mucha mayor rapidez.

La información es un recurso que se utiliza para informar, influenciar, evaluar, innovar y principalmente para tomar decisiones. Cuando la gente dispone de los hechos y la información necesarios, puede adoptar mejores decisiones, así como resoluciones más urgentes y en mayor cantidad. Tiene más confianza en su capacidad de decisión porque posee una base sobre la cual adoptarlas y es mayor la probabilidad de que sus determinaciones sean las adecuadas.

De aquí que la información sea tan importante, ya que desde este punto de vista la información pasa a ser no solo un recurso básico sino esencial, vital para una organización por lo cual debe ser resguardada y protegida porque su valor repercute en la productividad y eficiencia de todas las áreas que la integran (producción, ventas, finanzas, etc.).

1.7 AUTOMATIZACION DE LA INFORMACION

El ingrediente necesario para la toma de decisiones y para las actividades administrativas es la *información*..

Sencillamente, un negocio no puede sobrevivir sin ninguna información. Steiner ha expresado esa importancia: "... Los flujos de información son tan importantes para la vida y la salud de un negocio como lo es el flujo sanguíneo para la vida y la salud del ser humano"[6].

El cambio de la tecnología computacional, el crecimiento y el desarrollo de las empresas que antes contaban con sistemas pequeños , fueron tornándose más complejos demandando mayor cantidad de información, dando origen a que surgiera la necesidad de contar con sistemas más grandes que procesaran datos para obtener la información necesaria para tomar decisiones cada vez mas precisas y con mucha mayor rapidez

Al examinar las necesidades básicas de información de una compañía (grande o pequeña) y lo que constituye un sistema satisfactorio de información a la gerencia, podemos comprender mejor la forma en que las necesidades de información se hacen más complejas a medida que se hacen más grandes las operaciones de organización, así como la forma en que pueden desarrollarse o mejorarse esos sistemas de información, mediante la modificación de un sistema manual, o el diseño de un sistema basado en computadora.

La informática, que es la "ciencia enfocada al estudio de las necesidades de la información, de los mecanismos y sistemas

requeridos para producirla y aplicarla, de la existencia de insumos y de la integración coherente de los diversos elementos que se necesitan para comprender una situación"[7] , enfrenta este problema y estudia así el mejor modo de proporcionar dicha información.

Dr. Rivera Soler define Informática como "... es una ciencia, arte o técnica que con la ayuda de medios manuales, mecánicos, electromecánicos o electrónicos, permite mediante un proceso idóneo la captación de datos, que integrados en archivos conllevan al logro de informes, cuyo objetivo es la toma de decisiones".[8]

De esta forma, "la informática representa una importante ayuda para la empresa, la cual, se puede concretar en dos vertientes: una ayuda de gestión en cuanto a la toma de decisiones por presentación de distintas posibilidades y otra de ayuda a la gestión por manejo informático de la voluminosa información que acompaña a los procesos administrativos."[9] ver figura 1.6.

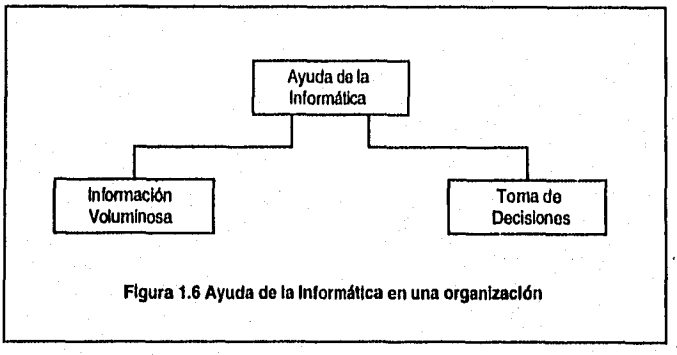

Figura 1.6 Ayuda de la Informática en una organización

Cuando la informática forma parte de una organización su función es de alguna manera como la de una compañía dentro de otra

compañía, opera tanto como un taller de bajo pedidos, como forma de producción continua y a menudo sirve a todos los segmentos de la organización

En este sentido puede decirse que el papel que cumple la informática dentro de una organización es la función de estar en primera y única instancia a su servicio.

LA SUPER CARRETERA DE LA INFORMACION

Durante la última década, las computadoras y las redes de comunicaciones han producido en nuestra sociedad un impacto de enormes consecuencias. Se dice que vivimos en la *"Era de las Telecomunicaciones"*. Lo cierto es que estas herramientas revolucionarias han multiplicado la productividad y eficiencia del trabajo, tanto para las empresas como para los usuarios individuales. Día a día, infinidad de usuarios acuden a las redes de telecomunicaciones para atender sus necesidades privadas o comerciales, y ésta tendencia se acentúa a medida que las empresas y los usuarios van teniendo acceso estos medios.

La principal finalidad de las telecomunicaciones es transferir e intercambiar datos entre computadoras y terminales. Es el intercambio de información lo que permite funcionar a los múltiples servicios de telecomunicaciones que consideramos ya parte de nuestras vidas.

La creación, uso, almacenamiento, representación y comunicación de la información juegan un papel muy importante

porque esta revolucionando la manera de pensar, trabajar e interactuar con las demás personas.

El término de Super Carretera de Información surgió por las necesidades locales de intercambio y transferencia de información en los Estados Unidos que dieron origen al surgimiento de la iniciativa para la creación de una Infraestructura Nacional de Información (NII). A la fecha no hay una definición exacta de lo que significa, incluso el Presidente del Subcomité de Telecomunicaciones y Finanzas de la Casa blanca en una conferencia de prensa dijo que "Las buenas noticias son que todos en Washington apoyan el concepto de Supercarretera de la Información, pero que las malas noticias son que nadie sabe lo que significa"[10]. Esto solo refleja que el término es una etiqueta que es utilizada por diferentes personas y aplicada a diversos ambientes.

La idea básica de la Supercarretera de la Información, involucra la la capacidad de un país en cuanto a su red de comunicaciones, tanto la instalada como la que puede ser instalada con la inversión apropiada. Esto es porque la infraestructura tencológica en comunicaciones que tenga un país puede determinar la capacidad competitiva de las empresas o compañías nacionales, repercutiendo ésta directamente en su economía nacional.

De acuerdo a esto, los países alrededor del mundo han tomado diferentes posiciones y han invertido en el desarrollo de la infraestructura de telecomunicaciones también de diferente manera.

La creación de esta infraestructura es la respuesta a las presiones competitivas del mercado mundial y a la deseabilidad de hacer un uso de la tecnología disponible en le actualidad. La necesidad de crear una infraestructura sólida, eficiente capaz de manejar grandes volúmenes

de información ha obligado a replantear a diferentes países en la conveniencia de crear para ellos su propia red nacional.

Así mismo el término de Supercarretera de la Información ha tenido tal repercución en otros países que ahora ya se habla de la creación de la Super Carretera Mundial.

En diversos medios se asegura que en la era de la información todos los mercados cambiarán gracias a la capacidad de cómputo y de telecomunicaciones que se han creado. Esto nos lleva a la conclusión de que la Super Carretera de Información hará posible una gran cantidad de aplicaciones que a su vez revolucionarán los mercados. En pocos años toda empresa deberá estar conectada a sus clientes y proveedores para manejar eficientemente la información.

REFERENCIAS

1.- *Informática Básica*,
Alcalde - García - Peñuelas,
E.D. McGraw Hill,
México 1992.

2.- *Sistemas de Información Administrativa*,
Murdick Robert G.,
E.D. Prentice Hall,
México 1988.

3.- *A fondo: Sistemas de Comunicación*,
Cannon - Luecke,
E.D. Anaya,
España 1988.

4.- *Sistemas de Información para la Administración*
Senn James A.,
E.D. Grupo Editorial Iberoamérica.
México 1990.

5.- *Information Systems Concepts*,
McLeod Raymond Jr,
E.D. Macmillan Publishing Company,
E.U.A. 1994.

6.- *Top Management Planning*
Steiner George A.,
E.D. Mcmillan Publishing Company,
E.U.A. 1994.

7.- *Introducción a la Informática*,
Mora - Molina,
E.D. Trillas,
México 1985.

8.- *Apuntes de Clase: Seguridad en Centros de Cómputo*
Rivera Soler Ricardo,
Fac. Contaduría y Aministración,
UNAM, 1993.

9.- *Biblioteca de Informática Vol. 6*,
E.D. Noriega-Limusa,
México 1990.

10.- *Summit Held to Move ISDN Nationwide*,
Lindstrom Anne,
Communications Week,
E.U.A. Junio 1993.

11.- *La Gerencia Liberadora*,
Tom Peters,
E.D. Atlántida,
Brasil 1993.

12.- *Introducción de los computadores en los negocios*,
Awad Elias M.,
E.D. Prentice Hall,
México 1977.

13.- ***Introducción al procesamiento de datos para los negocios,***
Orilia Lawrence S.,
E.D. McGraw Hill,
México 1986.

14.- *Sistemas de Información Gerencial,*
Tricker R. I.,
E.D. Continental,
México 1984.

15.- *La pirámide del poder,*
Tracy Diane,
E.D. Vergara,
Argentina 1991.

CAPITULO II

AMENAZAS Y RIESGOS RELACIONADOS CON LA PROTECCION DE LA INFORMACION.

La información oportuna y de acceso fácil representa la energía vital de la sociedad actual. Por desgracia, cuanto más accesible es la información, tanto mayor se hace el problema de su protección y por ello es básico contar con una planeación de como lograr asegurar la información y poder controlarla para evitar el acceso a personas no autorizadas, o cualquier daño que ésta pudiera llegar a tener.

Toda organización tiene objetivos muy generales que determinan lo que hará o dejará de hacer, y que definen en términos cualitativos, la clase de actividad en la que desea participar.

Se considera que una organización es capaz de elaborar cualquier futuro que desee.

De la naturaleza del compromiso que la organización contraiga para crear ese futuro, dependerá que una línea específica de desarrollo rinda ganancias o no.

La planeación "es proyectar el futuro deseado y los medios efectivos para conseguirlo".[1]

Es evidente que es un proceso de toma de decisiones y es necesaria cuando el hecho futuro que se desea proyectar implica un conjunto de decisiones interdependientes, de forma que el efecto de cada decisión sobre los resultados del conjunto depende de una o más de las decisiones restantes.

La planeación se interesa tanto por evitar las acciones incorrectas como por reducir los fracasos en aprovechar las oportunidades.

"Así como planear es tomar decisiones, el control es evaluar las decisiones."[1] Consiste en verificar si todo se realiza conforme a lo planeado.

Sin embargo cuando en la organización el control sobre los sistemas de seguridad es deficiente pueden darse consecuencias desastrosas.

Los empleados pueden robar datos o programas y venderlos; o alterar las transacciones con el fin de cometer fraude.

Así mismo los sistemas pueden ser vulnerables a ataques y a la penetración de diversos orígenes sino se establecen los controles adecuados. Algunas veces la causa de la penetración es simple curiosidad, el reto de resolver un problema o jugar una broma, o bien el propósito puede ser robar los secretos de un individuo o competidor u ocasionar una falla en su sistema.

En general las redes de computadoras, el procesamiento distribuido de datos y el acceso remoto a las compuladoras le confieren a las empresas y al gobierno instrumentos muy poderosos. El papeleo se reduce, los servicios mejoran y, con un costo más bajo, la información está a la disposición inmediata de quienes la necesitan.

La clave de ésto es el acceso difundido a una base de datos increíblemente amplia. Por desgracia, este instrumento poderoso con su potencial para tantas buenas aplicaciones, proporciona la misma

oportunidad a los que suelen utilizarlas para fines delictivos. (figura 2.1)

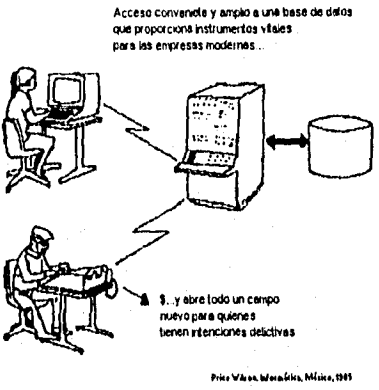

Figura 2.1

Con el acceso rápido, casi instantáneo y de consulta fácil, resulta también factible a distancia en el anonimato de una red telefónica violar los accesos, modificar y obtener información en forma ilegítima.

Es posible el acceso fraudulento y robo a datos e información almacenados en computadoras, interfiriendo líneas de transmisión de datos. De este modo se han interceptado líneas que usan los bancos para transferencia electrónica de dinero para traspasar sumas de cuenta bancaria a la de la persona que hace la interferencia.

La pérdida de información almacenada en la computadora puede ocurrir también por otras razones (no sólo delictivas), y las consecuencias de ésto está en relación con la utilización que tenga en las organizaciones, y a la dependencia que se tenga de ella en las mismas.

Por ejemplo en algunos casos, la pérdida de cantidades sustanciales de información podría resultar en extremo grave. De hecho muchas compañías sufrirían consecuencias desastrosas e incluso la bancarota, si todos sus archivos computarizados se perdieran en forma irrecuperable.

Así los problemas que puede haber con respecto a la información incluyen desde los daños físicos a los equipos que alteran los datos, ya sea por fallas mecánicas o por causas naturales como incendios, temblores, etc., fallas en los programas, errores humanos, hasta actos deliberados como los sabotajes, vandalismos y terrorismo, el acceso no autorizado, la diseminación de virus y delitos tales como el fraude, el espionaje industrial, la piratería, etc.

Se debe evitar que estos problemas se presenten y para ello es necesario conocerlos, y conocer las implicaciones que tienen en una organización, ya que no se puede solucionar un problema si no se sabe cuál es el problema y que lo ocasiona.

Es por esta razón que acontinuación se enumeran los riesgos y amenazas más comunes a que una organización puede enfrentarse con respecto a la protección de su información.

2.1 CAUSAS NATURALES

El peligro de la pérdida física de información es común a todas las formas de almacenamiento de datos, ya sea que la información se almacene en una forma computarizada o en documentos escritos a mano.

Los desastres naturales han sido típicamente muy destructivos y correspondientemente caros para los centros de cómputo, razón por la cual la mayor parte de los presupuestos para seguridad, están destinados a prevención o recuperación de estos desastres. Lo anterior se debe a que si un centro de datos se inunda a causa de una tormenta o huracán, o sufre un incendio grave, o un terremoto, no sólo los datos almacenados, sino también los equipos correrán peligro de ser destruidos.

Por ejemplo:

El fuego es un problema en cualquier organización, pero toma diferentes dimensiones con respecto a las computadoras por dos razones.

- La concentración de equipo caro e información valiosa, y
- El agua, remedio más común para el fuego, es una amenaza para el equipo y por ende a la información, como el fuego mismo ya que aún cuando los circuitos de las computadoras y los medios magnéticos no estén cerca del fuego estos pueden ser dañados

Uno de los desastres más espectaculares en relación con el fuego tomó lugar el 3 de Julio de 1959 en el Centro de Computo del Pentágono. El fuego empezó en una bóveda con paredes aislantes, donde un bulbo de 300 Watts se quemó. Cuando la bóveda se abrió, las flamas se dispersaron y toda el área de computadoras y todas las cintas que en ella estaban se destruyeron.[2]

2.2 FALLAS EN EL EQUIPO

Ocasionalmente, los componentes electrónicos o mecánicos de un sistema de computación suelen fallar, haciendo con ello que la computadora deje de funcionar. Generalmente, este tipo de suceso no da lugar a una pérdida irrecuperable de datos.

Aunque la pérdida real de una base de datos en disco por fallas en el equipo es poco común, suele suceder de diversas maneras:

Los errores en el hardware pueden ser causados igualmente por fallas en el aire acondicionado, por exceso en la temperatura y humedad en el lugar físico donde se ubica el equipo, por cambios bruscos en la corriente, fallas completas o transitorias de la misma, ó errores en los dispositivos

El resultado puede ser una falla de índole tal que provoque una grabación accidental masiva de datos inservibles en el disco; el mal funcionamiento en una unidad de cinta de forma que ésta no escriba los datos; que la cabeza de lectura/grabación de la unidad de disco entre en contacto con la superficie giratoria del mismo, haciendo que quede inutilizado; errores en el sistema de comunicaciones que causen que la información sea transmitida a la terminal errónea; ó que información incorrecta sea almacenada en un archivo procesado.

Por otro lado hay que considerar que el tiempo de máquina perdido es una amenaza real en sí mismo para una organización, ya que puede causar pérdidas costosas a la misma.

2.3 FALLAS DE SOFTWARE

Es la amenaza más común. El software es imposible de probar completamente, los programas modernos pueden extenderse a millones de líneas de código, las cuales son miles de secuencias interrelacionadas entre si.

Así puede ocurrir una situación que no fue probada o que posiblemente no ha sido programada, y presentar algunos problemas (bugs), como: que el programa cause basura y la escriba a un archivo o ignore datos verdaderos o los procese incorrectamente.

Por otro lado la información también puede perderse si un procedimiento no está bien definido o programado.

2.4 FALLAS HUMANAS

El uso no autorizado de prácticas, juegos de diversión, programas, u otros sistemas puede tener efectos deplorables en el propio sistema y sus datos. Tales efectos son: el usuario emplea gran parte de su tiempo valioso en jugar, utiliza los recursos de la empresa como tiempo, máquina, luz, etc. además puede dañar el sistema de seguridad.

Las fallas humanas inevitablemente ocurrirán, pero para asegurar la máxima eficiencia y confiabilidad, los procedimientos manuales dentro de la instalación deben ser reducidos al mínimo y evitar la intervención humana cada vez que sea posible. El descuido, la falta de capacitación, excesivo entusiasmo y el mal entendimiento pueden crear errores de programación y operación, los cuales, una vez introducidos, podrán ser mas difíciles de detectar, corregir y eliminar y tenderán a perpetuarse por siempre. Muy frecuentemente los detectores de errores que se construyen para instalarse dentro del software de la computadora, son diseñados para recoger los errores humanos, tienen el propósito de hacer mas agradable el trabajo evitando tener interrupciones por este tipo de fallas y hacer las cosas mas fáciles.

2.5 PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

El uso de las computadoras por parte de organizaciones, tanto privadas como públicas, para el manejo de información ha hecho surgir una serie de temores a la violación de la privacidad de datos que se almacenan. Este temor no sólo lo comparten los individuos sobre los cuales algunas organizaciones e instituciones guardan información, sino también las empresas y aún los gobiernos. Se protegen desde los secretos de Estado hasta simples datos económicos, financieros, de propaganda o mercadeo hasta datos militares y estratégicos para la empresa o la nación.

"El reconocimiento del derecho a la vida privada se da en función de tres categorías: espacio y propiedad, la persona y la información".[3]

La vida privada en el sentido espacial o territorial, se refiere a la propiedad, al dominio físico en el interior del cual el individuo tiene derecho a estar solo y tranquilo, y al cual ninguna persona puede introducirse sin su permiso.

La vida privada de la persona, consiste en el derecho de protección legal de las libertades de movimiento y expresión, y en la prohibición de la violencia física contra la misma.

La privacidad de la información por su parte, tiene que ver con la dignidad y la integridad de la persona en relación con la información que sobre ella se recaba y circula. El individuo tiene propiedad sobre esa información y es libre de comunicarla o callarla, y al hacer valer su derecho a la vida privada, requiere que la información personal no le sea arrancada por la fuerza, que no se recabe a sus espaldas y que no se

publique sin su consentimiento ni se comunique a terceros sin su autorización.

"La privacidad en el contexto de la computación, refiere al derecho de la persona a controlar el acopio y uso de la información por la persona misma".[4] Implica:

- El conocimiento por parte de las personas de la existencia de cualquier archivo que contenga información sobre ellas.
- El acceso a dicha información, su conocimiento de cómo es usada, por quién y para qué propósito.
- El tener la capacidad de corregir errores en la formación.
- El tener la facultad y capacidad de impugnar su empleo para el propósito establecido.
- El poder impedir que la información se utilice para otro propósito sin su consentimiento.
- El tener la seguridad de que quien maneje y procese sus datos tome las precauciones razonables para prevenir el uso incorrecto.

La privacidad de esta forma, es la confianza que tiene una persona de que los datos que proporcionó se empleen en su interés y no de manera contraria a lo que él espera.

La invasión de la privacidad implica el mal uso de la información en detrimento de uno o más individuos, su explotación para otro propósito para la que fue recabada y sin notificar al sujeto de la información.

Alan Westin (5), utiliza el término privacidad para enunciar tres aspectos de los derechos individuales respecto a la informatización:

- Cuestiones sobre qué tipo de información personal es legítimo colectar o registrar sobre un individuo o grupo, por parte de una institución u organización.
- Qué información personal requiere protección de su confidencialidad y cuando y como será desechada.
- Aspectos sobre el acceso a individuos a sus propios registros a fin de cuestionar o discutir su seguridad y los usos que se hacen de la información.

Esto es de suma importancia ya que en el ámbito organizacional, las organizaciones requieren de privacidad para alcanzar sus objetivos básicos. Privacidad contra la exposición de información referente a sus productos, procesos de toma de decisiones, procedimientos internos, etc.

En muchos casos la efectividad de una organización se basa en su imagen y la exposición de algún asunto interno puede ir en detrimento de ésta. Incluso puede ser la diferencia entre el éxito o el fracaso de la misma.

Es por ello que la violación a la privacidad puede ser un gran problema si la información llega a caer en manos de quien no debe tenerla.

2.6 ACTOS DELIBERADOS

2.6.1 SABOTAJE

Sabotaje en su sentido tradicional , "es el daño o deterioro que en las instalaciones, productos, etc., se hace como procedimiento de lucha contra los patronos, contra el estado o contra las fuerzas de ocupación en conflictos sociales o políticos".[6]

En la actualidad este concepto se ha extendido al ámbito de la computación donde se define como "la destrucción deliberada (borrado, alteración, entrada o supresión) de los datos o programas de cómputo, u otras interferencias con los sistemas de computadoras, con el intento de impedir el funcionamiento de una computadora o de un sistema de telecomunicaciones".[7]

Esta destrucción o daño de equipo puede ser perpetrada por empleados descontentos u otras personas que actúan en contra de los intereses de una organización.

El sabotaje puede ser el vehículo para ganar ventaja económica sobre un competidor, para promover actividades ilegales de terroristas motivados ideológicamente o para robar datos con propósitos de extorsión.

Por ejemplo, en 1979 la Administración Federal de Aviación de Estados Unidos, concluyó que alguien alteró la información acerca de un avión soviético que se aproximaba, con el embajador Anatoly Dobrynin a bordo.

La torre de control perdió la información en la computadora de la altura y la velocidad del avión, y después lo confundió con otro. El avión recibió permiso de descender 10 millas antes de lo debido y ocupó espacio aéreo que pudo estar ocupado por otro avión. Afortunadamente, el avión aterrizó sin problemas, sin embargo este acto fue el producto de una protesta política por la invasión soviética a Afganistán.[8]

Los actos de sabotaje pueden ser internos en la organización o no; incluso pueden no ser directos contra la misma computadora. Un ataque contra las líneas telefónicas o contra el sistema de aire acondicionado de las instalaciones de un centro de cómputo puede provocar fallas en el mismo.

Al hablar de sabotaje puede también incluirse el daño lógico a través de programas que pueden borrar la información, datos u otros programas en un sistema.

Uno de los tipos más peligrosos de sabotaje son los virus, caballos de troya, gusanos y bombas lógicas que son programas con códigos dañinos, algunos de ellos ocultos dentro de otros programas listos para actuar maliciosamente y que pueden ser programados para dañar, modificar o borrar información.

2.6.2 VANDALISMO

Se considera vándalo a "aquella persona que comete acciones propias de gente salvaje y desalmada".[6] Así por vandalismo se entiende al "espíritu de destrucción que no respeta cosa alguna, sagrada, ni profana".[6] Está estrechamente relacionado con el sabotaje ya que el tipo de daños que causa son similares, sin embargo, los motivos son difíciles de profundizar, ya que aquí generalmente son simplemente el querer hacer algo indebido.

2.6.3 ORGANIZACIONES TERRORISTAS

Terrorismo es "la sucesión de actos de violencia ejecutados para infundir terror".[6] En la actualidad, existen en el mundo numerosos grupos terroristas algunos de los cuales reconocen la importancia de las computadoras ya sea como fuente de información para facilitar sus actividades o como fuente principal para causar daños a terceros.

Es importante mencionar que generalmente este tipo de organizaciones utilizan el sabotaje como medio para lograr sus fines.

Uno de los casos de más conocidos relacionado con las organizaciones terroristas en el campo de la computación, es el del virus Jerusalem el cual fue creado por la Organización para la Liberación de Palestina (OLP) e introducido para contaminar y causar daños en las computadoras de la Universidad Hebrea.

2.7 DELITOS

La delincuencia con computadoras podrá fascinar y asombrar a mucha gente, pero no deja de ser otra forma de desfalco o fraude. A pesar de que es una forma relativamente nueva de delincuencia. Aún cuando la estimación de perdidas anuales de las corporaciones por el crimen con computadora se calcula en 300 millones de dólares, muchos creen que esta estimación es demasiado conservadora. La cifra real se desconoce, debido a que los ejecutivos de las corporaciones son muy renuentes a reportar estos crímenes por temor al ridículo y a las represalias de los accionistas.

Los periódicos y las revistas registran todos los tipos de delitos asociados a las computadoras.

Tradicionalmente la definición de delito es cualquier "acción u omisión voluntaria castigada por la ley con pena grave".[6]

Con respecto al delito cuando este es asociado a una computadora puede definirse como "*Incidente donde el conocimiento o el uso de computadoras es una condición necesaria para cometer el crimen*".[9] Es aquel delito en donde las computadoras están involucradas de alguna forma.

Conviene diferenciar claramente entre lo que es un error, evento anormal o no programado y lo que es un delito por computadora; el primero, es causado accidentalmente en el transcurso de operaciones normales y autorizadas, y el segundo, se corresponde con un intento maligno de cometer un acto ilegal o en contra de la ética.

Los delitos por computadora tienen una característica muy singular que es proporcionar facilidad relativa para el cuidadoso ocultamiento del delito cometido.

La computadora ofrece, a diferencia de muchos sistemas manuales, la posibilidad de borrar todas, o casi todas las huellas, de un acto ilícito. Tan es así, que la mayoría de los casos descubiertos, lo han sido por circunstancias fortuitas relacionadas con el cambio de modo de vida del delincuente, y no por la detección de los rastros dejados en el computador.

Además también influye la falta de tradición jurídica en la materia, ya que los delincuentes saben de antemano que es muy difícil que sean llevados a juicio, y que si lo son, sus sentencias no serán tan graves.

En general y principalmente en países como México, existe un vacío jurídico ya que el derecho penal es materialista y carece de figuras adecuadas cuando el objeto del delito es un intangible como la información. Así es muy difícil probar, el robo o hurto de horas de tiempo de computadora o la penetración en un banco de datos para obtener o modificar información.

Una complicación más al respecto, es el hecho de que la computadora no sólo puede ser el objeto o el instrumento de un delito sino que, los delitos también pueden producirse en cada uno de sus componentes tales como: la entrada de datos, programas de aplicaciones, sistema operativo, salida de datos y comunicaciones entre computadoras.

Existe un paralelismo entre los motivos para realizar delitos comunes y por el computador. Los objetivos de ganancia personal

causado por necesidades económicas , o ganancia institucional para beneficiar a una empresa, o inclusive el deseo de venganza en contra de una compañía, aunque por métodos diferentes, son aplicables a ambos tipos de delitos.

Existen sin embargo, motivos que son un producto de la existencia de la computadora:

- Es el blanco ideal porque no tiene sentimientos.
- Se presta para jugar y explorar sus límites.
- Con toda su tecnología, representa un reto al ego, y a la inteligencia humana.[3]

Los factores que han permitido el incremento en los crímenes por computadora son principalmente:

- Aumento del número de personas que se encuentran estudiando computación.
- El aumento del número de empleados que tienen acceso a los equipos.
- La facilidad en el uso de los equipos de cómputo.
- El incremento en la concentración del número de aplicaciones y consecuentemente de la información.[3]

Es importante mencionar que en muchos casos gran culpa de que haya la posibilidad de que alguien cometa un delito es culpa de la víctima. Esto sucede cuando se dejan desatendidas terminales conectadas a una aplicación, cuando las palabras claves de acceso se comparten y luego no se modifican, cuando se permite a programadores hacer pruebas con archivos de producción, etc.

2.7.1 ESPIONAJE INDUSTRIAL

Tradicionalmente espionaje es el "Uso sistemático de espías u otros agentes secretos por un país para obtener secretos militares, información estratégica, etc., de otros países".[10]

Pero, el espionaje no sólo se da entre países, también puede darse entre organizaciones, empresas o compañías que tratan de apoderarse de información secreta de sus competidores.

A este tipo de espionaje es a lo que se llama espionaje industrial, el cual se define como "La adquisición por medios impropios o la exposición, transferencia o uso de un trato o secreto comercial sin derecho u otra justificación legal, con el intento de causar pérdida económica a la persona titular del secreto o para obtener una ventaja económica ilícita para uno mismo o para una tercera persona".[7]

En la actualidad el espionaje industrial está especialmente dirigido hacia las tecnologías modernas, teniendo a las computadoras como primer objetivo.

Los espías modernos buscan obtener información de medios magnéticos en vez de los recursos tradicionales, ya que ésta es más fácil de identificar, ordenar, categorizar y copiar sin dejar rastro; además la cantidad de información almacenada en medios magnéticos es enorme y ocupa mucho menor espacio. Como prueba de esto podemos ver que una cinta magnética es tan pequeña que puede incluso ser guardada en el bolsillo.

Esto constituye un gran riesgo para una empresa, simplemente hay que imaginar el daño que puede sufrir si su información secreta sobre

productos nuevos que todavía no están en el mercado o de futuras estrategias se da a conocer a la competencia.

Años y años de investigación y desarrollo pueden ser inútiles si el nuevo producto es anunciado por otra compañía en vez de la que lo creó, y tal vez a menor precio, situación qué puede incluso sacar del negocio a una compañía.

2.7.2 FRAUDE

Fraude "es toda acción contraria a la verdad y a la rectitud que perjudica a la persona contra quien se comete".[6]

En el ámbito de la computación esto no es muy diferente ya que implica cualquier intromisión, alteración, borrado o supresión de datos, programas o procesos que influyan en el resultado del procesamiento de datos, causando con ello pérdidas económicas o de propiedad a otra persona con el intento de procurar una ganancia ilícita para uno mismo o para un tercero.[7]

En los negocios modernos el dinero se reemplaza o se mueve rápidamente con las transacciones de depósitos en sistemas de computadoras, creando un enorme potencial para el abuso por computadora. Además la característica del acceso remoto en que el delito se puede cometer sin estar presente físicamente en el lugar lo hace más atractivo.

La forma más común de fraude por computadora es la manipulación de entradas, ya que es fácil de perpetrar y no requiere de conocimientos sofisticados en cómputo de forma que puede ser cometido

por cualquiera que tenga acceso a funciones normales de procesamiento de datos en la etapa de entrada. Por ejemplo, una persona encargada de contar dinero y capturar el monto puede alterar la cantidad y cambiarla por una menor quedándose con la ganancia cuando el control sobre esto es deficiente.

Otra forma de cometer fraude es por manipulación de programas la cual es muy difícil de descubrir, requiere que el perpetrador tenga conocimientos específicos en computación, ya que involucra cambios a los programas existentes o la introducción de nuevos programas o rutinas.

Un ejemplo de la forma en que puede cometerse un fraude por computadora, lo vemos en el que se descubrió en 1978 en el Queens College en Nueva York, en el cual dos alumnos, uno de los cuales había laborado en el centro de cómputo de la institución, habían falsificado un total de 154 calificaciones de 19 estudiantes de 1974 a 1977.[11]

2.8 HACKERS

La palabra Hacker una vez denotó el tipo de super programador que trabaja toda la noche y podían hacer que la computadora hiciera cualquier cosa que él quisiera. Eso fue hace 20 años; hoy el medio ha hecho de Hacker un término que significa algo criminal.

Según el Diccionario para usuarios de computadora de QUE, Hacker es "aquel entusiasta aficionado a las computadoras con bastos conocimientos técnicos cuya diversión estriba en hacerle modificaciones a los programas o sistemas de computación y romper el sistema de seguridad de un sistema por el mero reto que ello ofrece".[12]

Se les puede encontrar casi en cualquier laboratorio de computación de colegios o universidades, donde pasan prolongados periodos de tiempo tratando de dominar un sistema de computación.

Existe una variante de Hackers a los cuales se les denomina Crackers y son aquellos que tratan de introducirse en un sistema de cómputo por diversas razones, la principal es ¡porque es posible!, pero más probablemente por afanarse de hacer algo ilegal o para ganar estatus entre un grupo similar.(14) Particularmente tienen un rasgo antisocial y vandálico; son los que borran archivos, provocan la caída del sistema o de procesos, etc.

Sin embargo, para esta tesis hablaremos de Hackers en general sin diferenciar el tipo de éstos.

Como ya se mencionó, los hackers pueden tener diversos motivos para hacer lo que hacen, y los usuales de beneficio o venganza también se aplican a ellos.

Algunos son simplemente psicóticos y causan daño como un acto de vandalismo insensible. Otros lo hacen por reto intelectual. Los mejores profesionales de cómputo pueden intentar responder a un reto como "*mi sistema es impenetrable*", o "*mi sistema es incopiable*".

El gusto por los retos intelectuales es una de las cosas que hacen a un buen profesional, pero uno como "*mi sistema es impenetrable*" ó "*mi sistema es incopiable*" sólo es una bandera roja para un Hacker.

También puede presentarse como motivación el hecho *de "ver si puedo hacerlo"*, o el hecho de "*obtener poder sobre otros*".

Es importante considerar que los Hackers tienen un comportamiento vandálico e improfesional y en muchos casos en contra de la ley.

2.9 VIRUS

Los virus informáticos son programas de computación. ¡Simples programas de computación elaborados por programadores!, similares al de un procesador de textos o una hoja de cálculo o un programa de base de datos o a un programa de control de inventarios; es decir, son programas que contienen instrucciones para que las ejecute la computadora. Provocan desde únicamente el despliegue de un mensaje, hasta la pérdida de los datos o archivos en los medios de almacenamiento de información, e incluso pueden ocasionar daños en el sistema y algunas veces incluyen instrucciones que pueden ocasionar daños al equipo. Casi nunca incluyen el nombre del autor, ni el registro o Derechos de Autor, ni la fecha. Se reproducen a sí mismos y toman el control o modifican otros programas.

A la fecha no se ha dado una definición exacta de los que son los virus, pero casi todos los autores coinciden en sus definiciones.

El diccionario para usuarios de computadoras QUE, los define como "Un programa de compulación diseñado como un elemento llamativo o un saboteador, que se copia a sí mismo, para lo cual se adjunta a otros programas y lleva a cabo operaciones indeseables y en ocasiones dañinas".[12]

Alberto Rojas en su articulo ¿Ya vacunó a su PC? publicado en la revista PC/TIPS, especifica que los virus nunca piden permiso y jamás avisan al usuario de su presencia en el sistema o en el programa infectado.[14]

De esta manera puede decirse que un virus de computadora es un programa de cómputo diseñado de forma que cumpla con tres objetivos básicos:

1. Que sea capaz de replicarse o fabricar copias de sí mismo utilizando para ello a otro programa, esto significa que requiere de un huésped para reproducirse por lo cual se le ha dado el nombre de virus ya que su comportamiento es análogo a los virus biológicos.
2. Que tenga una misión que cumplir. Que realice la tarea encomendada por el programador a la hora de crearlo (borrar archivos, bloquear la computadora, mandar un mensaje al usuario, etc.).
3. Que tenga una forma de autoprotegerse para sobrevivir, tales como tiempos de incubación, resistencia a la eliminación, actuar sigilosamente para no ser detectado, etc.

Así mismo, debido a la falta de consenso en cuanto a su definición, la palabra virus, se aplica como término genérico para todas las formas de programación dañina, aun cuando esta no cumpla totalmente con las características que se dice debe tener un virus propiamente dicho.

La elaboración de estos tipos de programación dañina o virus, se da por clases de personas entre las cuales se encuentran desde investigadores y estudiantes, hasta organizaciones ideológicas y grupos religiosos que pretenden desestabilizar el avance tecnológico. Lo anterior ha ocasionado que día con día existan más virus de forma que a la fecha hay más de 2100 virus diferentes lo cual genera un alto porcentaje de riesgo de infección y daños o pérdida de información".[15]

2.9.1 CLASIFICACION

Los programas "virulentos" han sido clasificados por cada autor en diversas categorías. Sin embargo, para efecto de ésta tesis diremos que se clasifican en las siguientes categorías:

1. CABALLOS DE TROYA

"Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final."[16] Parecen ser aplicaciones útiles, mientras que en realidad contienen una o más órdenes destructivas que se activan al ejecutar la indicación programada.

A diferencia de los virus ordinarios que consiguen entrar en el computador ocultándose en un programa normal, habitualmente como parte del sistema operativo, y se expanden a programas similares en el nuevo huésped, el software troyano depende de que sea atractivo o interesante para el futuro usuario.

En general estos virus son destructores de la información contenida en los discos.

2. BOMBAS LOGICAS

"Son programas que ejecutan órdenes informáticas destructivas condicionalmente, dependiendo del estado de variables ambientales."[17] Ejecutan dichas órdenes al producirse un hecho determinado con anterioridad, pero mientras esto no se produzca, permanecen ocultos sin más trascendencia que ocupar una porción de la memoria.

Hay muchas historias de programadores enfadados que colocan bombas lógicas porque creen haber sido despedidos injustamente.

Por ejemplo, el caso de Donald Burleson, un programador de la compañía aseguradora fundada en Forl Worth, USA. En septiembre de 1987 fue despedido por ser supuestamente pendenciero y resultar difícil trabajar con él. Dos días más tarde, se borraron a sí mismos aproximadamente 168,000 registros vitales de las computadoras de la compañía. Estalló una bomba lógica que hizo estragos con los archivos que eran el sustento de la compañía. Con esta acción Burleson se convirtió en la primera persona de América en ser encarcelada por acceso perjudicial a las computadoras.

3. GUSANOS INFORMATICOS

En el contexto de los programas dañinos, se utiliza gusano de forma figurada. Se dice que los gusanos "...son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se arrastran literalmente por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban y así sucesivamente. Esto hace que los programas o información que encuentran a su paso por la memoria, sean borrados, lo

que causa problemas de operación o pérdida de datos."[16] Algunos de ellos dejan mensajes burlones o misteriosos antes de trasladarse de un lugar a otro; generalmente su objetivo es simplemente reducir las capacidades de la máquina.

El caso más ampliamente publicado sobre los gusanos, tuvo lugar en noviembre de 1988 cuando Robert Morris, de 24 años, estudiante de la Universidad de Cornell, liberó uno a través del Internet. Básicamente, Morris escribió un programa que examinaba el archivo de claves de acceso de las computadoras de la red y aprovechando las características no documentadas del sistema enviaba información a otras computadoras para provocar la generación de otros gusanos. Al final, el gusano infectó a más de 6000 computadoras y bloqueó la mayor parte de la red Internet durante varios días.

Se ha discutido la diferencia que hay entre los virus y los gusanos, especialmente durante el incidente Internet-Morris. Por ejemplo, un corresponsal científico dijo "la red ampliamente extendida en América, Internet, cayó bajo el ataque de un gusano: un tipo de virus de computador que entra en una red y se multiplica a sí mismo un número de veces en las computadoras que haya conectadas". Sin embargo una revista de informática dijo que "debido a que no afecta otra función y no se disfraza como otro tipo de programa, la mayoría de la gente entendida había llamado al programa gusano y no virus".

La diferencia entre los virus y los gusanos puede decirse que radica en que los virus se reproducen y los gusanos tienden a crecer o viajar. Sin embargo la implicación de que se les clasifique dentro de los virus está en que los gusanos no suelen funcionar sin afectar negativamente a las computadoras donde se hospedan.

CLASIFICACION DE LOS VIRUS, SEGUN SU FORMA DE CONTAGIAR

Virus de sector de arranque. Son los que contagian usando como medio el proceso de arranque de la computadora. "Emplean el interior del controlador del sistema operativo del disco y sectores en buen estado para camuflarse y posteriormente marcarlos como defectuosos con el fin de no ser destruidos".[18] Pueden coordinar, o interferir la acción del sistema operativo ya que se almacenan en la memoria. Ejemplos típicos de éste tipo de virus son el Ping Pong, Italian, Pakistaní Brain, Stoned.

Virus de programas. Los que contagian usando como huésped los programas o archivos ejecutables. "Modifican la estructura de los archivos ejecutables con las extensiones .EXE, .COM, .SYS y .OVL".[18]

Están adheridos a un programa al principio o al final del archivo. "Cuando el programa se carga en memoria, el código maligno se hace residente y devuelve el control al programa que lo portaba"[15], con esto permite una ejecución normal. Una vez en la memoria si se pretende ejecutar otro programa no infectado, el virus se autocopiará para sumarse al nuevo programa y así sucesivamente. Los ejemplos más conocidos de este tipo de virus son Viernes 13 y Jerusalem.

VIRUS DE LA NUEVA GENERACION

Los virus de la nueva generación, también llamados virus inteligentes, son virus que presentan las mismas características que los demás virus, así como características adicionales que los hacen ser aún más peligrosos.

Estos virus se instalan como programas residentes que alteran el vector de interrupción del sistema operativo y acceden a rutinas de entrada y salida del BIOS. Escapan de algoritmos de verificación, de error y de programas diagnóstico.

Quizá el mejor ejemplo de los virus de la nueva generación, y el más conocido en México ya que ha atacado con enorme fuerza en este país, es el virus NATAS, este virus, infecta el primer sector de los discos duros, así como todos los archivos ejecutables, incluso puede destruir la tabla de asignación de archivos o modificarla lo cual lo hace extremadamente peligroso.

2.9.2 IMPACTO DE LOS VIRUS EN LAS ORGANIZACIONES

No se conoce una cifra exacta del número de computadoras que han sido víctimas de una infección viral, pero seguramente cada día es mayor, "en 1990 de cada 100 lugares en que se revisaba la existencia de virus, 18 de ellos estaban contaminados; para 1993 de cada 100 lugares inspeccionados se encuentran 90 con virus. Los costos que estos parásitos ocasionan a la industria en general son del orden de $10,000 dólares americanos en promedio y un 7% de estos sobrepasan los $100,000 dólares".[15]

El riesgo que constituye la presencia de estos virus, es de suma importancia ya que se arriesga información prioritaria, tal como la contabilidad de una empresa, los registros de sus clientes, registros de transacciones en línea, registros de inventarios, planos, proyectos y diseños, así como sistemas de comunicaciones corporativas; para algunas

empresas significa arriesgar la confiabilidad de sus clientes y hasta su reputación, e incluso puede arriesgarse hasta la vida humana.

"Los programas de virus han dado origen a una gran controversia en el campo de la informática. Mientras que los usuarios opinan que la creación de virus es una acción terrorista y de falta de ética, los fabricantes de software opinan que en algunos casos se justifica la utilización de esquemas de protección que (aunque no se llamen virus) contenga códigos muy parecidos.

Estos últimos justifican su proceder alegando que al detectar que se han hecho demasiadas copias de algún programa fabricado por ellos (demasiadas para tratarlas como copias legalmente autorizadas para uso personal), los esquemas de protección diseñados por ellos pueden proceder como agentes virales, destruyendo los archivos en el disco que supuestamente tiene una copia ilegal o pirata del software que desean proteger".[15]

Uno de los factores por los cuales en el presente, en la mayoría de los países aún no se ha legislado sobre la materia, es que por un lado se cuestiona la legalidad de incluir o no un esquema de protección tipo virus en el software original, mientras que por otro se tiene la duda de si es ético o no hacerlo.

Pero mientras esta duda se resuelve, los programadores y fabricantes se defienden de la injusticia que representa para ellos la piratería de programas y aplican sus conocimientos para proteger el software creado por ellos, mediante la inclusión de esquemas de protección.

La solución a este problema debe ser concientizar a los usuarios sobre la conveniencia de utilizar sólo programas originales, y a los programadores con respecto a los beneficios económicos que deben obtener de su software llegando a niveles de precio accesibles, de forma que no estimulen la proliferación de copias ilegales.

Lo anterior pone de manifiesto la necesidad de crear asociaciones serias y responsables (como la Computer Virus Industry Association que ya existe en E.U.A.), constituidas por usuarios y fabricantes de software y hardware, con el fin de establecer los pasos que se deben de seguir para erradicar los virus informáticos y contribuir al bienestar y tranquilidad de los usuarios, satisfaciendo también en gran medida los intereses de los fabricantes.

Así, "en 1984 en México, luego de haber discutido si se debían incluir en el registro de patentes, la Secretaría de Educación Pública expidió un acuerdo autorizando la inclusión de los programas de computación en el Registro Público del Derecho de Autor.

Aunque se trató de un avance muy significativo, la decisión no resuelve todo el problema. En primer lugar, por lo leves que son las acciones que se aplican a los infractores, y en segundo lugar por que se incluyó al software bajo una ley que fué creada para proteger obras intelectuales con características muy diferentes".[16]

Así mismo no se contempla lo que significa la programación, los virus informáticos, las medidas protectodestructivas en los programas comerciales, ni conceptos como sanciones al autor que se exceda en la aplicación de protecciones que puedan dañar la información o incluso el equipo del usuario.

2.10 PIRATERIA

La piratería es "el robo o destrucción de los bienes de otro".[6] Piratear, es "cometer acciones delictivas o contra la propiedad como hacer ediciones sin permiso del autor o propietario, contrabando, etc."[6]

La piratería de programas es "la copia sin autorización e ilegal de un programa con derecho de autor sin que medie el permiso expreso del editor del software".[12]

Piratear o copiar software ilegalmente equivale a un robo.

Un programa puede copiarse muy fácilmente. Ante la consternación de los desarrolladores de las aplicaciones la piratería es muy común y es uno de los grandes problemas que se presenta en el mundo de la computación.

Pero lo más grave es que incluso aquellas personas que jamás transgreden normas morales o legales participan en la piratería de programas sin ninguna vacilación. Tal parece que la revolución iniciada con la computación se ha dado con tal rapidez que las normas culturales y los valores éticos y morales no han tenido tiempo para ajustarse.

Quienes defienden a la piratería de programas presentan argumentos que llegan a ser excusas pobres y sólo muestran sus intereses particulares. (ver figura 2.2)

Los intentos por detener la piratería de programas por medio de esquemas de protección contra copiado han resultado contraproducentes para las compañías que los impusieron. Tales esquemas evitaban que un

usuario casual copiara un disco, pero también imponía sanciones a los usuarios registrados. En consecuencia, los usuarios legítimos procuraban no comprar programas protegidos contra copiado y los editores de software más importantes tuvieron que dejarlos.

PIRATA	JUSTIFICACION
Pirata Banquero	Se justifica diciendo: Cuesta mucho dinero
Pirata Acelerado	Argumenta: Nos urge y no hay en el mercado
Pirata Consiente	Acepta: El software está muy caro
Pirata Costumbrista	Se consuela: Aquí todo el mundo copia
Pirata Retador	Se envalentona: A nosotros no nos cachan
Pirata Ingenuo	Pregunta: ¿Acaso copiar software es ilegal?
Pirata Mártir	¿En esta empresa no nos dejan copiar software?
Pirata Ganio	Descubre: Es muy fácil copiar, no sea bruto
Pirata Macho	Reta: ¡A poco tú no copias!

Personal Computing México, Año 4 No. 46, México, 1992
Figura 2.2 Clasificación de los piratas

El principio básico de la piratería es que *"no hay nada como lo que es gratis"*. Sin embargo nada es gratis: alguien, algo, paga el costo de cualquier regalo. Un usuario puede ver que los programas que sus amigos le ofrecen son gratis, pero hay un costo extendido. La piratería extendida es una de las razones por la que los buenos programas pueden costar mucho dinero. Así como uno de los mayores y más comunes medios de transmisión de código dañino.

Los programas de cómputo no crecen en árboles, la gente o los programadores mejor dicho tienen que crearlos, diseñarlos, escribirlos y venderlos labor que no es fácil y no es barata.

La piratería significa que haya muchas copias gratis por cada uno de los programas que son pagados. "Se estima un rango de 2 a 30 o más copias piratas por cada copia legítima en el tiempo de vida del programa".[16]

Si un programa es bueno, la gente quiere copiarlo, y con el tiempo se harán más copias piratas, así podemos imaginar lo que ésto le hace a los beneficios y oportunidades del desarrollador en el mercado.

Un efecto de la piratería es forzar al desarrollador a usar una o dos estrategias de mercadotecnia: distribuir su producto como *Shareware* (software que se vende a bajo costo pero contiene un alto riesgo, y mucha exposición a la infección viral), o definir una campaña de mercadotecnia muy cara.

Volviendo al hecho de que nada es gratis, una razón de que el software es tan caro es que alguien tiene que pagar por su caro diseño, desarrollo, soporte y documentación. Si un desarrollador tiene un programa popular, suficientes copias para un beneficio decente podrán ser vendidas rápido. Pronto, la demanda lo conocerá por copias piratas y esto no pasará de ahí sin ningún beneficio para el desarrollador.

Aunque se practique en casa, la piratería es inmoral e ilegal; aún así, es difícil que llegue a ocurrir una demanda. Las compañías no por esta razón deben sentirse seguras ya que no son pocas las compañías demandadas por daños atribuibles al copiado sin autorización de programas.

En el caso de la piratería estudiantil, esta es muy fecuente ya que generalmente los estudiantes, no tienen la capacidad económica para comprar los programas originales y por lo mismo intentan copiar éstos de cualquier manera.

REFERENCIAS

1.- *Planeación,*
Ackoff,
E.D. Limusa,
México 1987.

2.- *A Contingency Plan for Catastrophe,*
Van Tassel, D.,
Datamation,
Julio 1971,
E.U.A.

3.- *Seguridad Informática e Ingeniería de Software,*
Rivera Porto Eduardo,
I Congreso Iberoamericano de Informática y Auditoría,
Puerto Rico 1987.

4.- *Computers and Social Change,*
Laver M.,
Cambridge University Press,
E.U.A. 1980.

5.- *Privacy and Freedom,*
Westin Alan,
Atheneum,
E.U.A. 1967.

6.- *Diccionario de la Lengua Española,*
Real Academia Española,
España 1992,

7.- *International review of criminal policy,*
United Nations Manual on the prevention and control of the computer-related crime.

8.- Informática, Presente y Futuro,.
Sanders,
E.D. Prentice Hall,
México, 1988.

9.- Newsweek,
Febrero 1995,
México.

10.- *Advanced Dictionary,*
Thorndike Barnhart,
Scoot, Foresman & Co.
E.U.A. 1973,

11.- Framingham,
Computer World,
Enero 1979,
E.U.A.

12.- *Diccionario para usuarios de computadoras QUE,*
Pfaffernberger Bryan,
Prentice Hall,
México 1992.

13. http://www.lib.ox.ac.uk/internet/news/faq/archive/securityfaq.htlm

14.- *Ya vacunó a su PC?*
Alberto Rojas
PC/Tips,
México.

15.- *The computer Virus Crisis,*
Fites-Johnston-Kratz,
Van Nostrand Reinhold,
E.U.A. 1992.

16.- *Virus en las computadoras,*
Ferreyra Cortés Gonzalo
Macrobit,
México 1990.

17.- *Virus Informáticos,*
Levin Richard,
Mc Graw-Hill,
México 1992.

18.- *Virus, Peligro latente,*
PC-Magazine en Español,
Agosto-1992,
México.

19.- *Computer Viruses,*
Mayo Jonathan,
Winderest-Mc Graw-Hill,
E.U.A. 1990.

20.- *Computer Security Handbook,*
Richard H. Baker,
Mc Graw Hill
E.U.A. 1985

21.- *Security of Information and data,*
Daler, Gulbrandsen, Melgard, Sjølslad,
Ellis Horwood Limited,
Inglaterra 1989.

22.- *La piratería y la protección legal del software,*
Personal Computing México,
Año 4 No. 46,
México, 1992

23.- *Informática,*
Price Wilson,
Interamericana,
México 1985.

CAPITULO III

SEGURIDAD DE LA INFORMACION

La información almacenada en una computadora puede llegar a tener tal importancia que la pérdida o destrucción de la misma puede (como se vio en el capítulo anterior) suponer un desastre para su propietario.

Bajo esta premisa es necesario tener el conocimiento de diversas medidas de seguridad, de forma que sea posible garantizar que la probabilidad de riesgo que puede afectar a la organización, se mantenga en niveles mínimos y ante la ocurrencia de algún riesgo, se contará con medios preventivos que permitan disminuir con oportunidad y eficiencia los efectos que de ésta se deriven.

3.1 DEFINICION DE SEGURIDAD

Seguridad según su definición, consiste en "mantener cualquier cosa libre y exenta de todo daño, peligro o riesgo".[1]

En cuestión de informática, también tiene sus acepciones.

Roger S. Pressman la define como "... el grado con el que un sistema y el acceso a la información están protegidos...".[2]

Para Banamex la seguridad informática "se orienta a conservar un alto nivel de integridad, confidencialidad, disponibilidad y autenticidad de la información del Grupo, a través de la aplicación de tecnología avanzada, desarrollo e implementación de estrategias y acciones que identifiquen, prevengan, reduzcan o transfieran los riesgos que puedan afectar la información".[3]

Sin embargo una de las definiciones más generales es la siguiente:

"Un sistema de cómputo es seguro si se puede confiar en él, si su software se comporta como se espera que lo haga, y la información almacenada en él se mantiene inalterada y accesible durante tanto tiempo como su dueño lo desee".[4]

En este aspecto la seguridad busca asegurar la confidencialidad, integridad, autenticidad, y disponibilidad de la información (Tabla 3.1). Así mismo, la Seguridad Informática busca mantener y conservar la operatividad de la organización y de sus sistemas a partir del resguardo de sus recursos.

Confidencialidad	Un sistema de cómputo no debe permitir que la información contenida en él sea accesible a nadie que no tenga la autorización adecuada.
Integridad y Autenticidad	Un sistema de cómputo no debe permitir modificaciones no autorizadas a los datos o a la información contenida en él. Esto comprende cualquier tipo de modificaciones: Por errores de hardware y/o software. Causados por alguna persona de forma intencional. Causados por alguna persona de forma accidental. La Autenticidad se maneja en cuestión de telecomunicaciones, y se refiere a contar con un medio de verificar quien envía la información, así como poder comprobar que los datos no fueron modificados durante su transferencia.
Disponibilidad	La información puede estar sana y salva en el sistema, pero de poco sirve si los usuarios no tienen acceso a ella. La Disponibilidad significa que los recursos del sistema, tanto de hardware como de software, se mantendrán funcionando de forma eficiente, y que los usuarios los podrán utilizar en el momento en que los necesiten. También significa que el sistema sea capaz de recuperarse rápidamente en caso de ocurrir un problema de cualquier especie.

Tabla 3.1 Fuente: Proyecto UNAM/CRAY de seguridad en el s.o. Unix. Diego Zamboni. 1995

3.2 OBJETIVOS DE LAS MEDIDAS DE SEGURIDAD

Los objetivos de las medidas de seguridad pueden ser vistos como una serie de niveles de control en donde si un nivel falla, entonces otro nivel toma posesión u ocupa su lugar y continúa con la operación del sistema, de forma que el impacto global que pudiera haber por causa de ello, se reduce. Estos objetivos son:

1. *Disuadir.* A este nivel la meta es prevenir cualquier tipo de amenaza o desastre que pueda ocurrir.

2. *Detectar.* La disuasión total generalmente no se consigue, por tanto en este nivel se establecen métodos de monitoreo y vigilancia que reporten cualquier riesgo o peligro, y que permitan tomar las acciones correctivas pertinentes.

3. *Minimizar el impacto de pérdida o desastre.* Si un accidente o contratiempo ocurre, deben establecerse procedimientos que ayuden a reducir la pérdida o el daño.

4. *Investigar.* Si la pérdida ocurre, puede realizarse una investigación que ayude a determinar lo que pasó. La información que derive de esta investigación puede servir para futuras planeaciones de seguridad.

5. *Recuperar.* Las medidas de seguridad implican que debe haber un plan de acción para recuperación en caso de que un accidente, o desastre ocurra, sea cual fuere su causa, y de la manera más pronta posible.[6]

3.3 CONSIDERACIONES SOBRE SEGURIDAD

La seguridad en cómputo como de cualquier otro tipo, cuesta tiempo, dinero y sobre todo esfuerzo.

Es posible obtener en general ciertos niveles mínimos de seguridad sin hacer un gasto considerable. Pero, el logro de protección adicional requiere niveles de gasto más altos y, con frecuencia, retribuciones menores. La economía siempre resulta necesaria y es importante asegurarse de que existe una relación costo/beneficio razonable con respecto a las medidas de seguridad.

Para ello es necesario establecer prioridades. No tiene caso disponer grandes cantidades de dinero, si la información que se va a proteger vale menos de lo que se va a gastar. Por eso antes de comenzar a planear la seguridad, es necesario hacerse las siguientes preguntas:

¿Qué se quiere proteger?

Es muy importante determinar el valor de la información que manipula un sistema y las tareas que realiza (que tan importante es para la organización en que se está trabajando). Esta valoración debe hacerse de forma individual, pues la información que es muy valiosa para una organización puede no tener ningún valor para otra.

¿Contra qué se quiere proteger?

Para no incurrir en gastos innecesarios, es importante determinar cuáles son los riesgos reales a los que está expuesta la información.

La seguridad efectiva debe garantizar la prevención y detección de accidentes, ataques, daños por causas naturales, así como la existencia de medidas definidas para afrontar los desastres y el restablecimiento de las actividades.[5]

¿Cuánto tiempo, dinero y esfuerzo se esta dispuesto a invertir?

Este punto es el más importante, ya que es realmente la cantidad de recursos de que dispone o que está dispuesta a invertir la organización lo que determinará en última instancia que se medidas se van a tomar. Estos recursos son:

Tiempo	Para tener un nivel de seguridad alto es necesario que alguien dedique tiempo a configurar los parámetros de seguridad del sistema, el ambiente de trabajo de los usuarios, revisar y fijar los permisos de acceso a los archivos, ejecutar programas de monitoreo de seguridad, revisar las bitácoras del sistema (logs), etc.
Dinero	El tener a alguien que se encargue de la seguridad de forma responsable cuesta dinero. Así mismo cuesta dinero adquirir lo productos de seguridad que se vayan a utilizar, ya sean programas o equipo.
Esfuerzo	Establecer y mantener un nivel adecuado de seguridad puede significar un esfuerzo considerable por parte del encargado. Sobre todo si ocurren problemas de seguridad.

Tabla 3.2 Proyecto UNAM/CRAY de seguridad en el s.0. Unix. Diego Zamboni. Junio 1995

Es importante también analizar los costos que tendría la pérdida o acceso no autorizado a la información. Dependiendo de esta, y en su caso, de quien haga el acceso no autorizado, el efecto puede ser pérdidas monetarias, poner en peligro la seguridad nacional, la pérdida competitiva, pérdida de la confianza pública, etc.[6]

Con base a esto, las consideraciones que deben tomarse al planear la seguridad son:

- Formulación de las medidas necesarias para lograr un nivel de seguridad adecuado, es decir, en equilibrio con los niveles de riesgo.

- Justificación de las medidas de seguridad en cuanto al costo que representan.

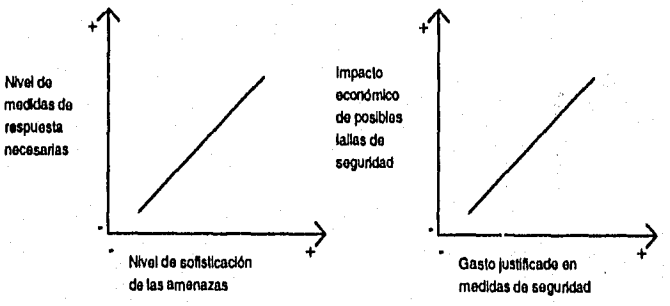

Figura 3.1 Consideraciones sobre seguridad

Así mismo es indispensable considerar que es prácticamente imposible hacer que un sistema sea totalmente seguro, debido a que no se pueden prever todas las posibles amenazas aún cuando la seguridad se incremente a niveles muy altos, ya que siempre habrá una manera de obtener acceso no autorizado (aunque esto signifique un gasto millonario y la inversión de varios años de trabajo). Pero con una planificación adecuada de la seguridad se hará posible una pronta recuperación ante una contingencia.

"El único sistema seguro es uno que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y guardias armados muy bien pagados. Aún así, no apostaría mi vida por él".

Gene Spafford

3.4 REGLAMENTACIONES SOBRE SEGURIDAD

Según lo que se ha expuesto a lo largo de la presente tesis, es clara la posibilidad de que el ciudadano quede desprotegido e indefenso ante el poder que reside en la acumulación de información personal, lo que podría dar lugar a limitar el derecho a la intimidad y a la vida privada, reconocido universalmente.

Este problema sin embargo, no solo afecta a los individuos como tales, sino también a las compañías las cuales pueden ver sus intereses afectados por un problema de esta índole.

Al respecto, los gobiernos de diversos países en el mundo han tenido que arbitrar medidas legales para protegerlos.

Algunas de estas legislaciones tienen ya varios años de funcionamiento, pero otras, están dando sus primeros pasos, y aún pasarán algunos años hasta que estén perfectamente desarrolladas y se puedan aplicar de manera efectiva.

La legislación española por ejemplo, contempla la protección de la información automatizada en el Artículo 18 Apartado 4 de la constitución:

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

Sin embargo, no obstante estos preceptos constitucionales, están pendientes aun el desarrollo de las leyes orgánicas que los definan explícitamente.

El país en el que se ha dado gran parte de la revolución computacional es los Estados Unidos de Norteamérica, de manera que también es de esperarse que sea dicho país donde se tengan los mayores avances en cuanto a reglamentaciones.

Entre ellas destacan primeramente cuatro actas o leyes básicas federales:

Acta de privacidad de 1974

Se refiere a la protección de la privacidad de los individuos cuyos datos personales figuran en bancos de datos del Gobierno Federal. Sus mandatos básicos son los siguientes:

- Prohibición de la existencia de bancos de datos secretos de información personal.
- Posibilidad del individuo de conocer que información existe acerca de él y cuál va a ser su uso.
- Posibilidad del individuo de corregir o rectificar la información registrada sobre él
- Prohibición de utilizar la información personal sin el permiso del individuo para otro propósito diferente de aquel para el que fue recopilada.
- Toda organización que recopile, use o distribuya información personal debe establecer los medios necesarios para asegurar su fiabilidad y prevenir los posibles abusos que se puedan realizar con la misma.

Acta de privacidad educacional.

Protege a la información registrada en instituciones docentes públicas. Sus puntos principales son:

- Los datos sólo pueden ser recopilados por aquellas personas u organismos autorizados por la ley.
- Los estudiantes y sus padres han de tener posibilidad de acceso a las informaciones educacionales sobre ellos.
- Solamente se permite la comunicación de esta información a las instituciones educativas públicas para usos administrativos, y a las autoridades en algunos supuestos legales.

Acta de privacidad financiera de 1978.

Proporciona protección a los individuos restringiendo el acceso del gobierno a las informaciones sobre los clientes de los bancos e instituciones financieras, estableciendo así un cierto grado de confidencialidad de los datos financieros personales.

Acta de libertad de información de 1970.

Establece el derecho de los individuos de acceder a los datos sobre ellos almacenados.

Además de las anteriores actas han sido promulgadas diversas leyes por parte de los diferentes estados en la misma línea de las anteriores, para desarrollarlas, y adaptarlas a sus ámbitos respectivos; destacando muchas de ellas por la obligatoriedad de que los datos sean relevantes, actualizados y precisos y prohibiendo su difusión sin autorización.

El Libro Naranja

El Departamento de Defensa publicó en agosto de 1983 la primera versión del Department of Defense Trusted Computer System Evaluation Criteria (Criterio de Evaluación de Sistemas de Cómputo Confiables del Departamento de Defensa), el cual fue revisado en diciembre de 1985 para dar lugar a la actual versión.

Este documento es conocido como el Libro Naranja (Orange Book), debido al llamativo color de su cubierta.

Surgió a por la necesidad que había de ofrecer una norma que permitiera cuantificar el nivel de seguridad en los sistemas de cómputo, debido a que cada organización y cada tipo de información dentro de ella, requiere de diferentes tipos de seguridad.

Así puede decirse que el Libro Naranja, establece los requerimientos que debe cumplir un sistema para poder ser calificado formalmente como confiable.

El Libro Naranja define cuatro divisiones jerárquicas de seguridad.

D Seguridad mínima
C Seguridad discrecional
B Seguridad obligatoria
A Seguridad verificable

Cada una de ellas se divide en clases numeradas, donde los números mayores indican un nivel mayor de seguridad (Tabla 3.2).

Por ejemplo, la división C contiene dos clases donde C2 ofrece mayor seguridad que C1. La división B contiene tres clases y la división A solamente contiene una.

División	Clase	Descripción
D		Protección mínima
C		Protección discrecional
	C1	Protección discrecional
	C2	Protección de acceso controlado
B		Protección obligatoria
	B1	Protección por etiquetas
	B2	Protección estructurada
	B3	Dominios de seguridad
A		Protección verificada
	A1	Diseño verificado

Tabla 3.3 Clasificación de la seguridad según el Libro Naranja.
Apuntes de Seguridad del Sistema Operativo Unix. Diego Zamboni.
Dirección General de Servicios de Cómputo Académico.

Cada clase se define por una serie de criterios que un sistema debe cumplir para obtener su clasificación. La Tabla 3.3 muestra una comparación entre las clases existentes, mostrando las características específicas que requiere cada clase y, en términos generales, cómo los requerimientos se incrementan de clase en clase.

El propósito del Libro Naranja según se define en el mismo, es lograr tres objetivos básicos:

Medición: Proveer a los usuarios con una medida de que tanto pueden "confiar" en un sistema dado, de acuerdo a su clasificación de seguridad.

Guía: Dar a los proveedores de equipo una guía para que sepan qué características incorporar en sus equipos si quieren cumplir con las especificaciones oficiales.

Adquisición de equipo: Proveer un criterio para la selección de equipo al momento de su adquisición. Una vez que un equipo ha sido certificado como perteneciente a una cierta clase, los compradores pueden estar seguros de que dicho equipo proporciona un cierto nivel mínimo de seguridad, y no tienen que revisar distintos aspectos uno por uno.

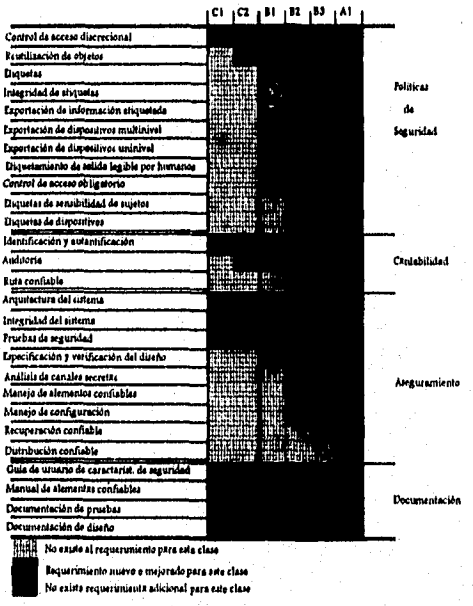

Tabla 3.4 Resumen del Criterio de Evaluación de Sistemas de Cómputo Confiables

3.5 ELEMENTOS ADMINISTRATIVOS

Para garantizar el mas alto nivel de seguridad computacional o seguridad de la información varios elementos deben estar continuamente activos y trabajar en conjunto, estos son:

- Políticas definida sobre seguridad en computación.
- Organización y división de las responsabilidades
- Políticas hacia el personal
- Seguros
- Clasificación de los datos

3.5.1 POLITICAS DEFINIDAS SOBRE SEGURIDAD EN COMPUTACION

Un requisito previo de cualquier enfoque sobre seguridad en computación consiste en definir una política clara de seguridad, sin embargo en muchas instituciones ésta se encuentra mal definida o no existe.

La seguridad depende, en ultima instancia, de la integridad de los individuos que conforman una institución. No existe una seguridad total y cada institución depende de su personal para lograr los niveles de seguridad requeridos.

Como ya se dijo anteriormente, es necesario considerar, ¿qué se quiere proteger?, ¿contra qué se quiere proteger? Y ¿cuanto tiempo, dinero y esfuerzo se está dispuesto a invertir?

No todas las instalaciones de computación tienen las mismas exigencias de seguridad, algunas son mayores que otras.

Cuando se establece el grado de riesgo, es importante considerar primero los tipos de riesgos a los que están expuestos las instalaciones de computación, por ejemplo:

- Accidentes causados por el mal manejo o negligencia
- Ataques deliberados en forma de robo, fraude sabotaje o huelgas. (expuestas en el capitulo II)

Algunas instalaciones de computación y sus aplicaciones son de alto riesgo, ya que la interrupción del procesamiento durante un periodo prolongado causa un impacto material en la institución o en la comunidad. Otras no forman parte material o integral de una organización y se pueden respaldar fácilmente por medio de procesamientos manuales. Por lo tanto, resulta evidente que no tiene sentido exagerar el nivel de los procedimientos de seguridad en las instituciones de riesgo bajo, por el contrario, donde existe un riesgo alto se debe dar protección equivalente. Sin embargo, la cuantificación del riesgo parece ser, a primera vista, un aspecto subjetivo, lo cual hace difícil su formulación en términos comerciales comunes y, en consecuencia, muchas instituciones evaden el problema o bien desisten en forma prematura a la cuantificación.

La cuantificación de los riesgos para la seguridad en las computadoras es quizá, una de las partes más importante del método que una organización adopte sobre la seguridad en computación. A menos que se cuantifiquen los riesgos, será difícil justificar después las medidas identificadas como necesarias.

En realidad, la falta de una política de seguridad cuantificada es la razón principal para que no se acepten muchas recomendaciones valiosas sobre seguridad, por parte de la gerencia.

La cuantificación de los riesgos de seguridad implica ciertos pasos:

- Clasificación general de las instalaciones en términos de riesgo alto, medio y bajo.
- Identificación de las aplicaciones que constituyen riesgos altos.
- Cuantificación del procesamiento en las aplicaciones de alto riesgo.
- Formulación de las medidas necesarias para lograr un nivel de seguridad adecuado, es decir, en equilibrio con los niveles de riesgo.
- Justificación de las medidas de seguridad en cuanto al costo que representan.[8]

A continuación se exponen detalladamente cada uno de los anteriores aspectos.

Clasificación general de las instalaciones

El primer paso consiste en establecer en términos generales si se trata de una instalación de riesgo alto, medio o bajo.

Instalaciones de alto riesgo

Las instalaciones de riesgo alto tienen las características siguientes:

- Datos o programas que contienen información confidencial de interés nacional o que poseen un valor competitivo alto en el mercado.
- Pérdida financiera potencial considerable para la comunidad a causa de un desastre o de un gran impacto sobre los miembros del publico.
- Pérdida potencial considerable para la institución y, en consecuencia, una amenaza potencial alta para su subsistencia.[8]

Todas las instalaciones de riesgo alto presentan una o más de estas características. Por tanto, generalmente resulta fácil identificarlas.

En cambio, la diferencia entre las de riesgo medio y bajo es mucho más difícil de establecer.

En la practica, no es tan importante hacerlo y lo que en realidad interesa es el impacto sobre el buen estado o la subsistencia de la empresa en caso de interrupción prolongada del procesamiento. De esta perspectiva, es posible clasificar a las instalaciones de la siguiente manera:

Instalaciones de riesgo medio:

Son aquellas con aplicaciones cuya interrupción prolongada causa grandes inconvenientes y posiblemente el incremento de los costos, sin embargo, se obtiene poca pérdida material.[5]

Un buen ejemplo de una aplicación de riesgo medio en muchas empresas es la nómina, la cual constituye una aplicación de tiempo crítico muy importante para la empresa. Si el pago es incorrecto o llega tarde, muchos empleados se sentirán agraviados, el trabajo se podrá interrumpir y quizá tenga que emplearse gran cantidad de tiempo administrativo para resolver el agravio resultante. Sin embargo, es relativamente fácil estructurar los procedimientos de apoyo para las aplicaciones de las nóminas, aunque en ocasiones esto puede implicar gastos adicionales.

Instalaciones de bajo riesgo:

Son aquellas con aplicaciones cuyo procesamiento retardado tiene poco impacto material en la institución en términos de costo o de reposición del servicio interrumpido.[8]

El procesamiento del libro mayor contable constituye un ejemplo de una aplicación de bajo riesgo, aunque en el mundo competitivo actual la necesidad del informe oportuno puede incrementar los niveles de riesgo. El libro mayor, aunque de tiempo crítico, no amenaza de manera permanente el estado de la organización, ni siquiera si el procesamiento se suspende durante tres o cuatro semanas. Por lo general, el trabajo atrasado se puede actualizar con facilidad y a bajo costo.

Aun dentro de una instalación provista de un alto nivel de seguridad, no todas las aplicaciones son de alto riesgo. Por lo tanto, resulta necesario analizar un poco mejor la seguridad, identificar las aplicaciones que implican el mayor riesgo para la institución y ordenarlas según la importancia del riesgo.

ELABORACION DE UNA LISTA DE APLICACIONES POR ORDEN DE RIESGO

Todas las aplicaciones se deben arreglar en forma tabular y en orden descendente de acuerdo con la importancia del riesgo. Es recomendable anotar los siguientes datos en cada aplicación:

- Títulos o descripción de la aplicación.
- Programas clave y naturaleza del riesgo
    - Aspectos secretos o de interés nacional.
    - Valor competitivo en el mercado debido al carácter único de los aspectos computacionales o a su escala y complejidad.[6]

INFORMACION DE LOS ARCHIVOS, TAMBIEN DE ESTA MANERA:

- Aspectos secretos o de interés nacional.
- Confidencialidad interna o valor de mercado.
- Nivel de riesgo (alta, medio o bajo) y una evaluación general sobre las consecuencias en caso de abuso o desastre.[6]

Al recabar esta información, se facilita la discusión preliminar sobre riesgos a nivel gerencial. También se facilita la identificación de las aplicaciones hacia donde se deben dirigir la mayor parte de los esfuerzos.

Cuantificación del riesgo

Este es un paso extremadamente difícil y requiere persistencia, pero se debe lograr. Su naturaleza es semejante a la cuantificación de los objetivos no financieros de una empresa. Con frecuencia, la primera reacción es que resulta imposible hacerlo, pero luego de una revisión cuidadosa y detallada se definen los objetivos cuantificables en términos de tiempo.

La experiencia indica que el método más practico para resolver el problema es comenzar por entrevistar a todos los gerentes directamente afectados por una suspensión en el procesamiento y pedirles que cuantifiquen el impacto causado por la situación. Las respuestas iniciales tal vez varíen en gran medida. Algunos mencionaran pérdidas mínimas debido a procedimientos de apoyo manuales y pérdidas altas. Pero cuando los gerentes comiencen a emitir juicios como "creo que es un gran riesgo", se les debe pedir que indiquen con mas claridad lo que quieren decir con esa frase. Esto lleva a la pregunta final que es la cuantificación del impacto. En ese momento ya se contará con una serie de expresiones cuantificadas sobre los niveles de riesgo de seguridad.

Obtención del consenso sobre niveles de riesgo

Este paso es indiscutible para lograr el compromiso de la gerencia con el nivel de riesgo definido. Se debe programar una reunión de los gerentes que corresponda, en la cual se informe sobre las expresiones sobre riesgos debidamente tabuladas, según se definieron. El propósito de la reunión será el consenso sobre los niveles de riesgo, que por lo general se representan como rangos más que como cifras absolutas.

El riesgo permite justificar de manera objetiva el costo de las medidas de seguridad.

En la etapa de revisión preliminar de la seguridad en computación, no es posible obtener todas las recomendaciones detalladas. Esto solo se logrará una vez que se lleve a cabo la revisión a fondo de la seguridad en computación, sin embargo, es posible definir la estrategia global que se debe seguir para afrontar los niveles de riesgo definidos. Esta estrategia incluye:

- Aplicaciones, programas y archivos específicos.
- Planes de detección y métodos para prevenir abusos o desastres.
- Prioridades, que son acciones que se requieren a corto plazo y los elementos que se deben considerar de manera detallada a mediano y largo plazo.[6]

Estos pasos conducen hacia la recolección y la presentación de todos los informes necesarios para una decisión bien fundada sobre los costos y los beneficios de la estrategia de seguridad en computación. Toda la información que se obtenga y las decisiones que se tomen se deben documentar de manera progresiva y esto consolidará el informe final ante la gerencia.

Es conveniente llamar a una reunión de la gerencia involucrada para evaluar tanto los hallazgos como las recomendaciones a fin de que se obtenga una decisión, y se apruebe un plan de acción destinado a la investigación y la aplicación mas detalladas. Así esta practica constituye un marco de trabajo para el método que se acepte y los niveles de costo en los cuales se incurra sin solicitudes redundantes a la gerencia.

Se ha mencionado la necesidad de consultar y comprometer a la gerencia pues ésta es, en ultima instancia, quien tome la decisión final sobre el método que se adopte y los niveles de gasto.

A menos que la gerencia haya participado en las fases anteriores, es improbable que se comprometa por completo con las decisiones que se adopten.

Para definir la política sobre seguridad, el primer problema consiste en determinar quien tiene la responsabilidad general de la seguridad en computación. Existen dos áreas que se necesitan diferenciar:

- Asuntos de riesgo comercial
- Asuntos de riesgo técnico de las computadoras.

Los asuntos de riesgo comercial son finalmente responsabilidad de la gerencia de línea. Después de un análisis final es difícil que se eluda esta responsabilidad.[6]

Los asuntos técnicos son de manera, evidente, responsabilidad de la gerencia de procesamiento de datos. Este es un modo practico de deslindar responsabilidades , pero se requiere cierta coordinación para garantizar un intercambio productivo entre las funciones comercial y técnica.

La necesidad de esta coordinación se cubre, en las grandes empresas, mediante un gerente de línea de alto nivel; esta persona pertenece, por lo general, al comité ejecutivo de la empresa.[8]

Este comité de seguridad para las computadoras se encarga entre otras cosas, de:

- Definir la asignación de responsabilidades
- Participar en la determinación de una política de seguridad
- Hacer el seguimiento de los logros e incluir la aplicación en detalle de las medidas correctoras.
- Revisar y comprobar en forma periódica la suficiencia de la seguridad en computación.[8]

Resulta útil contar con dicho comité desde el principio, cuando se revisa y define la política de seguridad en computación. Este hecho permite que los miembros correspondientes de la gerencia se comprometan desde el comienzo y, en consecuencia, se obtenga posteriormente un alto nivel de compromiso.

3.5.2 ORGANIZACION Y DIVISION DE LAS RESPONSABILIDADES.

La forma en que se organizan las actividades de computo incluye cuatro aspectos que afectan la seguridad en computación:

- División de responsabilidades
- Sistemas de control interno.
- Asignación de responsabilidad en cuanto a la seguridad.
- Sustitución del personal clave.

Cada uno de estos aspectos los exponemos a continuación de manera separada:

A. DIVISION DE RESPONSABILIDADES

Dentro de cualquier empresa, la división de responsabilidades permite lograr la revisión y los balances sobre la calidad del trabajo. Dentro del contexto de computación hay varios recursos que mejoran la calidad del control gerencial y, con ello, la seguridad.

El personal que prepara los datos no debe tener acceso a las actividades de operación.

Los analistas de sistemas y los programadores no deben tener acceso a las actividades de operación y viceversa.

Los operadores no deben tener acceso irrestricto a las funciones de protección de información o departamentos donde se localicen los archivos maestros.

Los operadores no deben tener los controles únicos del procesamiento del trabajo y se les debe prohibir que inicien las correcciones de los errores.

Existe un margen amplio de actividades que se pueden organizar para dar cabida a este tipo de divisiones en el trabajo. Los elementos clave de este criterio constituyen funciones claramente definidas y autónomas.

En el contexto de las actividades de computación, estas funciones clave son:

- Desarrollo de los sistemas
- Programación
- Mantenimiento de programas
- Preparación de los datos
- Operaciones centrales y remotas
- Control
- Preservación de los archivos.[8]

Las divisiones del trabajo también se deben aplicar a los procedimientos del usuario. Esto se realiza tradicionalmente a nivel de la aplicación. Con frecuencia, dentro del departamento de computación, se encuentra una resistencia fuerte contra la aplicación de una división efectiva de las responsabilidades sobre la base de que los procedimientos inhiben la flexibilidad y obstaculizan la eficiencia general.

Las medidas mínimas de seguridad reducirán la flexibilidad en el trabajo pero, mediante el diseño meticuloso, no se afectara la eficiencia. Muchas veces no se consulta con el personal afectado cuando se diseñan las divisiones del trabajo. En consecuencia, las personas no se comprometen con las medias y se pueden sentir muy desmotivadas. Esta situación genera un aumento del riesgo en la seguridad y se puede evitar fácilmente mediante la reflexión previa.

Los dos elementos clave que sirven de base para las divisiones subsecuentes de responsabilidad, son: las funciones de control y de archivo.[8]

Resulta conveniente que estas funciones sean autónomas y se adscriban a la autoridad más alta que se pueda, de preferencia al gerente del departamento de procesamiento de datos.

En algunas instalaciones, la función de control es reducida y se limita solo a los controles del procesamiento. En otras, tiene un alcance amplio y abarca las funciones de archivo, la responsabilidad de seguimiento de otras funciones como la documentación de los sistemas, la programación y las operaciones, los puntos de enlace clave de diferentes funciones y el mantenimiento de los sistemas existentes.

El grado de división entre las diferentes funciones depende del nivel de seguridad que la instalación requiera. La consideración prioritaria es la independencia de la función de control y el manejo de esta actividad por parte del personal preparado para afrontar las exigencias que se le harán.[8]

B. SISTEMAS DE CONTROL INTERNO

La división de responsabilidades y los sistemas de verificación interna se combinan para formar el sistema de control interno de una institución.

Los sistemas de verificación interna se definen como: "Las comprobaciones de evidencia que prueban que se realiza la recolección de datos de forma completa y precisa y que se trabaja de acuerdo con las divisiones de responsabilidades y de jerarquía."[8]

La típica verificación documentada de evidencias requiere que:

- Las modificaciones de los programas se autoricen y se prueben en forma adecuada.

- Se documente de manera adecuada y progresiva a los sistemas nuevos a través del trabajo para la producción.
- Los departamentos originadores documenten y verifiquen apropiadamente los datos de los archivos, tanto registros nuevos como corregidos, contra impresos que sean editados en la computadora.
- Los datos de entrada se agrupen y revisen de acuerdo con datos aceptados para procesamiento.
- Se documenten los errores y se autoricen y comparen las correcciones de los mismos con el material impreso por la computadora.

Los auditores internos y externos participan también en la verificación que hay en una empresa para el control interno y estos deben:

- Revisar la división de responsabilidades y los procedimientos para garantizar que estén correctos.
- Realizar pruebas que garanticen el cumplimiento de los procedimientos o sistemas de control interno predeterminados.

C. ASIGNACION DE RESPONSABILIDADES EN CUANTO A LA SEGURIDAD

En la descripción de las labores, tanto de la gerencia comercial como la de computación, es importante especificar esta responsabilidad. La seguridad es una área clave de resultados o de acción.

Un factor crítico para el éxito de la seguridad, es la gente. La organización y division de responsabilidades también debe adoptarse en esta área.

La organización que tenga esta área, se determinará por el tipo de gentes que se encargarán de las funciones de seguridad y que idealmente son:

- Supervisor de seguridad
- Oficial de seguridad
- Auditor de seguridad
- Analista de seguridad
- Coordinador de seguridad de la red

El siguiente cuadro muestra la distribución de la función del área de seguridad entre sus recursos humanos:

Funciones	Organización				
	Supervisor seguridad	Oficial seguridad	Auditor seguridad	Analista seguridad	Coordin seg RED
Análisis de riesgos	x	x	x	x	x
Evaluación de los servicios de seguridad	x	x			
Evaluación de las soluciones del dominio de seguridad	x	x			
Alarmas, acciones y reportes			x	x	x
Protección de los sistemas de admon de la red.	x			x	

SUPERVISOR DE SEGURIDAD

- Evaluar los riesgos de seguridad
- Preparar los planes de seguridad
- Supervisar los procedimientos de evaluación de las bitácoras de seguridad
- Asistir en la definición de límites para determinar una violación de seguridad
- Asistir en la elaboración de planes de seguridad para el sistema de administración de la red
- Establecer el programa educacional para su personal
- Supervisar los procesos de selección de productos

OFICIAL DE SEGURIDAD

- Evaluar los riesgos de seguridad
- Supervisar la seguridad en tiempo real
- Dictar las acciones contra los intrusos
- Ayudar en la evaluación de las bitácoras de vigilancia
- Ayudar en la elaboración de los planes de seguridad
- Supervisar la seguridad del sistema de administración de la red
- Administrar los pasaportes
- Ayudar en la selección de instrumentos

AUDITOR DE SEGURIDAD

- Evaluar las bitácoras de vigilancia
- Ayudar en la estimación de riesgos de seguridad
- Ayudar en el establecimiento de límites para determinar una violación a la seguridad
- Categorizar los riesgos de seguridad
- Ayudar a encontrar la mezcla correcta de precauciones físicas y lógicas

- Auxiliar en la selección de instrumentos
- Escribir los reportes de avance de los planes de seguridad

ANALISTA DE SEGURIDAD

- Definir las funciones de monitoreo y vigilancia
- Evaluar y seleccionar los servicios del área de seguridad
- Evaluar el impacto de las técnicas de seguridad en el desempeño de la red
- Construir la matriz de amenazas
- Recomendar instrumentos durante el proceso de selección de los mismos
- Supervisar la instalación de instrumentos
- Personalizar pasaportes y autorizaciones al control de acceso
- Programar los instrumentos
- Establecer procedimientos para asegurar el sistema de administración de la red

COORDINADOR DE LA SEGURIDAD DE LA RED

- Realizar el seguimiento del inventario y mantenimiento del directorio de la red
- Controlar la configuración de la seguridad en la red
- Controlar las autorizaciones de acceso a las aplicaciones, servidores, gateways, routers, bridges y firewalls de la red
- Revisar las bitácoras de vigilancia para estaciones y servidores de la red
- Administrar los pasaportes locales
- Educar a los usuarios en las técnicas y productos del dominio de seguridad
- Asistir en la toma de acciones contra los intrusos

D. SUSTITUCION DEL PERSONAL CLAVE

Un elemento que es esencial para la seguridad en computación consiste en garantizar que todo el personal clave tenga una sustitución adecuada. En la práctica no es posible asegurar la sustitución de todo el personal, por lo que se necesita restringir en forma cuidadosa la definición de personal clave. Se debe poner especial atención al evaluar la importancia del personal relacionado con la programación de las aplicaciones o de los sistemas de carácter avanzado.

Con frecuencia se argumenta el costo cuando se plantea el problema de la sustitución. Muchas instalaciones se justifican basándose en que el personal no es adecuado. Así, los niveles de costo no contemplan la sustitución. Si la instalación requiere medidas de seguridad de alto nivel, entonces los niveles de gasto deben contemplar la sustitución y el apoyo adecuados para los puestos clave.

3.5.3 POLITICAS HACIA EL PERSONAL

La mayoría de las instituciones han tomado conciencia de la creciente dependencia en la integridad, estabilidad y lealtad del personal y dedican mayor a esta área de la seguridad en computación.

La contratación de personal inapropiado para puestos de gran responsabilidad, como las operaciones y el control, no es raro y necesariamente aumenta el riesgo de accidentes.

Se revisarán cinco áreas:

- Políticas de contratación
- Procedimientos para evaluar el desempeño
- Políticas sobre permisos
- Rotación de puestos
- Actitudes del personal

A. POLITICAS DE CONTRATACION

Casi todas las instituciones cuentan con un procedimiento de contratación bien estructurado y de rutina; sin embargo, en muchos casos éste se aplica con demasiada flexibilidad. Desde el punto de vista de la seguridad, las características mas importantes de una política de contratación son:

- Verificación de referencias y antecedentes de seguridad.
- Pruebas psicológicas
- Exámenes médicos[8]

B. PROCEDIMIENTOS PARA EVALUAR EL DESEMPEÑO

Las actividades para evaluar el desempeño pueden cooperar con la seguridad en forma rutinaria. Aunque en primera instancia están destinadas a valorar la efectividad de los procesos administrativos y de trabajo, pueden colaborar con la efectividad de la seguridad. Al mismo tiempo, la evaluación del desempeño puede servir también para evaluar las actitudes hacia el trabajo y los sentimientos generales hacia la institución.

En las instalaciones de alta seguridad resulta muy valioso que los gerentes revisen de manera más frecuente las actitudes y el comportamiento del personal bajo su cargo.

C. POLITICAS SOBRE PERMISOS

El sobre tiempo excesivo es común en las instalaciones de computo. Al mismo tiempo, los permisos rara vez están reglamentados debido al nivel clave de los cargos del personal.

La reglamentación de los permisos es importante para asegurar que el personal expuesto al estrés descanse periódicamente de manera apropiada.

En todos los demás departamentos de una organización, los permisos se hallan reglamentados, en especial para los puestos de confianza. Este es también un buen sistema para detectar robos, fraudes y planes de sabotaje en potencia. La importancia y dependencia en el personal clave no debe obstruir la reglamentación de esta política en la función del procesamiento de datos.

D. ROTACION DE PUESTOS

La rotación de puestos constituye un buen antagonismo de fraudes, en especial cuando se trata del personal de puestos altos en confianza. Este principio también se aplica al personal de cómputo.

Se debe tener en cuenta que existe una desventaja propia de la rotación de puestos, sobre todo en un ambiente de alta seguridad. Esto es que un solo individuo tiene acceso a las actividades de un frente muy

amplio. Sin embargo, la rotación de los puestos es mas recomendable en los niveles de responsabilidad medio y bajo , donde esa situación no se presenta. Aún así, las ventajas de la rotación generalmente sobre pasan cualquier posible desventaja.

E. EVALUACION DE LAS ACTITUDES DEL PERSONAL

No es probable que un empleado bien motivado sea desleal. De igual manera la posibilidad de que surjan brechas en la seguridad debido a accidentes o ataques deliberados es mas alta en un ambiente donde la motivación es baja.

En muchas instalaciones, especialmente las de mayor tamaño, resulta difícil vigilar las actitudes todo el tiempo. El uso de encuestas sobre actitudes puede ser un instrumento valioso para el seguimiento de rutina en este aspecto de la política hacia el personal.

3.5.4 LOS SEGUROS

Los seguros existen desde hace mucho tiempo, provisto de criterios y prácticas bien definidas. Sin embargo, cualquier institución que busque asesoramiento y orientación sobre cobertura de sus riesgos de computación, corre el riesgo de enfrentar dificultades considerables. Existen dos problemas principales:

La existencia de un gran vacío en la comunicación: en general, los aseguradores saben mucho sobre riesgos comerciales pero muy poco acerca de computadoras, mientras que el personal de cómputo conoce poco acerca de seguros y mucho cobre computadoras.

No hay un entendimiento cabal respecto a los riesgos y sus consecuencias, debido a que la profesión computacional es reciente y a que los antecedentes en relación con las reclamaciones sobre seguros son pocos. [8]

El resultado de lo anterior es que muy pocos usuarios de computadoras gozan de una cobertura adecuada para todos los riesgos. La tendencia es cubrir una o dos áreas de riesgo evidente, como la reposición del equipo o contra los incendios. Otras áreas como el costo de la recaptura de datos o el límite de responsabilidad ante esta pérdida, casi siempre se pasan por alto.

Existen tres aspectos en particular:

- Las áreas de riesgo asegurables
- Los servicios de seguros especializados
- El cambio del tipo de riesgo.

A. AREAS DE RIESGO ASEGURABLES

La National Computing Centre(NCC), publico un material excelente llamado Computer Guide 7: Insuring a Computer System, el cual comprende las principales áreas de riesgo:

- Ambiente
- Equipo
- Programas y datos
- Interrupción comercial y su recuperación
- El personal
- Responsabilidades a terceras personas

B. SERVICIOS DE SEGURO ESPECIALIZADOS

En la actualidad, ciertas instituciones ofrecen servicios especializados para usuarios de computadoras. Estos servicios incluyen la adopción de personal altamente capacitado en el manejo de computadoras y, en consecuencia de los riesgos inherentes. Además varias compañías internacionales de seguros cuentan ahora con pólizas especializadas para usuarios de computadoras.

Normalmente una póliza de seguro de equipo de cómputo cubre:

- Daños materiales al equipo

  Ampara cualquier pérdida o daño físico, súbito e imprevisto de tal forma que necesitara reparación o reemplazo. Excluye:

  - Pérdidas o daños causados por terremoto, temblor, maremoto, erupción volcánica, ciclón, tifón o huracán.
  - Pérdidas o daños causados por hurto o robo sin violencia
  - Pérdidas o daños causados por fallo e interrupción en el suministro de corriente eléctrica, de gas o de agua
  - Pérdidas o daños que sean consecuencia del uso continuo o deterioro gradual debido a condiciones atmosféricas.

  Sin embargo este tipo de exclusiones se pueden prever mediante la contratación expresa de otra póliza.

- Portadores externos de datos

  Cubre al indemnización sobre daños causados a dispositivos de almacenamiento de datos así como la información contenida en éstos.

Excluye, cualquier gasto resultante de la falsa programación, perforación, clasificación, inserción, anulación accidental de informaciones, pérdidas de información causada por campos magnéticos y virus informáticos.

- Incremento en el costo de operación

Esta cobertura se aplica si un daño material indemnizable diera lugar a una interrupción parcial o total de la operación lo que causara un desembolso adicional al usar un centro de cómputo ajeno y/o suplente.

Los seguros a los equipos de cómputo, se aplican a los bienes que estén operando o en reposo, desmontados para propósitos de limpieza o reparación o durante su traslado dentro del predio establecido en la póliza.

Generalmente excluyen los daños causados por:

- Guerra, invasión, actividades de enemigo extranjero, hostilidades (con o sin declaración de guerra, guerra civil, rebelión, revolución, insurrección, motín, tumulto, huelga, paro decretado por el patrón, conmoción civil, poder militar o usurpado, conspiración, etc).

- Reacción nuclear, radiación nuclear o contaminación radiactiva.
- Acto intencional o negligencia manifiesta del asegurado o de sus representantes.

Sin embargo existen algunas pólizas adicionales que pueden contratarse y que cubren lo siguiente:

- Huelgas, alborotos populares y conmoción civil
- Gastos extraordinarios y flete expreso
- Gastos por flete aéreo
- Daños por fallo de la instalación de climatización
- Robo sin violencia (hurto)
- Equipos móviles y portátiles fuera de los predios señalados
- Cláusula de terremoto y erupción volcánica
- Cláusula de huracán, ciclón y tifón
- Daños o pérdidas debido a incendio, rayo, explosión, aviones, vehículos y humo.
- Daños mecánicos y eléctricos internos
- Equipos de climatización.

Es importante contar con un seguro que cubra no solo el hardware y software, sino también la construcción. Se deben revisar y evaluar las diferentes alternativas de seguro que ofrecen las compañías dedicadas a este rubro. También se debe considerar que las sumas aseguradas deben ser igual al costo de reparación o reposición del bien asegurado, así como el tiempo en que se recibirá el reemplazo o indemnización del bien por parte de la compañía de seguros.

C. SEGUIMIENTO DE LOS CAMBIOS EN LOS RIESGOS

Los riesgos asegurables cambian en forma progresiva dentro de la institución como un todo y en el interior de sus actividades de cómputo. Es importante garantizar que los nuevos riesgos se encuentran cubiertos y que las pólizas estén actualizadas.

Un método valioso es la formación de un comité de seguridad de computo, sus objetivos serían:

- Identificar y cuantificar los riesgos directos y consecuentes de la instalación de computo en la empresa.
- Garantizar que la cobertura se revise para tomar nota de los incrementos en los costos o en los precios de reproducción.
- Garantizar la existencia de los planes de contingencia adecuados, en especial cuando no se puede obtener la cobertura del seguro.
- Asegurar que la pérdida consecuente se excluya de las responsabilidades de la institución hacia terceras personas.
- Obtener asesoría y orientación especializadas cuando se requiera.[8]

Además, el comité debe contar con representantes de las siguientes dependencias:

- La gerencia de procesamiento de datos,
- La compañía de seguros.
- Los gestores de seguros.
- El departamento de control secretarial o financiero.
- La auditoria interna o la externa.

Por medio de las reuniones periódicas, cuatrimestrales a anuales, según el tamaño de la institución, es posible asegurar que la cobertura de riesgos esta claramente identificada y actualizada.

3.6 CLASIFICACION

3.6.1 SEGURIDAD FISICA

Las técnicas de seguridad física implican medidas que tienen como objetivo mantener la información, el equipo, las instalaciones, y el personal del centro de procesamiento de datos, libre de todo riesgo, evitando interrupciones en las operaciones (debido a contingencias ya sean naturales, accidentales o deliberadas), y en caso de una ocurrencia, seguir con un medio de emergencia hasta que el servicio sea restaurado.

Incluyen también las precauciones que deben tomarse referentes al material y construcción del edificio del centro de cómputo, así como la ubicación del mismo.

Entre los aspectos a considerar dentro de la seguridad física se tienen:

a) Ubicación Física y Disposición del Centro de Cómputo

b) Instalaciones Físicas del centro de cómputo.

c) Control de Acceso Físico

d) Suministro de Energía

e) Aire Acondicionado

f) Protección, detección y extinción de incendios

g) Protección contra inundaciones

h) Mantenimiento

A. UBICACION FISICA Y DISPOSICION DEL CENTRO DE COMPUTO

Anteriormente se acostumbraba ubicar los equipos de cómputo en un lugar visible con grandes ventanales y constituían el orgullo de la organización, por lo que se consideraba necesario que estuviera a la vista del público.

Esto ha cambiado de manera radical, principalmente por el riesgo de terrorismo o sabotaje, y hoy en día, la ubicación de centros de cómputo se ha vuelto cada vez más clandestina y conservadora.

Las computadoras deben colocarse lejos de aeropuertos, equipos eléctricos tales como radares y equipos de microondas, zonas urbanas de escasos recursos, áreas de alto tráfico, etc. El objetivo es mantenerlas tanto como sea posible lejos de cualquier tipo de amenaza.

En la medida que sea posible, el centro de cómputo no debe contener señal alguna que lo identifique como tal a los externos.

Incluso se recomienda que el sistema de cómputo sea construido en un edificio separado, de forma que facilite el control de acceso y disminuya el riesgo.

Entre los aspectos que deben considerarse al planear la ubicación física del centro de cómputo, están los riesgos concernientes a desastres naturales, inundaciones, fuego, fallas eléctricas, polvo, etc. Así como la luz solar; si la exposición es muy fuerte, debe evitarse el uso del vidrio, en los casos en que esto no sea posible, pueden utilizarse persianas externas.

En los sitios donde la información es altamente sensitiva. Debe tomarse en cuenta también el riesgo producido par las emanaciones

electromagnéticas o acústicas del hardware, ya que éstas pueden ser interceptadas con relativa facilidad en una distancia menor a los 300 metros. Para ello, una opción es la separación de los dispositivos de los puntos potenciales de intercepción.

B. INSTALACIONES FISICAS DEL CENTRO DE COMPUTO.

Es importante considerar las características físicas que deben tener las instalaciones para proporcionar seguridad. Entre ellas podemos mencionar las siguientes:

1.- Piso falso

Se debe tener en cuenta la resistencia para que soporte el peso del equipo y personal. Entre otras consideraciones están:

- Sellado hermético.
- Modularidad precisa, que los cuadros ensamblen perfectamente.
- Nivelado topográfico.
- Permita cambios en la situación de unidades.
- Aterrizado para evitar cargas electrostáticas. [9]

2.- Cableado

El cableado en el cuarto de computadoras es un punto vital. Debe procurarse que todo el cableado quede por debajo del piso falso, donde es importante ubicar los cables de forma que se aparten:

- Los cables de alto voltaje para la computadora
- Los cables de bajo voltaje conectados a las unidades de las computadoras
- Los cables de telecomunicación
- Los cables de señales para dispositivos de monitoreo o detección (fuego, temperatura, humedad, etc).

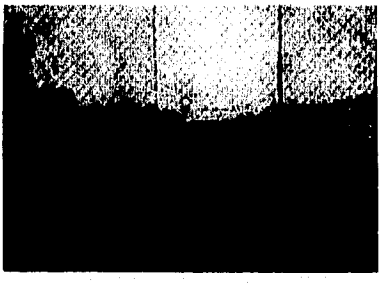

Fig. 3.2 Cableado bajo el piso falso

Las tapas de los cuadros que conforman el piso falso, deben ubicarse al menos 10 cm sobre el piso, de forma que un corto circuito, o algún otro daño se evite en el caso de alguna filtración.[9]

3.- Paredes y techo

- Las paredes irán con pintura plástica lavable para poder limpiarlas fácilmente y evitar la erosión.
- El techo real deberá pintarse, así como las placas del falso techo y los amarres si éste se emplea como plenum para el retorno del aire acondicionado.
- Es mejor usar placas metálicas o de madera prensada que el yeso.
- La altura libre entre el falso suelo y falso techo, debe estar entre 2,70 y 3,30 metros para permitir la movilidad del aire.[9]

4.- Puertas

- Las puertas del local serán de doble hoja y con una anchura total de 1.40 a 1.60 cm.
- Es necesaria una salida de emergencia
- Tener en cuenta las dimensiones máximas de los equipos. [9]

5.- Iluminación

- Los reactores deben estar fuera de la sala, ya que generan campos magnéticos, o en su caso deben aislarse.
- La iluminación no debe alimentarse de la misma acometida que los equipos de cómputo. [9]

6.- Filtros.

- Se requieren filtros con una eficiencia del 99% sobre particulas de 3 micrones.
- Si hay contaminantes elegir los filtros adecuados.
- El aire de renovación o ventilación será tratado tanto en temperatura y humedad como en filtrado antes de entrar en la sala

7.- Vibración.

Si hay vibraciones superiores a las normales, es necesario estudiarlas antes de colocar los equipos y utilizar los dispositivos antivibratorios necesarios, ya que esto podría dañar el equipo. [9]

C. CONTROL DE ACCESO FISICO

El principal elemento de control de acceso físico involucra la identificación positiva del personal que entra o sale del área bajo un estricto control. Si personas no autorizadas no tienen acceso, el riesgo se reduce.

Los controles de acceso físico varían según las distintas horas del día. Es importante asegurar que durante la noche sean tan estrictos como durante el día. Los controles durante los descansos y cambios de turno son de especial importancia.

Estructura y disposición del área de recepción:

En las áreas de alta seguridad donde se necesita considerar también la posibilidad de ataque físico. Se debe identificar y admitir tanto a los empleados como a los visitantes de uno en uno. También se pueden utilizar dispositivos magnéticos automáticos y otros recursos en el área de recepción. Si es necesario usar vidrio en la construcción de esta área, debe ser de tipo reforzado.

Acceso de terceras personas:

Dentro de las terceras personas se incluye al personal de mantenimiento, los visitantes, y el personal de limpieza. Estos y cualquier otro personal ajeno a la instalación deben ser:

- Identificados plenamente.
- Controlados y vigilados en sus actividades durante el acceso.

El personal de mantenimiento y cualquier otro personal ajeno a la instalación se debe identificar antes de entrar a ésta. El riesgo que proviene de este personal es tan grande como el de cualquier otro visitante.

IDENTIFICACION DEL PERSONAL

Algunos parámetros asociados típicamente a la identificación del personal son:

Algo que se porta

Consiste en la identificación mediante algún objeto que porta tal como, tarjetas magnéticas, llaves o bolsas. Por ejemplo, las bolsas pueden incluir un código magnético, estar codificadas de acuerdo al color (rojo para los programadores, azul para los analistas, etc), e inclusive llevar la foto del propietario.

Un problema con esta técnica, sin embargo, es la posibilidad de que el objeto que se porta sea reproducido por individuos no autorizados. Es difícil pero no imposible reproducir una tarjeta con código magnético. Es por esto que usualmente esta técnica se utiliza en conjunción con otros identificadores para proveer una identificación positiva.

Algo que se sabe

Implica el conocimiento de algún dato específico, este puede ser, el número de empleado, algún número confidencial, contraseña o combinación.

Alguna característica física especial.

En este paso la identificación se realiza en base a una característica física única. Estas características se dividen en dos categorías:

1. Neuromuscular: tales como firma o escritura.
2. Genética: tales como la geometría del cuerpo (mano, iris, retina, etc), huellas digitales, reconocimiento de patrones de voz, apariencia facial, impresión de las huellas de los labios, patrones de ondas cerebrales, etc.[6]

Por ejemplo: La utilización de las huellas digitales ha mostrado ser una característica de identificación positiva. Inicialmente se realiza un registro holográfico de las huellas digitales. Entonces, cuando un individuo pone sus huellas en un verificador, éste a través de una luz láser realiza un nuevo registro. Si ambos registros coinciden, el individuo ha sido identificado.

Así mismo pueden utilizarse los siguientes elementos:

1.- Guardias y escoltas especiales.

Los cuales pueden ser ubicados en lugares estratégicos donde exista más vulnerabilidad. Es recomendable que todos los visitantes que tengan permiso para recorrer el centro de cómputo sean acompañados de una persona designada como escolta.

2.- Registros de Firma de entrada y de salida.

Consiste en que todas las personas que entren al centro de cómputo, firmen un registro que indique la hora de entrada, el motivo por el que entran, y la hora de salida.

FECHA	NOMBRE	PROCEDENCIA	DEPTO QUE VISITA	PERSONA QUE BUSCA	ASUNTO	HORA DE ENTRADA	FIRMA	HORA DE SALIDA	FIRMA

Fig. 3.3 Forma de registro de entrada y salida.

3.- Puertas con chapas de control electrónico.

Ya sea que tenga que teclearse un código para abrirla, disponer de una tarjeta con código magnético, o que tenga implementado algún dispositivo para el reconocimiento de alguna característica física especial tal como la huella digital, la geometría de la mano, etc.

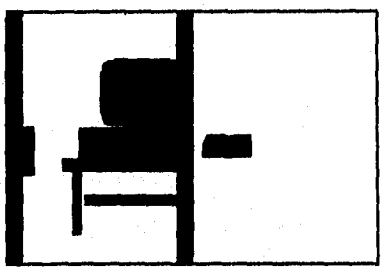

Fig. 3.4 Puerta con chapa de control electrónico

4.- Tarjetas de acceso y gafetes de Identificación.

Puede tratarse de simples gafetes que identifiquen a la persona, hasta tarjetas con código magnético que permiten abrir la puerta. Así

mismo, los dispositivos de lectura de las tarjetas pueden ser conectados a una computadora que contenga información sobre la identidad del propietario. La autorización puede manejarse individualmente para cada puerta, y controlarse aspectos como la hora y día en que estas funcionan. Así la actividad puede monitorearse, y cualquier intento de entrar que no sea autorizado será detectado.

5..- Entradas de doble puerta.

De forma que la entrada a través de la primera puerta, deja una área donde la persona queda atrapada y fuera de las facilidades de la computadora. Una segunda puerta debe ser abierta para entrar al centro de cómputo.

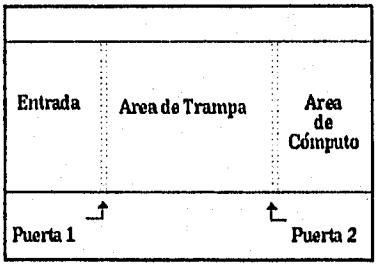

Fig. 3.5 Mecanismo de entrada de doble puerta

6.- Equipos de monitoreo.

La utilización de dispositivos de circuito cerrado de Televisión, tales como monitores, cámaras y sistemas de intercomunicación conectados a un panel de control manejado por guardias de seguridad,

permiten controlar áreas grandes concentrando la vigilancia en los puntos de entrada y salida principalmente.

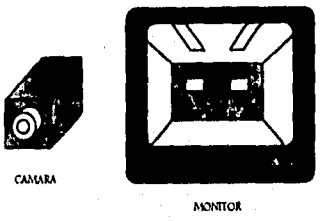

Fig. 3.6 Dispositivos para monitoreo.

6.- Alarmas contra robo.

Todas las áreas deben estar protegidas contra la intrusión física, las alarmas contra robo, las armaduras y el blindaje se deben usar, hasta donde sea posible, en forma discreta, de manera que no se atraiga la atención sobre el hecho de que existe un dispositivo de alta seguridad. Tales medidas se deben aplicar no sólo en el área de cómputo, sino también en las áreas adyacentes. La construcción de puertas y ventanas debe recibir especial atención para garantizar su seguridad.

7.- Trituradores de papel.

Los documentos con información confidencial nunca deben ser desechados en botes de basura convencionales. En muchos casos los espías pueden robar la información buscándola en estos lugares. Es por ello que dichos documentos deben ser desmenuzados o triturados antes de desecharlos.

Existen dispositivos que desintegran el papel convirtiéndolo en pedacitos o confeti los cuales no pueden ser reconstruidos.

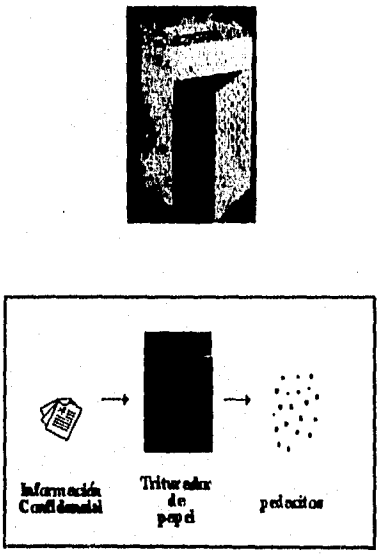

Figura 3.7 Triturador de papel.

D. SUMINISTRO DE ENERGIA.

El suministro de energía para los equipos y el aire acondicionado, es muy importante.

En las instalaciones de alto riesgo, especialmente las que cuentan con procesamiento en línea o en tiempo real, el suministro de respaldo es imprescindible.

Así mismo, éste puede ser necesario para los sistemas conectados en red y con terminales. No es posible apoyar todos los componentes de la red, pero se debe poner alención cuidadosa a los elementos claves de ella.

> Para una minicomputadora que consume electricidad en el rango de 3 a 8 kWatts, se utiliza una batería aproximadamente del tamaño de un gabinete de TV, mientras que un centro de cómputo más grande que consume de 300 a 500 kWatts, requiere de una estación en un cuarto separado de aproximadamente 400 pies^2. Esto para respaldar la capacidad eléctrica por aproximadamente 20 minutos.[10]

Para proporcionar energía eléctrica por más de este tiempo, es necesario instalar un generador eléctrico (normalmente de diesel), que permita que el equipo siga trabajando mientras no se restablezea el servicio.

Sin embargo, la continuidad en el suministro de energía eléctrica, no es el único aspecto. La estabilidad es lo más importante. En las áreas adyacentes a los sitios industriales o a grandes complejos de oficinas, las variaciones de voltaje, son un problema frecuente. Estas variaciones pueden dañar los datos almacenados, los programas o el equipo, por lo

que se debe instalar un equipo regulador donde se presenten con frecuencia estos problemas.

> Además, hay que considerar que no todos los países manejan los mismos estándares para el suministro de energía eléctrica; esto es que las características de voltaje, frecuencia de onda y corriente son diferentes. Por ejemplo, el estándar europeo maneja 50 Hertz, mientras que en E.U.A. y México se manejan 60 Hz. Por lo tanto, en este caso, si el equipo fué fabricado en un país europeo, para utilizarlo en México, se requiere un convertidor que convierta la frecuencia de salida de 50 Hz a 60 Hz.[10]

Por otro lado hay que considerar que las líneas eléctricas sean aterrizadas conforme a las especificaciones de los fabricantes, y que incluso algunos de ellos recomiendan que las computadoras y los periféricos se conecten en líneas separadas.

E. AIRE ACONDICIONADO

Aun cuando el aire acondicionado es indispensable en un centro de cómputo, suele ocasionar graves problemas; las fluctuaciones o los desperfectos de consideración en éste, pueden ocasionar incluso que las computadoras tengan que ser apagadas.

Además en muchas ocasiones, las instalaciones de aire acondicionado son una fuente de incendios muy frecuentes y también son muy susceptibles al ataque físico, especialmente a través de los ductos.

Para poder afrontar estos riesgos se requiere lo siguiente:

- Instalar equipos de aire acondicionado de respaldo donde ya se hayan establecido las aplicaciones de alto riesgo.

  En centros de cómputo grandes, los intercambiadores de calor y torres de enfriamiento son a menudo ubicados en las azoteas, y dentro del cuarto de computadoras estarán las tuberías, válvulas, bombas, unidades de enfriamiento, y otros equipos relacionados. También es recomendable instalar unidades modulares de forma que los componentes se puedan reemplazar fácilmente.

- Instalar redes de protección en todo el sistema de ductos al interior y exterior.
- Instalar extinguidores y detectores de incendios en los ductos.
- Instalar monitores y alarmas para humedad, temperatura y flujo de aire efectivos.[8]

Aun cuando el equipo de aire acondicionado funcione adecuadamente, la habilidad de regular y dirigir el flujo de aire, representa otra dificultad ya que difícilmente alguien trabajará a gusto, si la corriente de aire es muy fuerte.

Otro aspecto referente a los sistemas de aire acondicionado, es el efecto del polvo. las entradas de aire fresco no deben estar al nivel del suelo y deben ubicarse lejos de las áreas donde haya polvo. Deben utilizarse los filtros adecuados para proporcionar aire limpio al centro de cómputo.[10]

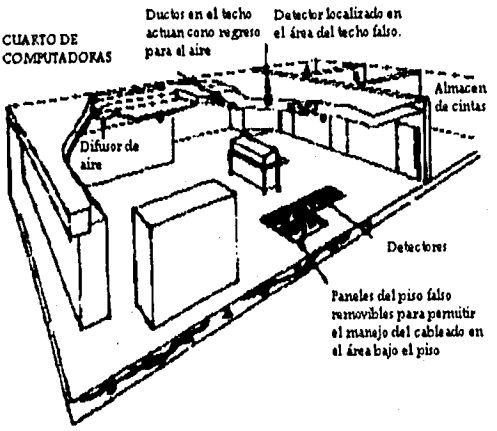

Fig. 3.8 Aire Acondicionado.

F. PROTECCION, DETECCION, Y EXTINCION DE INCENDIOS

Existen considerables métodos y aparatos para detectar incendios. Sin embargo, no es objeto de esta tesis describirlos detalladamente, sólo puntualizar algunos elementos de especial importancia.

La protección contra el fuego es lograda de una mejor manera a través de una correcta construcción del edificio (el cual debe procurarse sea resistente al fuego). Sin embargo, siempre habrá materiales combustibles y equipo dentro del edificio, así que es necesario asegurar que el equipo contra incendios, esté disponible de forma inmediata, y que se pueda controlar el fuego con relativa facilidad.

Un punto a enfatizar es la importancia de escoger detectores de fuego y humo, de alta calidad, capaces de detectar distintos tipos de gases que desprendan los cuerpos en combustión. Algunos no detectan el

humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y, en consecuencia, los incendios producidos por un corto circuito tal vez no se detecten.

Estos detectores deben ubicarse en un número adecuado, y cuidadosamente en relación con los aparatos de aire acondicionado, ya que los conductores de éste puede difundir el calor o el humo y no permitir que se active el detector. Generalmente se instalan en la sala de cómputo, junto a las áreas de oficinas y en el perímetro físico de las instalaciones. Es necesario colocar detectores de humo y calor bajo el piso, en los ductos de aire acondicionado y arriba del techo.

Las alarmas contra incendios por su parte, deben estar conectadas con la alarma central del lugar, o bien directamente al departamento de bomberos.

Por otro lado, es importante que estas mismas medidas de detección, se apliquen también a las áreas adyacentes al centro de cómputo.

Es importante establecer lugares especiales de almacenamiento para las cintas y los discos magnéticos (preferiblemente fuera del cuarto de computadoras y protegidos contra fuego), así como para la documentación de los sistemas, la programación y las operaciones que también requieren de protección contra incendios.

Establecer procedimientos de respaldo que garanticen la actualización de todos los programas, archivos y documentación como rutina y que las copias de seguridad se almacenen en un lugar lejano.

Los sistemas de extinción del fuego son esenciales si el área contiene algo valioso, si hay equipo importante, o si se están protegiendo

funciones vitales de la compañía. Tales sistemas son destinados a detectar y suprimir el fuego dentro de los primeros segundos, reduciendo así la dependencia contra las técnicas manuales las cuales pueden llegar demasiado tarde.

En la mayoría de las instalaciones se utiliza algún gas como extintor, sin embargo existen también extintores de espuma, de agua o de polvo seco (ver tabla 3.5).

El uso del bióxido de carbono en algún tiempo generalizado, debe reservarse, debido al efecto letal que tiene sobre los humanos.

Es por esto que en la actualidad los sistemas de control de fuego utilizan preferiblemente Halón 1301 como agente de extinción. Este gas y el número 1301 indican que su fórmula es 1 parte de carbón, 3 partes de fluorina, 0 de clorina y 1 de bromina. Una concentración del 5% de Halón 1301, es suficiente para extinguir un fuego en un cuarto cerrado y no es considerada como peligrosa para el ser humano, ya que reduce el oxigeno del aire solo en un 20 o 21%.[8]

Tipo de material	Tipo de extintor			
	Agua	CO_2	Espuma	Polvo Seco
Materias secas (papel, madera, tela, etc)	EXCELENTE A chorro o pulverizada, satura el material, refrigera y evita la reignición	En fuegos de pequeña importancia debe emplearse inmediatamente después del agua	EXCELENTE Cubre y humedece la materia inflamada	En fuegos de pequeña importancia se emplea inmediatamente después del agua
Liquidos inflamables (gasolina, aceites, pinturas, etc)	Con los menos volátiles: AGUA PULVERIZADA Con los restantes: NO	EXCELENTE Sofoca y refrigera. Es más indicado su uso de locales cerrados.	EXCELENTE Cubre el fuego e impide la combustión	EXCELENTE
Material eléctrico (motores, cuadros transformadores, etc)	no usarlo	EXCELENTE No es conductor, no deja residuos y no deteriora	NO El agua que contiene pude ser conductora	SI No es conductor deja residuos

Tabla 3.5 Tipos de extintores.

Se necesita ubicar los extinguidores apropiados en lugares de acceso inmediato. Estos extinguidores y el equipo de gas se deben revisar con regularidad para asegurar su funcionamiento efectivo.

Es necesario definir y documentar los procedimientos que se deben seguir en caso de incendio; además, se debe entrenar al personal acerca de su uso, ya que frecuentemente éste no sabe que hacer en caso de incendio.

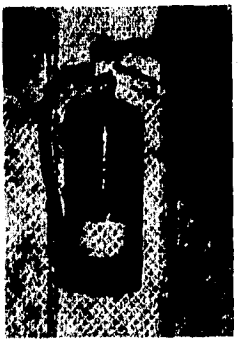

Figura 3.9 Extinguidor

La participación del cuartel de bomberos tanto en el diseño como en la aplicación de los procedimientos para detectar, prevenir y extinguir incendios podría ser muy valiosa, sin embargo, la mayoría de las brigadas trabajan de manera tradicional y no cuentan con la instrucción adecuada para este tipo de emergencias. Incluso en muchos casos los bomberos pueden dañar seriamente el equipo de cómputo.

G. PROTECCION CONTRA INUNDACIONES

En muchas partes del mundo, el daño y riesgo de inundación es algo común. El riesgo para las computadoras es considerable. En estos lugares, las computadoras no se deben colocar en sótanos o en las áreas de planta baja sino, de preferencia, en las partes altas de una estructura de varios pisos. Claro que la mejor opción es no colocar el centro de cómputo en áreas donde el riesgo de inundación sea evidente.

Los daños por inundación o agua han ocurrido aún cuando las instalaciones no se encontraban cerca de un río o una costa donde estuvieran expuestas a tornados, huracanes o tormentas, ni en áreas

bajas. La situación se ha originado de la ruptura de cañerías o por el bloqueo del drenaje. Por lo tanto la ubicación de las tuberías en la construcción de instalaciones de cómputo es una decisión importante (no deben ponerse por encima de las áreas donde se localizan los equipos). El daño causado por el drenaje bloqueado es un riesgo, cuando la computadora se localiza en algún sótano. Deben instalarse, si es el caso, detectores de agua o de inundación, así como también bombas de emergencia para resolver inundaciones inesperadas.

H. MANTENIMIENTO

Aún con el mejor sistema de respaldo y configuraciones duplicadas, de vez en cuando se requiere asistencia externa. En este caso muchas compañías establecen contratos de mantenimiento.

Al establecer estos contratos de mantenimiento, debe considerarse la posibilidad de que una crisis se presente durante la noche, en sábado o domingo.

El servicio y mantenimiento preventivo no debe ser olvidado, debe establecerse el tiempo indicado y seguir las instrucciones de los fabricantes.

Es vital guardar el centro de cómputo limpio, pero hay que recordar que el agua y el detergento pueden dañar el equipo, es por eso que debe instruirse al personal de limpieza al respecto. Es muy común en muchas empresas que el personal de limpieza utiliza trapo mojado para "limpiar " el equipo, pudiendo con ello dañarlo.

3.6.2 SEGURIDAD LOGICA

Es difícil dibujar una línea entre las técnicas o medidas de seguridad física y las de seguridad lógica, esto es porque muchas de ellas se traslapan. Por ejemplo, el control de acceso por personal no autorizado.

Además una técnica puede trabajar en conjunción o en beneficio de la efectividad de otra. La seguridad física, está más orientada hacia los dispositivos e instalaciones, mientras que la seguridad lógica, está más orientada hacia la parte lógica del sistema, como son: las aplicaciones, la información almacenada en él y los sistemas operativos.

En muchas instancias, las técnicas de seguridad lógica, no son más que el uso o utilización de una técnica de seguridad física, sin embargo, pensar en términos de utilizar una en vez de la otra, no conduce a un buen sistema de control de la seguridad. Por ejemplo, un banco puede ser físicamente seguro contra accesos, pero aún así puede ser vulnerable a accesos no autorizados a través de sus sistemas de información.

Mientras las técnicas de seguridad física tratan con un número de amenazas incluyendo el fuego, desastres naturales y similares; las técnicas de seguridad lógica tratan casi exclusivamente con el control de acceso, y en algunos casos, una técnica lógica requiere la aplicación de una técnica física.

Dentro de los medidas de seguridad lógica se encuentran:

A. Integridad
B. Aislamiento
C. Control de acceso
D. Monitoreo
E. Respaldos

A. INTEGRIDAD

Un sistema debe hacer solamente lo que está supuesto que hará y nada más. Debe funcionar de acuerdo a las especificaciones planteadas (aún cuando falle).

"Integridad es básicamente la seguridad que el sistema está funcionando correcto y completo"[6]. La ausencia de integridad contribuye a la inefectividad de todas las demás técnicas de seguridad.

Para cada estímulo al sistema la respuesta debe ser predecida. La siguiente figura muestra un sistema con integridad que encuentra un estímulo anormal. Aún así su respuesta puede ser predecida.

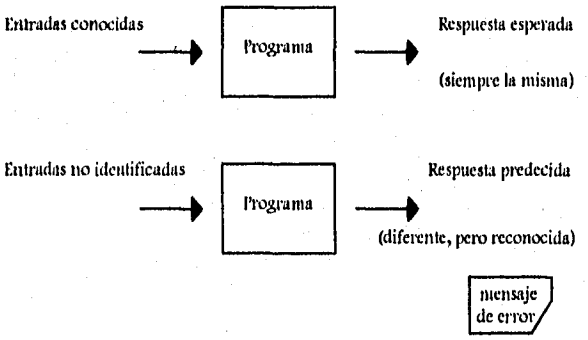

Fig. 3.10 Integridad de un sistema

La idea de integridad es por ejemplo una situación en la cual un usuario está supuestamente en modo de sólo lectura; entonces el sistema debe garantizar que éste no puede hacer nada más, como escribir.

Significa entonces que el sistema debe comportarse como se espera que lo haga.

B. AISLAMIENTO

La protección se logra aislando el objeto valioso y controlando el acceso a él. En la historia abundan los ejemplos con respecto a esto: las fortalezas, las bóvedas de los bancos, etc. La mayor parte de las medidas de seguridad física incluyen esta técnica.

En cualquier sistema donde se requiera mantener un alto nivel de seguridad, ninguna parte de la organización debe tener disponibles todos los componentes o subsistemas que formen un todo. Así este concepto se refiere a una departamentalización y es muy utilizado en el diseño y construcción de armas secretas por ejemplo.

En los sistemas de información basados en computadoras, el aislamiento puede ser mantenido entre usuarios e información, hardware y software, recursos y procesos, etc.

Se reconoce y trata con el compartimiento simultáneo de las facilidades y procesos, y el extenso uso de las redes de comunicaciones de datos en los sistemas de cómputo actuales.

Los coincidentes procesos de usuarios diferentes, requieren la separación y protección de cada información individual y trabajos

procesados. El incremento del uso de las redes ha abierto un campo a exposiciones que deben ser protegidas.

Algunos de los procedimientos de protección que involucran el aislamiento son:

1) Desconexión y separación.

"El aislamiento es ejecutado por la distribución lógica y geográfica en la cual no hay conexiones entre ciertos elementos del sistema".[6] Por ejemplo: La persona que introduce las transacciones al sistema (captura), no tiene acceso a los programas que las procesan.

2) Mínimo privilegio de acceso.

Estos privilegios asignados deben contener la mínima autoridad de acceso necesaria para el funcionamiento de los procesos requeridos. Por ejemplo, a un dependiente ordinario se le es dado el privilegio de accesar sólo las cantidades que hay a la mano y el precio de los registros de un archivo de inventario, pero no puede accesar al precio de costo, proveedor, etc.

3) Ofuscación.

La protección se consigue mediante el aislamiento (pero sin controlar el acceso) basado en la ofuscación. Los objetos de valor se ocultan al quitarlos de la vista o por camuflaje para dificultar la búsqueda. La criptografía representa el ejemplo supremo de esta estrategia.

Otro ejemplo es la llamada: *Seguridad por obscuridad*, la cual se deriva de la *necesidad del saber*. "La información es dividida y a cada quien sólo se le proporciona la que requiere para realizar su trabajo".[11] Esto tiene como ventaja que permite proteger partes confidenciales de la información e impide la obtención de información por inferencia; sin embargo, debe manejarse con extremo cuidado ya que reduce el número de personas preparadas para reaccionar adecuadamente ante una emergencia.

1. CRIPTOGRAFIA

La definición de criptografía, se deriva de dos palabras griegas KRYPTOS (oculto o secreto) y GRAFOS (escritura), que de una u otra forma se ha practicado desde que el hombre ha comunicado sus pensamientos a través del habla o de la escritura.[12] Referencias de esto se encuentran incluso en la Biblia.

Así, se puede definir a la criptografía como un método de protección de información mediante un proceso en el cual los datos entendibles o legibles, son transformados en datos no entendibles o ilegibles para personal no autorizado.

Para lograr esta seguridad de los datos se utilizan diferentes métodos, lo importante es cambiar o cifrar el mensaje con el objeto de que su significado no sea entendido por personas que no estén autorizadas a leerlo.

Los términos de encripción y decripción son sinónimo de cifrado y descifrado de datos.

Existen diferentes ciencias derivadas que se encarga del estudio de la criptología, por ejemplo, la criptología es el estudio de la escritura secreta, criptografía es la ciencia de la escritura secreta, criptanálisis es el arte de obtener el significado de la escritura secreta sin tener conocimientos de la llave de encripción.

BREVE HISTORIA DE LA ESCRITURA SECRETA

Uno de los ejemplos mas antiguos de la criptografía esta en Esparta: Plutarch le dijo como el general Lacedaemnian realizaba cambios en los mensajes con solo introducir de forma circular una cinta estrecha en un pergamino espiral alrededor de una vara cilíndrica. El mensaje entonces se inscribía en el pergamino. Cuando la cinta estaba enrollada, lo escrito podía ser solo leído por la persona que tuviera un cilindro exactamente del mismo tamaño, y por encima de este regresarlo, para que la carta pudiera reapareeer en el orden normal.

Criptogramas mas científicos fueron ideados por los Griegos, quienes frecuentemente utilizaban figuras aritméticas. Uno de sus métodos de sustitución por figuras matemáticas de cartas fue introducir por bloques el alfabeto en una figura cuadrada (tabla 3.6) y numerar cada columna vertical y horizontal del uno al cinco. Una letra de nuestro alfabeto era eliminada, siendo esta la letra J. [12]

	1	*2*	*3*	*4*	*5*
1	A	F	L	Q	V
2	B	G	M	R	W
3	C	H	N	S	X
4	D	I	O	T	Y
5	E	K	P	U	Z

Tabla 3.6 Ejemplo de criptogramas

Cada letra del mensaje esta indicado por los números de intersección de columnas y renglones, se lee primero el número de la columna vertical. Por ejemplo la letra C representa el numero 31, donde la intersección del renglón horizontal es 3 y de la columna vertical es 1. La H es el 32 y así sucesivamente.

Para ilustrar esta el siguiente mensaje:

42-33-12-43-24-23-11-44-42-31-11

El rápido avance en la tecnología de cómputo, ha traído como consecuencia un incremento en la posibilidad de que sean accesados (con o sin fines de fraude), los sistemas de cómputo actuales, por muy complejos que éstos puedan parecer.

Datos estadísticos en Estados Unidos señalan pérdidas en sistemas de cómputo por 3 billones de dólares al año.[12] Cada día, las instalaciones que cuentan con algún equipo de cómputo, son más conscientes de los riesgos existentes en el acceso no autorizado a su información, ya que no existe forma de conocer e identificar a las personas que pueden utilizar sus conocimientos técnicos para realizar un fraude.

Según datos del FBI, aproximadamente un 95% de los fraudes realizados por computadora no son detectados. [13]

A la fecha, la mejor defensa contra accesos no autorizados a la información procesada de centros de computo, consiste en implantar medidas de seguridad, tanto físicas como lógicas, que reduzcan la probabilidad de que ocurra un evento, el cual pueda repercutir en una pérdida para la institución.

En el ambiente de teleproceso de la criptografía es la única técnica de protección disponible para proteger la información sensitiva, que se transmite a través de la red; aunque también puede ser usada para proteger información almacenada en dispositivos magnéticos.

Comercialmente los bancos han sido los primeros en proteger sus redes de teleproceso. Sin embargo, la necesidad de la seguridad de datos es evidente en una gran cantidad y variedad de organizaciones, desde compañías petroleras y empresas de manufactura hasta instituciones educacionales. De hecho, cualquier organización que transmite información sensitiva, necesita protección y privacidad.

Existen básicamente dos métodos para la transformación de mensajes:

1. A través de códigos

Para transformar un mensaje las palabras o agrupamiento de ellas se buscan en una tabla conteniendo los códigos equivalentes, ya sean numéricos o alfabéticos. [14]

Este método no es muy recomendado en el uso computacional, debido a la gran demanda de memoria requerida para almacenar los códigos, lo que repercute en mayor tiempo para realizar la función de encripción/decripción de la información, además de que se ha comprobado que son susceptibles de ser descifrados fácilmente por personal ajeno.

2. A través de cifras

Este método transforma los mensajes por medio de la sustitución y transposición de datos. [14]

ENCRIPTAMIENTO POR SUSTITUCION

Es uno de los dos principios básicos de la criptografía moderna y consiste en reemplazar los caracteres por enviar, por otros diferentes.

		MENSAJE							
		A	B	C	D	E	F	R	Z
	A	A	B	C	D	E	F	R	Z
	B	B	C	D	E	F	G	S	A
	C	C	D	E	F	G	H	T	B
L	D	D	E	F	G	H	I	U	C
	E	E	F	G	H	I	J	V	D
L	F	F	G	H	I	J	K	W	E
A									
V									
E	R	R	S	T	U	V	W	I	Q
	.								
	.								
	.								
	.								
	.								
	Z	Z	A	B	C	D	E	Q	Y

Tabla 3.7 Encriptamiento por sustitución

LLAVE:	CEDER	
MENSAJE A TRANSMITIR:	"ACABA DE CAER"	
FORMANDO GRUPOS DE 8 CARACTERES TENEMOS:		
LLAVE:	CEDERCED	ERC
MENSAJE:	ACABADEC	AER
MENSAJE:		
ENCRIPTADO:	CGDFRFIF	EVT

Tabla 3.8 Ejemplo de encriptamiento

ENCRIPCION POR TRANSPOSICION

Es el segundo principio de la criptografía moderna y consiste en cambiar el orden lógico de los caracteres por enviar. [14]

EJEMPLO DE ENCRIPCION DE DATOS POR TRASPOSICIÓN

LLAVE:

1 2 3 4 5 → 2 3 5 1 4

(INDICA LA PERMUTACION A EFECTUAR EN GRUPOS DE 5 LETRAS)

MENSAJE A TRANSMITIR:

"ATACAREMOS EL PROXIMO MARTES"

SE FORMAN LOS GRUPOS DE 5 LETRAS Y SE APLICA LA LLAVE

MENSAJE: ATACA REMOS ELPRO XIMOM ARTES

MENSAJE

ENCRIPTADO: TAAAC EMSRO LPOER IMMXO RTSAE

Todos los mecanismos de encripción siguen un algoritmo para transformar un mensaje. Ahora bien, con el objeto de estandarizar la forma de cómo encriptar y que no existieran diferentes algoritmos, se diseño un algoritmo llamado DES (Data Encryption Standard), basado en la técnica de sustilución y transposición de datos, el cual fue adoptado por la NBS (National Bureau of Standards) de los Estados Unidos de Norteamérica.

Sin embargo, la seguridad no puede depender de un solo elemento como es el algoritmo de encripción, ya que la persona que quisiera accesar la información confidencial protegida, lo único que tendría que hacer sería enfocar sus esfuerzos a descubrir los detalles del algoritmo. Es por ello, que se requiere de un segundo elemento llamado "Llave de

Encripción", la cual debe ser un número generado en forma aleatoria, con el objeto de mantener su confidencialidad.

Es decir para tener un mecanismo seguro de encripción de datos se requieren 2 elementos:

- El algoritmo de encripción
- La llave de encripción

Las llaves o códigos de seguridad, son variables de entrada, y es un dato de 56 bits, que se aplica al texto inicial para llevar a cabo la transformación. [1] Una vez que se tiene el texto encriptado, es necesario aplicarle la misma " Llave" para obtener nuevamente el texto inicial.

El número de posibles combinaciones de transformación que puede existir en 56 bits es de 72 cuatrillones, es decir 2^{56}.

En criptografía, el texto inicial pasa por el proceso de transformación o encripción, y al texto resultante se le llama texto encriptado. [1]

1. ENCRIPCION

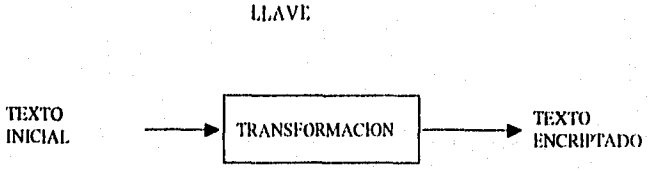

Fig. 3.11 Encripción

2. DECRIPCION:

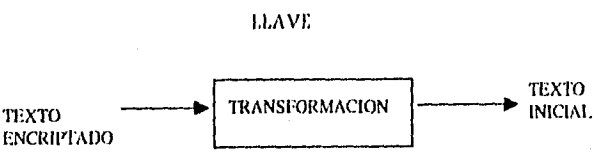

Fig. 3.12 Decripción

El incremento en los sistemas de información distribuidos ha permitido que en un incremento de igual correspondencia, tengan necesidad de contar con servicios de seguridad criptográfica. Por ejemplo, una transacción de negocios completa entre el comprador, vendedor, y el banquero puede ser llevarse a cabo electrónicamente.

Todavía muchas aplicaciones electrónicas relacionadas con la transmisión de datos están sobre líneas de comunicación sin protección, y la transmisión es muchas veces almacenada en intermediarios conmutadores de comunicación desconocidas. La transmisión entre computadoras es alterada frecuentemente y en muchos de los casos, la criptografía provee el único y efectivo medio de protección en la transmisión de datos.

La criptografía puede también ser utilizada para protección de datos dentro de la computadora. Los algoritmos criptográficos pueden utilizarse para proteger grandes volúmenes de datos almacenados en discos de computadoras. Por ejemplo, un usuario de datos en un disco puede protegerse del acceso no autorizado por otro usuario quien usa el mismo disco. Además, los algoritmos criptográficos pueden utilizarse para asegurar un programa del contagio de virus.

La criptografía puede incluso utilizarse para el control de acceso a las computadoras. Los mecanismos criplográficos pueden ser diseñados para ofrecer significativamenle mas protección que el sistema tradicional de password, el cual ha probado su vulnerabilidad con los corruptores de computadoras (hackers). Por ejemplo, un desafiante y responsable sistema que transmite por un lado un desafiante generador de randoms y por el otro que requiere de un responsable para que sea encriptado, lo cual ofrece un alto nivel de seguridad en comparación con los passwords tradicionales de acceso. Además el potencial hacker no tiene conocimiento del generador de randoms de la llave de encripción usada para el algoritmo criplográfico.

El costo del equipo de encriplamiento ha rebasado significativamente de los pasados cinco años anteriores a la fecha; sin embargo, la criptografía muchas veces no es implementada por la naturaleza de su técnica compleja. Como resultado, muchas sistemas de información hoy día están inadecuadamente protegidos.

TECNICAS BASICAS

Hay dos tipos básicos de algoritmos criptográficos: Algoritmos de llave simétrica (también llamados algoritmos de llave privada) y criptografía de llave asimétrica (frecuentemente llamado algoritmo de llave privada). [13] Los cuales los explicare a detalle enseguida.

CRIPTOGRAFIA DE LLAVE SIMETRICA

El algoritmo criptográfico de llave simétrica hace uso de una sola llave compartida por dos personajes el originador y quien recibe los datos. Si los datos confidenciales están a condición de que, ninguna parte pueda encriptar o decriptar los datos con la llave que comparten. Si los datos confidenciales están condicionados, ninguna parte puede encriptar o decriptar datos con la llave compartida. Si el servicio de datos integrados están condicionados, ninguna parte puede generar un mensaje autentico. Los sistemas de llave simétrica están construidos con la suposición de que las dos partes quienes comparten la misma llave confíen el uno con el otro y que utilicen la criptografía para protegerse contra la destrucción de un tercer personaje. [12]

Como se mencionó anteriormente, existe un algoritmo llamado DES. Este está considerado como el mejor y más conocido algoritmo de llave simétrica es Data Encryption Standard (DES). Aunque la adecuación de la seguridad condicionada por el algoritmo ha sido cuestionada por algunos, sin embargo DES se recuerda como el algoritmo criptográfico mas aceptado y pulido, aparte de ser el único algoritmo de llave simétrica publicado y aprobado por la protección de datos del gobierno federal, el cual ha sido altamente aceptado por el sector comercial. El instituto nacional de estándares estadounidense (ANSI), ha adoptado al algoritmo DES para aplicaciones comerciales y se ha basado en varios estándares para su integridad y llaves de dirección.

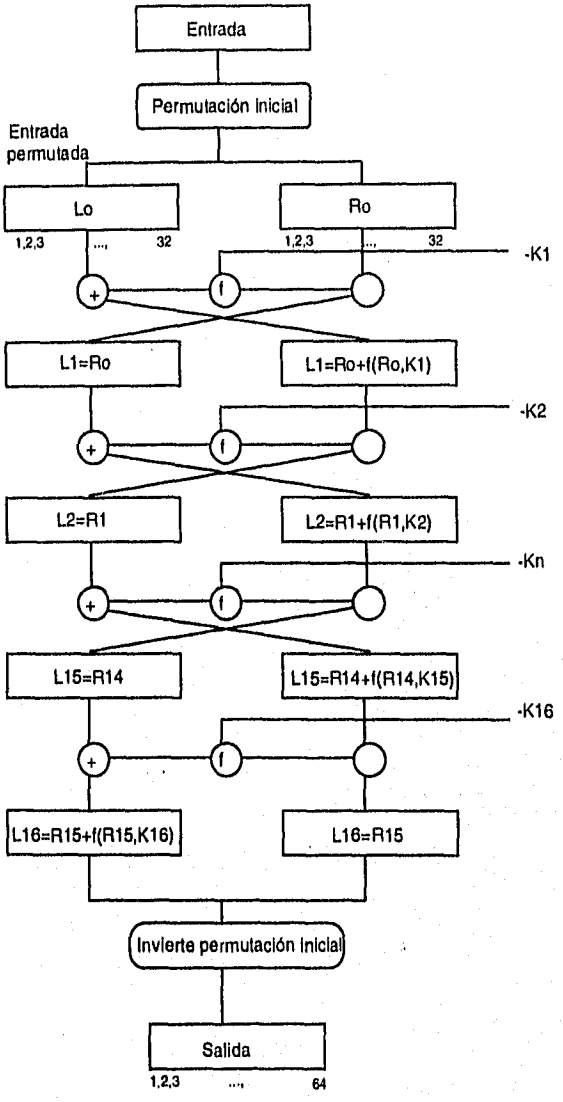

Figura 3.13 Diagrama del algoritmo DES

CRIPTOGRAFIA DE LLAVE ASIMETRICA

Con la criptografía de llave asimétrica, un algoritmo criptográfico emplea dos llaves asimétricas: uno para encriptar y el otro para decriptar. No es posible obtener la llave de desencriptar de la llave de encripción. Un usuario puede generar ambas llaves y hacer la llave de encripción publica mientras que se mantiene la llave de descripción privada. Cualquiera con la llave publica de encripción puede encriptar un mensaje y enviar este a el dueño de la llave privada. Sin embargo, solo el dueño de la llave privada puede descifrar el mensaje. Este arreglo ofrece ventajas sobre el algoritmo de llave asimétrica cuando proporciona un servicio de manejo de direccion.[15]

El mejor y más conocido algoritmo de criptografía asimétrica es el algoritmo Rivest-Shamir-Adleman (RSA). El algoritmo RSA es notable no solo porque éste es el primer algoritmo de llave asimétrica, sino porque su seguridad esta relacionado con un bien conocido problema matemático llamado factorial, que es el producto de varios números primos. [15]

El algoritmo RSA es considerado versátil porque puede ser utilizado para proporcionar varios servicios de seguridad. Varias aplicaciones de la criptografía de llave asimétrica están diseñados para acomodar sus características.

SISTEMAS HIBRIDOS

Los algoritmos de llave simétrica tienen ciertas ventajas sobre los algoritmos de llave asimétrica. Uno de los principales es que tiene deficiencia computacional. La mayoría de las implementaciones practicas del encriptamiento de llave asimétrica corre a miles de bits por segundos, mientras que los algoritmos de llave simétrica pueden

procesar 10 o incluso miles de millones de bits por segundo. Por lo tanto, los diseñadores de sistemas criptográficos seguido utilizan un algoritmo de llave simétrica para encriptar grandes volúmenes de datos y un algoritmo de llave asimétrica para automatizar las llaves de distribución. El algoritmo de llave asimétrica usa lo que recibe la llave publica para encriptar la llave asimétrica que encripta todo el volumen de datos. Este tipo de sistema híbrido proporciona varias ventajas para ambas llaves de criptografía y criptografía de llave asimétrica mientras se minimizan las desventajas.

MECANISMOS Y SERVICIOS DE LA CRIPTOGRAFIA

Un diseño de red debe decidir cual servicio de criptografía es necesario de antemano para las aplicaciones y entonces seleccionar el apropiado mecanismo para proporcionar el servicio adecuado. Los datos deben encriptarse por mantener la confiabilidad, autenticidad para proteger su integridad, o ambos encriptados y autenticidad para proporcionar una combinación de características de protección. Si las llaves criptograficas están apropiadamente restringidas, la criptografía debe utilizarse para certificar la identidad de envío. Finalmente, todas las aplicaciones de criptografía requieren que la llave sea manejada de una forma segura.

CONFIDENCIALIDAD DE LOS DATOS

La confidrncialidad en los datos puede lograrse con los algoritmos de encripción y decripcion. Los algoritmos de encripción y decripcion están diseñados para que solo el que deseamos que reciba los datos tenga el numero binario, llamado la llave, que es necesario para decifrar los datos. Por consiguiente, el mensaje secreto debe enviarse de una parte a otra sin miedo a descubrir los datos.

INTEGRIDAD DE LOS DATOS

En sistemas automatizados, no siempre es posible que el ser humano busque datos para determinar si los bits han sido modificados o robados. Incluso si una búsqueda fuera posible, los datos podrían haber sido modificados de tal manera que sería difícil para la búsqueda detectar la alteración. Por ejemplo, $ 1,000 puede ser cambiado por $ 10,000. Esto es por lo tanto, deseable para tener una automatización que significa la detección de ambos tipos de modificaciones de datos la intencional y no intencional. La detección ordinaria de errores de códigos no es suficientes, porque si el algoritmo de generación de códigos es conocido, un adversario podría generar el código correcta por cualquier modificación de los datos. Las modificaciones serían entonces no detectables. Un criptográfico detector de errores de códigos se requiere para protección en contra de individuos quienes podrían modificar datos legítimos con datos falsos que parezcan legítimos.

Los algoritmos criptográficos pueden utilizarse conjuntamente con una llave secreta para calcular un código de error detección criptográfico, llamado código de mensaje auténtico, en datos quienes deben mantener su integridad. El código de mensaje auténtico es enviado con el texto de datos original a el recibidor, quien con la correcta llave puede calcular el código auténtico del mensaje en los datos que recibe y compararlos con el código del mensaje auténtico recibido. Si los dos están de acuerdo, los datos están considerados integrales. De lo contrario, se asume una modificación sin autorizar. Cualquier individuo que trate de modificar los datos sin conocimiento de la llave no podrá calcular la autenticidad del mensaje apropiado que corresponde a los datos alterados.

AUTENTICIDAD DEL ORIGEN DEL MENSAJE

Si un mecanismo criptográfico se utiliza para protección de datos y la llave utilizada por el mensaje criptográfico es compartida solo por el origen y el destino de los datos. El destino del mensaje puede autentificar el mensaje origen proporcionando que la llave no ha sido arreglado. Por ejemplo, si la parte A y B comparten una llave secreta y parte B recibe un mensaje con un mensaje de código autentico que esta correctamente validado utilizando la llave compartida, parte B podría asumir que el mensaje fue enviado por parte A. Por lo tanto, la autenticidad del mensaje origen es obtenido tan bien como el mensaje autentico

CERTIFICACION ELECTRONICA Y FIRMAS DIGITALES

Los sistemas automatizados de procesamiento de información permite a las corporaciones y empresas almacenar y procesar documentos de una forma electrónica. Tener documentos en forma electrónica permite un rápido procesamiento y transmisión, aumentando la eficiencia de los sistemas de información. Sin embargo, la aprobación de los documentos basados en papel ha sido tradicionalmente indicado por la escritura de una firma. Existe la necesidad de una forma electrónica equivalente para la escritura de una firma que pueda ser reconocido para tener el mismo estatus legal. Principalmente la digitalización de la escritura de una firma no es una alternativa aceptable, porque la firma digitalizada no tiene relación con los datos que han sido firmados. Además, los documentos basados en papel ofrecen la misma resistencia a la alteración y falsificación. Modificar un documento en papel como borrar o reemplazar texto, es una manera no detectable, y falsificar una firma requiere un cierto grado de practica y habilidades. Un documento electrónico con una firma digitalizada no proporcionaría protección contra modificaciones sin autorizar. El documento puede ser alterado sin cambiar la firma, y la firma digitalizada puede ser remplazada en otro documento sin detección.

Los algoritmos criptográficos pueden proporcionar protección en contra modificaciones y falsificaciones de documentos electrónicos. Estos algoritmos hacen uso de una llave criptográfica para generar una firma digital que esta basada en la llave y todos los bits del documento electrónico. La firma digitalizada es verificada por quien recibe el documento. Con solo cambiar un simple bit en los resultados del documento es un cambio impredecible para la firma. Por lo tanto, cuando la firma digitalizada se verifica, cualquier alteración es inmediatamente detectado.

Si un algoritmo de llave simétrica es utilizado para formar la firma. La misma llave es compartida por ambos, el originador y el que recibe el mensaje, pero no es conocida por las otras partes. Si la firma se verifica, quien recibe conoce que el documento viene del origen y no ha sido modificado. Tales sistemas han sido aprobados en uso por el gobierno federal como un reemplazo de firmas escritas en ciertos documentos electrónicos

CONSIDERACIONES CUANDO SE IMPLANTA CRIPTOGRAFIA

Los algoritmos criptográficos son implementados en un plan físico llamado modulo criptográfico. En lo siguiente se expondrán varios factores que deben ser considerados por diseño de sistemas cuando se implementa los módulos de criptografía en sistemas de información.

SERVICIOS DE SEGURIDAD

Los algoritmos criptográficos son miembros de la clase de mecanismos de seguridad que son utilizados para proporcionar servicios

de seguridad. Los servicios de seguridad son utilizados para reducir la probabilidad de una específica amenaza de seguridad, con eso mejora la seguridad en los sistemas. Un diseñador de sistemas debe contemplar las probabilidades de seguridad que tuvieran en contra de las amenaza de seguridad cuando ocurriera y las pérdidas que se tuvieran. Al momento de considerar el riesgo específico para el sistema, el diseñador debe intentar determinar cuales son los relevantes y cuales son imprácticos. Los mecanismos de seguridad pueden, entonces ser utilizados para proteger en contra de amenazas relevantes, tratando de que el costo de los mecanismos no exceda la perdida esperada que podría resultar para salvaguardarlos en contra, si una amenaza fuera cometida.

Algoritmos criptográficos proporcionan varios servicios de seguridad, por ejemplo, confidencialidad de datos, integridad de datos, autentificación del mensaje origen, autentificación de usuarios, firmas digitales. Estos servicios pueden proveerse por encripción, decripción, autentificación, firma digital, y otros mecanismos de seguridad. Una lista de servicios de seguridad y de mecanismos criptográficos son proporcionados por la International Standars Organization. El diseñador debe determinar cual servicio de seguridad se necesita para encontrar todos los requerimientos de diseño de sistemas y cuales mecanismos de seguridad son los mejores para las necesidades de servicio.

CONFIGURACION

La siguiente configuración debe ser considerada en un módulo criptográfico que será implementado:

- Inline
- Offline
- Embedded
- Standalone

INLINE

Las configuraciones Inline o front-end requiere que el módulo criptográfico sea capaz de aceptar los datos del texto a encriptar del origen, ejecutar y pasar el proceso de datos directamente al equipo de comunicación de datos sin regresar el mensaje fuente.[13] El módulo criptográfico también debe ser capaz de aceptar datos (ej. Cipertexto) de los equipos de comunicación de datos. El módulo procesado (ej. Decriptado) de datos y pases dentro y al final del sistema.

Para configuraciones inline, el equipo de comunicación esta en el módulo criptográfico o externo al host. Los datos no pueden dejar el host sin pasar a través del módulo.

OFFLINE

Las configuraciones Back-end u Offline requieren que el módulo criptográfico sea capaz de aceptar datos del origen, ejecutar el proceso de encriptamiento, y pasar los datos procesados de regreso al origen. Los controles de almacenamiento del origen o la transmisión más distante de

los datos y es responsable por el mantenimiento de la separación entre los datos que tienen protección y los que no la tienen. Cuando la transmisión de datos, la configuración del host debe estas diseñada o confiable para no transmitir datos que no tienen protección. La configuración del offline permite en el tablero comunicaciones separadas internas dentro del host. [13]

EMBEDDED

Esta configuraciones requieren que el módulo sea físicamente adherido dentro de una computadora y tener interfaz con la computadora. La configuración embedded puede tener cualquiera de las dos configuraciones de offline o inline. La configuración embedded tienen a ser menos cara, pero su seguridad física (ej. Detección y protección) es muchas veces deficiente y carente. [13]

STANALONE

Este tipo de configuración requiere que el módulo esté contenido en la parte física de la computadora del host. La configuración stanalone puede tener cualquiera de las dos configuraciones de offline o inline. [13]

SEGURIDAD FISICA

La seguridad de un módulo criptográfico depende de la seguridad de la llave y del apropiado funcionamiento del algoritmo criptográfico. Porque ambos la llave y el algoritmo están contenidos en el módulo, esto es importante para proteger el contenido del módulo contra manipulaciones.

La Security Requirements for Cryptographic Modules, describe cuatro niveles de seguridad física. El primero y el más bajo nivel requiere no requiere seguridad física más allá de lo que típicamente se implementa en aplicaciones comerciales. El segundo nivel requiere características evidentes de indicadores y examinación, en cualquiera de los módulos que puedan ser atentados contra el. El tercer nivel requiere seguridad de circuitería responsable en cualquier módulo abierto o para hacer modificaciones. Cuando un intruso a traspasado este nivel y es detectado, los parámetros de seguridad critica (ej. La llave criptográfica) es llenada por ceros. El nivel cuarto y el mas alto requiere que el módulo de circuitería responsable esle diseñado para detectar penetraciones a través de todos los módulos adheridos. [13]

La seguridad física nunca será efectiva al 100%, y cualquier protección que se le haga puede incrementar significativamente el costo de los módulos. El diseñador debe por lo tanto estar seguro de que el equipo seleccionado de seguridad ofrezca un compromiso razonable entre el costo y la seguridad.

ESTANDARES Y VALIDACIONES

El diseñador de sistemas criptográficos debe estar familiarizado con los estándares de seguridad en las aplicaciones. Los estándares son útiles porque ellos proporcionan un nivel común de seguridad e interoperatividad entre los usuarios . Algunos vendedores ofrecen algoritmos criptográficos que son propietarios de ellos, por consiguiente el cliente requiere confiar en el vendedor con respecto al diseño del algoritmo y evaluar su seguridad. Los diseñadores no son siempre expertos en encontrar debilidades en su propio trabajo. Los algoritmos estándares son públicamente conocidos, así que ellos pueden ser evaluados por cualquier persona que este interesada. Si un algoritmo

criptográfico estándar es utilizado con protocolo de comunicaciones común , existe una probabilidad muy alta de que los módulos de diferentes vendedores podrán comunicarse de una manera segura. Las desventajas de los algoritmos estándares es que si es utilizada excesivamente, esto se convierte en un punto para el ataque.

Porque la implementación de seguridad involucra mucho mas que un algoritmo de seguridad, mas que estándares criptográficos distribuidos con la implementación de criptografía en aplicaciones particulares o protocolos de comunicación.

NIST mantiene programas que utilizan para certificar la información de los estándares procesada. Bajo estos programas, los vendedores pueden tener sus productos validados para ser confrontados por el estándar. El producto debe seguir una serie de pruebas que compare la operación de los productos con el resultado requerido por el estándar. Una vez que el producto pasa la prueba, un certificado de validación se extiende para el vendedor. El diseñador de sistemas y los usuarios generalmente tienen un alto grado de confidencialidad que valida al producto conforme a los estándares. Los vendedores voluntariamente validan sus productos porque este muestra que ellos diseñaron sus productos poder ser aceptado por los estándares.

Porque los algoritmos criptográficos son ahora utilizados para proporcionar una variedad de servicios de seguridad que protegen datos de significativos ataques.

C. CONTROL DE ACCESO

Si un sistema instala procedimientos de aislamiento para prevenir accesos no autorizados, entonces también deberá tener la posibilidad de

identificar y validar a los usuarios e interfaces apropiadas para poder controlar el acceso a éste.

Es decir, que debe ser capaz de distinguir entre aquellos usuarios que tienen permitido el acceso y aquellos que no lo tienen.

1) Elementos del control de acceso:

Identificación

Dependiendo del nivel de seguridad requerido, para cada persona, la termina, el archivo y/o el programa debe identificar y verificar el derecho al uso del sistema.

Los parámetros de identificación efectiva como se explicaron en el inciso C del punto 3.4.1, son:

- Algo que se porta
- Algo que se sabe
- Alguna característica física especial

Autorización

Una vez que una persona ha sido identificada como usuario válido, la pregunta es: ¿Qué autoridad tiene?, esto es, ¿Qué poderes o derechos puede tener para hacer algo? (Por ejemplo, para la seguridad de los archivos de una base de datos, deben definirse procedimientos que determinen quién puede accesar que archivos, quién tiene derecho a modificar o borrar y quién es responsable de la administración de los archivos). Para ello es necesario primeramente evaluar las partes de la

información o diferentes sistemas a los cuales se puede acceder. Así pueden definirse los niveles de autorización personal de acuerdo al nivel de clasificación al cual tendrán acceso y en adición a estos niveles, deberán definirse las restricciones de acceso a que se sujetarán.

Clasificación de la autorización

Este paso determina autoridades específicas para los usuarios, programas y equipos. Las clases de autoridad pueden incluir cosas como: usuario de los archivos, usuario de los programas, usuario del equipo, programa de un programa, programa de un archivo, terminal de un programa, etc.

En conjunción con estas autoridades, deben asignarse las actividades a que tendrán privilegio: leer, escribir, borrar, adicionar, cambiar, copiar, desplegar, crear, etc.

Por ejemplo: un usuario tiene derecho a utilizar el programa I para leer el archivo A (entera o parcialmente).

Autentificación

Los procedimientos de autentificación son requeridos para mostrar que algo es válido y genuino.

una vez que alguien ha sido apropiadamente identificado y se le ha dado autoridad para accesar algo o realizar alguna actividad, el sistema no puede asegurar que el usuario es realmente válido, especialmente si el usuario ha sido identificado en base a *algo que porta* o *algo que sabe* (como una tarjeta o un password en cada caso). Es por

Una vez que alguien ha sido apropiadamente identificado y se le ha dado autoridad para accesar algo o realizar alguna actividad, el sistema no puede asegurar que el usuario es realmente válido, especialmente si el usuario ha sido identificado en base a *algo que porta* o *algo que sabe* (como una tarjeta o un password en cada caso). Es por esto que en algunos casos, especialmente si la información es altamente sensitiva, la validación del usuario debe ser confirmada.

Esta confirmación puede incluir alguno de los siguientes procedimientos de autentificación:

- La observación física. Por ejemplo, enviar a alguien para confirmar que el usuario es quien dice ser.
- Desconexiones periódicas y procedimientos de llamadas. Por ejemplo, que la máquina desconecte una terminal y la llame para ver si ésta responde adecuadamente.
- Requerimientos periódicos de información o reverificación del usuario.

2) Passwords

Una vez que un sistema de control de acceso ha sido implementado, algún tipo de sistema de identificación o password es necesario para asegurar que sólo personal autorizado tenga el acceso garantizado.

Un password "es un autentificador que se usa para comprobarle al sistema operativo que el usuario es quien dice ser".[11] "Es una clave personal que ayuda a prevenir que personas no autorizadas obtengan acceso".[16] Más que eso, una identificación basada en un sistema de passwords, puede ser utilizada selectivamente para permitir o negar el

acceso a determinadas partes del sistema, mediante la definición de varios niveles de passwords.

En general los passwords se utilizan para obtener acceso a:

- Terminales
- Computadoras o partes de las computadoras
- Areas en la memoria
- Programas o partes de programas
- Archivos o registros
- Categorías de información
- Comandos específicos

La mayoría de los fabricantes de computadoras o mainframes actualmente proporcionan a sus clientes más o menos sofisticados sistemas de passwords. Lo cual permite al usuario, decidir como utilizar el sistema y, de acuerdo a la aplicación y sensitividad de la información en cuestión, decidir cuales niveles utilizar.

A menudo es necesario implementar sistemas de passwords realizados por uno mismo en adición a los provistos por el fabricante, especialmente si la información o el sistema es de naturaleza altamente sensitiva.

Para implementar un sistema de passwords, estos deben cumplir con ciertos requisitos mínimos esenciales:

- Los passwords no deben crear problemas operacionales debido a su complejidad. Los caracteres deben ser combinaciones que puedan ser memorizadas. Si uno no puede recordar su password significa que tendrá que escribirlo en un papel y éste podría ser fácilmente visto

por personal no autorizado. Así que si un password debe ser escrito por alguna razón, debe mantenerse seguro bajo candado y llave.

- El número de caracteres en un password debe ser al menos de 4 o 6, y por el factor de memoria (poderlo recordar), no mayor de 8.

- Junto con el password, deberá haber también un código de identificación de usuario para identificar al usuario del password.

ADMINISTRACION DE UN SISTEMA DE PASSWORDS

Un efectivo sistema de passwords requiere de un cuidado especial. Los passwords son tan comunes que no hay un estándar para manejarlos. Cada usuario debe tener su propio password y debe almacenarse en el sistema.

Una alternativa es dejar que la computadora genere passwords en forma aleatoria y sean asignados a los usuarios; o que el administrador de software pueda inventar el código de acceso y asignarlos (estos passwords, son generalmente de buena calidad pero también generalmente son difíciles de recordar).

Un usuario con varios passwords (para sistemas diferentes) tendrá problemas para recordarlos si utiliza una técnica aleatoria, lo cual puede provocar que tenga que escribirlos cosa que no es recomendable.

Si se usa un grupo de passwords, se tiene que cambiar cada vez que alguien salga del grupo, particularmente si esa persona deja la compañía. Los passwords deben cambiarse regularmente en cada evento. Mientras más privilegios tenga el usuario, el password debe cambiarse con mayor frecuencia.

Es recomendable mantener los registros de los passwords en un archivo bien protegido dentro del sistema de la computadora. Inevitablemente si alguien pierde u olvidara su password asignado, se le debe asignar uno nuevo.

Procedimientos para cambiar de password son esenciales. la responsabilidad de trabajar lales procedimientos normalmente cae en una persona responsable de la seguridad. Si el sistema lo permite cada persona deberá poder cambiar su propio password. Chequeos frecuentes deben ser realizados para ver que los passwords son cambiados y se debe asegurar que el sistema siempre pregunte un nuevo password cuando un usuario nuevo ingrese en el sistema.

Años recientes han mostrado un incremento dramático en los reportes de intrusiones de personal no autorizado en los sistemas de cómputo desde sus propias terminales. Tales intrusiones son usualmente realizadas vía la red pública y pueden tener lugar a través de grandes distancias. El patrón común es que esos "hackers", han tenido passwords prestados o adivinados, o los han obtenido de fuentes que tienen el mismo "hobby".

Si un password permanece sin cambiar por un periodo largo de tiempo, las oportunidades de ser adivinado por personal no autorizado se incrementan. Los password iniciales provistos por los fabricantes en los sistemas instalados son conocidos y deben ser borrados o cambiados después de la instalación. En efecto, esta parece ser una de las mayores causas de muchas de las intrusiones.

¿Porqué es entonces, que muchos passwords no son cambiados frecuentemente? Podría haber diversas razones. Pobre administración de la seguridad, mala implementación y seguimiento de los sistemas de

password, carecer de motivación por la seguridad o disciplina son sólo unas pocas.

También, la gente puede objetar que es fácil para ellos recordar sus passwords si ellos no son cambiados todo el tiempo.

SELECCION DE PASSWORDS

"Un password bueno es aquel que es difícil de adivinar".

Lo ideal en un password es que sea fácil de recordar y difícil de adivinar. Para conseguir esto , pueden utilizarse los siguientes criterios:

- No debe haber conexión lógica entre la clave y el usuario. Es decir, no poner el nombre, ni el de algún familiar, amigo, mascota, etc.
- No debe haber conexión lógica entre la clave y el contenido del archivo o de la máquina para la cual se utiliza el password.
- No debe ser una palabra contenida en algún diccionario, ni ésta al revés.
- Debe incluir una mezcla de caracteres, tanto mayúsculas como minúsculas, además de números y símbolos de puntuación.

Algunas sugerencias para seleccionar buenos passwords son:

- Combinar palabras cortas.
- Usar acrónimos (no conocidos)
- Si se utiliza el mismo password en varias máquinas utilizarlo ligeramente en cada una de ellas.
- No escribir los passwords. Si se debe escribir un password debe considerarse lo siguiente:
    - No identificarlo como tal.

- No escribir a que máquina o cuenta pertenece.
- No pegar el papel en la máquina.

- Mezclar caracteres aleatorios.
- Nunca mandarlo por correo electrónico.

ESQUEMA DE PASSWORD	VENTAJAS	DESVENTAJAS
Proceso de selección:		
Seleccionado/usuario	Fácil de recordar	Es más fácil de adivinar
Generado por el sistema	Difícil de adivinar	Más difícil de recordar. Generado por un algoritmo podría ser más fácil de deducir.
Tiempo de vida:		
Indefinido	Fácil de recordar	Más vulnerable con una numeración exhaustiva e intento de adivinar. Difícil de decir si el password es robado.
Combinado	Fácil de recordar si el intervalo de tiempo no es muy largo por ejemplo un mes o una semana. Más seguro que el indefinido	La vulnerabilidad depende del intervalo de tiempo.
Una vez	El tiempo de vida tan corto prohibe exhaustivas pruebas	Difícil de recordar al menos que se escriba. si logra entrar se valida al usuario que entra.
Tamaño y alfabeto Largo	Más difícil de adivinar menor necesidad de duplicación en los passwords	Difíciles de recordar y requieren más espacio de almacenamiento.

Tabla 3.9 Clasificación y características de los passwords

Ejemplos de los passwords débiles:

- Nombres (del usuario, de su esposa, su mascota, su hijo, etc.)
- El nombre del sistema operativo que se está usando.
- El nombre de la máquina que se está usando.
- Información que sea fácilmente obtenible acerca del usuario (cumpleaños, teléfono, calle, etc.)
- Palabras que aparezcan en un diccionario.
- Nombres de lugares.
- Letras repetidas.
- Patrones de teclado (como qwerty)
- Ninguno de los anteriores escrito al revés.
- Ninguno de los anteriores seguido de un sólo dígito.

3) Otros Controles

El uso de los sistemas de passwords hace posible restringir al personal del acceso más allá de lo que ellos necesitan. Tales restricciones pueden ser empotradas en el sistema operativo, en programas de transacción y de aplicación. Se recomienda que la mayoría de las restricciones programadas basadas en el uso de passwords, sean puestas en un módulo central de control de acceso. Esto ayudará a proteger el control de acceso en si mismo durante la evaluación, mantenimiento y pruebas de dicho módulo.

En adición a las restricciones a programas e información, podría ser una buena idea restringir el monto de la información que aparece en la pantalla de la terminal en un momento. Consideraciones deben también ser dadas para restringir el uso (tipo de acceso) de la

información de acuerdo con las diversas necesidades (por ejemplo lectura, modificación, escritura, borrado).

En años recientes se ha incrementado comúnmente la implementación de controles automáticos tales como los siguientes los cuales guardan el tiempo y proveen mejor seguridad:

- Una terminal puede ser automáticamente desconectada entre las 4 p.m. y las 8 a.m., para prevenir que el personal de mantenimiento y otros con horarios anormales de trabajo obtengan acceso a los sistemas.

- Cuando no se registre actividad en una terminal por más de 15 minutos, está automáticamente será desconectada.

- También puede ser relevante para restringir el acceso a ciertas transacciones o tipos de información, predefinir periodos en que éstas pueden ser procesadas durante el día.

Es vital probar las restricciones automáticas frecuentemente, para asegurar que trabajan de acuerdo a los requerimientos.

Sistemas dedicados

Una diferente pero algunas veces efectiva forma de restringir el acceso a la información es adquirir una computadora, solamente para el uso de un sistema sensitivo en particular. De esta forma toda la información será accesible únicamente para aquellos con acceso a esa computadora.

De esta manera se separa a los usuarios de diferentes tipos de información.

Si tales computadoras dedicadas pueden ser guardadas bajo una protección física satisfactoria, no será necesario implementar un sistema de passwords. Los pocos usuarios con acceso físico serán los únicos con autorización para entrar al sistema.

4) Seguridad Multinivel.

En un sistema confiable, se conoce como objetos a todos los datos, y como sujetos a las entidades que pueden actuar sobre esos datos, como procesos, usuarios, etc.

La Seguridad Multinivel, se basa en el concepto de etiquetas de seguridad. A cada sujeto y a cada objeto se le asigna una etiqueta, que indica su clasificación de seguridad.

Cada etiqueta está compuesta de dos partes:

- Un nivel de seguridad
- Un conjunto de categorías de seguridad

Por ejemplo:

SECRETO [contabilidad, ventas]

Los niveles de seguridad están organizados jerárquicamente, y los niveles más altos se consideran de mayor seguridad que los más bajos. Una etiqueta de seguridad puede contener solamente un nivel.

Los niveles de seguridad pueden ser por ejemplo:

NO CLASIFICADO, CONFIDENCIAL, SECRETO Y ULTRA SECRETO.

Las categorías de seguridad, no están organizadas jerárquicamente, y sirven para especificar áreas de información diferentes, incluso dentro del mismo nivel de seguridad. También se les llama *compartimientos de seguridad.*

El conjunto de categorías asignado a una etiqueta puede tener un número arbitrario de categorías. Por ejemplo: contabilidad, desarrollo, ventas, mercadotecnia.

Dominio de etiquetas

Se dice que una etiqueta de seguridad A domina a otra B si:

1. El nivel de seguridad A es mayor o igual que el de B.
2. El conjunto de categorías de A incluye a todas las categorías de B.

Para que un sujeto pueda realizar una lectura sobre un objeto, la etiqueta del sujeto debe dominar a la del objeto. A esta regla se le llama no lectura hacia arriba (no read up).

Para que un sujeto pueda realizar una escritura sobre un objeto, la etiqueta del objeto debe dominar a la del sujeto. El objeto de esta regla es impedir la declasificación de información. A esta regla se le conoce como no escritura hacia abajo (no write down), o propiedad.

Las etiquetas se pueden comparar solamente si sus niveles son diferentes y sus categorías son iguales, o sus niveles son iguales y sus categorías son diferentes.

No se pueden comparar entre sí etiquetas que difieren tanto en nivel como en las categorías.

Ventajas de MLS

Ofrece un alto nivel de seguridad. En aplicaciones de alta seguridad (como en organizaciones militares), es la forma más confiable de asegurar la privacidad de la información.

Desventajas de MLS

Es muy difícil de administrar, y sobre todo de utilizar. un usuario que apenas empieza puede encontrarse repentinamente con que ha creado un archivo que no puede leer. Las primeras experiencias con MLS pueden ser muy frustrantes, tanto para los usuarios como para los administradores.

D. MONITOREO

Monitoreo es "el acto de observar, checar o vigilar algo"[10]. Este concepto reconoce tarde o temprano cualquier intento de acceso accidental o intencional no autorizado y permite neutralizarlos o bloquearlos.

La operación exitosa de un sistema seguro depende no solamente de las técnicas de seguridad utilizadas para construirlo, sino del

monitoreo continuo de estas técnicas para detectar cualquier vulnerabilidad. El monitoreo con éxito requiere de habilidad para vigilar la operación o comportamiento de los objetos dentro del sistema. Este seguimiento permite tomar acciones evasivas o correctivas en el caso de que este comprometida la seguridad del sistema.

Algunos sistemas específicos que apoyan los procedimientos de monitoreo son:

1. *Detección de violaciones a la seguridad.* Un sistema de seguridad debe ser instalado para detectar cualquier violación tan pronto como ocurra.

2. *Bloqueo del sistema.* Si cierta violación a la seguridad es seria, el sistema debe definir el bloqueo automático, para cualquier uso. Por ejemplo: una terminal será bloqueada automáticamente después de n intentos no autorizados de acceso.

3. *Reporte de excepciones.* Todas las condiciones excepcionales deben ser reportadas para posteriores revisiones.

4. *Reporte de tendencias.* El sistema debe colectar datos concernientes a todos los accesos de usuarios. Los datos típicos en este reporte incluyen: usuario, terminal, tipo de procesamiento, fecha, hora y aspectos accesados.

Algunos sistemas cuentan con sistemas de archivos de registro (bitácoras o logs) en los que se registra los que sucede en el sistema. Por ejemplo:

- Qué usuarios entran
- Cuánto tiempo permanecen en sesión
- Qué comandos ejecutan

La revisión cuidadosa de estos archivos puede ayudar a descubrir actividades no autorizadas en el sistema, debido a que a través de ellos se puede decir exactamente qué pasó. Al revisarlos hay que buscar cosas fuera de lo común, por ejemplo:

- Usuarios en sesión en horas extrañas.
- Intentos fallidos de conexión repetidos
- Usuarios conectándose desde sitios no conocidos.

Mecanismos de detección

La detección de un intruso en un sistema puede darse por diversas razones, entre ellas:

- Descubrir al intruso en el acto. Para esto podemos tomar como parámetro por ejemplo, alguna de las siguientes conductas: si el usuario está conectado al mismo tiempo desde lugares diferentes, cuando un usuario está ejecutando un programa que no suele usar, o haciendo uso excesivo de la red, manejando comandos como superusuario, o si está conectado a terminales en horas inusuales.

- Deducirlo en base a cambios en el sistema: cuentas nuevas, archivos nuevos, modificación

- Deducirlo en base al comportamiento del sistema: caídas frecuentes, mal desempeño, negación de servicio, etc.

- Recibir el mensaje del administrador de otro sitio reportando actividad extraña originada desde la máquina local.

¿Qué hacer cuando se descubre una violación a la seguridad?

- Ignorarlo
- Tratar de comunicarse con el intruso

Es importante registrar todo lo que diga o envíe (si lo hace). Aveces basta hacer el intento de comunicación para que el intruso desaparezca. Aveces es posible hacer entender al intruso el daño que está causando.

- Tratar de rastrear la conexión

Es posible que el sistema tenga comandos que ayuden a verificar desde donde está conectado el usuario, ó ver que usuarios están conectados en la máquina remota. Es importante comunicarse con el administrador del sitio remoto.

- Cortar la conexión

Para ello se puede: apagar la computadora, matar los procesos del usuario o dar de baja la máquina.

Regla #1: ¡No asustarse!

- ¿Realmente es una violación a la seguridad?
- ¿Se ha hecho algún daño?
- ¿Es importante obtener y proteger la evidencia que pueda servir en una investigación?
- ¿Es importante tener el sistema en funcionamiento normal lo más rápido posible?
- ¿Cómo asegurar que no haya archivos modificados?
- ¿Importa si alguien se entera del incidente?
- ¿Puede suceder nuevamente?

Regla #2: ¡Documentar TODO!

Es muy importante registrar todo lo que sucede, detalladamente. Se pueden usar las siguientes técnicas:

- Escribir todo lo que se hace y se encuentra en una libreta.
- Imprimir los archivos de texto que se examinen. (la evidencia)
- Todo lo que esté impreso en papel debe tener la fecha y la firma de la persona responsable.

AUDITORIA

Etimológicamente la palabra auditoría proviene de la raíz latina "auditorius" que significa tener la virtud de oír; derivada de los términos "audis", oir y "auditor", el que escucha.

Auditoría es "el examen de la información por parte de una tercera persona, distinta a la que la prepara, con la intención de establecer su razonabilidad dando a conocer los resultados de su examen, a fin de aumentar la utilidad que tal información posee".[16]

Así, la auditoría consiste en una evaluación analítica y sistemática valiéndose de un conjunto de técnicas y procedimientos que aplica el auditor para que por medio de señalamientos de cursos alternativos de acción, proporcione los elementos de juicio necesarios para fundamentar de una manera clara y objetiva, la opinión que emite como resultado de su revisión acerca de la situación de una organización o área en específico.

En este sentido la auditoría cumple una labor de monitoreo, ya que mediante la aplicación de métodos de investigación, técnicas formales, procedimientos y pruebas, el auditor puede cerciorarse de la autenticidad razonabilidad y confiabilidad de los hechos e información, del área bajo estudio.

Existen dos tipos generales de auditoría, por ejemplo:

La Auditoría externa, "es la auditoría que se realiza a solicitud de las organizaciones con el objeto de presentar una opinión profesional independiente acerca de la razonabilidad y confiabilidad de la información y los recursos a examinar expresada bajo los principios y políticas de la misma".[16]

La Auditoría interna, "es una evaluación independiente de las operaciones realizadas por lor los empleados o funcionarios de la organización con propósitos de control".[16]

Este tipo de auditoría mide y valora la eficacia de los controles, políticas y procedimientos definidos por la organización para que se cumplan de acuerdo a lo establecido.

Como cualquier disciplina, la auditoría toma características diferentes de acuerdo al campo de acción o área de aplicación en que se desenvuelve. Así las técnicas tradicionales de auditoría, también se pueden aplicar al área de sistemas o de informática, entendiendose por auditoría informática: "Examen que se realiza en un ambiente que cuenta con el procesamiento electrónico de los datos y que, por las características de este ambiente se deben adecuar los procedimientos, las técnicas y las herramientas tradicionales de la auditoría a los cambios sustanciales que presenta el computador al desarrollar los sistemas de información de la entidad".

Auditar la seguridad implica dos actividades diferentes:

Tareas de monitoreo de seguridad diarias: Los administradores de seguridad de tiempo completo deben realizar estas tareas diariamente, mientras los administradores de medio tiempo pueden realizar el monitoreo en base a períodos menos frecuentes.

Auditorías de seguridad periódicas: Las revisiones y auditorías periódicas pueden realizarse por auditores internos o externos. Las revisiones periódicas se desarrollan anualmente o en períodos menos frecuentes, dependiendo del tamaño y necesidades de seguridad de la organización.

TIPOS DE AUDITORIA

Revisión de seguridad.

Determina el estado de seguridad del área. Busca determinar el cumplimiento de las bases de seguridad estándares de control que han sido especificados por las políticas corporativas y los mandatos legales/regulatorios. Es una vista o foto instantánea de las condiciones actuales. Los auditores pueden realizar una revisión de seguridad como parte de una auditoría regulatoria o de una auditoría externa.

El auditor evalúa los resultados de la revisión de seguridad independientemente de las funciones y aplicaciones del negocio. Los procedimientos incluyen básicamente el cuestionamiento y la observación. El ámbito que abarca incluye típicamente:

- Seguridad Física y ambiente
- Respaldo, recuperación y planes de contingencia
- Acceso al sistema

Auditoría del sistema.

Es más profunda que una revisión de seguridad e incluye procedimientos de evaluación para resaltar preguntas y observaciones. Los estudios de perfeccionamiento de procesos o auditorías de cumplimiento normalmente incluyen detalle y ámbito de una auditoría del sistema.

Normalmente se evalúan estas categorías:

- Políticas procedimientos y estándares
- Seguridad física y ambiente
- Respaldo, recuperación y planes de contingencia
- Operaciones del sistema, mantenimiento y resolución de problemas
- Acceso al sistema
- Utilización de recursos
- Desarrollo y adquisición de software

Auditoría de aplicaciones.

Es un tipo de auditoría altamente personalizada que destaca lo relacionado con control, seguridad y usos de una aplicación. Estos puntos de control y seguridad pueden cambiar significativamente la estrategia básica de seguridad.

Los auditores realizan primero una auditoría de aplicación para evaluar la integridad, disponibilidad y confidencialidad de los controles y prácticas que soportan una aplicación específica.

Una vez que se ha decidido sobre qué tipo de auditoría o revisión se va a basar, se puede uno enfocar a la situación ambiental y expandir los pasos de la auditoría en forma más apropiada.

E. RESPALDOS

Los datos son el componente más valioso de un sistema de cómputo.

> *"Para mi, los datos de los usuarios son de importancia inigualada. Cualquier otra cosa es generalmente reemplazable. Se pueden comprar más discos, más computadoras, más energía eléctrica, pero si se pierden los datos, por un incidente de seguridad o por cualquier otra cosa, se van para siempre".*
>
> *Russell Brand.*

Hay un hecho notorio sobre la seguridad de los datos y es que la mejor protección contra la pérdida de éstos consiste en hacer copias de seguridad almacenando copias actualizadas de todos los archivos valiosos en un lugar seguro, con el fin de evitar cualquier tipo de riesgo al que puedan estar expuestos, tales como errores de usuarios, errores de programación, fallas del hardware, intrusos, robo o destrucción de los equipos, desastres naturales, etc.

Facilitar las copias de seguridad implica tomar decisiones sobre hardware y software.

- ¿Qué soporte de copias de seguridad se va a usar (diskettes, cintas, discos ópticos, cartuchos especiales, etc)?
- ¿Se van a usar dispositivos especializados para copias de seguridad? Si no es así, ¿qué software especializado de copia de seguridad se va a

utilizar para ayudar a la copia de seguridad en diskettes? Si la decisión tomada es usar las órdenes de copia de seguridad del sistema operativo,

- ¿se crearan macros, scripts o archivos por lote para facilitar los procedimientos?

Pero, mas allá de esas cuestiones, un elemento crucial al decidir realizar copias de seguridad es la identificación de las aplicaciones críticas para la compañía y de la información que éstas requieren para realizarse. Ya que en base a esto se decide la frecuencia con la que se realizaran las copias de seguridad, los archivos que se copiarán, así como dónde se almacenará el soporte de las copias.

1. TIPOS DE RESPALDO

Respaldo de día cero. Es el tipo de respaldo que se hace al sistema con su configuración original, tal como lo entrega el fabricante y antes de realizar cualquier cambio en él.

Respaldos completos. Consiste en hacer un respaldo completo del sistema, es decir de todos los archivos que hay en el incluyendo los archivos ocultos, archivos del sistema, áreas del sistema o temporales, archivos con líneas cruzadas o ligas, etc.

Respaldos parciales. Como alternativa a una copia de seguridad completa, el usuario puede seleccionar los archivos y/o directorios que desea copiar, y el software los leerá y escribirá de uno en uno. Esto permite la restauración rápida de un archivo o grupo de archivos.

Sin embargo debe prestarse atención aciertos detalles. Un disco fijo completamente operativo dentro de una computadora representa el

resultado de un proceso de evolución. Se ha instalado y en algunos casos personalizado el software, se han incorporado utilidades, creando scripts o macros, y se han afinado los archivos del sistema para obtener un mejor rendimiento. Reconstruir un disco fijo tras un problema importante requiere mucho más trabajo que el presentado por la simple copia de los archivos de datos o programas. La instalación del software puede resultar un proceso largo que en ocasiones requiere de numerosos parámetros, cuya combinación adecuada se determina generalmente mediante un amplio proceso de prueba y error. Si no existe una copia de seguridad de los archivos de configuración del sistema, y de las aplicaciones, devolverlo a un estado de funcionamiento normal puede ser bastante complicado.

Una solución adecuada es realizar copias de seguridad completas a intervalos mayores, mientras se hacen copias de seguridad de los archivos de datos con mayor frecuencia.

Respaldos incrementales. Otro de los tipos de copias de seguridad a considerar es la incremental. Consiste en realizar exclusivamente copia de seguridad de los archivos que han sido modificados desde la última copia de seguridad. La idea consiste en que las copias de seguridad sucesivas de todos los archivos de datos contendrán probablemente archivos de los que ya se ha hecho copia de seguridad. Esto hace más lento el proceso de copia. Se pueden realizar respaldos incrementales que se apliquen exclusivamente a los archivos modificados o incluidos desde la última copia de seguridad.

2. ESTRATEGIAS DE RESPALDO

La estrategia de respaldo consiste en ver cuándo deben realizarse las copias de seguridad. Obviamente esto depende de la frecuencia con que se modifica la información en un sistema. Debe tomarse en cuenta lo siguiente:

- Tiempo y esfuerzo representado por las modificaciones a los archivos.
- Tiempo y esfuerzo representado por la copia de seguridad de los archivos.
- Valor del contenido de los archivos.

Así mismo, pueden combinarse los niveles descritos anteriormente, basados en intervalos distintos.

Intervalo 1 Copia de seguridad total
Intervalo 2 Copia de seguridad de archivos de datos
Intervalo 3 Copia de seguridad incremental de archivos de datos.

Por ejemplo:

- Hacer un respaldo completo el primer día de cada mes.
- Hacer un respaldo de los archivos de datos semanalmente.
- Hacer un respaldo incremental todas las noches, de todo lo que ha cambiado desde principio de mes.

El punto principal es que no todas las copias de seguridad tienen que ser completas-lentas, y un esquema con copias completas y parciales necesitará menos tiempo y por lo tanto, presentará más posibilidades de ser respetado.

ROTACION DE COPIAS DE SEGURIDAD

Una vez estudiados los factores que determinan que se necesita para realizar un respaldo y cuando hacerlo, se debe considerar la manipulación física de los soportes de copia de seguridad.

- ¿Dónde almacenarlos?
- ¿Cuántas copias se van a tener?
- ¿Cuál puede ser un buen lugar fuera de la instalación?

Una propuesta al programa de gestión de los soportes de copia es el método rotativo en tres fases. Este requiere el uso de dos soportes de copia de seguridad, lo que implica que los archivos siempre estarán en tres lugares a la vez: la copia de seguridad 1, la copia de seguridad 2 y el original. Este régimen se inicia haciendo la copia de seguridad 1 y almacenándola en un lugar seguro, fuera de la instalación, llamado posición A (figura 3.14).

Tras un intervalo adecuado, se realiza la copia de seguridad 2. Esta se lleva a la posición A. Después se pasa la copia 1 a un lugar seguro, dentro de la instalación, llamado posición B (figura 3.15)

Transcurrido otro intervalo, se saca la copia de seguridad 1 de la posición B y reutiliza el soporte para hacer la copia de seguridad 3. Entonces, ésta se lleva a la posición A, y la copia 2 se pasa a la posición B y así sucesivamente (figura 3.16).

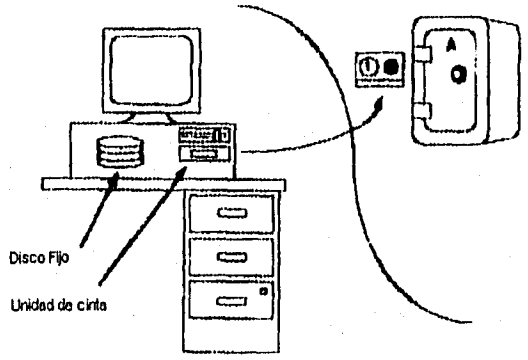

Fig. 3.14 El primer paso en el régimen de copias de seguridad es guardar la copia más reciente fuera de la instalación.

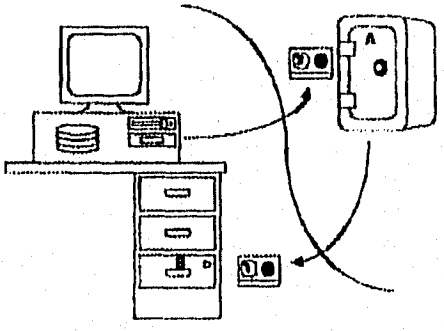

Fig. 3.15 El segundo paso del régimen de copia de seguridad

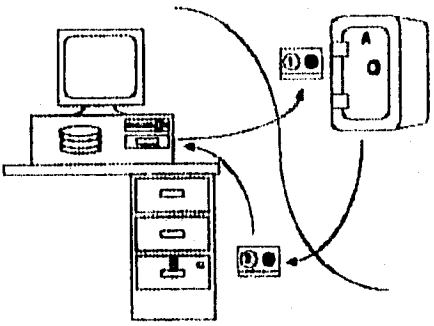

Fig. 3.16 El tercer paso del régimen de copia de seguridad

La copia de seguridad almacenada fuera de la instalación será siempre la más actualizada. La copia guardada en la instalación corresponde al intervalo inmediatamente anterior. Si los archivos sufren algún daño, se puede utilizar la copia almacenada fuera de la instalación. En el caso de que ésta última también presente problemas, se puede usar la copia guardada en la propia instalación como punto de partida.

Una recomendación adicional cuando se manejan conjuntos rotatorios de copias de seguridad es marcar cada uno con etiquetas de diversos colores, además de identificar claramente en la etiqueta a que conjunto pertenecen los medios.

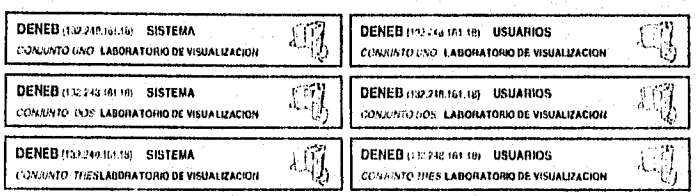

Fig. 3.17 Etiquetas para conjuntos de cintas de respaldo.

TIEMPO EMPLEADO EN COPIAS DE SEGURIDAD.

Es muy importante considerar la hora del día en que deben realizarse los respaldos.

Por ejemplo, parece natural hacer copias de seguridad al final de la jornada y entonces guardarlas. Como algunos sistemas de seguridad, tales como las unidades de cinta, permiten activar automáticamente las copias de seguridad, algunas personas dejan sus equipos conectados durante la noche y hacen que la copia de seguridad se realice bajo el control del software. Esto minimiza las molestias para los usuarios. Sin embargo, aunque el equipo trabaje de forma fiable, esto representa el problema de realizar la copia de seguridad en una hora de alto riesgo.

El robo de computadoras, el sabotaje de archivos y catástrofes tales como incendios suelen suceder con menor probabilidad de detección durante la noche. Una operación de respaldo nocturna sin vigilancia no tiene protección alguna frente a estas amenazas. Además si el soporte de copia permanece en la computadora hasta la llegada de un operador por la mañana, puede estar expuesto a algún robo.

Una alternativa por ejemplo, es combinar las técnicas de realizar copias de seguridad, con una adecuada y eficiente seguridad física.

3. SOPORTES EMPLEADOS PARA COPIAS DE SEGURIDAD

Diskettes

A pesar de las mejoras que se ha realizado a los diskettes en cuanto a capacidad, en los últimos años, éstos siguen representando el nivel inferior de la escala de eficiencia a la hora de archivar copias de información.

Los diskettes son un soporte económico para copias de seguridad. Bien probados y certificados son fiables, asequibles, resultan familiares a todos los usuarios y pueden considerarse como muy efectivos para copias de seguridad de datos a pequeña escala.

Sin embargo, en relación al tamaño de los discos fijos, ofrecen una capacidad de almacenamiento muy limitada. Por ejemplo, para hacer una copia de seguridad de un disco fijo de 450 megabytes, se requerirían alrededor de 322 discos de 3.5" de 1.44 megabytes.

Aunque los discos son económicos, el costo se incrementa cuando se habla de decenas de diskettes. Además la limitada capacidad de éstos se hace enojosa al almacenar un archivo grande, como una base de datos. Si el archivo no cabe en un disco, debe distribuirse en varios, lo que requiere el uso de un programa de copia de seguridad en lugar de una simple orden de copia. Esto impide el uso de los diskettes como un modo de almacenamiento en línea para grandes archivos.

Por otro lado, el funcionamiento de los diskettes es relativamente lento. "Un disco fijo normal gira a unas 3000 rpm. Un diskette puede girar a 300 rmp. Esto da alguna idea de la diferencia de velocidad entre los diskettes y los discos fijos". Almacenar datos en un diskette necesita tiempo, más de un minuto por megabyte. Multiplicado por el número de

megabytes de los que hacer copia de seguridad, este factor de velocidad se convierte en factor de aburrimiento.

Además la gran cantidad de discos requeridos para realizar una copia de seguridad completa seguramente resultará difícil de manejar y gestionar física y lógicamente.

Cintas

Las ventajas principales ofrecidas por las unidades de cinta son su alta capacidad y su simplicidad mecánica. Mientras que los diskettes necesitan una cabeza de lectura-escritura que requiere ser posicionada con exactitud, la cabeza de una unidad de cinta es estática, y la cinta simplemente para por ella. El proceso de lectura-escritura sólo tiene que tratar con la distancia a lo largo de la cinta. Sin embargo, esta simplicidad, implica el inconveniente de que el acceso a una posición específica tiende a ser mucho más lento.

Los problemas de la cinta se presentan cuando se comienza a almacenar y recuperar datos. Recorrer la cinta de principio a fin para localizar unos datos determinados puede requerir mucho tiempo.

La velocidad con que las unidades de cinta pueden hacer copia de un disco fijo varía según el diseño del hardware y el tipo de respaldo realizado.

Algunos sistemas de cinta utilizan un tipo de formato en el cual dejan una serie de marcas en la cinta para permitir que el mecanismo maneje posiciones relativas. Sin embargo, esto tiene que llevarse a cabo antes de usar la cinta para copia de seguridad lo cual requiere tiempo adicional.

Existe un método para almacenar datos en cinta que evita la necesidad de formateo previo, el streaming, en el que los datos son introducidos en la cinta en un flujo (stream) continuo (dando lugar al término unidad de cinta streamer). Estas unidades de cinta ofrecen una transferencia rápida de datos para realizar la copia de seguridad, pero resultan algo más lentas a la hora de localizar los datos.

Una solución al problema de localización de los datos usada por algunas unidades de cinta streamer consiste en emplear el método conocido como posición de bloques, en el que la unidad de cinta introduce señales en la cinta a intervalos regulares a medida que introduce los datos.

Para resistir el esfuerzo y desgaste que supone el funcionamiento, los cartuchos de cinta usados para copia de seguridad están construidos siguiendo normas más estrictas que las cintas normales para música. Además, se pueden usar cintas más fuertes y anchas.

Existen diversos tipos de cintas que pueden utilizarse, tales como las cintas de 8mm o las cintas de 9 pistas. Así mismo podemos utilizar unidades que emplean la tecnología DAT (Digital Audio Tape). Este utiliza un método de grabación en cinta mucho más preciso y sofisticado, que en aplicaciones de audio por ejemplo pueden superar la fidelidad de los CD. Las unidades DAT para copias de seguridad utilizan cinta de alta calidad de 4mm y tienden a ser ligeramente más lentas que las cintas de 8mm. Ofrecen un gigabyte de almacenamiento, y en algunos sistemas hasta dos gigabytes.

Medios de almacenamiento óptico

En la superficie de un disco óptico puede introducirse cualquier información, incluyendo imágenes y datos. Estos medios funcionan digitalizando la información y almacenando los datos digitales como patrones en una superficie circular. El patrón de la superficie puede ser reproducido económicamente con las técnicas modernas de modelado y la superficie codificada puede ser protegida por una capa de plástico transparente. Al introducir el disco en una unidad, gira a alta velocidad y es recorrido por un haz de luz láser que barre la superficie. Los datos son leídos como reflexiones en la superficie grabada.

Su durabilidad y precisión hacen que los discos ópticos ofrezcan un gran potencial como dispositivo de almacenamiento. Sin embargo la desventaja de estos medios de almacenamiento que es que tanto los discos como las unidades son bastante caros.

CD-ROM

Abreviatura de memoria de sólo lectura en compact disc, CD-ROM es un sistema de almacenamiento de datos en discos ópticos. Los discos CD-ROM están diseñados para ser creados por un distribuidos de información producidos en masa. Estos discos pueden leerse en unidades CD similares a las utilizadas en los CD musicales. La cuestión importante consiste en que el CD-ROM no permite en absoluto que el usuario escriba algo en el disco. Aunque esto descarta al CD-ROM como dispositivo de copia de seguridad en el sentido normal, sigue siendo una tecnología valiosa para aquellos que trabajan con grandes cantidades de datos. Por ejemplo, algunos sistemas de información ofrecen ahora datos históricos en compact disc. Estos pueden ser actualizados en forma regular. El proceso de actualización es simple: se tira el CD anterior cuando llega el nuevo. Esto es posible porque el costo de los CD ordinarios es bastante bajo, frente a los dispositivos ópticos reescribibles.

4. SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

Los discos y las cintas magnéticas son usadas para almacenar datos entre los pasos de trabajo y para almacenar archivos de los sistemas. El manejo idóneo de discos y cintas es necesario para prevenir la pérdida de datos y para reducir errores de lectura y escritura.

Algunas reglas que deben seguirse para el manejo de los discos son:

- Poner los discos una caja cerrada, excepto cuando sean montados en los drives.
- No permitir fumar cerca al funcionar los drives o cuando los operadores estén manejando los discos.
- Mantener los drives cerrados excepto cuando se estén descargando o cargando discos.
- Manejar los discos de acuerdo a las instrucciones definidas por los supervisores y los fabricantes.

Así mismo, los operadores deben observar las siguientes reglas cuando monten o desmonten cintas en las unidades de cinta:

- Manejar las cintas universales (soportadas en un carrete), cerca de las unidades de cinta, para evitar quebrar los lados de las cintas al transportarla. Aplicar una presión normal en la parte central en vez de forzarla al oprimir o empuñar en borde para que entre el carrete.
- Mantener cerradas las puertas de la unidad de cinta excepto durante el montaje o desmontaje, y verificar que la secuencia de descarga electromecánica sea finalizada antes de que la puerta se abra.
- Limpiar las cabezas de lectura y escritura regularmente en acuerdo con a las políticas establecidas por el supervisor.

- Asegurarse que sus manos estén limpias cuando maneje las cintas ya que las partículas saladas y aceites pueden contaminarlas.
- Mantener las cintas universales en contenedores protegidos cuando no están en uso y cerrarlos para asegurar de guardar fuera el polvo.

Las cintas en mal estado pueden ocasionar señales de falla. Las abolladuras ocurren cuando una partícula es rolada en la parte de arriba de una cinta y ésto ocurre cuando la cinta es pinchada o cuando es tratada descuidadamente o removida desde la guía. Las abolladuras pueden ser evitadas por cintas limpiadoras que vienen dentro al contacto con materia extraña. Las arrugas pueden ser evitadas con un manejo muy cuidadoso de las cintas.

Si una cinta se ha caído debe ser cuidadosamente examinada por el operador para ver si el devanado está hundido o si la cinta esta dañada de cualquier forma. Si una cinta está arañada, debe ser etiquetada como una cinta caída y ser regresada a la biblioteca de cintas para su mantenimiento. Si un devanado está hundido, debe hacerse un esfuerzo para copiar la información a una nueva cinta.

Biblioteca de cintas y discos.

El acceso a una biblioteca de discos debe ser restringido para el bibliotecario y su personal. El acceso temporal puede ser concedido temporalmente a personal específico por el supervisor de operaciones o el supervisor de control de producción.

El bibliotecario, es el encargado del resguardo de las cintas y los discos. Para llevar a cabo esta función debe realizar lo siguiente:

- Mantener una lista de inventario de todas las cintas y discos con la siguiente información: archivo del usuario, número de serie del volumen, nombre de archivo y descripción, trabajo o número de proyecto, fecha de creación y período de retención.
- Documentar la posesión de un material prestado por otras locaciones por el archivo del usuario, número de serie del volumen, nombre del archivo y descripción, fecha recibida y fecha de regreso.
- Grabar las nuevas cintas y discos como parte del inventario.
- Checar y limpiar periódicamente las cintas. Las cintas viejas y discos deben ser desahuciadas antes de ser destruidas. El gerente del centro de procesamiento de datos a su vez, debe certificar la destrucción de todas las cintas dañadas e inventarios periódicos deben hacerse para asegurar que la biblioteca posea listas de inventarios correctas.

El bibliotecario es responsable de arreglar la transferencia de archivos de respaldo hacia una locación externa como parte de un plan de desastre. Todas las cintas magnéticas y los discos deben ser almacenados en la biblioteca cuando no se usen y no es permitido fumar en esta área.

Así mismo, es responsable de las entradas y salidas de todas las cintas y discos de la biblioteca, así como de las acciones pertinentes a la recuperación del material prestado.

Antes de entregar cualquier cinta, debe recibir una lista donde especifique trabajo, numero de control, nombres de los archivos, numero del volumen y nombre de la persona que está realizando el requerimiento, con estos datos debe checar que la persona se encuentre dentro de la lista de usuarios autorizados, para poder proporcionarle lo que requiere.

En adición a las medidas que deben tomarse referentes a las instalaciones físicas del centro de cómputo, las cuales también deben ser tomadas para el área de la biblioteca. También debe considerarse lo siguiente:

- La temperatura debe estar entre los 15 y 25 Centígrados y la humedad relativa entre el 40 y 60 por ciento. Todas las cintas que ingresen deben tener un periodo de 24 horas para ajustarse a las condiciones normales del cuarto antes de ser usadas.
- Las cintas magnéticas y los discos deben ser almacenados al menos a 4 pulgadas de las columnas del edificio y de estructuras similares reforzadas con acero. Esto es para prevenir los campos magnéticos generados.

3.6.3 SEGURIDAD EN PC'S

Las pc's están siendo cada vez más importantes herramientas tanto para uso privado como para los negocios. Pero pasa que ésta tecnología es desarrollada e implementada antes de que haya alguien habilitado para manejar el equipo. Las pc's rápidamente se han dispersado y son utilizadas para diversas funciones. Esto ha causado que la seguridad de la información no sea planeada adecuadamente. Este problema es especialmente claro cuando están conectadas a redes de telecomunicaciones. Recordaremos que la seguridad de la información, también incluye la protección física de las pc's, así como la protección de la información de la compañía, sistemas y organización. La experiencia ha mostrado lo necesario que es implementar medidas para combatir el uso incontrolado de las computadoras, lo cual ha causado serias brechas de seguridad de la información.

Procedimientos y medidas de seguridad

La siguiente es una lista de procedimientos de seguridad y sugerencias de medidas. Estos tips pueden parecer superficiales pero debe tenerse en mente que los nuevos usuarios de computadoras a menudo no están familiarizados con los conceptos de seguridad de la información y para ello es una nueva situación el tener responsabilidad por el equipo, el software y los medios de almacenamiento.

Aspectos críticos que deben tomarse en cuenta a la puesta en marcha.

Las reglas y las estrategias deben ser trabajadas para permitir el control de cómo y dónde las pc's serán usadas y cómo será la

compatibilidad con otros equipos. Las reglas deben ser flexibles, pero no tan liberales. El administrador deberá aprobar y soportar las reglas.

Todas las negociaciones sobre la compra de pc's y asociadas al software deben ser aprobadas por un grupo de especialistas para obtener el mejor control posible sobre la compatibilidad y precio antes de firmar el contrato.

Clarificar la responsabilidad del usuario.

El usuario tiene la responsabilidad de la producción del sistema; debe tener cuidado del equipo, del software y proveer seguridad a los programas y a los datos. El usuario no puede adelantarse a las expectativas y a los datos para tener cuidado con estos.

Es vital reforzar los derechos de la compañía a checar el software y los datos en uso. Debe haber reglas claras para el uso privado del equipo, especialmente para el uso del software y de la información.

Seguridad cuando las pc's están conectadas a un mainframe.

Antes de conectar una pc a un mainframe, asegurarse que la pc está sujeta a las mismas reglas y control de acceso, passwords, códigos de identificación y autorización como otros equipos terminales.

Es posible conectar una pc a la computadora por medio de una línea telefónica, pero debe haber reglas para guardar el número telefónico y el password en secreto. Equipos especiales de controles de

línea pueden ser una buena idea si el acceso será dado a información sensitiva.

Manejo de los medios de almacenamiento de las pc's.

Como regla general los medios de almacenamiento de las pc's deben ser manejados de acuerdo a las políticas para documentos, microfilms, etc. Si una pc tiene un disco duro, el acceso debe ser controlado por una protección de password y posiblemente también por el encriptamiento de la información. Nunca permitir a los usuarios dejar diskettes o información lista para usar en una pc desalendida. Asegurar que los medios sean destruidos y los datos borrados cuando éstos ya no tengan relevancia.

Proveer instrucciones para manejo de los medios que puedan prevenir daños por polvo, calor, comida, bebidas, campos magnéticos, etc. Asegurar que los medios particularmente importantes y/o grandes volúmenes de información o datos (fuentes de software, diskettes originales, etc) sean guardados en lugares específicos protegidos contra fuego y contra altas y bajas temperaturas.

El implemento de reglas de etiquetado físico o lógico para los medios, con número de serie, número de archivo, número de programa, clave del dueño, nivel de clasificación, etc., evita mezclar programas y archivos en el mismo diskette. Los datos privados y la información de la compañía no deben ser mezclados tampoco. Los medios con información sensitiva deben ser marcados con etiquetas de diferentes colores. Siempre debe procurarse tener respaldos de archivos en los discos duros, diskettes y cintas. Es una buena regla realizar copias de respaldo tan pronto como los archivos y programas importantes sean alterados.

Control del software y de la documentación

Los usuarios deben ser informados que está prohibido copiar medios protegidos con derecho de autor (Copyright) y que esa violación puede traer grandes problemas tanto a ellos mismos como a la compañía.

Asegurarse que los programas desarrollados sean documentados propiamente para que otros usuarios en la compañía puedan hacer uso de ellos. Asegurarse que todos los programas sean completamente probados y que sus resultados sean confiables. Los reportes deben pasar a través de los mismos controles. Esto es especialmente verdadero cuando los reportes contienen información vital para los negocios.

Seguridad física de las pc's

Implementar reglas para el lugar de trabajo de las pc's: incluir cualquier requerimiento concerniente al mobiliario de oficina, extinguidores, suministro de energía, como prevenir la electricidad estática, la seguridad de los medios, etc.

Generalmente hablando de pc's y equipos para pc's, éstos son fáciles de cargar y revender. Las oficinas deben permanecer cerradas cuando las personas autorizadas no estén presentes. Si el equipo está localizado donde hay mucho tráfico (una recepción por ejemplo), debe asegurarse con cerraduras extras. Los equipos localizados en planta baja y visibles desde afuera, deber ser cubiertos después de las horas de oficina. También asegurarse que las pólizas de seguro cubren el equipo y los medios.

En general el procesamiento distribuido de datos por medio de pc's, proporciona recursos para ser utilizados en forma racional, particularmente en términos de eficiencia de la oficina. Los usuarios deben ser informados acerca de las medidas especiales de seguridad que requieren las pc's. Así mismo debe haber un seguimiento activo para verificar que las medidas de seguridad están funcionando.

REFERENCIAS

1.- Diccionario de la lengua española,
Real Academia Española,
España 1992.

2.- Roger S. Pressman,
Ingeniería del software: un enfoque práctico,
E.D. Mc Graw Hill,
México 1988.

3.- Manual de inducción,
Banamex.

4.- Simson Garfinkel and Gene Spafford,
Practical Unix Security,
E.D. O'Reilly & Associates, Inc.,
E.U.A. 1992.

5.- Diego Zamboni,
Poyecto UNAM/CRAY de Seguridad en el S.O. Unix,
México 1995.

6.- John G. Burch Jr.,
Computer Control and Audit: A Total Systems Approach,
E. D. Willey,
E.U.A. 1978.

7.- Department of Defense Trusted Computer System Evaluation Criteria,
Departmen of Defense of the U.S.A.
E.U.A. 1985

8.- Leonard H. Fine,
Seguridad en Centros de Cómputo,
E.D. Trillas,
México 1988.

9.- Ricardo Rivera Soler,
Apuntes de la materia de Administración de Centros de Cómputo,
Lic. en Informática. FCA. UNAM.

10.- Daler, Gulbrandsen, Melgard, Sjølstad,
Security of Information and Data,
E.D. Ellis Horwood Limited,
Inglaterra 1989.

11.- Diego Zamboni,
Apuntes de Seguridad en el S.O. Unix,
Dirección General de Servicios de Cómputo Académico.

12.- Laurence Dwight Smith,
Cryptography,
E.U.A. 1955.

13.- *Handbook of Computer Communications Standards*,
Stallings William,
E.D, Macmillan Computer Publishing,
E.U.A. 1990

14.- *Communication Networks Management*,
Terplan Kornel,
E.D. Prentice Hall,
E.U.A., 1992.

15.- Stephen Cobb,
Manual de Seguridad para Pc y Redes Locales,
E.D. McGraw Hill,
México 1994.

16.- Slosse Carlos,
Auditoría. Un nuevo enfoque empresarial,
E.D. Ediciones Macchi,
Argentina 1990.

17.- E. Alcalde, M. García, S. Peñuelas
Informática Basica
E.D. Mc Graw Hill
México 1988

18.- Royal P. Fisher,
Information Systems Security,
E.D. Prentice Hall Inc.
U.S.A. 1984.

CAPITULO IV

SEGURIDAD EN REDES Y TELECOMUNICACIONES

Como se vió en el capítulo I, la informática ha facilitado el manejo y proceso de la información, sin embargo cada vez y con mayor frecuencia se precisa la información en un lugar distinto, algunas veces lejano, de donde es producida. De igual modo los datos no se obtienen siempre en el mismo lugar en el que van a ser procesados.

La sociedad actual exige disponer tanto de los datos como de la información con rapidez y fiabilidad. Por ejemplo, en la reserva de pasajes de avión desde una agencia de viajes o en el manejo de una cuenta corriente desde una sucursal bancaria.

Ante el problema de la distancia entre el lugar de la producción de datos y el lugar de procesamiento de los mismos, las telecomunicaciones juegan un papel muy importante. Esto es debido a que implican todo lo relacionado con la comunicación y la transmisión de información a distancia.

El hecho de que se haya decidido incluir un capítulo referente a la seguridad en redes y telecomunicaciones parte de que para la mayoría de la gente involucrada en las actividades de comunicación, el área de seguridad es hasta cierto punto desconocida. En general, no existen políticas claras sobre lo que se debe proteger en este ambiente; si deben ser las aplicaciones, bases de datos, archivos, nodos, enlaces de comunicación, dispositivos del usuario final o una combinación de todo éste.

Podemos iniciar diciendo que la seguridad en redes y comunicaciones comienza por aplicar todo lo que se ha visto hasta ahora, pero también involucra ciertos aspectos específicos a las redes como los que mencionaremos a continuación.

4.1 DEFINICION DE TELECOMUNICACIONES Y REDES.

Podemos entender por telecomunicaciones un "sistema de comunicación a distancia por medio de cables y ondas electromagnéticas".[1]

Así mismo denominamos red de telecomunicaciones al medio físico empleado para la transmisión de datos e información.

De forma genérica y en términos de computación puede decirse que una red "es un sistema de intercambio de comunicaciones e información basado en computadora, creado mediente la conexión física de dos o más computadoras".[2]

4.2 CLASIFICACION DE LAS REDES

4.2.1 POR SU USO

De acuerdo a la utilización que se les de a las redes, éstas se clasifican en:

A. REDES DE USO EXCLUSIVO

Se caracterizan porque son instaladas o alquiladas por uno o varios usuarios para su uso exclusivo, estando cerradas, por tanto, a las comunicaciones de otros usuarios ajenos.

Red punto a punto.

Consiste en una conexión fija reservada en exclusividad entre dos estaciones . Es la forma de conexión más utilizada hasta ahora.

Red multipunto.

En ella se conectan varias terminales a una computadora central por medio de una sola línea de teleproceso.

B. REDES PUBLICAS DE TELECOMUNICACION.

Son las redes que pertenecen a grandes compañías u organismos oficiales y están abiertas a la comunicación de cualquier usuario que se conecta a la misma, normalmente mediante un contrato de alquiler, asignandole un identificativo que le permite intercambiar información con cualquier otro usuario.

RDI

La red digital integrada(RDI) se basa en la red publica telefónica pero completamente digital, capaz de transportar voz, vídeo y datos, buscando ofrecer a los usuarios una solución integral confiable, flexible y disponible.

La RDI esta formada por dos elementos:

- Red Terrestre
- Red Satelital

Red Terrestre

Constituye la infraestructura fundamental de RDI y se basa en sistemas de transmisión y conmutación completamente digitales. La arquitectura de la red contempla la utilización de nodos jerárquicos distribuidos dentro del área urbana e interconectados entre si mediante sistemas de transmisión de alta capacidad, que permiten establecer comunicación entre dos puntos dentro de una ciudad o en distintas localidades.

Red Satelital

Creada para ofrecer servicios a usuarios en zonas donde no se cuente todavía con infraestructura de red terrestre, cuenta con dos aplicaciones principales:

- Estaciones terrenas remotas de baja capacidad (VSAT) para servicios de voz y datos.
- Estaciones terrenas semimaestras para alta densidad de trafico, tales como zonas turísticas, zona hoteleras o parques industriales.

4.2.2 POR SU DOMINIO GEOGRAFICO.

Las redes se comunicaciones se clasifican de acuerdo al tamaño del lugar donde se sitúan en:

- Redes de áreas local
- Redes de área metropolitana
- Redes de área amplia.

A. REDES DE AREA LOCAL (LAN)

Una red de área local (LAN del inglés Local Area Network) se define como "aquella que está instalada en un dominio geográfico limitado".[3] se caracteriza, porque abarca áreas relativamente pequeñas, usualmente son confiadas a edificios, campus y parques industriales. Generalmente son usadas en un 80% para procesar la información local. Básicamente estas son usadas para compartir recursos, procesamiento, almacenamiento de datos, software y periféricos.

Las redes de computadoras en área local, en los últimos años, han experimentado un crecimiento explosivo. Las redes se pueden conectar a otras redes, las LAN se conectan a cables públicos para crear una extensa área de redes, los cuales, en su momento utilizan conexiones internacionales para crear redes de área global.

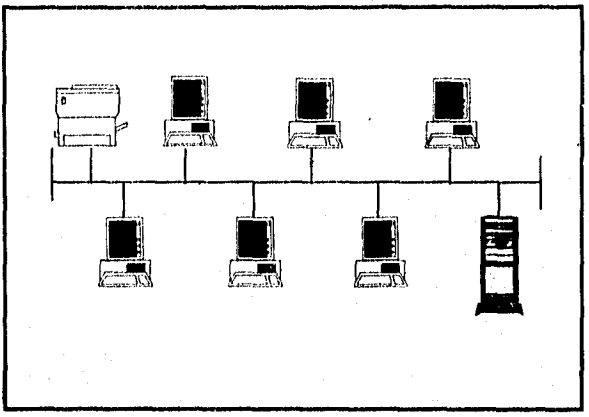

Figura 4.1

B. REDES DE AREA METROPOLITANA (MAN)

Las redes de área metropolitana o redes MAN (del ingles Metropolitan Area Network) son redes que cubren el territorio geográfico de una ciudad, que a su vez pueden tener conectadas redes de área local.

En años recientes, un nuevo tipo de redes llamadas Redes de Area Metropolitana (MAN), se han estado desarrollando. Las redes de área metropolitana contienen todas las características de las redes de área

local; la diferencia es que las MAN cubren distancias mucho mas grandes (alrededor de 50 kms) y, generalmente, operan distancias mucho más grandes (alrededor de 50 kms) y generalmente operan a altas velocidades (mayores de 45 Mbps)

Este tipo de redes que se utilizan en el área metropolitana interconectando, edificios, compañías, campus, etc. Que se localizan en diferentes colonias, delegaciones, municipios de la misma ciudad o estado.

Las redes MAN pueden tener interconexión con redes WAN y LAN mediante algún dispositivo de interconectividad (gateways, routers, etc.)de redes correspondiente. Una red de área metropolitana puede ser usada por una organización o por diversas organizaciones y puede ocupar también la red publica conmutada.

C. REDES DE AREA AMPLIA (WAN)

Una red de área amplia generalmente es interpretada como una red internacional, las redes de área amplia o redes WAN (del ingles Wide Area Network) son sistemas que enlazan computadoras y otros dispositivos, a otras computadoras o redes en localidades remotas. Las redes de área amplia comunican áreas geográficas muy grandes; como diferentes ciudades, diferentes estados, diferentes países e incluso diferentes continentes.

Los medios de transmisión generalmente usados son los enlaces satelitales, enlaces de microondas digitales y transmisión por fibra óptica.

Durante la década de los 80's se hablaba del beneficio de tener microcomputadoras conectadas entre si, compartiendo recursos, sin embargo, las necesidades del mercado actual ya no se basan en las comunicaciones locales, sino en comunicaciones remotas, constituyendo ahora el concepto de red de área amplia (WAN). Ahora con el simple hecho de levantar el teléfono estamos en línea directa con cualquier punto del mundo, cumpliendo con la expectativa esperada en los 90s de tecnologías de conectividad e interoperabilidad que sean independientes del protocolo y de equipos propietarios.

Una red local se convierte en parte de una WAN cuando se establece un enlace a un mainframe, a una red publica de datos o incluso a otra red, esto a través del uso de módem, líneas telefónicas, satélites o conexiones directas.

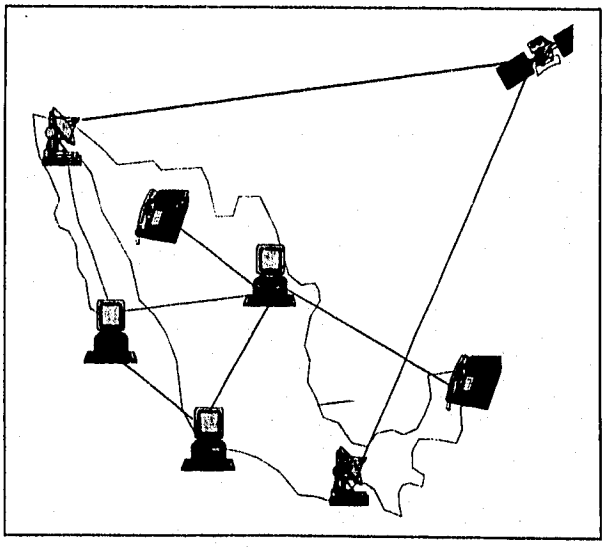

Figura 4.2

DIFERENCIAS ENTRE LAN, MAN, WAN

Cuatro características básicas distinguen a cada uno de estos tres tipos de redes:

Primera: La delimitación y extensión de la red (la distancia que separa a los dispositivos) y las velocidades de transmisión de datos empleados, este punto se encuentra íntimamente relacionado con el medio de transmisión;

Segunda: La probabilidad de errores durante la transmisión y por lo tanto los mecanismos de detección y recuperación de errores que deben implementar los protocolos correspondientes;

Tercera: El carácter privado de la sudred, esto es, la propiedad de la información que se contiene en los diversos dispositivos conectados a las subredes y

Cuarta: Los eventos que se consideran al momento de su plancación. Mientras que los diseñadores de una WAN se ven forzados (por razones legales, económicas ó políticas) a utilizar la telefonía publica existente los diseñadores de las MAN y LAN tienen completa libertad de hacer uso de la tecnología de red o medio de transmisión que consideren conveniente.

4.3 ELEMENTOS DE UNA RED

A continuación se describe cada uno de los elementos que conforman una red:

SERVIDOR

El servidor es la computadora central que nos permite compartir recursos y es donde se encuentra alojado el sistema operativo de red.[1]

El servidor es el corazón de la red. Ya que nos provee el acceso controlado a los archivos, permite compartir impresoras y otros recursos dentro de la red.

Existen varias reglas que hay que tomar en cuenta para escoger el servidor más adecuado. La más importante es que este sea compatible con el tipo de sistema operativo de red que se escoja.

Adicionalmente, esta máquina debe tener la suficiente capacidad de procesamiento para llevar a cabo las tareas de la red y contar con suficientes ranuras para expansión (tarjeta de expansión, tarjetas de interfase, etc.). El disco duro utilizado en el servidor debe ser soportado por el sistema operativo de red y debe tener la capacidad adecuada para cubrir requerimientos actuales y futuros de almacenamiento de información.

ESTACION DE TRABAJO

Las estaciones de trabajo son computadoras interconectadas por una tarjeta de interfase. Ellas compartirán recursos del servidor y realizaran un proceso distribuido.

El proceso de datos en una red es distribuido, por lo tanto el desempeño de la estación de trabajo se debe definir en función a la aplicación que se estará manejando en ella. Analizar el tipo de aplicaciones que estarán manejando en la red es de suma importancia para lograr que la estación sea la adecuada.

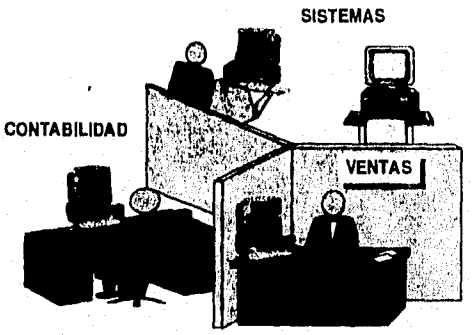

figura 4.3

TARJETA DE INTERFASE

Las tarjetas de interfase nos permitirán el enlace a la red. Es decir cada estación de trabajo contara con una tarjeta de interfase (NIC) en la cual se conectara al cableado de red.

Las variedades de las tarjetas de interface están determinadas por la topología de la red y el tipo de cableado. Existen dentro del mercado una gran cantidad de tarjetas de interfase y no existe una cifra exacta de la base instalada (cantidad de tarjetas instaladas en el mundo) de cada una de ellas. La mayoría de los estudios muestran el predominio de las tarjetas Ethernet, Arcnet y Token Ring.

SISTEMA OPERATIVO DE RED

Es el software que se encarga de administrar los recursos que se estarán compartiendo (discos duros, impresoras, etc.) y a los usuarios.

El sistema operativo se escoge según las necesidades de control de nuestra información. Existen algunas consideraciones como son: el tipo de información que se estará compartiendo, los programas que se utilizaran, quien tendrá acceso a cierta información, etc. El sistema operativo escogido nos debe dar toda la seguridad que se requiere dentro de la red. Esta debe ir desde que máquina se pueda usar, a que hora se puede entrar a la red y que día se puede trabajar, hasta que clave de acceso tendremos, los archivos que se podrán compartir y los programas que se ejecutaran, etc.

CABLEADO

Las redes utilizan diferentes tipos de cable para su conexión. El cable que se utilizara en las instalaciones es de suma importancia ya que cada uno ofrece diferentes características en costo, facilidad de instalación, confiabilidad de conexión, distancia máxima, etc. Por ejemplo, el cable telefónico permite una distancia de 100 mts., el cable coaxial grueso nos da una distancia máxima de 500 mts. , mientras que la fibra óptica nos puede da una distancia hasta de 2 kms. Todo esto dependerá de la ubicación física de las máquinas que estarán conectadas dentro de la red.

También, es importante tomar en cuenta el tipo de topología que se estará utilizando, ya que esto también nos indicara el cable que se debe colocar.

Actualmente las instalaciones que mas predominan son las de cable coaxial, básicamente por costo y la facilidad de instalación. Este tipo de cable se utiliza para las topología Arcnet y Ethernet, aunque también se utiliza el cable telefónico para Ethernet.

El cable telefónico nos permite una instalación menor, es más barato y fácil de instalar ya que se puede utilizar los ductos por los cuales están pasando las líneas del conmutador que tenemos instalado en el edificio.

El cable coaxial grueso, al igual que la fibra óptica, se utiliza cuando las distancias son muy grandes o cuando el cable va a estar pasando por áreas de gran concentración magnética.

CABLE TELEFONICO

El cable telefónico (UTP, STP), utiliza dos alambres que se encuentran aislados y torcidos. El beneficio que se tiene con el torcimiento de los pares, es que se evita interferencia entre señales. El par torcido esta protegido por una capa exterior aislada llamada Jacket.

Las ventajas que ofrece este tipo de cable son las siguientes:

- Tecnología conocida
- Fácil y rápido de instalar
- Emanación mínima de señales magnéticas

CABLE COAXIAL

El cable coaxial esta compuesto de un alambre (un conductor) cubierto de una placa que actúa como tierra. El conductor y la tierra están separados por un aislante, con todo el cable protegido por un jacket aislante en la parte exterior.

El cable coaxial puede ser de varios tipos y anchos. El cable coaxial grueso transporta las señales a distancias más grandes que el cable delgado. El cable grueso es más caro y menos flexible.

Las ventajas principales del cable coaxial son las siguientes:

- Soporta dos diferentes sistemas de transmisión que son banda ancha y banda base.
- Transmite voz, vídeo y datos.

- Instalación relativamente sencilla.
- Tecnología fácil de entender.
- Gran disponibilidad en instalaciones ya existentes.

FIBRA OPTICA

La fibra óptica (F.O.) es utilizada cuando se requiere de grandes velocidades, alta capacidad de aplicaciones de comunicación, especialmente cuando la ausencia de ruido y la interferencia eléctrica son importantes.

Un cable de F.O. consiste de una fibra muy delgada hecha de dos tipos de vidrio, una para la parte interior y la otra para la exterior. Los dos vidrios tienen diferentes índices de refracción. Esta combinación previene que la luz penetre en una parte de la fibra hasta la parte exterior. La fibra por si misma esta protegida por una placa para darle mayor integridad estructural. Algunas de las ventajas de la F.O. son las siguientes:

- Aplicaciones de alta velocidad.
- No genera señales eléctricas o magnéticas.
- Inmune a interferencia, relámpagos y corrosión.
- Potencialmente mas barato que el cable coaxial.
- Puede propagar una señal, sin la necesidad de un amplificador, a distancias muy largas.
- No puede ser unido, es mas útil en topología punto a punto.

TOPOLOGIAS Y PROTOCOLOS

La disposición geométrica de los nodos y las conexiones de cables en una red de área local se conoce como topología.

Una puede ser en esencia un círculo, la cual se conoce normalmente como *anillo.*

Otra forma de organización puede ser la configuración con topología en *estrella*, donde todos los equipos están conectados mediante líneas independientes a un controlador central, encargado de realizar la conmutación de comunicaciones y la gestión de los recursos de la red.

Así mismo, la comunicación que queda establecida de todos a todos, por medio de una línea única de comunicacion que los recorre, es conocida como de ***bus lineal.***

Para posibilitar la interconexión entre los diferentes equipos a través de las diferentes redes de comunicaciones, ha sido necesario establecer una serie de normas que incluyen los requerimientos físicos y los procedimientos a seguir.

Estas normas que controlan la comunicación y la transferencia de información entre las computadoras a través de telecomunicaciones, son conocidas como protocolos.

Para cada una de estas topologias existen diferentes protocolos, los cuales determinan la forma de acceso al medio esto es ya que el

protocolo es el conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.

Así mismo cada topologia y protocolo esta de alguna manera relacionado con el medio de transmisión que se utilizará.

Dentro de este marco algunas de las topologias más conocidas son:

Bus Lineal (Ethernet)

Anillo Modificado (Token Ring)

Anillo Doble Redundante (FDDI)

Siendo los principales protocolos son:

Token Passing Bus

Token Passing Ring

TCP/IP

4.4 ASPECTOS DE LA SEGURIDAD

La seguridad es necesaria en un ambiente donde los elementos que lo constituyen o la información que se maneja en él no deben estar disponibles para cualquier persona.

En las redes de comunicaciones tiene interés primordial la seguridad de la información que pasa entre los sistemas interconectados.

Así como evolucionan las técnicas de comunicación, las oportunidades de interceptar la información mejoran y la necesidad de más y mejores mecanismos de protección crece.

La llegada de técnicas de comunicación y el arribo de las computadoras con vastas y mejores capacidades de procesamiento y almacenamiento de la información, trajo consigo nuevas formas de comprometer dilica información.

El control de seguridad como parte del modelo funcional de la administración de red, comprende el conjunto de funciones que aseguran la protección de la red y sus componentes en aspectos tales como: ingreso a la red, acceso a una aplicación, transferencia de información, protección de las herramientas de administración de red, minimización de riesgos, implementación del Plan de Seguridad de la red, y monitores de la estrategia de seguridad. Incluye también algunas funciones especiales como el examen de indicadores de seguridad, administración de pasaportes y generación de mensajes de advertencia o alarma en caso de violaciones.

Las empresas deben establecer políticas de seguridad para el uso de sus recursos de cómputo y telecomunicaciones así como para salvaguardar la información mientras sea almacenada o procesada por el sistema. Las políticas también deben reglamentar el mal uso o robo del equipo de computo y telecomunicaciones de la empresa, software, datos y documentación asociado a ellos. Las actividades del control de seguridad auxilian a:

* Minimizar la posibilidad de ataques mediante el uso de un sistema de seguridad en capas que combine políticas y herramientas de hardware/software que construyan una trinchera uniforme contra los intrusos.

* Proporcionar una forma rápida y eficaz para detectar el uso no autorizado de recursos y determinar la cuenta de usuario donde se originó la violación. Esto aporta pistas de auditoria de la actividad del intruso.

* Facilitar al administrador de la red la reconstrucción manual de cualquier archivo o aplicación dañados y restaurar el sistema al estado previo al ataque. Esta característica de reconstrucción ayuda a disminuir los daños y permite recuperar el sistema.

* Finalmente, monitorear a los intrusos y atraparlos por medio del grupo de operación de la red, finalizando con el castigo o prosecución consecuente.[5]

El control de la seguridad y sus actividades le aquejan en la actualidad algunos problemas. Estos son:

El área de seguridad es desconocida para la mayoría de la gente involucrada en las actividades de comunicación de voz y datos, quienes además no cuentan con indicadores que señalen cuando se presenta una violación, consideran complicadas las técnicas de protección de la red y sus responsabilidades no estén claramente asignadas.

No existen políticas claras sobre que es lo que debe protegerse en un ambiente de red complejo; si deben ser las aplicaciones, base de datos, archivos, nodos, enlaces de comunicación, dispositivos del usuario final, o una combinación de todo esto. Sin un análisis profundo y adecuado, los presupuestos no pueden asignarse apropiadamente a ninguna de estas áreas.

Existe poco de conocimiento de quien comete las violaciones de seguridad y porque. En este sentido no están disponible reportes y registros para las organizaciones. Las razones son:

a) Las violaciones no son detectadas por el grupo de operación de la red.

b) Las violaciones son detectadas, pero no reportadas por la administración porque admite que una violación puede originar que los usuarios tengan conciencia de la compañía a la que pertenecen y de la red que operan.

c)Las violaciones son realizadas por usuarios legítimos de la red que han encontrado formas de accesar aplicaciones y datos a los que no están autorizados.[5]

La mayoría de las violaciones a la seguridad de los sistemas las cometen los empleados de la compañía.

Existen instrumentos pobres para el monitoreo de las instalaciones, LAN y dispositivos de usuario final. La mayoría de las soluciones de monitoreo disponibles protegen al procesador y a sus aplicaciones.

El control de la seguridad es considerado un gasto, por lo que es tratado con poca prioridad, lo que resulta en un presupuesto insuficiente.

Este panorama nos muestra la poca aceptación que tiene esta función para los administradores de una red. La falta de conocimiento en su instrumentación, técnicas y procedimientos provoca gran parte de estos problemas. A pesar de ello, un estudio profundo de la organización puede desarrollar un esquema de seguridad ad-hoc a ella.

Veamos el ambiente típico de seguridad de un sistema. En el se diferencian claramente tres segmentos principales (Figura 4.4):

- Segmento de los intrusos potenciales, los cuales violan las reglas de forma activa y pasiva
- Funciones de monitoreo e inspección que detectan la violación y realizan acciones activas o pasivas en contra de ella, generando respuestas inmediatas o retardadas en contra del atacante
- Segmento de los agentes de seguridad. Esto incluye la definición de indicadores de seguridad y sus límites, utilizando guías para la generación de reportes, análisis de bitácoras, análisis de reportes, y toma de decisiones que deben tomarse contra los atacantes.

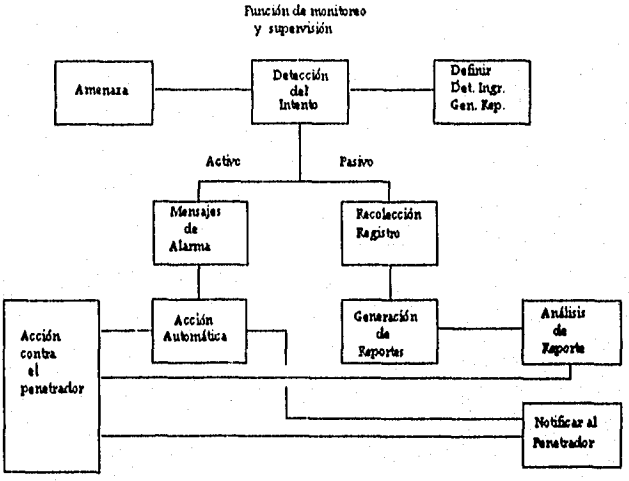

Figura 4.4

4.5 SEGURIDAD EN REDES

Las redes WAN, están planeadas por expertos, los cuales se basan en los extensos requerimientos de comunicación de una organización para poder implementarlas. Comúnmente las WAN utilizan servicios de comunicación públicos, líneas rentadas u otros medios de valor agregado, los cuales obligan al diseñador a seguir las normas establecidas por tales medios. Generalmente cualquier requerimiento de seguridad para estas redes se satisface mediante la adición del hardware y software especial (sistemas de control de redes, modems inteligentes, dispositivos de encriptamiento, etc.) al circuito de la red. Si bien los diseñadores y operadores de una WAN pueden instalar centros de control y administración de la red para proporcionar servicios de seguridad, la aplicación adecuada de las medidas de seguridad es responsabilidad del usuario de estos servicios. Los responsables de la WAN mantienen con esto, un nivel de servicio confiable sin aceptar totalmente la responsabilidad por la seguridad de la información que viaja en dicha red.

Con las LAN se presenta una situación diferente. Si bien la LAN puede conectarse a una o más redes WAN, o a otras, normalmente es planeada de forma menos estricta, es decir *ad-hoc* a las necesidades de la organización. Las LAN son redes de computadoras mucho más integradas y cerradas que una WAN, y los sistemas que las administran representan hoy en día una nueva forma de administrar redes para muchos responsables de esta actividad. En una LAN, el control del flujo de la información de operación y la protección de la misma son responsabilidad compartida entre los responsables de la red y los usuarios de las estaciones de trabajo. Los responsables de las redes LAN prestan servicios relacionados con la seguridad (como respaldos de archivos) y dependen de los usuarios para identificar las necesidades

de seguridad de la LAN, estableciendo valores para los diversos elementos de información procesados en ella.

Las razones por las cuales se deben establecer e instrumentar diferentes medidas de seguridad en las LAN que en las WAN y/o MAN son las siguientes:

- Los usuarios de una LAN generalmente poseen más conocimientos de su red que los usuarios de una WAN; manejan algunos conceptos del sistema operativo y tienen un entendimiento más amplio de las estructuras de seguridad internas
- En un ambiente de LAN, existen muchos dispositivos que almacenan y mantienen los datos. Por lo tanto, la protección de la información se torna más difícil a medida que se incrementan dichos elementos
- En la actualidad, no disponemos de muchas utilerías para: proteger las copias, evitar la exposición del contenido de discos y realizar copias sofisticadas de archivos y/o discos. [6]

Normalmente, las LAN que son construidas con poca seguridad son baratas y pueden elegir entre una amplia variedad de hardware y software, sin embargo, las redes que requieren de mucha seguridad reducen sus opciones en forma considerable ya que requieren generalmente de hardware y software adicional más caro.

Es por estas razones que en éste capítulo si bien abordaremos el tema en general, pondremos más énfasis el aspecto de seguridad en las LAN.

4.5.1 CARACTERISTICAS DE SEGURIDAD

Existen una serie de factores que son comunes al establecer servicios de seguridad, Estas características son:

ADMINISTRATIVAS

Un aspecto importante en la seguridad de las redes, pero frecuentemente descuidado es el papel del administrador de la LAN. Este individuo es el responsable del control de los accesos físicos y/o lógicos a la red, y de los procedimientos para efectuar la recuperación de errores, los respaldos y el monitoreo de las infracciones potenciales a la seguridad de la red.

La primera actividad de los responsables de la red será definir el conjunto de elementos de seguridad (Figura 4.5), por lo cual es necesario contestar las siguientes preguntas:

1. ¿ CUALES SON LAS APLICACIONES A LAS QUE DEBE SERVIRSE Y CUALES SON SUS REQUERIMIENTOS DE SEGURIDAD Y CONTROL CUANDO CIRCULAN EN LA RED ?

Cuando hablamos de aplicaciones nos referimos a los sistemas de administración de clientes, administración de personal, etc. Los archivos estratégicos del negocio y su material para trabajar -lo cual es natural se incluye en una red-, son las piezas que deben protegerse cuidadosamente y controlarse estrictamente en su distribución.

En muchos casos, una estrategia más estricta para la protección de la información consiste en aplicar el encriptamiento en los niveles normales de control de acceso a los archivos.

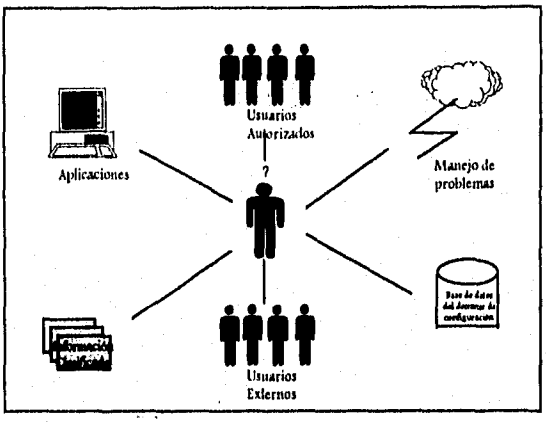

Figura 4.5

2.- ¿ SON SUFICIENTES LOS CONTROLES DEL NEGOCIO EXISTENTES ?

Una función de la organización que involucra la recuperación de información de archivos importantes puede ser una candidata atractiva para desarrollar una aplicación que funcione en la red. Sin embargo, hay que estar conscientes de que no todos los controles manuales pueden adecuarse. A menos que la red proporcione controles flexibles

y conserve registros de todas las actividades, no podrá ser capaz de asegurar que solo se están efectuando las transacciones adecuadas.

3. -¿COMO SE MANEJARA LA INFORMACION CLASIFICADA DE LA COMPAÑIA ?

Asumiendo que las decisiones de valorización de la información están hechas, debe determinarse como controlar y proteger dicha información en la red. Si por ejemplo, en el procedimiento manual se utilizan etiquetas para indicar la clasificación de alguna información, se podrían adecuar estas etiquetas en una aplicación, que despliegue la información solamente si el usuario está autorizado.

4. ¿ QUIENES DEBEN SER LOS USUARIOS AUTORIZADOS DE LA RED ?

Es muy importante durante el proceso de planeación tomar la decisión de quienes estarán autorizados a ingresar a la red, porque de lo contrario , los individuos compartirán sus identificaciones, el control dependerá y será imposible encontrar a los auténticos responsables de acciones no autorizadas (ataques). Aunque muchas redes cuentan con un proceso efectivo de identificación y autentificación de usuarios, el uso apropiado de pasaportes y otros métodos para autentificar recaen en el comportamiento del usuario, por ello, es importante la concientización del mismo mediante capacitación, seminario, etc.

5.- ¿ QUE PRIVILEGIOS DE RED ESTARAN AUTORIZADOS A LOS EXTERNOS ?

Los coordinadores de la red deben determinar si la red será cerrada (disponible sólo para empleados) o abierta (disponible para empleados y externos). Aunque los responsables decidan inicialmente hacerla cerrada, con el tiempo se impondrán las aplicaciones que se conectan con externos. Cuando ingresen externos se debe definir claramente cómo utilizarán la red dichos usuarios y cómo se controlarán sus actividades para que esté preparada con mejores sistemas de control e ingreso. La coordinación de la red debe establecer privilegios precisos en términos de accesos y acciones así como determinar quién esta activo en la red y que sucede con dicho usuario en un momento determinado, especialmente en ubicaciones críticas de la red, como las que se localizan en las oficinas centrales de la organización.

6.- ¿ COMO SE PROTEGERA LA INFORMACION DE ALTO VALOR ?

Para manejar la información de alto valor de forma segura se podría :

- Etiquetar todos los documentos, archivos y mensajes de alto valor con un bit o marca de seguridad para asegurar que la protección que la red proporciona es consistente dondequiera que se encuentren dichos elementos de datos.
- Encriptar todos los datos de alto valor cuando deban viajar sobre la red u otras líneas comunes de comunicación en áreas fuera del control de la compañía.
- Establecer un control de autentificación extra para accesar a archivos que contienen datos valiosos. Esto es con el fin de no dar

acceso a dicha información al personal técnico u operativo de la red, quienes normalmente lo tendrían por su grado de autoridad.

- Establecer un mecanismo para registrar todos los accesos a los archivos importantes, incluyendo marcas de tiempo, fecha e identidad del usuario.

7.- ¿ QUE CONTROLES DE ADMINISTRACION GENERAL SE UTILIZARAN PARA MINITOREAR Y CONTROLAR LA ACTIVIDAD DE LA RED?

Deben establecer de acuerdo a los lineamientos de cada organización.

Algunos recomendados son:

- Administrar de acuerdo a los estándares de la compañía en cuanto a la operación de la red.
- Controlar el ambiente de la red (cambios de infraestrucutra, servicios, topología, etc)
- Definir y monitorear los servicios de operación y soporte de la red.
- Definir los niveles de servicio esperados (incluyendo los servicios de seguridad), de manera que la red preste un servicio consistente en todas las estaciones de trabajo
- Resolver los problemas de la red, incluyendo un proceso de intensificación en la resolución de problemas técnicos y un proceso que genere reportes eventuales al proveedor del equipo o software de la red.
- Establecer formalmente el dominio de configuración de la red, incluyendo los métodos para adicionar nodos o servicios de forma

controlada dentro de la capacidad de la red dado un nivel de servicio acordado.

- Crear un procedimiento formal para implementar las actualizaciones de equipo o la instalación de nuevas versiones de software.

8.-¿COMO SE MANEJARAN LOS PROBLEMAS, INCLUYENDO LOS DE SEGURIDAD ?

Es necesario establecer un sistema de generación de reportes de incidentes y problemas que informe a los niveles superiores de la organización, a fin de asegurar la corrección e investigación del problema. Muchos incidentes de seguridad requieren un doble reporte de actividad, esto es, el reporte debe enviarse a través de los canales administrativo de la red y a los canales de seguridad de la organización. Este reporte informará sóbre la integridad dañada de la red y además información involucrada

A. ACCESO FISICO

FACTOR DE MULTIPLICIDAD

Este factor se expresa en base a los problemas de seguridad asociados con una computadora *stand-alone* multiplicado por el numero de computadoras conectadas en la red.

La seguridad de las computadoras personales que se conectan en una LAN inicia con la seguridad individual de cada computadora. No es posible contar con una red segura si las computadoras que conforman su fundamento no lo son. Mientras que cualquier sistema operativo decente incluye amplias medidas de seguridad. Cada computadora conectada debe estar:

- Protegida en los aspectos de: lugar, sistema y control de acceso a los archivos.
- Soportada por fuentes de energía ininterrumpible compatibles y por equipo de respaldo de datos apropiados.
- Supervisada por un administrador-operador que la vigile.

El factor de multiplicidad implica que la protección de dos computadoras es al menos dos veces mas difícil que proteger que una.[7]

Al conectar n computadoras en una red, sobresalen algunos aspectos de seguridad positivos. Si todos los archivos importantes utilizados por X usuarios son almacenados en una máquina, entonces es más efectivo hacer uso de un sistema de respaldo de archivos rápido y automatizado, el cual además deberá ser más confiable y realizarse con más frecuencia que si fuera delegado a cada uno de los X usuarios con instalaciones de respaldo menos sofisticadas. Una fuente de energía ininterrumpible es también más fácil de asignar a una máquina que sirve a muchos usuarios que a cada estación de trabajo en lo individual. Por otro lado, desde una perspectiva de software, el sistema operativo de red adiciona generalmente características de seguridad no encontradas en sistemas operativos para stand-alone.

Entre los aspectos negativos de la seguridad se incluye el hecho de que un ataque a la seguridad de una de las computadoras personales puede suponer la capacidad de acceder a los datos de muchas computadoras. Esto hace que una computadora conectada en red sea un objetivo mucho mas atractivo, y por tanto la pone ante un riesgo mayor que el de una computadora stand-alone.

FACTOR DEL CANAL

Este factor se refiere a que las conexiones entre computadoras suponen abrir canales de comunicación entre las maquinas, que se divide en tres área que son los siguientes:

1.- Control del canal.

El control del canal se refiere al evitar que un canal de comunicación pueda ser una vía amplia de ataque, para lo cual se necesita controlar quien: abre el canal, quien utiliza el canal y quien cierra el canal

2.- Verificación del canal.

En este punto la verificación del canal implica no correr riesgos por lo cual se debe considerar al canal como un paso a través de territorio enemigo y se debe asegurar la verificación de: Autenticidad de los usuarios, la integridad de los datos, la integridad del canal.

3. Soporte del canal.

La comunicación entre computadoras solo se puede establecer si se coordinan adecuadamente una gran cantidad de parámetros distintos. Una vez que se ha establecido, la comunicación se ha de mantener. Esto requiere un alto grado de fiabilidad en el hardware y software de comunicaciones. La necesidad de fiabilidad y protección se centra sobre los componentes que utiliza mas de un usuario, estando en proporción al numero de usuarios que atiende. Por ejemplo, en una red LAN en la que una computadora personal actúa como servidor de archivos de las otras, un mal funcionamiento o fallo del servidor puede tener unas consecuencias mucho peores que el fallo de una computadora personal que funciona aislada. Una vez que se han establecido, se debe dar soporte a los canales de comunicación, porque si no las tareas que dependen de estos pueden peligrar.

Aunque se necesita mucho trabajo para establecer conexiones entre las computadoras y estas pueden suponer un cambio en el modo de funcionamiento de la organización, vera como la organización asimilara rápidamente la existencia de los nuevos canales de comunicación. En conjunto, esta es una tendencia positiva, que contribuye a un uso eficiente de la tecnología. Sin embargo, se ha de mantener alerta respecto a las implicaciones en la seguridad de las nuevas conexiones.

El hecho de que un grupo de computadoras personales configuradas como una red local pueda realizar tareas mucho mas sofisticadas que un grupo de maquinas sin conexión, hace que las redes realicen en la actualidad trabajos críticos para la misión , actividades de procesamiento de datos que son esenciales para la existencia de la organización. El nivel de alerta en cuanto a la seguridad ha de corresponder con la importancia del trabajo que se ejecuta con la red.

Sin duda, el rendimiento de la red se mide cada vez mas por estándares que anteriormente estaban reservados para las computadoras medias y grandes. Se habla de los requisitos de puesta en activo, la cantidad de tiempo necesario para que funcione continuamente sin interrupción. También entra en acción la idea de tolerancia a fallos, que representa la capacidad de un sistema de mantenerse en funcionamiento independientemente de un fallo de un componente u otros problemas.

CONTROLANDO EL ACCESO A LOS RECURSOS DE LA RED

La seguridad en cualquier ambiente de procesamiento de datos también implica el control de acceso al equipo. Aunque el riesgo se encuentre intrínsecamente distribuido en toda la topología de la LAN, la protección de sus recursos principales requiere que los servidores de archivo y las impresoras se ubiquen en habitaciones de acceso controlado y seguro.

También es importante considerar el acceso al sistema de cables por la relativa facilidad para interceptar la red, insertar nuevos nodos u observar el tráfico de datos. Si la información que se maneja es importante, no debemos descartar la protección de la propia estación de trabajo.

Aquí se pueden utilizar cualquiera de las armas de defensa mencionadas anteriormente, en función del valor de los datos que se protegen y la sofisticación de los posibles atacantes:

- Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biometricos.
- Restringir la posibilidad de conectar las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biometricos.
- Identificación para la red con clave de acceso.
- Protección con clave de acceso de todas las áreas sensitivas de datos y restricción de acceso a los programas, según un esquema de >>uso según necesidad<<.
- Registro de toda la actividad de la estación de trabajo, identificada por el identificador del usuario.
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
- Monitorizacion de todas las operaciones de copia en disquete en las estaciones de trabajo.

SUMINISTRO ININTERRUMPIBLE DE ENERGIA ELECTRICA

Ciertamente, un servidor de archivos requiere un UPS (uninterruptible power supply). Muchos de los UPS tienen integrada la capacidad de enviar señales al servidor de archivos mediante un cable de conexión para indicar que la energía ha fallado y que hay un suministro limitado de energía en las baterías del UPS.

Si todas las estaciones de trabajo cuentan con un sistema UPS, cuando suceda un corte de energía eléctrica, se podría evitar al administrador de la red la labor de comunicar dicho evento a todos los usuarios a través del correo electrónico. Si el corte se prolonga, el administrador puede organizar que las estaciones de la red salgan

ordenadamente. Algunos sistemas pueden *dar de baja* automáticamente la red, finalizando las sesiones de los clientes de forma ordenada y haciendo respaldos esenciales mientras haya energía eléctrica disponible.

TERMINALES SIN DISCO

Claramente existe necesidad de impedir la copia de programas y datos fuera de la red en disquetes y de eliminar la posibilidad de que se puedan copiar de estos a la red virus y otros programas dañinos. Por otro lado, la persona responsable de mantener en marcha la red requiere de un acceso de amplio rango a todas las unidades. Una posible solución a esto es dotar a los usuarios vulnerables con estaciones de trabajo sin disco.

Muchos fabricantes de PC ofrecen en la actualidad equipos sin disco. Estas unidades poseen en esencia la misma arquitectura que el PC IBM estándar, excepto en la importante diferencia de que no poseen disquera ni disco fijo. El usuario almacena los datos en el disco fijo del servidor de la red. Al eliminar la unidad de disco, es muy difícil que se puedan introducir virus en la red desde un PC sin disco. Las PC sin disco también impiden que pueda robar información o software de la empresa.

PROTECCION DEL SERVIDOR

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

- Control del acceso al servidor. Significa establecer mecanismos que impidan el ingreso de personal ajeno al centro de la red.

- Respaldo del servidor. Dada la importancia del servidor y el monto de datos que éste maneja, están justificadas las opciones de respaldo más exóticas (Figura 4.2). Una de ellas señala que múltiples unidades de respaldo pueden arreglarse en sistemas automáticos que proporcionen varios gigabytes de almacenamiento mediante mecanismos que coloquen los discos magnéticos en dichas unidades.

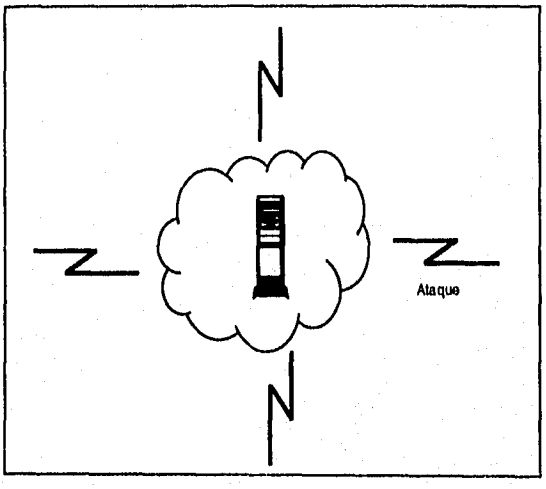

Figura 4.6

Es importante recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiendo quedar guardados en un lugar cerrado. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro. Tener cuidado con los sistemas de copia de seguridad en cinta mas lento que han de trabajar de noche, en muchos casos sin vigilancia

EQUIPO ESPEJO (DUPLEXING AND MIRRORING)

Los primeros sistemas de tolerancia de fallas consistían de una unidad de disco secundaria que se mantenía como un "espejo" de la unidad principal. Cualquier dato que era escrito en la primera unidad tenía también que escribirse inmediatamente en la segunda (figura 4.7). Si la unidad primaria fallaba por cualquier razón, la unidad de disco secundaria tomaba su lugar, permitiendo que el disco primario fuera reemplazado sin interrumpir las operaciones del servidor de archivos.

Aun dentro del sistema de disco espejo existen diferentes niveles de redundancia y tolerancia de fallas. Mientras algunas soluciones duplican los datos de un disco a otro, otras duplican solamente los datos críticos.

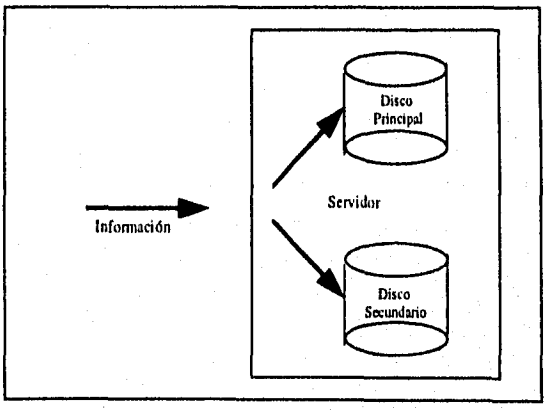

Figura 4.7

Un aspecto positivo de la duplicación de canal es que mejora el rendimiento de la red. Con dos controladores reparados, el sistema tiene la capacidad de una búsqueda dividida. No solo los usuarios pueden buscar archivos simultáneamente, sino que el servidor puede determinar que disco puede servir una petición de lectura con mayor velocidad. Un servidor con unidades duplicadas también puede leer de un único disco, escribir en otro y, a continuación , una vez que ha terminado la lectura, duplicar los datos que se han escrito en el disco secundario.

Aunque no todos están de acuerdo en que la duplicación requiera de mas de un controlador, la mayor parte esta de acuerdo en que independientemente de como se definan los niveles, la duplicación de canal supone un mayor grado de redundancia que la de disco. En lo básico, sin embargo, los términos son sinónimos. Ambos hacen relación a tener una copia de datos en tiempo real sobre un disco secundario, que entra en acción automáticamente en caso de fallo del primario.

En una red de computadoras personales tipica, el software de red le permite a una computadora con disco fijo hacer que haya espacio de ese disco disponible para los otros, normalmente dándole un nombre especial. Otros usuarios pueden acceder a los archivos de esa área, almacenar sus archivos allí y cargar programas desde esa área. Un servidor de archivos, una computadora que pone su disco fijo a disposición de las otras, representa claramente un riesgo añadido para la seguridad. Se debe controlar quien puede iniciar esa compartición y a quien se le permite ser un cliente, es decir, usuario del área compartida. Se deben de controlar los limites del área compartida, asegurándose de que los clientes no acceden al resto del servidor de archivos. Por otro lado, los clientes quieren estar seguros de que pueden controlar el uso de la conexión realizada con la red.

TOLERANCIA A FALLOS EN LA RED

Las redes como las computadoras personales y las estaciones de trabajo individuales, deben funcionar cuando se necesita que lo hagan, y mantenerse en funcionamiento. La tolerancia a fallos es la capacidad de la red de continuar funcionando en el caso de que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie perceptiblemente. Por lo general, la tolerancia a fallos conduce a un elemento hardware redundante que entra en funcionamiento de forma automática en el caso de que el componente primario falle. Sin embargo puede ser algo reducido como duplicar una labla de localización de archivos (FAT) y las entradas de directorio en áreas distintas de un mismo disco, o una simple verificación de lectura tras lectura, con lo que se asegura que los datos nunca se escriben en un sector dañado del disco.

La tolerancia a fallos tiene varios niveles. En el ultimo nivel, estará duplicado todo hardware, o incluso triplicado, para asegurar un rendimiento de la red sin interrupción. La forma mas usual de tolerancia a fallos es el nivel bajo, en que solo se duplica el componente responsable de nueve decimos de los fallos en la red, el disco fijo del servidor de archivos. Esta es la parte de la red mas proclive a fallos porque es la única que tiene partes movibles. Estas pueden desgastarse, romperse o sufrir cualquier otro fallo. Aparte del fallo catastrófico, los sectores de la superficie del disco a menudo quedan dañados por el uso normal, quedando dañados los dalos escritos en estos sectores. La tolerancia a fallos, por tanto, se refiere no solo a la redundancia, sino a la detección de errores.

B. ACCESO LOGICO

Las técnicas de acceso físico están diseñadas para conservar a usuarios no autorizados fuera de la red. Las técnicas de acceso lógico están diseñadas para limitar el acceso de usuarios autorizados a archivos no autorizados. El control de acceso a la información es responsabilidad del sistema operativo de la red y de sus utilerías. El acceso al servidor mediante un pasaporte y los derechos/permisos sobre directorios o archivos representan los puntos de seguridad básicos proporcionados por un sistema operativo en red.

En una típica LAN de Pcs, el software de red permite que una computadora con disco duro pueda compartir su espacio de almacenamiento con otros usuarios, los cuales podrán accesar archivos en dicha computadora, almacenar ahí sus archivos y ejecutar programas de la misma. Un servidor de archivos -la computadora que dispone su disco duro a otros - representa claramente un riesgo de seguridad. Se debe controlar quién puede realizar tal comparación de recursos y quién tiene permitido ser usuario de un área compartida, así como los límites del área compartida, asegurando que los clientes no puedan accesar el resto de los archivos contenidos en el servidor.

La seguridad lógica de la red se debe establecer a través de los niveles lógicos del sistema operativo, como lo muestra la figura 4.8:

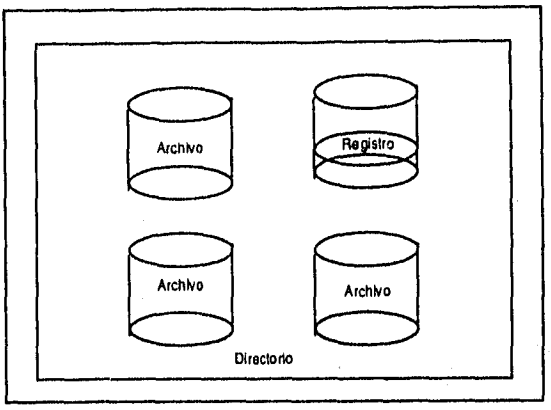

Figura 4.8

SEGURIDAD A NIVEL DE CLAVES DE ACCESO:

La seguridad de redes incluye una clave de acceso opcional para cada cuenta de cliente en cada servidor. Una vez que el cliente escribe la clave adecuada, el cliente pasa a disponer de una vista predefinido de los recursos de la red. Es más, la clave de acceso protege la vista personalizada para el cliente de la red. A continuación se describe las utilidades de seguridad que permiten a los administradores de sistemas configurar las condiciones de las claves de acceso según las cuentas.

Claves de acceso obligatorias.

Para aquellas cuentas que requieren de una seguridad forzosa, el supervisor del sistema puede activar en la cuenta la necesidad de una clave de acceso. Esta característica se puede utilizar también para la cuenta del supervisor.

Forzar cambios periódicos de la clave de acceso.

La cuenta se deshabita, lo que supone que el usuario deberá hablar con el supervisor para poder acceder posteriormente a la cuenta. La cuenta del supervisor no admite esta caracteristica.

Claves de acceso modificables sólo por el supervisor.

El supervisor puede especificar que la clave de acceso de una cuenta no pueda ser modificada por el usuario. Esto es de utilidad en cuentas como huésped, en las que el supervisor puede que desee que la cuenta no tenga clave de acceso. El usuario no podrá cambiar la clave de acceso incluso en el caso de que se conozca la clave de acceso actual de la cuenta.

Longitud mínima aceptable para la clave de acceso.

El supervisor puede especificar una longitud mínima aceptable para la clave de acceso del cliente. Todas las claves de acceso dadas por los clientes deben cumplir la limitación, ya que en caso contrario serán rechazados por el sistema operativo.

Obligación de clave de acceso distinta.

Si el supervisor le asigna a una cuenta la obligación de una clave de acceso distinta, el sistema operativo hará seguimiento de la(s) clave(s) de acceso anterior(es) utilizada(s) por la cuenta. Cuando se le pide una nueva clave de acceso, el usuario se ve forzado a dar una clave distinta, la cual no debe haber sido utilizada anteriormente.

Forzar cambios periódicos de la clave de acceso.

La cuenta se deshabita, lo que supone que el usuario deberá hablar con el supervisor para poder acceder posteriormente a la cuenta. La cuenta del supervisor no admite esta caracteristica.

Claves de acceso modificables sólo por el supervisor.

El supervisor puede especificar que la clave de acceso de una cuenta no pueda ser modificada por el usuario. Esto es de utilidad en cuentas como huésped, en las que el supervisor puede que desee que la cuenta no tenga clave de acceso. El usuario no podrá cambiar la clave de acceso incluso en el caso de que se conozca la clave de acceso actual de la cuenta.

Longitud mínima aceptable para la clave de acceso.

El supervisor puede especificar una longitud mínima aceptable para la clave de acceso del cliente. Todas las claves de acceso dadas por los clientes deben cumplir la limitación, ya que en caso contrario serán rechazados por el sistema operativo.

Obligación de clave de acceso distinta.

Si el supervisor le asigna a una cuenta la obligación de una clave de acceso distinta, el sistema operativo hará seguimiento de la(s) clave(s) de acceso anterior(es) utilizada(s) por la cuenta. Cuando se le pide una nueva clave de acceso, el usuario se ve forzado a dar una clave distinta, la cual no debe haber sido utilizada anteriormente.

Encriptamiento de la clave de acceso.

Todas las claves de acceso se encriptan con un algoritmo de encriptamiento irreversible antes de almacenarlos en el disco del servidor. De esta forma se evita que una persona capaz de acceder directamente al servidor pueda encontrar las claves de acceso. Además, el supervisor no podrá ver la clave de acceso en distintos servidores, sin que el supervisor de un servidor pueda saber su clave de acceso para otros servidores. En este sentido se puede aplicar lo establecido en el capitulo anterior.

SEGURIDAD EN DIRECTORIOS:

Este punto es uno de los más problemáticos en la temática de la seguridad de las redes. El control de acceso a directorios significa que el sistema de seguridad debe autentificar a los usuarios para poder determinar cuales elementos de información pueden utilizar. Este procesos presupone que el propietario de la información ha asignado un valor a la información y ha especificado quién puede ver u operar dicha información

El acceso a diretorios normalmente es controlado mediante el perfil del usuario, el cual describe a un usuario de acuerdo a los privilegios que posee sobre la información relacionada con su trabajo. Esta descripción se encuentra descrita en la tabla de derechos contenida en el objeto Usuario. Otro método de establecer el control de directorios es mediante la asignación de un pasaporte a cada usuario para el acceso a algún directorio. Esta última propuesta tiene diversas deficiencias y sólo es utilizado fuera en el área local, es decir, se

localiza en las computadoras personales donde los individuos pueden establecer pasaportes para proteger sus directorios privados.

El control de acceso a directorios se implementa mediante la autorización de determinadas acciones de los usuarios sobre los directorios, tales como:

- Leer archivos
- Escribir archivos
- Abrir archivos
- Crear archivos y directorios
- Borrar archivos y directorios
- Derechos de padre a un directorio, manejando libremente los subdirectorios
- Buscar en directorios
- Modificar las banderas de estado de archivos/directorios

SEGURIDAD A NIVEL DE ARCHIVOS

El servidor de archivos ofrece una seguridad estricta de acceso a archivos, asegurando que a los clientes solo se les permite acceder a los archivos sobre los que se les ha dado derecho de acceso. Además de las restricciones impuestas a un cliente por sus derechos de acceso a directorios, cada archivo posee una mascara de marcas de archivo que controla sus caracteristicas de acceso. Los bits de la mascara de marcas de archivos esta definida como sigue:

Bit 0: Fija si el archivo es de solo lectura.
Bit 1: Fija si el archivo esta oculto.
Bit 2: Fija si el archivo es un archivo de sistema.
Bit 3: Fija si el archivo es un archivo de solo ejecución que se puede ejecutar, pero no se puede copiar ni leer.
Bit 4: No utilizado.
Bit 5: Fija si el archivo se ha modificado desde la ultima copia.
Bit 6: No utilizado.
Bit 7: Fija si el archivo puede ser compartido por varios usuarios.

De hecho, cuando se gestionan adecuadamente las marcas de archivo y los derechos de acceso a directorios, suponen una gran capacidad para diseñar entornos multiusuarios seguros.

CONTROLANDO LA ACTIVIDAD A NIVEL REGISTRO

La autorización de acceso a un archivo no cubre totalmente las necesidades de seguridad, sobre todo de sistemas críticos. Es común que se requiera la autorización expresa de lectura a un archivo, sin embargo, si deseo cerrar más la restricción, se puede determinar sobre cuales campos tiene autorización leerlos. Esta utilidad es muy apreciada en documentos legales o información clasificada.

C. SEGURIDAD ENTRE REDES

En una conexión entre redes debe garantizarse que la distribución será segura y confiable. Los servicios de seguridad en cada subred serán manejados por el servidor local de la red que está prestando los servicios solicitados. De esta forma, los recursos con niveles de seguridad mayores a los solicitados por el cliente sea cual sea la ubicación de éste, serán invisibles para él(no podrá verlos), y por lo tanto no podrá leerlos, escribir en ellos o destruirlos.

ANALIZADOR DE PROTOCOLOS

Un analizador de protocolos en las manos de la persona equivocada puede ser una amenaza a la seguridad. Si un infiltrador puede obtener acceso a un conector de la red o es capaz de interceptar el cable, el analizador puede revelar información útil para el intruso. Un analizador puede capturar todo el diálogo que toma lugar sobre la red o inclusive desplegar pasaportes en forma desencriptada. La apropiación de pasaportes es fácil mediante el uso de los analizadores, pero los pasaportes no siempre pueden ser útiles, sobre todo si la red fue bien diseñada. Esto es, podemos restringir las estaciones a las que un usuario pueda ingresar. Así, aunque el infiltrador posea el pasaporte de la cuenta del supervisor, no podrá ingresar como él si no utiliza la terminal de éste. Adicionalmente, las utilerías para generar pistas de auditoría pueden reportar ingresos y salidas de la red, poniendo atención especial al perfil del supervisor.

Mientras que los analizadores de protocolos pueden representar un problema para la seguridad de la red, por otro lado pueden utilizarse para monitorear infracciones que ocurran en la red. Una

técnica sencilla consiste en buscar las estaciones de trabajo que no deben estar conectadas a la red. El administrador puede utilizar una aplicación que despliegue la red para señalar las estaciones desconocidas. Facilitamos esta actividad si asignamos un identificador fácil de leer a cada estación en la red. Con algunos modelos de analizadores, el administrador de la red puede escribir pequeños programas en C que realicen funciones especializadas, por ejemplo, un programa que busque a través de los datos para localizar las estaciones que ingresaron en el servidor de archivos y que no muestran actividad por largos períodos de tiempo. Esta aplicación podría indicarnos si en una estación el usuario ha dejado la misma conectada a la red y no la está utilizando, lo cual es una violación a las reglas de seguridad en muchas instituciones.

PROTECCION OE MOOEMS

Los módems son dispositivos que permiten a las computadoras transmitir información sobre líneas telefónicas ordinarias. La palabra por sí misma explica como trabaja el dispositivo: módem es un acrónimo formado de "Modulador/Demodulador". Los módems trasladan una cadena de información en una serie de tonos (modulación), los transmite sobre la línea telefónica, y traslada la serie de tonos nuevamente a la cadena de información en el otro extremo de la conexión (demodulación). Los módems son bidireccionales, esto es, cualquier módem contiene ambos elementos, el modulador y el demodulador, de forma que una transferencia de datos puede tomar lugar en ambas direcciones al mismo tiempo. Aun en esta era de las redes y redes Ethernet, una de las maneras más comunes de accesar una computadora en forma remota es por teléfono, con los módem.[8]

MODEMS Y SEGURIDAD

Los módems originan un número de consideraciones en materia de seguridad porque crean enlaces entre una computadora y el mundo exterior. Los módems pueden utilizarse por individuos dentro de la organización para obtener información confidencial y también pueden utilizarse por gente ajena a la organización para ganar acceso no autorizado a nuestros equipos, y si el módem puede reprogramarse o de otra forma corromperse, puede utilizarse para engañar a los usuarios y descubrir sus pasaportes.

El primer paso para asegurar los módems es proteger los números telefónicos. Trate los números telefónicos justo como se trata a los pasaportes: no los haga del conocimiento de nadie que no tenga necesidad de conocer ya que al darlos a conocer, se incrementan las oportunidades de que alguien trate de utilizarlos y viole los sistemas. Desafortunadamente, es posible conservar los números telefónicos de los modems como secreto, ya que, después de todo, la gente necesita llamar a ellos. Y aún si fuéramos extremadamente cuidadosos con los números, un intruso podría siempre descubrirlos "accidentalmente". Por esta razón, el secreto por sí solo no es la solución, los modems necesitan medidas más restrictivas.

Para adicionar seguridad a los modems se puede implementar el esquema de llamadas de verificación, que es aquél en el cual un extremo llama a nuestra máquina, se conecta al sistema y proporciona alguna forma de identificación. El sistema entonces retiene la conexión y hace una llamada de verificación al externo a un número telefónico predeterminado. Esto fortalece la seguridad porque el sistema llamará solamente a números preautorizados, de forma que un intruso sin autorización no pueda ingresar al sistema.

Desafortunadamente, muchos sistemas telefónicos, no desconectan la llamada del exterior hasta que ésta se desconecta de la línea. Por lo tanto, un intruso puede conservar la línea abierta después de que el sistema lo desconecta la primera vez. El problema ocurre cuando el módem invierte el papel y trata de llamar fuera de la línea telefónica. El intruso necesita solamente "capturar" la línea en el momento en que el módem la abra, y entonces podrá engañar al sistema haciéndolo creer que se ha desconectado con el número telefónico autorizado previamente. Los módems que detectan "tono de marcar" pueden ser engañados frecuentemente por un intruso si éste reproduce un "tono de marcar" grabado previamente sobre la línea abierta, de modo que cuando el módem se ponga a verificar, escuche el "tono de marcar" y autorice el ingreso.

La forma de evitar que un intruso trate de hacer este tipo de trucos es contando con dos conjuntos de módems - uno para recibir llamadas y otro para enviarlas. Para lograrlo, se debe pedir a la compañía de teléfonos que instale las líneas de manera que las líneas de ingreso no se puedan utilizar para llamar y las líneas de salida no tengan número telefónico para ingresar. Esto tiene un costo adicional al de una línea normal, pero adiciona una medida de seguridad extra para las conexiones telefónicas.

PROTECCION FISICA DE LOS MODEMS

Aunque la protección física es pasada por alto frecuentemente, es importante proteger el acceso físico a la línea telefónica, así como se asegura la computadora a la cual están conectados el módem y la línea telefónica.

Este esquema puede seguir las siguientes guías:

- Proteja el acceso físico a la línea telefónica. Asegúrese que su línea telefónica está físicamente segura. Cierre todas las cajas de conexión y las rosetas. Dirija la línea telefónica en un conducto eléctrico insertado en las paredes o en áreas cerradas. Un intruso que obtiene acceso físico a la línea telefónica puede conectar su módem a la línea e interceptar las llamadas antes de que lleguen al cliente, engañando a los usuarios, y aprendiendo inclusive sus perfiles y pasaportes.
- Asegure que su línea telefónica no permita la transferencia de llamadas. Si su teléfono puede programarse para transferir las llamadas, un intruso puede transferir todas las llamadas que reciba el sistema al numero que escoja. Si en el nuevo número hay una computadora que ha sido programado para actuar como el sistema original, sus usuarios pueden ser engañados, e introducirán sus perfiles y pasaportes.
- Línea privada (arrendada). Si todo el uso de módem es con una sola ubicación externa, considere obtener una línea privada. Una línea privada es un circuito dedicado entre dos puntos proporcionado por la compañía de teléfonos. Actúa como un cable dedicado y no puede utilizarse para hacer o recibir llamadas. Por lo tanto, nos permite conservar la conexión con el sitio remoto, pero no permite que alguien llame a nuestro módem e intente violarlo. Las líneas privadas son más caras que las lineas regulares, pero la seguridad que proporcionan supera el costo de las mismas.

SEGURIDAD ADICIONAL EN MODEMS

- Módems con pasaporte. Requieren que el usuario ingrese un pasaporte antes de que el módem lo conecte a la computadora. Normalmente, estos módems pueden almacenar una docena de pasaportes solamente. El pasaporte almacenado en el módem no debe ser el mismo que el pasaporte del usuario.
- Módems con encriptamiento. Debe utilizarse en terminales semejantes, las cuales encriptan toda la información transmitida y recibida de las líneas telefónicas. Estos módems ofrecen alto grado de seguridad no solamente contra intentos individuales de acceso en forma no autorizada, sino también conlra la intercepción de cables.
- Esquemas IAN, es el acrónimo de Identificación Automática de Números (Automatic Number Identificación). En este esquema, la compañía de teléfonos proporciona el número telefónico del usuario que llama al inicio de la conversación. El receptor podrá entonces verificar en su lista de números autorizados el número telefónico del usuario que intenta conectarse.

Los informes sobre piratas informaticos que crean una gran confusión accediendo de forma illeita a las computadoras a través de los módems, es fácil pensar instalar uno en la computadora personal propia. Por esta razón, es importante hacer hincapié en que nadie puede acceder a nuestra computadora a través de un módem a menos que:

- La computadora esté conectada
- El módem esté conectado a la línea telefónica
- El software de comunicaciones este programado para contestar al teléfono.

Se debe de tomar la precaución mas básica de un sistema de verificación de llamada. Esto requiere, al menos, que la persona que llama a la computadora escriba un identificador, un nombre o número que la computadora comprueba respecto a una lista de identificadores de usuarios autorizados. Si el identificador dado no esta en la lista, la computadora puede colgar o darle al comunicante otra posibilidad para que escriba una identificación correcta. Se debe dar solo un número limitado de posibilidades antes de terminar con la llamada. Además, se puede pedir una clave de acceso tras la identificación.

Por consiguiente es importante proponer una serie de contramedidas básicas:

1. Mantener los números secretos. Amenos que se trabaje con un servicio de telefonia publico, tratar los números de teléfonos de las computadoras como información muy sensible, que se revela según un esquema de darla cuando se necesita.

2. Limitar los intentos de acceso repetidos. No permitir mas de res intentos de conexión antes de romper la conexión y obligar a que la persona que llama lo tenga que intentar de nuevo.

3. Revelar lo menos posible sobre el procedimiento de conexión . Esta es un área en la que no se ha de ser amigable con el usuario.

MAQUINAS FIREWALL

Cuando se construyen departamentos o edificios de oficinas, normalmente son equipados con paredes a prueba de fuego (firewall) - que son paredes construidas especialmente para resistir el fuego. Si se inicia el fuego en el edificio, éste podrá arder sin control soló en un área, porque la "pared" detendrá o disminuirá el progreso del fuego hasta que llegue la ayuda.

La misma filosofía puede aplicarse para la protección de redes contra ataques externos. En las redes, las maquinas firewall hacen difícil para los intrusos el "viajar de red en red. La instalación de máquinas firewall puede ayudar a detener o reducir daños e intrusos.[8]

FIREWALL INTERNAS

La propuesta mas sencilla en cuanto a esta técnica es conservar a las subredes independientes y de tamaño pequeño. Como ya hemos visto, una vez que el intruso compromete una máquina en una red, es más fácil que comprometa a otras. La tarea de penetrar las redes es más sencilla si se tiene todo el equipo conectado a la misma red física y lógica. En lugar de colocar todas las máquinas en una red local, se debe separar la instalación para formar conjuntos de LAN comunicándose a través de gateways o routers. Para lograr esto, siga los siguientes lineamientos. [8]

- Cada red debe tener su propio servidor. Cada servidor y sus clientes deben tener su propio dominio de red.
- Ningún servidor o estación de trabajo en una red puede confiar sus computadoras a cualquier otra red.
- Los usuarios que tengan cuentas en más de una red local deben contar con diferentes pasaportes para cada subred, y no permitir el acceso entre las redes sin el pasaporte respectivo.
- Los gateways deben tener habilitado el nivel de acceso y el nivel de seguridad lo más restrictivo posible. Si es posible, no permita cuentas de usuario en los gateways.
- No instale archivos de sistema de una red local a otra.

Las firewalls internas ofrecen muchos beneficios:

- Ayudan a aislar fallas físicas de la red en un número pequeño de máquinas.
- Limitan el número de máquinas que pasan información en cualquier segmentofísico de la red, limitando por lo tanto el daño que puede hacerse al "intereceptar" las conexiones.
- Limitan el número de máquinas que pasan información en cualquier segmento físico de la red, limitando por lo tanto el daño que puede hacerse al "intereceptar" las conexiones.
- Limitan el número de máquinas que pueden afectar por ataques del tipo de inundación.
- Son una barrera contra intrusos internos y externos, que traten de atacar máquinas específicas en algunas de las redes.

FIREWALL EXTERNAS

Además de la partición de la red en pequeñas redes locales para disminuir o frenar a los intrusos, es importante instalar firewall externas, esto es, una máquina (o conjunto de máquinas) que formen una barrera entre la instalación local y el mundo exterior. Esta barrera puede configurarse para permitir que se ejecuten determinadas operaciones y para hacer difícil o imposible que un intruso externo la utilice para penetrar las redes que protege.

REFERENCIAS

1.- *Diccionario Escolar de la Lengua Española*,
E.D. ESPASA
México, 1995.

2.- *Diccionario para Usuarios de Computadora*,
Pfaffenberger,
E.D. Prenlice Hall,
México, 1993.

3.- *Informática Básica*,
Alcalde- García Peñuelas,
E.D. McGraw Hill,
México, 1992.

4.- *Handbook of Computer Communications Standards*,
Stallings William,
E.D, Macmillan Computer Publishing,
E.U.A. 1990

5.- *Communication Networks Management*,
Terplan Kornel,
E.D. Prenlice Hall,
E.U.A., 1992.

6.- *Protecting Information on local Area Networks*,
Schweitzer James,
E.D. Butterworth Pub.
E.U.A., 1988.

7.- *Manual de Seguridad para Pc y Redes Locales*,
Cobb Stephen,
E.D. McGraw Hill,
México, 1994.

8.- *Local Networks*,
Stallings William,
E.D, Macmillan Computer Publishing,
E.U.A. 1988.

9.- *Practical Unix Security*,
Garfinkel - Spafford,
E.D. O'Reilly Associates, Inc,
E.U.A., 1992.

10.- *Computer Segurity Basic*,
Russell - Gangemi Sr.
E.D. O'Reilly & Associates, Inc.
E.U.A., 1992

CAPITULO V

PLAN DE CONTINGENCIA

A través del desarrollo de ésta tesis, se ha remarcado la importancia que tiene la información para las organizaciones las cuales en la actualidad cada día son más dependientes de los sistemas electrónicos para procesamiento de datos.

Así mismo se ha dicho que existen diversos tipos de vulnerabilidades, riesgos y/o amenazas que pueden ocasionar la pérdida de la información o la reducción o pérdida parcial o total de las facilidades de procesamiento de datos, lo cual puede resultar en consecuencias financieras, de mercado, de competencia o legales, desastrosas; situación que obliga a las organizaciones a la búsqueda de mantener un nivel adecuado de seguridad mediante el establecimiento de los diversos controles y medidas encaminados a salvaguardarla, es decir, a considerar aspectos relacionados con la seguridad de la información.

El no contar (por cualquier causa) con el equipo de cómputo necesario para acceder a o para almacenar la información equivale a no poder utilizarla, siendo el efecto el mismo que en el caso de no tenerla. Las consecuencias son graves.

Por lo anterior, no es exagerado decir que el significado real de seguridad en las computadoras es de supervivencia, ya sea de una operación vital o de todos los procesos de la organización.

Sin embargo aun cuando las medidas de seguridad se incrementen, el riesgo no se puede eliminar definitivamente, los desastres ocurren y son algo real. l'or eso, las empresas deben estar preparadas para tratar de evitar al máimo su ocurrencia o para que en caso de que ocurran se puedan minimizar las pérdidas.

Es por ello que es de suma importancia desarrollar e implementar un plan de emergencia que permita el restablecimiento de las operaciones del sistema de cómputo en caso de contingencia

La presencia o ausencia de un plan de contingencia es el factor más importante para que una empresa sobreviva o desaparezca después de un desastre.

Por lo anterior, el plan de contingencia es uno de los aspectos comprendidos dentro del rubro de seguridad de la información en una empresa. Cada uno de los aspectos mencionados con anterioridad en esta tesis es independiente de los demás; sin embargo, para optimizar la seguridad de la información, es necesario que se trabaje de manera integral en todos ellos.

No serviría de mucho tener una perfecta clasificación de la información y no tener nada de seguridad física, por ejemplo.

Así para que el plan de contingencia pueda ser efectivo, debe existir conjuntamente con planes de seguridad física, lógica y de las comunicaciones entre otros.

5.1 DEFINICION

La planeación formal implica diseñar un futuro deseado e identificar las formas para lograrlo. Su esencia consiste en la identificación sistemática de las oportunidades y peligros que surgen en el futuro, los cuales combinados con otros datos importantes, proporcionan la base para que una empresa tome mejores decisiones en el presente para explotar las oportunidades y evitar los peligros.

Sin embargo esta planeación está basada en eventos con una alta probabilidad de ocurrencia (las más probables) y que en caso de que se presenten no tienden a crear serias dificultades para una empresa.

Esto implica que existen ciertos eventos o condiciones que pueden suceder de imprevisto no dando tiempo para planear u organizar y cuyas consecuencias pueden ser desastrosas.

Estos eventos son el tema de los planes de contingencia.

La Planeación de contingencia implica proporcionar a los directivos una mejor posición para tratar con desarrollos inesperados. Al fracasar de anticipar ciertos eventos, los ejecutivos pueden no actuar tan rápido como deberían en una situación crítica, y el evento puede crear más daño del que hubiera provocado de otra manera.

En términos sencillos, un plan de contingencia es una "preparación para tomar acciones específicas, cuando surge un evento o condición que no está planeado en el proceso de planeación formal"[1].

Un plan de contingencia en otras palabras es un conjunto de procedimientos de recuperación para casos de desastre, es decir es un plan formal que describe pasos apropiados que se deben seguir en caso de un desastre o emergencia.

De esta forma consiste en un amplio estado de acciones consistentes para ser tomadas, antes como un plan de respaldo, durante como un plan de emergencia y después como un plan de recuperación de un desastre.

Un adecuado plan de contingencia ayuda a una instalación de cómputo y a la organización en general a minimizar sus pérdidas, en caso de desastre, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

Llegado a este punto se hace necesario acotar el concepto de desastre.

"El término desastre en este conteto significa la interrupción en la capacidad de acceso a información y procesamiento de la misma a través de las computadoras, necesarias para la operación normal del negocio".[2]

Es decir, el concepto de contingencia o desastre va enfocado a una consecuencia más que a una causa. Por lo tanto al utilizar cualquiera de estas dos palabras no se hará tanto referencia a algún tipo de catástrofe ya sea natural o causada por el hombre, como a las consecuencias que dicha catástrofe provoca en la organización. Así mismo el concepto de desastre se refiere tanto a una pérdida de la capacidad de procesamiento de la información, como a la pérdida de la misma.

El plan de contingencia constituye de una manera un control netamente preventivo, ya que se configura como un instrumento que permite prevenir la eventualidad de un desastre, así como mantener el nivel de operación del ambiente informático; formando un control correctivo en la medida en la cual se materializa un riesgo, ya que pretende reducir el impacto de éste.

Aquellas organizaciones que se han preocupado por su desarrollo y crecimiento, han establecido dentro de su estructura orgánica una función definida como administración de riesgos, obteniendo estupendos resultados, ya que a través de un programa adecuado de identificación de siniestros potenciales, la disminución del impacto físico y económico en la organización ha sido considerable.

A pesar de esto, algunas compañías se resisten a tener un plan para casos de desastre considerando que "eso no les pasará a ellos", o que "la probabilidad de que ocurra es muy rara". En otras palabras la estrategia de preparación es aceptar el riesgo.

La razón por la que los directivos no preparan un plan de emergencia puede ser que éste no les parece particularmente interesante así que le dan poca prioridad.

Además, este tipo de plan implica invertir tiempo, dinero y esfuerzo y su verdadero valor sólo se podrá medir en el caso en que se presente alguna contingencia.

Por otro lado, también existen organizaciones que piensan que cuentan con planes adecuados de recuperación, mientras que la realidad es que un buen número de estos planes son superficiales, no estructurados e inadecuados para afrontar las complicaciones que

surgen de un desastre, lo cual también implica un riesgo grande para esas organizaciones.

Un ejemplo de esto lo constituye un estudio realizado en los E.U.A. en el cual se muestra que las actividades operacionales de una organización se decrementan dramáticamente cuando el centro de cómputo sufre una contingencia que interrumpe sus operaciones. (fig. 5.1)

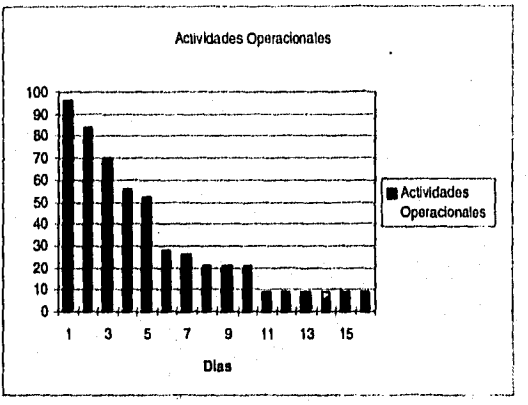

Figura 5.1

5.2 OBJETIVO

El propósito principal de un plan de contingencia es, "mantener a la compañía y sus actividades operando aun en una situación de desastre"[1]; es decir, habilitar a la organización a responder y sobrevivir a problemas críticos o catastróficos de forma que permita una pronta recuperación de la operación normal del centro de cómputo.

Este plan dependerá de la naturaleza de la organización e inevitablemente incurrirá en costos altos. sin embargo, es importante tener en mente que su importancia no depende de la probabilidad de un desastre, sino del efecto de tal, sin importar que tan remota sea su probabilidad.

Igualmente se debe considerar que la pérdida parcial o total de las facilidades del procesamiento de datos puede causar entre otras:

- Pérdidas financieras directas
  - Pérdida de ventas
  - Pérdida de la producción
- Pérdidas financieras indirectas
  - Pérdida de clientes
  - Costos extra para apoyo
  - Fraudes, maluso
  - Costos de compensación
- Pérdidas de control
  - Información errónea o incompleta
  - Bases pobres para la toma de decisiones
  - Pérdida de contratistas y oferentes

- Otros problemas
  - Pérdida de confiabilidad
  - Pérdida de apoyos
  - Mala imagen

Dicho lo anterior el plan de contingencia debe cubrir la restauración de sistemas prioritarios o la totalidad de las operaciones de procesamiento, para lo cual durante su desarrollo e implementación se deben cumplir las siguientes metas:

- Identificar las debilidades e implementar un plan de prevención de desastres
- Elaborar un plan de respaldo.
- Minimizar la duración de una seria interrupción en las operaciones
- Establecer procedimientos de restauración y/o recuperación
- Facilitar la efectiva coordinación de las tareas de recuperación
- Reducir la complejidad de los esfuerzos de recuperación.
- Establecer responsables de la ejecución e implantación del plan

5.3 CARACTERISTICAS

En una organización el plan de contingencia ha de contemplar dos aspectos: operacional y administrativo.

En el *nivel operacional*, cada usuario debe saber que hacer cuando aparezca el problema. Como mínimo debe saber la respuesta a la pregunta ¿a quién hay que llamar?.

Es muy importante que el plan de contingencias determine quién debe tomar las decisiones durante la recuperación del desastre y establezca la disponibilidad y entrenamiento del personal suficientemente experimentado.

En el *nivel administrativo*, el plan contempla aspectos como:

- Definición de riesgos y porcentajes de factibilidad a que está expuesta la organización.
- Identificación de las aplicaciones críticas para la empresa.
- Procedimientos de recuperación para la reproducción de información.
- Especificación de las alternativas de respaldo.
- Localización de los medios de respaldo
- Quién contacta los medios de respaldo
- Qué archivos o base de datos deben ser reconstruidos primero
- La configuración del equipo de cómputo similar y su localización (centro de cómputo alterno o espejo)
- En dónde puede encontrarse el software de reemplazo

- La localización de otro equipo de apoyo, tal como generadores y aire acondicionado
- La ayuda que se puede esperar del proveedor del equipo
- La acción a ser tomada en cada de un daño parcial inesperado
- Procedimiento para la imposición de controles extraordinarios durante el desastre y hasta que regresen los sistemas a la normalidad

En este punto también debe considerarse que para el desarrollo y mantenimiento de una buena recuperación se debe tomar en cuenta:

a) Respaldo de configuración del equipo de cómputo y de la programación (software).

b) Documentación y almacenamiento seguro de los procedimientos de recuperación. Un aspecto importante de la documentación es el entrenamiento de los individuos que se encargarán de las operaciones de recuperación.

c) Respaldo y almacenamiento seguro de los programas de forma que se pueda disponer de ellos cuando se requieran.

d) Respaldo y almacenamiento seguro de los archivos de datos que sean esenciales para la operación continua de la organización.

Ahora bien, un plan de contingencias no evita los desastres, sino que prevé los medios para salvaguardar al máximo los recursos del área de procesamiento electrónico de datos y reducir así las posibles pérdidas consecuencia de éstos.

Al identificar un plan de contingencias como un proceso dentro de la función administrativa de riesgos, es necesario concientizar a todo el personal que está involucrado en el mismo, que su implantación es al mismo tiempo un dispositivo de control, el cual entra en acción en el momento en que otros controles ya sean preventivos o detectivos, fallan.

De esta manera, se debe enfatizar el seguimiento de los siguientes puntos clave:

- Dar a los directivos las bases necesarias para el entendimiento de los esfuerzos totales que se requieren para desarrollar y mantener un efectivo plan de recuperación.
- Obtener el consentimiento de los directivos apropiados para apoyar y participar en los esfuerzos.
- Definir los requerimientos de recuperación desde la perspectiva que establece la misión de la empresa.
- Converger apropiadamente en la prevención de desastres y minimización del impacto.
- Definir como integrar las consideraciones del plan de contingencia dentro de los planes generales de la organización y los procesos de desarrollo de los sistemas de forma que el plan se mantenga factible todo el tiempo.

El esfuerzo que implique la realización de un plan de contingencia no proporciona ningún beneficio si éste no es actualizado y probado frecuentemente en base a la identificación de los sistemas prioritarios para la organización así como la atención que se le dé a las consecuencias económicas y probabilidad de ocurrencia de un desastre.

Es por ello que el plan de recuperación y considerar los puntos anteriores se debe tener en mente que este plan debe ser entendible, fácil de usar y de mantener. Es decir que debe cumplir con las siguientes características:

Actual Debido a que nada permanece estático dentro de las operaciones de procesamiento del centro de cómputo. Cualquier plan de recuperación debe ser actualizado por la persona que se haya establecido para ese fin, con el objeto de mantener al día todas las implicaciones de recuperación de las facilidades de procesamiento.

Entendible El plan de contingencia debe especificar paso a paso todas las actividades que se realizarán, quién las realizará y en que momento.

Factible Debe ser posible llevar a cabo todas las actividades del plan de contingencia en cualquier momento.

Probado El plan de recuperación debe ser probado periódicamente. Esta prueba puede consistir desde solo un análisis minucioso de los pasos a seguir dentro del plan hasta la simulación de desastres lo que implica la suspensión de los servicios así como mayor tiempo.

Documentado El plan debe formalizarse a través de un plan escrito que deberá estar disponible en cualquier momento.

5.4 CONSIDERACIONES

Dentro de las actividades que se deben realizar para que el desarrollo e implantación de un plan de contingencia sea el adecuado son recomendables las siguientes:

- Designar al grupo encargado de elaborar el plan de contingencias
- Dar a la organización propuesta prioridad sobre la organización tradicional para ejecutar las acciones especificadas dentro del plan de contingencia.
- Considerar a los niveles de contingencia como una aplicación vital del negocio y como registros vitales, los documentos que estos generen.
- Tomar en cuenta los factores externos e internos que puedan afectar la operación de la organización al elaborar el plan de contingencia.

5.4.1 ORGANIZACION GERENCIAL

Es la autoridad máxima de la organización en materia de administración y operación del plan de contingencia.

ATRIBUCIONES

1. Actuar como unidad administrativa para realizar la coordinación de planeación, organización, integración, dirección, ejecución y control, en materia de planes de contingencia.
2. Ejercer el nivel de autoridad máxima en caso de contingencias

ESTRUCTURA ORGANICA

1. Director General.
    1.1. Coordinador General.
        1.1.1. Coordinador del Grupo Administrativo.
        1.1.2. Coordinador del Grupo de Bienes Inmuebles.
        1.1.3. Coordinador del Grupo de Servicios Técnicos.
        1.1.4. Coordinador del Grupo de Sistemas Vitales.

FUNCIONES

1. Director General.

- Decidir la puesta en operación de la organización encargada de la aplicación del plan de contingencia.
- Coordinar las acciones y aprobar las decisiones de la organización gerencial.

1.1. Coordinador General.

- Establecer, coordinar, y administrar el plan de contingencia para el control de las operaciones.
- Obtener, interpretar y analizar los informes de cada uno de los grupos de coordinación específica.
- Establecer los enlaces de comunicación eficientes entre la dirección general y la estructura operativa.
- Establecer y emitir la comunicación con el exterior.
- Coordinar las pruebas para asegurar la operabilidad del plan.

1.1.1. Coordinador del grupo.

- Actuar y decidir en el ámbito de su competencia.
- Informar de los avances y resultados de sus funciones asignadas.

5.4.2 ORGANIZACION OPERATIVA

Es el área encargada de ejecutar las acciones necesarias para el cumplimiento del plan de contingencia.

ATRIBUCIONES

- Realizar las actividades establecidas por el coordinador respectivo.

ESTRUCTURA ORGANICA

1.1.1 Grupo Administrativo.

A. Recursos Humanos.
B. Recursos materiales.
C. Recursos financieros.
D. Apoyo legal.
E. Relaciones públicas.

1.1.2. Grupo de bienes Inmuebles.

1.1.3. Grupo de Servicios Técnicos.

A. Hardware.

B. Software.

C. Comunicaciones.

1.1.4. Grupo de sistemas o aplicaciones vitales.

FUNCIONES

1.1.1. Grupo Administrativo.

- Proporciona a todos los demás grupos en cuanto a recursos financieros, humanos y materiales.

A. Recursos Humanos.

- Servicios Médicos.
- Localización de personal.
- Transportación.
- Recursos extraordinarios.
- Registro de asistencia y permanencia.
- Alojamiento.
- Transportación.
- Alimentación.
- Evaluación.

B. Recursos Materiales.

- Servicios de oficina.
- Contratación de servicios.
- Suministros.
- Relación de Proveedores.
- Adquisición de equipos:
  - De cómputo.
  - Comunicaciones.
  - Auxiliares.

C. Recursos Financieros.

- Gastos de emergencia.
- Contabilidad en el pago de la nómina.
- Seguros.
- Indemnizaciones.
- Financiamientos para garantizar la continuidad de la operación y la recuperación.

D. Apoyo legal.

- Representar a la organización en todos los asuntos de carácter jurídico y emitir opciones en las consultas de tipo legal que le sean formuladas por las diferentes áreas.
- Responsabilidad legal.
- Reclamación de seguros.
- Contratos y convenios.
- Suspensión de pagos.

E. Relaciones Públicas.

- Mantener el contacto con:
  - Organización gerencial.
  - Clientes.
  - Servicios de emergencia.
  - Organización operativa.
  - Proveedores.

1.1.2. Grupo de Bienes Inmuebles.

- Tener disponibles en el tiempo requerido las instalaciones y servicios para la operación.
- Coordinar con los otros grupos de operación la selección y diseño de instalaciones.
- Supervisar la instalación física de equipos, servicios y mobiliario.
- Mantener informada a la organización gerencial.

1.1.3. Grupo de Servicios Técnicos.

- Restablecer la infraestructura de cómputo.
- Evaluación del daño.
- Proporcionar opciones de evaluación.
- Asegurar que el procesamiento normal pueda llevarse a cabo tan pronto como los datos, equipos y comunicaciones requeridos estén disponibles.
- Coordinar que los grupos de hardware, Software y comunicaciones, restablezcan al ambiente de cómputo.
- Realizar pruebas de equipos para determinar las consideraciones de operabilidad.

1.1.4. Grupo de Sistemas o Aplicaciones Vitales.

- Restablecer la operación de los sistemas en el menor tiempo posible, con base en el programa de registros vitales.
- Establecer los procedimientos de recuperación y respaldo.
- Asegurar que cualquier aplicación crítica sea procesada dentro del tiempo requerido.
- Control de documentación.

Aunque la mayoría de los planes de contingencia en caso de desastre se dirigen únicamente a las actividades relacionadas con el procesamiento de datos, un amplio plan también incluye áreas de operación fuera del proceso de datos principal, el plan debe tener un extenso alcance si es para dirigir efectivamente los muchos escenarios de desastre que pueden afectar la organización.

Esto no sugiere que un plan debe incluir procedimientos separados para varios tipos de desastres, porque muchas actividades pueden ser comunes en cualquier emergencia. Sin embargo, en el peor de los casos deben ser considerados en el proceso del plan, en el cual la principal instalación es destruida. Una vez que esta alternativa es considerada, el equipo de planeación para recuperación en caso de desastre, puede considerar actividades o cambios que pueden ser requeridos en una situación menos crítica.

5.5 ASPECTOS BASE

Los aspectos base de un plan de contingencias pueden dirigirse sobre algunas de las siguientes áreas:

1. Facilidad de destrucción.

El equipo de planeación debe considerar la total destrucción de la operación principal y/o la instalación de procesamiento. El plan debe incluir revisiones que podrían ser necesarias en caso de que las instalaciones primarias fueran únicamente parcialmente destruidas.

2. Disponibilidad de personal.

El organigrama para el plan de contingencia en caso de desastre debe ser un subgrupo que incluya personal de toda la organización, con las posiciones clave identificadas como necesarias para ejecutar el plan. La mayoría de las organizaciones asume un mínimo de personal que podría estar disponible para ejecutar las funciones críticas del plan.

3. Determinar los tiempos del desastre.

Las consideraciones deben ser dadas para varios tiempos en que un desastre puede ocurrir, para tratar de identificar los tiempos en que podría haber los mas devastadores efectos sobre la organización.

Algunas organizaciones dependen totalmente del procesamiento nocturno, mientras otras pueden creer que la falta de disponibilidad de sistemas en la línea durante las horas pico de servicio a la clientela, pueden ser el mas devastador periodo de tiempo. Otras consideraciones pueden incluir el efecto sobre la organización en fin de mes, fin de cuatrimestre o fin de año, si estos procesos fueran demorados a causa de un desastre.

4. Instalaciones de almacenamiento fuera del Centro de Cómputo.

Muchas organizaciones suponen que estas instalaciones sobrevivirán al desastre, esto puede ser un falso supuesto si la instalación esta cerca al desastre. Ciertamente, los medios magnéticos protegidos y aprovisionamientos críticos y otros registros proveerán los medios para recuperar la normalidad de operación.

Otros aspectos que el equipo de planeación debe de considerar incluyen :

- Desastres que afecten únicamente a departamentos usuarios específicos.
- Trabajos sin procesar y trabajos en proceso.
- Destrucción de microcomputadoras.
- Redes inoperables de telecomunicaciones.

El plan de contingencia debe ser un documento con vida, esto es, dinámico, por lo que se deberá estar modificando cada vez que cambien algunos de los siguientes factores:

1. Cambio de personal.
2. Cambio de equipo de instalación.
3. Cambio de teléfonos.
4. Cambio de sistemas.
5. Cambio de contratos de mantenimientos.
6. Cambio en las pólizas de seguros.
7. Ruptura de privacía en el plan de contingencia y recuperación.
8. Cambio en las instalaciones de respaldo y alternas.

5.6 ELEMENTOS DEL PLAN DE CONTINGENCIA

El plan de contingencia contempla tres tipos de acciones, las cuales son:

- Acciones de emergencia.
- Acciones de recuperación.
- Acciones de respaldo.

1) ACCIONES DE EMERGENCIA. Deben contener el daño en el momento, así como limitar el daño, contemplando todos los desastres naturales y eventos mal intencionados.

2) ACCIONES DE RECUPERACION. Abarcan el mantenimiento de partes críticas entre la perdida del servicio, recursos y su recuperación o restauración.

3) ACCIONES DE RESPALDO. Conjunto de acciones a realizar una vez que se ha presentado cualquier contingencia que afecta la continuidad operativa ya sea en forma parcial o total del centro de procesamiento de datos, a las instalaciones auxiliares, recursos, información procesada, en tránsito y almacenada, con la finalidad de estar preparados para hacer frente a cualquier contingencia, minimizando su impacto permitiendo restablecer a la brevedad posible los diferentes servicios interrumpidos.

5.6.1 PLAN DE RECUPERACION EN CASO DE DESASTRES.

Las acciones del plan de recuperación en caso de desastre, se implementan como medidas previsoras, pero entran en función una vez que se constate el daño.

Su objetivo es establecer la metodología y recursos necesarios con la finalidad de restablecer los servicios de cómputo en forma oportuna, al presentarse cualquier contingencia.

Para la implantación del plan, se debe someter a la firma, revisión y aprobación de los niveles directivos correspondientes, con lo que quedará debidamente formalizado para su observancia en la organización.

A. RESPONSABILIDADES DEL PLAN DE RESPALDO

Se definen a continuación los responsables de la ejecución del Plan de respaldo y las responsabilidades que competen a cada uno de ellos.

1. El área de sistemas que diseña una aplicación es responsable de:

- Definir las estrategias de respaldo, y conjuntamente con el usuario, verificar su validez y eficacia.
- Elaborar los programas y procedimientos de cómputo necesarios para obtener y validar el contenido de los respaldos y la vigencia de su contenido.

- Definir, conjuntamente con el usuario, los mecanismos de respaldo que permitan continuar con la operación normal ante la presencia de una contingencia grave o desastrosa en el Centro o en los sistemas de cómputo.
- Elaborar los programas y procedimientos que permitan la generación de los mecanismos de respaldo necesarios para cubrir las contingencia graves en los sistemas y equipos de cómputo.

DESCRIPCION DEL PROGRAMA

La planeación del plan de recuperación es un proceso muy completo e intenso, que por lo tanto requiere de la redireccion y evaluación técnica del personal y recursos del procesamiento de información de una forma apropiada. Para minimizar el impacto de una empresa que podría tener escasos recursos, el proyecto para el desarrollo e implementación del plan de recuperación de desastres y plan de reanudación del negocio debe ser parte del plan de actividades normales de la organización.

Metodología del abajo: proyecto puede consistir de ocho partes separadas, como se describe a continuación:

FASE 1. ACTIVIDADES DE PRE-PLANEACION (PROYECTO INICIAL)

la fase uno se utiliza para obtener y entender de la existencia y ambientes de proyectos de computación de la organización. Esto permite que el equipo del proyecto este para: referirse al alcance del proyecto y la asociación del programa de trabajo; desarrollar proyectos

de programación; e identificar y direccionar cualquier problema que pueda tener un impacto en la entrega y el éxito del proyecto.

Durante esta frase un comite de dirección debe estar establecida. El comite debe tener cubierta toda la responsabilidad para informar a la dirección y guiar al equipo de trabajo. El comite también debe hacer todas las decisiones relacionadas con los esfuerzos del plan de recuperación. El director del proyecto debe trabajar con el comite de dirección para finalizar detalles de trabajo y desarrollar programas de entrevistas para conducir la seguridad y el análisis de ios impactos en el negocio.

Otras dos claves para esta fase se dan: el desarrollo de una política para apoyar el programa de recuperación; y un programa de conciencia para educar a la dirección y a los demás individuos quienes se requerirán para participar en el proyecto.

FASE 2 EVALUACION DE VULNERABILIDADES Y DEFINICION GENERAL DE REQUERIMIENTOS

La seguridad y el control dentro de una organización concierne continuamente. Es preferible, desde la perspectiva de una estrategia económica y de negocios, concentrarse en actividades que tienen el efecto de reducir la posibilidad de que ocurra un desastre, en lugar de concentrarse primariamente en minimizar impactos de un actual desastre. Esta fase direcciona medidas para reducir la posibilidad de ocurrencia.

Esta fase incluye las siguientes tareas clave:

- Una seguridad absolutamente completa en la evaluación del equipo de computo y en el ambiente de las comunicaciones incluyendo practicas personales; seguridad física; procesos operativos; planes de contingencia y respaldos; desarrollo de sistemas y mantenimiento; seguridad en base de datos; seguridad en las comunicaciones de voz y datos; software de seguridad para sistemas y controles de acceso; seguros; administración y planes de seguridad; control de aplicaciones y computadoras personales.

- La evaluación de la seguridad permite que el equipo del proyecto mejore cualquier plan de emergencia y medidas para la prevención de desastres y para implementar los requerimientos en el plan de emergencias y medidas de prevención de desastres donde no los exista.

- Definir el alcance en la planeación del esfuerzo

- Analizar, recomendar y comprar planes de recuperación y requerimientos en el mantenimiento del software para apoyar el desarrollo de los planes y para mantener actualizados los planes o/y para la siguiente implementacion.

- Desarrollar del marco del plan de trabajo.

- Reunir el equipo del proyecto y conducir sesiones de trabajo.

FASE 3 ANALISIS DEL IMPACTO EN LOS NEGOCIOS

El análisis del impacto en los negocios en cualquier ambiente y para cualquier parte del negocio permite al equipo del proyecto: identificar sistemas críticos, procesos y funciones; evaluar el impacto económico de incidentes y desastres que resultan de los accesos denegados a servicios del sistema y otros servicios y facilidades; y fijar el "dolor del umbral", esto es, la medida de las unidades del tiempo que pueden sobrevivir sin el acceso a sistemas, servicios y facilidades.

El reporte debe de presentarse al comite de dirección. Este reporte identifica las funciones de los servicios críticos y el tiempo en el cual ellos deben ser recuperados después de una interrupción. Este reporte por lo tanto debe de utilizarse como algo básico para identificar sistemas y requerimientos de recursos para apoyar los servicios críticos que proveen procesamiento de información y otros servicios y facilidades.

FASE 4 DEFINICION DETALLADA DE REQUERIMIENTOS

Durante esta fase, el perfil de los requerimientos para la recuperación debe desarrollarse. Este perfil es para ser utilizado como una base para analizar las estrategias alternativas para la recuperación. Así, con este perfil esta desarrollado para identificar recursos que se requieran para apoyar las funciones criticas identificadas en la fase 3. Además, se debe incluir hardware (mainframe, comunicaciones de voz y datos. y computadoras personales) software (proveedores, vendedores, desarrolladores en casa, etc.) documentación (usuarios, procedimientos), soporte externo (redes publicas, servicios, etc.) y personal para cada unidad del

negocio. Las estrategias de recuperación estarán basadas en un periodo corto, mediano plazo y largo plazo en general.

Otra llave de liberación de esta fase es la identificación de un plan de alcance de objetivos y suposiciones.

FASE 5 PLAN DE DESARROLLO

Durante esta fase, los componentes del plan de recuperación están definidos y los planes están documentados. Esta fase también incluye la implementación de cambios para utilizar los procedimientos, las actualizaciones de procedimientos de datos existentes, operación de procedimientos requeridos para apoyar las estrategias de recuperación y alternativas seleccionadas, negociaciones con contacto de vendedores, (quienes proveen los servicios de recuperación) y la definición del equipo de recuperación , sus roles y responsabilidades. Los estándares de recuperación también pueden ser desarrollados durante esta fase.

FASE 6 PROGRAMA DE PRUEBAS

El programa de pruebas es desarrollado durante esta fase. El objetivo de las pruebas y ejercicios esta establecido y las alternativas para la estrategia de pruebas son evaluados. Las estrategias de pruebas para el ambiente deben ser seleccionadas y el programa de pruebas continuas debe establecerse.

FASE 7 PROGRAMA DE MANTENIMIENTO

Los planes de mantenimiento son críticos para el éxito de una recuperación actual. El plan debe reflejar los cambios para el ambiente que están apoyados por el plan. Esto es crítico ya que existen cambios para el manejo de procesos lo cuales son revisados para tomarlos en cuenta. En áreas donde el manejo de los cambios no existe, un procedimiento para manejo de cambios y la implementación es recomendable. Varios productos de software para recuperación toman en cuenta este requerimiento.

FASE 8 PLAN INICIAL DE PRUEBAS E IMPLEMENTACION

Una vez que los planes son desarrollados, las pruebas iniciales del plan son conducidas a el plan que han sido elaborados e incluso si fuera necesario alguna modificación basados en un análisis de test de resultados.

Las actividades especificas para esta fase incluye lo siguiente:

- Definición de metas y objetivos del test
- Identificación de equipos para el test
- Estructurar el test
- Conducir el test
- Analizar resultados del test, y
- Modificaciones del plan apropiadamente.

El objetivo tomado para probar el plan depende, en gran parte, de las estrategias de recuperación seleccionado para encontrar los

requerimientos de recuperación de la organización. Una vez que las estrategias de recuperación son definidas, los procedimientos específicos de pruebas deben ser desarrollados para asegurar que los planes escritos son comprensibles y actuales.

PLANEACION DEL ALCANCE Y OBJETIVOS DEL PLAN

El objetivo primordial de la planificación de recuperaciones es permitir que una organización sobreviva ante un desastre y continúe sus operaciones del negocio normalmente. Para sobrevivir la organización se debe de asegurarse que las operaciones críticas pueden continuar su procesamiento normal. a través del esfuerzo de recuperación, el plan establece claramente líneas de autoridad y prioridades en los esfuerzos del trabajo. Los objetivos claves para el plan de contingencias deben ser:

- Proporcionar seguridad y entrenamiento a las personas que participaran al momento de un desastre;
- Continuar con las operaciones críticas del negocio;
- Minimizar la operación de un disturbio serio en las operaciones y resultados (ambos, información de los procesos y otros recursos);
- Minimizar inmediatamente el daño y las perdidas;
- Establecer sucesores de la dirección y fuerzas de emergencia;
- Facilitar la efectiva coordinación de tareas de recuperación;
- Reducir la complexibilidad de los esfuerzos de la recuperación;
- Identificar líneas críticas de los negocios y funciones de soporte;

A través de la estadística la probabilidad de un mayor desastre es remoto, las consecuencias de una ocurrencia puede ser catastrófico, en

ambos sentidos, en el impacto de las operaciones y en la imagen publicitaria. La administración aprecia las implicaciones de una ocurrencia, por lo tanto este puede asignar roles y responsabilidades para la planeación de la recuperación a un empleado dedicado a este servicio esencial.

La dirección debe tomar una decisión para controlar un proyecto que satisfaga los siguientes objetivos:

- Determinar vulnerabilidad para significantes servicios de interrupciones en el centro de datos y negociar facilidades y definir medidas preventivas que pueden tomarse para minimizar la probabilidad e impactos de interrupciones;
- Identificar y analizar la economía, servicio, imagen publicitaria y otras implicaciones en el servicio de interrupciones extensas en el centro de datos y otras facilidades en el negocio;
- Determinar inmediatamente, necesidades de recuperación a corto y largos periodos y fuentes de requerimientos;
- Identificar las alternativas y seleccionar el mas efectivo acercamiento para realizar operaciones de respaldo en las operaciones y servicio de restauración;
- Desarrollar e implementar planes de contingencia que direcciones en ambos sentidos corto y largas necesidades para el centro de datos y otras facilidades del negocio.

ORGANIZACION DEL PROYECTO Y DEL PERSONAL

La organización del equipo encargado del proyecto esta diseñado para maximizar la flexibilidad de las necesidades para tratar con la implementación del plan de la manera mas eficientemente posible. Como ya se ha explicado anteriormente en este capitulo la recuperación de un desastre y el plan de recuperación en los negocios esta en un completo e intensivo labor de un programa. Una clave de éxito en el desarrollo e implementacion de un programa para la recuperación en las organizaciones que estén dedicadas de tiempo completo con recursos para la recuperación de los negocios en la planeación de la continuidad.

Los planes de la recuperación deben ser tratados como documentos de la cotidianidad. En ambos casos el procesamiento de la información y el ambiente de los negocios están en constante cambio y se vuelven mas complejos e integrados. Los planes de recuperación deben mantenerse en paz con estos cambios. Continuamente las pruebas y ejercicios de los planes es esencial si la organización quiere asegurarse que recuperar la capacidad en el mantenimiento de tan solo un ambiente. La organización también debe asegurarse de que el personal con responsabilidades especificas para la recuperación este preparada para ejecutar el plan.

Esto no se puede lograr sin recursos de tiempo completo con responsabilidades como son: mantenimiento a los planes; coordinación de componentes y planes de pruebas completos; personal capacitado con responsabilidades para recuperación; y actualizar los planes para reflejar los cambios de la información procesada y el ambiente del negocio.

COMITE DE LA DIRECCION

El comite de la dirección debe incluir representantes de áreas claves de la organización como son:

- Sistemas de información
- Soporte tecnológico
- Desarrollo de sistemas
- Servicio de operaciones y redes
- Comunicaciones
- Unidas clave en el negocio

EQUIPO DEL PROYECTO

La composición del equipo del proyecto puede variar dependiendo de los ambientes y del negocio para los cuales el plan se desarrolle. Es importante hacer notar que los directores del ambiente y del negocio para los cuales el plan se desarrolla serán los responsables del mantenimiento y prueba de sus respectivos planes. Sin embargo, el personal y el personal de las unidades responsables de la recuperación y continuidad de la planeación debe realizar el rol de coordinador de las actividades de prueba, revisiones de planes y mantenimiento del plan maestro.

El equipo del proyecto core es automáticamente parte de otros equipos de proyectos. La auditoria interna debe ser invitada para ser parte de todos ellos. Los directores representativos de varios de ellos pueden escojerse para recomendar otros individuos en su área para representarlos o para juntar específicos grupos donde su experiencia será requerida para el desarrollo de sus planes.

SUGERENCIAS PARA LA COMPOSICION DE UN EQUIPO DE BASICO

- Dirección del proyecto
- Operaciones de redes y computo
- Soporte de sistemas
- Voz, redes y comunicaciones

SUGERENCIAS PARA SISTEMAS DE INFORMACION Y SORTE A LA TECNOLOGIA

- Redes y comunicaciones
- Facilidades de dirección
- Desarrollo y soporte de redes
- Administración de base de datos
- Sistemas de seguridad informática
- Operaciones
- Soporte de redes
- Implementacion de redes

CONTROL DEL PROYECTO

El control y manejo de este proyecto debe estar apoyado por el proyecto de manejo de software. El software debe utilizare para programar al personal de recursos para tareas especificas e identificación para liberaciones y sus fuentes.

PROGRAMACION DE LIBERACIONES

Lo siguiente es un programa de liberaciones por fase que se desarrollaran y liberaran como parte de este proyecto:

FASE 1 ACTIVIDADES PRELIMINARES (PROYECTO INICIAL)

- Revisión detallada del plan de trabajo
- Programación de entrevistas
- Enunciar políticas
- Planear la recuperación del programa de conocimientos

FASE 2 EVALUACION DE VULNERABILIDADES

- Reporte de evaluaciones de seguridad
- Planeación del esfuerzo de personal
- Plan de la estructura
- Recomendaciones del software para el plan de recuperaciones
- Implementacion del software para el plan de recuperaciones

FASE 3 ANALISIS DE IMPACTO EN LOS NEGOCIOS

- Reporte del impacto en los negocios

FASE 4 DEFINICION DETALLADA DE REQUERIMIENTOS

- Necesidades del perfil de recuperación
- Plan de alcance, objetivos y perfiles

FASE 5 DESARROLLO DEL PLAN

- Plan de recuperación del centro de datos
- Recuperación de estándares
- Plan prototipo para su continuación del negocio

FASE 6 PROGRAMA DE PRUEBAS

- Pruebas principales
- Pruebas estratégicas
- Pruebas de procedimientos

FASE 7 PROGRAMA DE MANTENIMIENTO

- Procedimientos de mantenimientos
- Recomendaciones para el manejo del cambio

FASE 8 IMPLEMENTACION Y PRUEBAS PARA EL PLAN INICIAL

- Reporte de pruebas inicial
- Implementación

FUENTES DE REQUERIMIENTOS

En algunas organizaciones que han tratado de desarrollar planes para la continuación de sus labores cuando se presentan desastres sin enfocarse a las fuentes de requerimientos que han fracasado en la implementacion efectiva del plan de recuperación. Algunas

organizaciones, después de pasar tiempo y dinero desarrollando planes de recuperación fracasan en el mantenimiento de sus recuperaciones comparado con la competencia. Esto es básicamente debido a la carencia de compromiso para mantener sus planes actuales o para hacer las regulaciones en las pruebas de recuperación.

Es por lo tanto esencial, que el manejo este comprometido para el desarrollo, implementacion y mantenimiento de su programa, que requiere fuentes que están al tanto durante el ciclo del desarrollo y que un recurso este dedicado al diario mantenimiento de programa.

Las fuentes de requerimientos pueden están divididos dentro de tres categorías, las cuales son:

- Personal
- Costo de capital
- Costos diarios

REFERENCIAS

1.- *Computer Security Basics*
Deborah Rusell G.T.
O'reilly & Associaes, Inc.
E.U.A., 1992

2.- *Computer Security Administration,*
University of Toronto
January 17, 1996

3.- *Handbook of Computer Communications Standards,*
Stallings William,
E.D, Macmillan Computer Publishing,
E.U.A. 1990

4.- *Security of Information and Data,*
Daler, Gulbrandsen, Melgard, Sjølstad
E.D. Ellis Horwood Limited,
Inglaterra 1989.

CONCLUSIONES

Existen muchos aspectos involucrados en el campo de la seguridad en cómputo los cuales lo hacen realmente extenso. La mayor parte de los textos existentes se enfocan a uno en particular o son un poco más generales, pero tratan el tema desde el punto de vista de una plataforma o de un tipo de sistema específico.

El mundo de la informática es tan complejo y diverso que dar recomendaciones específicas para cada conjunto posible de circuntancias está más allá de las posibilidades de un único texto.

Esto significa que es importante disponer de guías y principios básicos con que trabajar y que nos den una idea general de los mecanismos y medidas que podemos aplicar para fortalecer la seguridad en nuestros sistemas sin importar cual sea éste.

Una vez que estamos concientes del valor de nuestra información, sabemos que debemos cuidarla y protegerla, para ello debemos conocer los peligros y situaciones que constituyen una amenaza para su seguridad, así como las técnicas y medidas existentes para protegerlas.

Como se ve, hasta este punto, aún no se requiere de estudiar a fondo las características específicas de nuestro sistema, sino únicamente estudiar y conocer los conceptos básicos que se involueran en la seguridad de la información.

Si tomamos en cuenta que el objetivo de esta tesis ha sido ofrecer las bases teóricas a aquellos que deseen incursionar en el estudio y/o conocimiento de la seguridad en cómputo, podemos entonces decir que el objetivo se ha cumplido. La tesis es una recopilación de los conceptos básicos y da una visión general del tema.

Sin embargo no queremos dar por concluido el trabajo, ahora nos viene a la mente la siguiente inquietud:

Una vez que tengo los conocimientos básicos. ¿Qué hago con ellos?

la conclusión que nosotros tomamos como respuesta fué:

Aplica los conocimientos adquiridos, analiza y planifica la seguridad de tu propio sistema.

Podemos decir que el primer paso para revisar la seguridad es prepararse mediante una evaluación de riesgos. Esto supone la exploración de la posibilidad de una pérdida, las consecuencias de ésta y las probabilidades de que ocurra. (cap I y II)

El resultado final deberá permitirle a los responsables preparar y fijar las normas de seguridad (cap. III). De acuerdo a éstas se establecerán reglas y controles para los usuarios, incluyendo las técnicas, dispositivos y modos de trabajo a implementar para que se mantenga el nivel de seguridad deseado (cap. III y IV).

Una vez fijadas las normas de seguridad se puede desarrollar el plan de contingencia (cap. V). En éste se describe la respuesta adecuada ante los incidentes dando los procedimientos que se han de seguir cuando se produce una violación en la seguridad.

De esta aproximación podemos concluir que la seguridad puede ser resumida en:

- Evaluación de riesgos
- Normas de seguridad
- Plan de contingencia

Cabe decir que al realizar la evaluación de riesgos debemos ir más allá de calcular la posibilidad de que ocurran cosas negativas. Debemos poder realizar una evaluación económica del impacto de éstas. De esta forma este valor se podrá utilizar para contrastar el costo de la protección frente al valor de lo que se protege, lo cual nos ayudará a poder implementar las medidas adecuadas de seguridad a nuestro sistema, en base a los recursos con que contamos.

Recordemos que los niveles de seguridad que se implementen están sujetos a las siguientes consideraciones básicas: ¿Que se quiere proteger?, ¿contra qué se quiere proteger? y que consecuencias podría provocar, y ¿Cuánto tiempo, dinero y esfuerzo estamos dispuestos a invertir?

Por último creemos necesario recalcar que el crecimiento tecnológico en sí mismo es neutral, no posee ningún contenido moral. Los usuarios de las computadoras son los que determinan si se aplica con una orientación positiva o negativa.

La mejor forma de favorecer la seguridad es promover actitudes maduras y responsables entre los usuarios. No se puede obtener una seguridad duradera con las computadoras existentes, ni con restricciones para quienes la usan. La verdadera seguridad solo se puede obtener con el compromiso de los usuarios y ésto sólo se puede lograr a medida que la sociedad en conjunto tenga una mayor cultura informática y los usuarios comprendan el valor tanto de las computadoras como de la información que en ellas está contenida.