UNIVERSIDAD NACIONAL
AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA
Y ADMINISTRACION

SEGURIDAD INFORMATICA

SEMINARIO DE INVESTIGACION
INFORMATICA

Que para obtener el Título de:
LICENCIADO EN INFORMATICA

p r e s e n t a:

MA. DOLORES CEJA HERNANDEZ

Asesor del Seminario:
Act. Ricardo Vite San Pedro

México, D. F. 1995

A MIS PADRES:

CON CARIÑO POR LA OPORTUNIDAD QUE ME BRINDARON PARA ESTUDIAR

A MIS HERMANOS:

JAVIER, ALEJANDRO Y JUAN CARLOS

A DANY:

POR TODO SU APOYO, ENTUSIASMO Y OPTIMISMO

AL P. CARLOS CANTU:

POR HABER SIDO MI MEJOR GUIA DURANTE MI VIDA UNIVERSITARIA

A MI ASESOR DE TESIS ACT. RICARDO VITE:

POR SU PACIENCIA Y ORIENTACION QUE ME AYUDARON A LOGRAR UNA META MAS PARA MI TITULACION

A TODOS MIS AMIGOS Y COMPAÑEROS:

QUE DE UNA U OTRA FORMA ME AYUDARON EN LA ELABORACION DE ESTA TESIS, EN ESPECIAL A JAVIER SANCHEZ, JOSE JUAN ALVAREZ, HECTOR ZARATE Y HUMBERTO SERRALDE

INDICE

BACKUPS

SEGURIDAD LOGICA

INTRODUCCION

La gran proliferación y diversificación de computadoras ofreció desde su inicio enormes bondades y facilidades aunque también originó la presencia de nuevos riesgos en el procesamiento de información que van desde daños físicos a las instalaciones causados por agresiones internas, externas o naturales, hasta el daño accidental o premeditado de la información, sabotaje de proyectos, fraudes, espionaje o soborno; lo que produce una serie de consecuencias como pérdidas financieras, de mercado o legales, indudablemente indeseables por cualquier organización ya que le pueden causar un gran impacto.

RIESGOS		
INTERNOS	EXTERNOS	NATURALES
DAÑO A LA INFORMACION DAÑO EN DISPOSITIVOS DE ALMACENAMIENTO ERROR HUMANO FRAUDE SABOTAJE ESPIONAJE SOBORNO	 SABOTAJE ESPIONAJE SOBORNO	 INCENDIO TERREMOTO INUNDACION

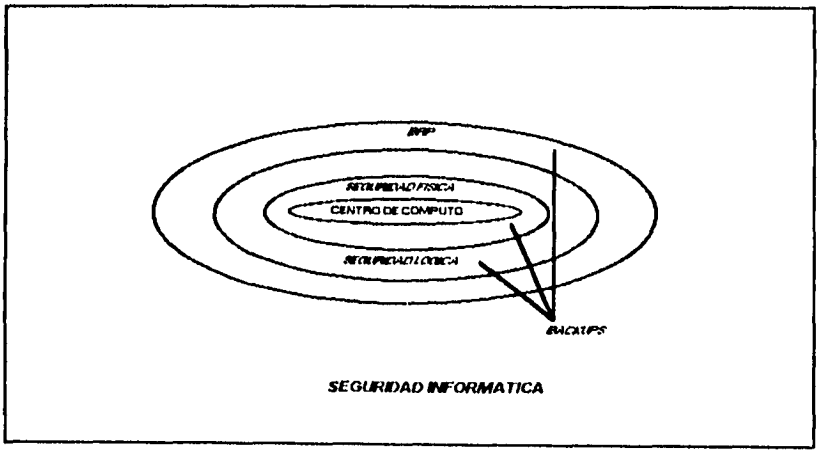
Actualmente el funcionamiento de cualquier empresa mediana o grande depende en gran medida de su información, la cual debe ser oportuna, confiable y fácilmente recuperable, ya que de no cumplirse alguna de estas características la empresa no puede garantizar una adecuada toma de decisiones así como su óptima operación, incluyendo el servicio a clientes. Esta dependencia implica la existencia de una gran variedad de riesgos latentes a que está expuesto cualquier centro de procesamiento de datos y que en caso de ocurrencia de alguno de estos puede ser ocasión de grandes pérdidas económicas para la organización.

El reconocimiento de éste tipo de riesgos tanto internos como externos y naturales fomento el desarrollo en primera instancia de medidas de seguridad físicas aplicables a los centros de cómputo a fin de garantizar la continuidad de servicios previniendo el acceso de personas no autorizadas a las instalaciones así como protección en caso de siniestros; sin embargo el desarrollo de medidas de seguridad lógica que son aquellas que mantienen la integridad y confiabilidad de la información no fue paralelo a la seguridad física, ya que no se le había tomado la suficiente importancia, no fue que se comenzó a fijar la atención en este punto sino hasta que se detectaron accidentalmente fraudes por grandes cantidades de dinero en empresas de Inglaterra y Estados Unidos. No por esto se debe pensar que organizaciones de otros países incluyendo el nuestro están exentas de este riesgo o que no han experimentado este tipo de situaciones.

Debido a lo anteriormente expuesto, además de no existir material en español o referencias de nuestro país sobre la seguridad informática la presente tesis muestra un esquema de seguridad informática aplicable en cualquier ambiente "mainframe", basado en la consulta de bibliografía extranjera y del conocimiento de políticas y procedimientos de seguridad informática en una compañía de seguros; abarcando una serie de conceptos y medidas aplicables para controlar o negar el acceso a los recursos utilizados en el procesamiento electrónico de datos, los cuales pueden ser aplicados en cualquier organización que así lo requiera siempre tomando en cuenta su tamaño, los riesgos a

que está expuesta y sus requerimientos de seguridad.

Esta tesis presenta dicho esquema de seguridad desglosado en cuatro capítulos, siendo el primero referente a la seguridad física, conceptualizandose como la primera protección para accesar físicamente cualquier centro de cómputo así como las medidas de control aplicables en caso de daños naturales; el segundo capítulo se enfoca a los métodos de respaldo existentes; el tercero a la seguridad lógica, es decir el medio de acceso a la información que se procesa, la parte intangible y finalmente el plan de recuperación de servicios en caso de desastre mejor conocido como DRP o BRP, necesario para garantizar la continuidad de operaciones en caso de cualquier desastre.



SEGURIDAD INFORMATICA

ANTECEDENTES

Durante los últimos años el incremento de computadoras ha sido realmente notable, de solo dos computadoras que utilizaba el gobierno de Estado Unidos en 1950 se incrementaron a más de 8000 en la década de los 70's. Anteriormente bastaba la protección física del centro de cómputo contra agresiones internas, externas o naturales para salvaguardar su integridad; actualmente con la gran proliferación y diversificación de usuarios e instalaciones de los centros de cómputo ha surgido la necesidad de adoptar una seguridad diferente que antes no había sido necesaria.

Básicamente se pueden identificar tres tipos de riesgos a los que está expuesto cualquier centro de cómputo siendo los siguientes:

- RIESGOS
  - NATURALES
    - Temblor
    - Incendio
    - Inundación
  - MATERIALES
    - Falla de equipo
    - Falla de energía
  - HUMANOS
    - Error
    - Fraude
    - Sabotaje
    - Espionaje
    - Soborno

Estos tipos de riesgos pueden afectar de una u otra forma el centro de cómputo, la información que se procesa; así como la gente involucrada en dicho centro de cómputo.

Los riesgos naturales se pueden presentar en cualquier momento inesperadamente, y pueden causar graves pérdidas, estos casos deben ser previstos mediante la implantación de medidas cuyo objetivo principal es mantener la ininterrupción de los servicios, ya que un temblor, incendio o inundación puede causar la suspensión de la actividad de cualquier organización.

La falla de equipos puede limitar la producción normal de un centro de cómputo, así como la pérdida de información o flujo de documentos, sin embargo este riesgo se puede reducir mediante una adecuada administración de respaldos y de la disponibilidad de dispositivos que se puedan utilizar temporalmente mientras se restablece el funcionamiento normal del equipo primario. En cuanto a fallas de energía se deben considerar las sobrecargas o bajas de voltaje que pueden ocasionar daños en diferentes dispositivos, por lo que se debe considerar la utilización de no-breaks, ya que estos permiten que se continue con el flujo de energía eléctrica hacia al centro de cómputo a pesar de las diferencias de voltaje.

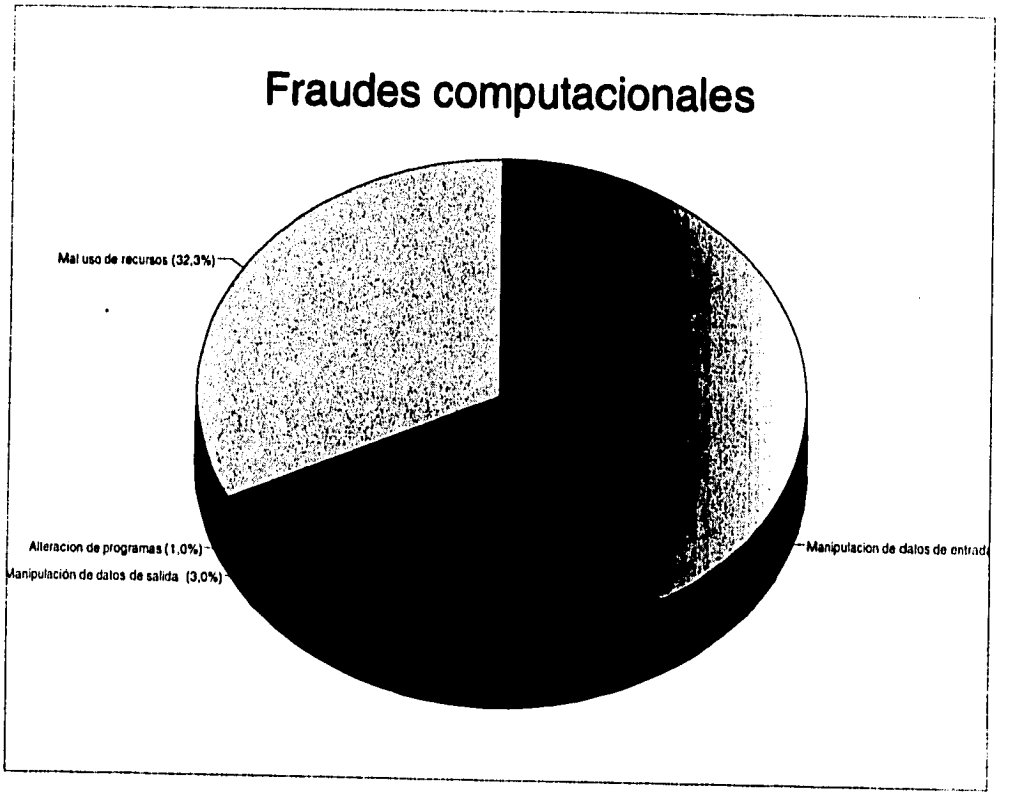
La existencia de crímenes computacionales es un hecho real pero muy poco documentado y escondido por aquellas organizaciones que lo han experimentado, aún en países como Estados Unidos e Inglaterra. La vulnerabilidad de los sistemas permite que estos sean susceptibles de fraude, desfalco, sabotaje, mal uso o daño deliberado, causando pérdidas que van desde pequeñas cantidades hasta varios millones de dólares, además este tipo de situación suele identificarse accidentalmente la mayoría de las ocasiones; normalmente los autores de estos delitos son los mismos empleados de la compañía quienes por determinadas circunstancias son motivados a cometer dichos actos; son tres los factores que se mueven alrededor de estas situaciones:

- Oportunidad
- Habilidad técnica y/o conocimientos
- Presiones económicas

Quizás la oportunidad determine más la actividad delictiva que la misma cantidad de dinero involucrada, esto aunado a la gran cantidad de literatura informática existente permite el mal uso de las habilidades computacionales de uno o varios individuos.

No fue sino hasta 1981 en Inglaterra que se realizó un reporte de auditoría que consistió en enviar una encuesta a 319 organizaciones diferentes, de las cuales sólo contestaron 119 y de éstas sólo 67 admitieron haber sufrido fraudes a través de sus sistemas computacionales, así mismo se menciona que sólo el 10% del valor total de fraudes computacionales que ascendía a 150 millones de dólares en 1981 fue reportado. De los 67 fraudes, 42 casos fueron debido a la manipulación de datos de entrada, 2 casos por manipulación de datos de salida, 1 por alteración de programas y 22 por el mal uso de recursos. Dicho reporte mostró que la mayor parte de fraudes se realizan a través de la manipulación, alteración o falsificación de los datos de entrada que alimentan el sistema, siendo la parte contraria la alteración de programas ya que esto requiere de más conocimientos computacionales.

Relativo al sabotaje computacional éste es en algunas ocasiones motivado políticamente o realizado como consecuencia de la frustración de empleados, extorsión o por simple agresión.


Fraudes computacionales
Mal uso de recursos (32,3%)
Alteracion de programas (1,0%)
Manipulación de datos de salida (3,0%)
Manipulacion de datos de entrad

EJEMPLOS

A continuación conoceremos algunos tipos de crímenes computacionales que fueron registrados en Estados Unidos en la década de los 80's:

"El fraude de la Corporación Equity Funding en 1973 fue organizado por el esfuerzo concentrado de almenos 20 procesadores de datos y personal a niveles gerenciales. Resultó en la pérdida de 600 millones de dólares en acciones, y la pérdida de 1000 millones de dólares en pólizas de seguros. Existe alguna indicación de que el fraude no fue particularmente bien planeado, pero si una respuesta a la oportunidad justificada por el deseo en prospectos financieros." [1]

"Referencia: Daily Telegraph, febrero 13 1981.
Fecha: 1979
Perpetrador: Concesionario y Supervisor contable
Víctima: Fábrica de cerveza
Esquema: Los supervisores ingresaron información incorrecta en la computadora de la compañía para que el propietario recibiera entregas de cerveza por las cuales no había recibido facturas. El supervisor había trabajado para la cervecería desde que terminó la escuela. Cuando llegó a ser supervisor en auditoría de entregas, tuvo la oportunidad de defraudar a la compañía mediante la alteración de registros. Como no manejaba efectivo, necesito al arrendatario, a quien había conocido desde hacía 10 años, para unirse en el fraude.
Cantidad: 8162 libras esterlinas.
Cómo se descubrió: Desconocido.
Pena: El concesionario fue encerrado por 15 meses y el supervisor por 18.

---

[1] Traducción de: A Handbook of computer security, Keith Hearnden, Kogan Page, London, 1987, pag. 52.

Comentarios: El concesionario no tenía necesidad de dinero. Sus ganancias habían excedido 35 000 libras por año. El mismo se permitió involucrarse porque su amigo no tenía dinero. La modificación de registros de entrada debió ser estrictamente supervisada y checada independientemente. La autorización adecuada debió ser obtenida antes de permitir tales modificaciones." [2]

"Referencia: Comunicación privada
Fecha: 1970s
Perpetrador: Empleado de nómina
Víctima: Hospital
Esquema: El empleado hizo uso del conocimiento que tenía de que la lista de salarios de empleados y personal no podría ser checada por la creación de empleados ficticios. Agregó varios empleados incluyendo dos doctores altamente pagados y hasta dio a sus falsos empleados incrementos de salario y tiempo extra. Exageró a sus personajes ficticios con otros atributos que les permitían más ingresos, con un individuo promovido del mínimo al máximo salario, y a otro otorgándole concesiones extras. Entre Octubre y Junio, extrajo cheques cobrables generados por la computadora, colocándolos en cuentas en tres sucursales bancarias, usando los nombres en los cheques y su propia dirección.
Cantidad: Arriba de 5000 libras esterlinas
Cómo se descubrió: Durante el tiempo en que se llevó a cabo el fraude, el auditor del departamento de salarios estaba en el hospital y el departamento fue estafado. Cuando regreso el fraude fue rápidamente descubierto.
Pena: El perpetrador, que era una viuda con dos hijos, admitió siete cargos de robo, cinco por contabilidad falsa y tres por falsificación. Estuvo en prisión por un año ." [3]

---

[2] Op. Cit. pag. 103.

[3] Op. Cit. pag. 106.

"Referencia: Sunday Standard, Mayo 3 1981.
Fecha: 1980
Perpetrador: Empleado de nómina
Víctima: Compañía de pinturas de Edinburg
Esquema: El empleado de 19 años de edad abrió cuentas bancarias falsas con nombres falsos, preparó entrada de documentos falsos para trabajadores no existentes, y uso el sistema de la computadora para transferir el dinero. Gastó sus mal obtenidas ganancias en motocicletas, un Ford Cortina y en un sistema de sonido. Este caso fue el primer fraude computacional registrado en la historia de Scotloand.
Cantidad: 17000 libras durante 6 meses
Como se descubrió: Por accidente, cuando un pago real fue requerido mientras el estaba de vacaciones.
Pena: Sentencia de 18 meses de prisión.
Comentarios: Este caso ilustra la falta de supervisión y control del trabajo del defraudador." [4]

"Referencia: Comunicación privada
Fecha: 1982
Perpetrador: empleado bancario
Víctima: casa de bolsa
Esquema: El empleado de 19 años de edad tuvo acceso a la cinta magnética maestra de la sucursal para actualizaciones diarias, en deudas y transacciones de crédito de todas las cuentas más grandes. Primeramente logró borrar su saldo de 189 libras de su tarjeta de crédito mediante el pago de una transacción de crédito falsa en la actualización diaria de la cinta. Después aumentó el límite de crédito a la cuenta de un amigo por 15 000 libras. El dinero fue gastado en el oeste de Londres. El fraude habría continuado si hubiera seguido confiando sus actividades a su propia sucursal. Sin embargo, trató de

[4] Op. Cit. pag. 106.

transferir 182 000 libras a la cuenta de otro amigo en una sucursal diferente. Para todas las transferencias interbancarias determinados documentos son requeridos para acompañar la transferencia, y estos no fueron encontrados.
Cantidad: 197 000 libras
Cómo se descubrió: El documento que acompaña la transferencia interbancaria faltaba y el fraude fue un rastro para el delincuente. El admitió el robo y fue suspendido de sus tareas.
Pena: El y su amigo quienes obtuvieron 15 000 libras, recibieron de sentencia la suspensión por un año. El caso de la persona involucrada en la transferencia de 182 000 libras no pudo ser probada, ya que el titular de la cuenta negó tener cualquier conocimiento de la transferencia." [5]

Resumiendo lo anterior podemos concluir que la falta de procedimientos de control y supervisión en sistemas computacionales así como la oportunidad permiten que se lleven a cabo acciones que causen pérdidas a las organizaciones que van desde pequeñas cantidades hasta grandes sumas de dinero, aunado a las consecuencias secundarias como falta de confiabilidad en la empresa o mala imagen de ésta. No se deben sobreestimar los riesgos computacionales mencionados anteriormente ya que nadie está exento de dichos riesgos.

A fin de minimizar o erradicar la probabilidad de este tipo de riesgos a que está expuesta la actividad de un centro de cómputo explicaré en los siguientes capítulos las características de seguridad física y lógica que cualquier centro de procesamiento de datos debe considerar a fin de mantener la continuidad de sus operaciones en todo momento así como la integridad de su información. Dichos temas se enfocarán al procesamiento de datos en un ambiente de equipo mainframe.

---

[5] Op. Cit. pag. 108.

SEGURIDAD

A pesar del gran desarrollo de tecnologías en dispositivos físicos y herramientas de software de seguridad un centro de cómputo que haga uso de lo anterior no puede tener la certeza de la confiabilidad e integridad de su centro de procesamiento si no cuenta además con adecuados controles y una buena auditoría. Es por eso de vital importancia conocer todos los elementos que conforman una "SEGURIDAD INFORMATICA" a fin de establecer y llevar a cabo eficientemente una serie de controles de seguridad. Para tal efecto comenzaremos definiendo la palabra seguridad. Algunas definiciones de dicho vocablo derivado del latín: ***securitas*** son:

> "ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que éste falle, se frustre o se violente" [6]

> "dícese de la existencia e imposición de técnicas que limitan el acceso a los datos y de las condiciones bajo las cuales pueden ser obtenidos." [7]

> " Impedir el acceso a/o uso de datos o programas sin autorización" [8]

---

[6] Enciclopedia Universal Ilustrada Europero Americana, Tomo LIV, Espasa-Calpe, Madrid, 1927, pag. 1514

[7] Diccionario MacGraw-Hill de Computación, Tomo II, Sybil P. Parker, MacGrawHill, México,1989, pag. 467

[8] Diccionario de procesamiento de datos, Jeff Maynard, Diana, México, 1978, pag. 256

"el estado obtenido por hardware, software o datos como resultado de esfuerzos satisfactorios para prevenir daño, robo o corrupción." [9]

Atendiendo a las definiciones anteriores y aunado al significado de la palabra informática (automatización de la información, del vocablo francés information y automatique) podemos entonces entender por **SEGURIDAD INFORMATICA** el conjunto de medidas establecidas para controlar y permitir o negar el acceso a los recursos utilizados en la automatización de la información. Para efectos de ésta tesis dichas medidas se estudiarán en cuatro tópicos relacionados a la seguridad física, backups, seguridad lógica y plan de recuperación en caso de desastre.

Hablando de la seguridad física podemos entender por ésta el conjunto de medidas a seguir con el objetivo de preservar las instalaciones físicas y el equipo de procesamiento de cualquier riesgo que pudiera afectar la operación normal del centro de cómputo.

Los backups o respaldos son copias de información (normalmente en dispositivos de almacenamiento secundario) de forma que permitan su pronta recuperación.

Referente a la seguridad lógica podemos entender por ésta el conjunto de controles y procedimientos aplicables a fin de garantizar la integridad y confiabilidad de la información.

El plan de recuperación en caso de desastres (BRP) es un plan de contingencia a seguir a fin de garantizar la continuidad de las operaciones así como la integridad de la información en caso de presentarse algún evento que pudiera interrumpir la operación normal o dañar la información.

---

[9] Traducción de: Webstors' World Dictionary of Computer Tonns, Darcy Laura and Boston Louise, Prentice Hall Press, New York, 1988, pag. 335.

SEGURIDAD FISICA DEL CENTRO DE COMPUTO

Las instalaciones del centro de cómputo son áreas restringidas internas ya que mantienen controles de acceso físico adicionales por la importancia del trabajo que se desarrolla y la información que alberga. Cuentan con una gran inversión tanto en hardware como software, y permiten la operación normal y continua de las operaciones de procesamiento. Para efectos de éste tema mencionaré aquellas características y medidas que se deben tomar en cuenta para garantizar la seguridad física de cualquier centro de cómputo, siendo su objetivo principal mantener la operación normal de los servicios en todo momento, que se podrían ver afectados como consecuencia de ataques deliberados o agresiones naturales. Asi mismo para efectos de este tema nos abocaremos a un ambiente de equipo mainframe.

CONSIDERACIONES

UBICACION. Es importante determinar la elección del lugar donde se establecerá un centro de cómputo, para ésto se debe considerar lo siguiente:

- **Suelo sólido**. No deben existir túneles o drenajes principales de la localidad en el subsuelo.

- **Facilidad de acceso**. Se refiere al tiempo, distancia, tipo de transporte y vías de acceso para llegar al lugar de las instalaciones.

- **Necesidad de espacio**. En este punto se debe garantizar la cantidad de espacio suficiente para la construcción del centro de cómputo, además de considerar futuras ampliaciones.

- **Alimentación de energía eléctrica**. Es decir la disponibilidad de energía, frecuencia de sobrecargas y descargas de voltaje, así como ausencia total de energía.

- **Líneas Telefónicas**. Considerar la disponibilidad de líneas, así como prestación de servicios por parte de la compañía telefónica.

- **Empresas Vecinas**. Conocer el giro o actividad de las empresas circunvecinas, ya que éstas pueden emitir sustancias muy contaminantes y pequeñas, o ser muy riesgosas.

- **Indice de fenómenos naturales**. Como terremotos, incendios, inundaciones o huracanes.

CONSTRUCCION El diseño y edificación del centro de cómputo debe ser cuidadosamente planeado. Básicamente se refiere a los tipos de materiales que se utilizarán para la edificación del centro de cómputo así como algunas características de ingeniería. En este apartado se deberán considerar los siguientes puntos:

- Capacidad de carga del suelo
- Sistema de drenaje en el suelo real
- Edificación de una construcción sólida y resistente
- Altura libre entre suelo y techo
- Extensión de la pared entre piso y techo falso para evitar comunicación entre cuartos
- Resistencia de los materiales
- Instalaciones eléctricas
- Instalaciones telefónicas
- Utilización de material incombustible en piso, techo y paredes

- Puertas blindadas
- Número de entradas y salidas
- Puertas de emergencia controladas por "crash bars" las cuales solo pueden ser usadas por dentro
- Vidrios blindados con un espesor de 5mm para mayor protección
- Bóveda de seguridad
- División del centro de cómputo en cuarto de impresión, cintoteca, almacén de papeleria, área de teleproceso, área de consolas, área de cpu's y otros dispositivos
- Utilización de alarmas contra fuego e incursión no autorizada
- Detectores de inundación
- Cuarto de vigilancia
- Vigilancia del exterior e interior a través de circuito cerrado de t.v.
- Area de backup alejada al menos 100 metros de distancia del computador central.

CONTROL DE ACCESOS

El control de acceso a las instalaciones del centro de cómputo no debe visualizarse aisladamente ya que forma parte de la totalidad de las instalaciones en una organización. Hablando específicamente del control de acceso a las instalaciones del centro de cómputo se pueden adoptar ciertas medidas como las siguientes:

1. **Guardias.** Los guardias sólo deben estar en las entradas o en el panel de control, pero no deben estar caminando en el cuarto del centro de cómputo. Además deben contar con una capacitación adicional que les permita controlar y monitorear el panel de control ya que son los responsables de su adecuado manejo.

2. **Registro.** Se debe llevar un registro de los proveedores o visitantes que accesan el centro de cómputo, nombre, hora de entrada, salida, motivo, número de gafete que portará así como nombre y firma de quien autoriza la entrada.

3.- **Gafetes**. En todo momento se debe portar el gafete, que permite identificar fácilmente si se trata de un empleado, proveedor o visitante ya que los gafetes deben ser completamente diferenciables, a través del tamaño y/o color.

4.- **Sistemas de control de accesos**. Estos sistemas permiten o restringen el acceso a determinadas areas del centro de cómputo. Para complementación de este punto haré referencia de cinco tipos de esta clase de sistemas:

*A) **Mecánico***. Este tipo de sistema utiliza cerrojos, candados y/o la combinación de llaves. Es el más barato aunque no permite determinar ni quien, ni la hora en que se acceso algún sitio, por lo que el nivel de seguridad es bajo.

*B) **Electrónico***. Este tipo de sistema funciona a través de tarjetas con código que se insertan en cajas electrónicas y a través de lectores ópticos o magnéticos sobre el código se permite o niega el acceso. Se puede usar en combinación con alarmas audibles o silenciosas en el panel de control para efectos de identificación de intrusos. En este caso sí se puede determinar la persona y hora en que se accesó algún sitio. El nivel de seguridad es medio.

*C) **Electromecánico***. Este tipo de sistema requiere un esfuerzo manual como presionar un botón en combinación con una lectora de tarjeta. Al igual que el sistema electrónico se puede utilizar en combinación con alarmas. El sistema de seguridad es medio.

*D) **Digital***. Los dispositivos digitales permiten la digitación de cualquier combinación de código que se haya asignado o que el usuario haya elegido para permitir el acceso a determinado lugar. Este tipo de sistema de acceso proporciona un nivel de seguridad alto aunque también es más costoso que los anteriores.

*E) **Computarizado**.* Este tipo de sistema es el más automático, ventajoso y sofisticado, permiten el acceso a través de reconocedores de formas o sonidos, así como la utilización de lectoras de códigos y la digitación de claves. Están equipados con alarmas audibles y silenciosas que se activan al detectar cualquier intento de acceso no autorizado o durante cambios ambientales como la temperatura, humedad y corriente de aire. El nivel de seguridad es muy alto, aunque también es de los más costosos..

5.- **Detectores de movimiento.**

Circuito cerrado de televisión (CCTV). Este tipo de dispositivos permiten observar y detectar movimientos en lugares cercanos y remotos que requieren una constante vigilancia. Las cámaras se deben colocar en lugares estratégicos en toda la instalación. El monitoreo se realiza en un cuarto con páneles de control en donde existen pantallas que permiten observar la actividad captada por las cámaras.

Cámaras infrarojas. Estos dispositivos son sensores que detectan el cambio de radiación térmica dentro del ambiente, generalmente sólo se utilizan en áreas que requieren un alto grado de seguridad ya que son bastante costosas.

PROTECCION CONTRA FUEGO

Debido a la gran cantidad de material combustible que se almacena en el centro de cómputo y a la complejidad eléctrica, existe la posibilidad de incendio. Debido a esto se deben adoptar medidas de seguridad, de lo cual hablaré en este apartado. Así, para la prevención de incendios se deben tomar en cuenta los siguientes puntos:

- Prohibir fumar en el área de cómputo
- Establecer inspecciones regulares del lugar
- Mantener la papelería fuera del cuarto principal
- Reportar a mantenimiento cualquier desperfecto eléctrico que se observe.

Estas medidas se deben llevar a cabo junto con la implementación de un buen sistema contra incendio, el cual deberá combinar sistemas de alarma, prevención, detección y supresión de fuego.

Algunas de las características que debe tener un buen sistema de protección contra fuego son:

- ☐ Colocación de alarmas manuales y automáticas en lugares estratégicos en toda la instalación
- ☐ Colocación de extinguidores manuales en lugares estratégicos en toda la instalación
- ☐ Existencia de un sistema automático que disperse el supresante adecuado: agua, CO_2 o halón
- ☐ Marcar claramente extinguidores y salidas
- ☐ Existencia de un panel de control que muestra en que parte de la instalación se ha activado una alarma manual o automática
- ☐ Desactivación del aire acondicionado en caso de activarse la alarma contra fuego
- ☐ Corte automático de energía al activarse la alarma

DETECTORES DE HUMO

Los detectores de humo y calor deben estar colocados en toda la instalación a fin de detectar cualquier indicio de fuego, y activar la alarma, esperando un período de tiempo durante el cual se puede onfirmar la presencia de fuego y entonces se activará el sistema que disperse el supresante adecuado, ya sea CO_2, halón o agua.

ELEMENTOS DE EXTINCION

Normalmente el control y extinción del fuego se realiza a través de distintos supresantes, dependiendo del lugar y naturaleza del fuego. A continuación mencionaré los supresantes más comúnes:

Bióxido de Carbono (CO2). Este supresante se recomienda para fuegos eléctricos, sin embargo se expulsa a tan bajas temperaturas que puede causar tanto daño al equipo como lo hacen las regaderas de agua.

Halón. Este gas es el supresante tradicional para los centros de cómputo. Su función es consumir el oxígeno lo que provoca que termine el proceso de combustión, no daña el equipo pero durante su expulsión se debe evacuar inmediatamente al personal. Algunas de sus características son:

- La instalación de sistemas de halón es cara.
- Almacenado en forma líquida bajo presión puede tener fugas y estar vacío al momento de su utilización.
- Una vez descargado necesita ser reemplazado.
- Para ser efectivo el área necesita estar sellada.
- A muy altas temperaturas puede producir gases tóxicos.

Agua. Funciona a través de regaderas, es un sistema barato, efectivo en cualquier tipo de fuego, disponible inmediatamente para su reuso, además de permitir la entrada de personas al área afectada durante el desastre. Sin embargo causa daños irreparables al equipo y medios de almacenamiento.

Mist Actualmente se ha desarrollado un nuevo sistema de supresión contra fuego llamado mist (vapor o llovizna) que consiste en una niebla fina de gotitas de agua y al parecer cuenta con las ventajas del halón sin sus respectivas desventajas. Además su descarga no causa el daño que causaría la utilización de una regadera.

La elección e instalación de un sistema contra incendio se debe adecuar a las necesidades y características del centro de cómputo sin olvidar que aunque las pérdidas por hardware pueden ser muy altas, suelen ser rebasadas por la pérdida de programas, archivos y/o documentación.

PROTECCION CONTRA AGUA

Algunas de las consideraciones que se deben contemplar para proteger la instalación contra daños por inundación son:

- Uso de techos, paredes y pisos a prueba de agua
- Existencia de un sistema de drenaje adecuado
- Instalación de alarmas en puntos estratégicos
- Instalación de detectores en los lugares más bajos
- Uso de tela protectora para cubrir el hardware cuando no está en uso
- Existencia de bombas

Dependiendo de la ubicación del centro de cómputo, puede ser que sea nula la posibilidad de una inundación, sin embargo puede generarse como resultado secundario de un incendio al activarse un sistema de regaderas, por lo que no se debe subestimar.

VARIACIONES DE VOLTAJE

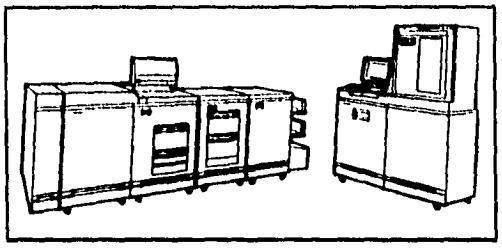
Las variaciones de voltaje se refieren a los incrementos o decrementos de energía o a la pérdida total de ésta. Se debe considerar el uso de reguladores que protegen el hardware de incrementos eventuales en el voltaje, a fin de que éste no se dañe. El uso de breakers es eficiente para proteger el equipo cuando llegan fuertes sobrecargas de voltaje y que quizás un regulador no soportaría. En cuanto a la instalación y/o utilización de baterías o plantas suministradoras de energía, éstas son de gran ayuda para prevenir la interrupción de los servicios como consecuencia de bajas de voltaje, en éste último punto se debe considerar la necesidad que se tenga de mantener la continuidad de las operaciones, dependiendo de ésto se optará por el uso de baterías o la instalación de una planta propia de energía.

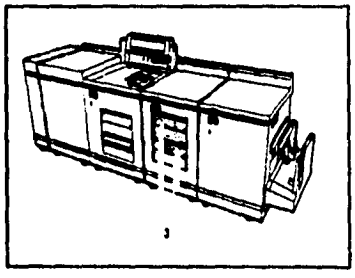
Así mismo hay que recordar que el suministro de energía no sólo sirve para mantener la operación de los procesadores sino también para conservar un ambiente óptimo dentro del centro de cómputo. La temperatura del centro de cómputo se debe mantener dentro de los límites especificados por el proveedor del equipo, normalmente alrededor de 19o C o 22o C. Por otro lado el hardware requiere un enfriamiento y humedad adecuados.

La implementación de medidas de control de acceso físico al centro de cómputo así como las relacionadas a la protección contra fuego o inundación dependerán del tamaño e importancia de las actividades de procesamiento electrónico de datos que se efectúen en una organización. Hablando de ambientes mainframe se deben establecer las medidas mínimas de seguridad mencionadas anteriormente.

POLIZA DE SEGURO PARA CENTROS DE COMPUTO

Debido a la naturaleza de los centros de cómputo, es imprescindible contar con un seguro que ampare sus contenidos ya que como cualquier otra entidad está sujeto a diversos riesgos que podrían ser causa de la pérdida parcial o total de dichos contenidos.





Normalmente una póliza de seguro de equipo electrónico cubre:

I) Daños materiales al equipo
II) Portadores externos de datos
III) Incremento en el costo de operación

Este seguro se aplica para 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.

Excluye los daños o pérdidas causados por:

"a) 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, grupos de personas maliciosas o personas actuando a favor o en conexión con cualquier organización política, conspiración, confiscación, requisición o destrucción o daño por orden de cualquier gobierno de jure o de facto, o de cualquier autoridad pública.

b) Reacción nuclear, radiación nuclear o contaminación radioactiva.

c) Acto intencional o negligencia manifiesta del Asegurado o de sus representantes."

A continuación mencionaré algunas de las características generales de los apartados que cubre esta póliza de seguros.

I) **Daños materiales**

Ampara cualquier pérdida o daño físico, súbito e imprevisto de tal forma que necesitara reparación o reemplazo. Entre las exclusiones destacan:

- Pérdidas o daños causados por terremoto, temblor, maremoto, erupción volcánica, tifón, ciclón o huracán.
- Pérdidas o daños causados por hurto y/o robo sin violencia
- Pérdidas o daños causados por fallo o interrupción en el suministro de corriente, eléctrica, de gas o 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 preveer mediante la contratación expresa de otra póliza.

II) Portadores Externos de Datos

Cubre la indemnización sobre daños causados a dispositivos de amacenamiento de datos así como la información contenida en éstos, bajo la sección I de daños materiales. Principalmente 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.

II) 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.

Polizas Adicionales

Algunos de los endosos adicionales que pueden contratarse para este seguro cubren lo siguiente:

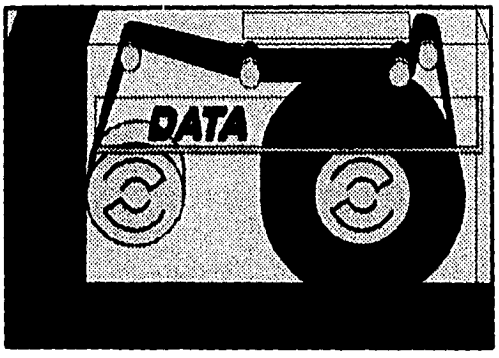
- Huelgas, alborotos populares y conmoción civil
- Gastos Extraordinarios y flete expreso
- Gastos por flete aéreo
- Daños por fallo de la instalación de climatización
- Robo sin violencia (hurto)

- Equipos móviles y portátiles fuera de los predios señalados
- Cláusula de terremoto y erupción volcánica
- Cláusula de huracán, ciclón y tifón
- Exclusión de daños o pérdidas debido a incendio, rayo, explosión, aviones, vehículos y humo
- Exlcusión de daños mecánicos y eléctricos internos
- Equipos de climatización

Es de suma importancia 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.

BACKUPS

Un backup o respaldo es una copia de información, archivos y/o documentación que se hace normalmente en dispositivos de almacenamiento secundario como cintas o cartuchos. En adelante me referiré al término archivos considerando que pueden ser programas, datos, librerías del sistema, módulos de carga, archivos de base de datos y de información en general.



La importancia y necesidad de contar con backups radica en que permiten restablecer físicamente archivos en caso de pérdida o daño parcial o total de éstos. La pérdida de archivos puede ser originada por muchas causas y en cualquier momento; normalmente tales pérdidas o daños son el resultado de:

Errores en el programa
Errores en el software del sistema
Errores en hardware
Errores en procedimientos
Errores ambientales
Sabotajes

Errores en el programa. Puede darse el caso de que un mantenimiento, programa no autorizado o una versión incorrecta de éste actualice durante su ejecución ciertos registros o archivos erróneamente, causando un daño parcial o total a los archivos.

Errores en el software del sistema. Aunque se asume que el software del sistema ha sido totalmente probado y es casi nula su falla, puede suceder que el empleo de alguna utilería provoque daños a los archivos que son manipulados por ésta.

Errores en el hardware. Eventualmente se puede dañar un disco, o cinta, y provocar la pérdida de archivos que se encuentren almacenados en dicho dispositivo.

Errores en el procedimiento. A pesar de existir políticas y procedimientos establecidos para la ejecución de programas o activación de discos, es posible que algún operador ponga on-line un disco incorrecto y de esta forma dañar la información contenida en éste, o equivocarse en la secuencia de ejecución de un proceso ya que la salida de uno es la entrada del siguiente.

Errores ambientales. Fortuitamente puede darse el caso de pérdida de archivos como consecuencia de un temblor, incendio, inundación o variaciones drásticas en la temperatura que afectan directamente a los medios de almacenamiento.

Sabotajes. Intencionalmente puede provocarse un daño tanto al equipo como a la información, ya sea por personal de la misma compañía o ajena a esta.

TIPOS DE BACKUP

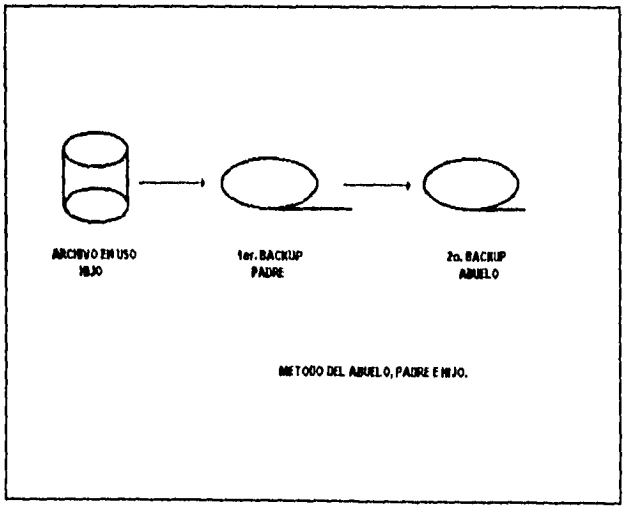
Básicamente existen cuatro métodos para llevar a cabo un backup o respaldo, conocidos también como estrategias de backup siendo las siguientes:

- Método del abuelo, padre e hijo
- Dual Recording (respaldo simultáneo)
- Dumping
- Logging

Estos procedimientos de respaldo pueden ser llevados a cabo en forma simultanea, dependiendo de las necesidades de respaldo que se requieran así como su justificación.

Método del abuelo, padre e hijo

En este método el archivo en uso (hijo) que radica en dispositivos de almacenamiento primario se copia normalmente a un dispositivo de almacenamiento secundario (padre) convirtiéndose en la primera versión anterior, posteriormente se repite el proceso; la primera versión se convierte en la segunda versión creándose una nueva primera versión de la copia del archivo en uso, y así sucesivamente. En este tipo de backup se pueden generar tantos abuelos como se requiera.



METODO DEL ABUELO, PADRE E HIJO.

Este método es simple y recomendado para sistemas batch, ya que permite fácilmente el reproceso de procedimientos, además de no ser muy costoso.

Dual recording (respaldo simultáneo)

Este tipo de método se realiza en dispositivos de almacenamiento primario; se llevan dos copias separadas actualizándose simultáneamente, la primaria que es la que está en uso y la secundaria que es el backup. En caso de dañarse el archivo en uso se switchea al backup, es decir a la secundaria, se desactiva la primaria y la secundaria se convierte en la primaria.

Este tipo de backup es recomendable para sistemas on-line altamente prioritarios. Además se debe tener un segundo método de backup, ya que ofrece una mínima protección contra errores de software y hardware además de ser elevadamente costoso.

Dumping

Este método copia total o parcialmente bases de datos en dispositivos de almacenamiento secundario como cintas o cartuchos. Durante la recuperación reescribe el dump en el medio de almacenamiento primario y reprocesa transacciones desde que se tomo el dump.
Hay dos tipos de dump: el dump físico y el dump lógico. En el caso del dump físico se leen y copian secuencialmente los registros físicos (track por track), y es recomendado para la recuperación global de la base de datos. En el caso del dump lógico se leen y copian secuencialmente los registros lógicos de un archivo siendo utilizado para restauraciones selectivas. Ambos tipos de dumping consumen muchos recursos por lo que debe ser muy evaluado su uso.

Logging

Esta estrategia de backup graba en disco las transacciones que cambian la base de datos generando una imagen del registro modificado por la actualización. Además requiere que los usuarios reprocesen transacciones. Este tipo de backup también consume muchos recursos ya que debe grabar las transacciones de entrada, imágenes previas y posteriores al registro cambiado, así como parámetros de cambio.

CONSIDERACIONES ADMINISTRATIVAS

Independientemente del tipo de backup que se realice, se deben tomar en cuenta los siguientes aspectos:

- Determinar el tipo de backup a realizar, atendiendo a las necesidades de restauración
- Asignar la responsabilidad de las operaciones de backup y restauraciones a una persona específica
- Documentar las políticas y procedimientos de backup y restauración
- Determinar la frecuencia en que se realizarán los backups
- Determinar el lapso de vida de un backup
- Establecer una bóveda de backups en una localidad o lugar diferentes al lugar donde normalmente se llevan a cabo las operaciones del centro de cómputo.

Muchas variables afectan los procedimientos y políticas para la realización de backups, como la tolerancia de tiempo para la recuperación en una caída, necesidad de actualizaciones, disponibilidad de hardware y software para restauraciones o necesidades particulares de backups por aplicaciones, sin embargo es de vital importancia tener un efectivo sistema de backups que permita las operaciones de recuperación parciales o totales a fin de evitar contratiempos durante las operaciones de procesamiento.

Hay que recordar que la administración de backups consume recursos tales como gente, dispositivos de almacenamiento, tiempo de CPU, espacio para su almacenamiento en el centro de cómputo y en bóveda de seguridad. La realización de ésta actividad dependerá de la vulnerabilidad e importancia de la información, siempre tomando en cuenta el costo y tiempo que implicaría una recuperación manual recapturando la información o reprocesar procesos contra el beneficio de recuperar la información sólo con la ayuda de un backup.

SEGURIDAD LOGICA

Con el auge de las computadoras surgió la necesidad de implementar medidas de seguridad que mantuvieran aislados tanto el hardware como las instalaciones de cualquier centro de cómputo contra agresiones externas como mencioné anteriormente; sin embargo la gran diseminación y diversidad de computadoras conectadas en diversos puntos a un Host aunado al gran número de sistemas multiusuarios generó que se comenzaran a diseñar e implementar características y mecanismos de seguridad de acceso lógico a fin de garantizar la integridad y confiabilidad de la información.

Entendiéndose como seguridad lógica el conjunto de políticas y procedimientos que permiten controlar y garantizar la integridad y confiabilidad de la información.

Debido a la vulnerabilidad de los sistemas y a falta de seguridad de acceso lógico en éstos, ha sido factible destruir información accidental o deliberadamente, cometer fraudes, sabotajes o hacer uso de información altamente confidencial distinto al cual fue destinado, por otro lado el reconocimiento de efectos secundarios como pérdida de confianza, pérdida de imágen, pérdida de activos o pérdida de penetración en el mercado, ha concentrado la atención en buscar medidas para contrarrestar estos efectos. Es así que en la década de los 60's se comenzaron a realizar investigaciones y desarrollos en seguridad de sistemas multiusuarios. Entonces surge un concepto llamado monitoreo referenciador en que que se involucran cuatro entidades:

- Los objetos
- Los sujetos
- Una base de datos de autorizaciones
- Un registrador de eventos

Para comprender mejor este concepto se entendera por cada una de las entidades mencionadas anteriormente lo siguiente:

Los objetos son entidades pasivas como dispositivos, volúmenes, cintas, archivos, programas, comandos, CICS, aplicaciones VTAM o transmisión de mensajes. Los **sujetos** son entidades activas como procesos iterativos o batch que requieren hacer uso de los objetos para lo cual se requiere verificar previamente la **base de datos de autorizaciones** que contiene los atributos de los sujetos y objetos; entendiéndose por atributos la determinación de uno o más privilegios o restricciones que un sujeto tiene al usar el sistema. Además se debe contar con un **registro de eventos** a fin de monitorear y auditar la actividad del sistema, entre ella los accesos.

Esto es sólo un concepto de seguridad lógica que conllevo una serie de consideraciones e implicaciones que iré detallando durante la redacción de este tema.

REQUERIMIENTOS DEL CONTROL DE ACCESO LOGICO

Inventarios

Antes de realizar cualquier actividad debemos conocer los recursos con los que contamos a fin de identificarlos, organizarlos y decidir que se pretegerá, cómo y en que proporción.

Se debe realizar un inventario de hardware en el que se identificarán y clasificarán las terminales, impresoras, discos, cintas, cartuchos y otros dispositivos, según el ambiente ya sea productivo o de desarrollo así como el uso al que está destinado.

Por otro lado se debe realizar un inventario de archivos, programas, transacciones, productos y subsistemas en el que igualmente se definirá su tipo, descripción y dispositivo en el que se almacena.

VOLUMEN	TIPO	CAPACIDAD EN GB	USO	AREA QUE LO UTILIZA
SPR285	3380-K	1.89	PRODUCCION	SOPORTE TECNICO
SPR410	3380-K	1.89	PRODUCCION	NOMINA
SPRDBA	3380-K	1.89	DESARROLLO	SEGURO DE VIDA
MVKS01	3390-3	2.83	DESARROLLO	POLIZAS AUTOS

INVENTARIO DE DISCOS

ARCHIVOS PRODUCTIVOS	TIPO	DISPOSITIVO	DESCRIPCIÓN
NOMINA FUENTE	SECUENCIAL	DISCO	ARCHIVO MAESTRO DE EMPLEADOS
NOMINA BACKUP	SECUENCIAL	CINTA	RESPALDO DE ARCHIVO MAESTRO DE EMPLEADOS

INVENTARIO DE ARCHIVOS

Clasificación de la información

Con el creciente número de aplicaciones automatizadas, la computadora ha llegado a ser una herramienta administrativa esencial de donde se extrae información para su análisis y toma de decisiones. Dicha información debe ser confiable por lo que se debe contar con una adecuada protección de acceso a archivos, programas y transacciones. Se debe saber que se va a proteger y a qué nivel, para lograr ésto y evitar un mayor costo sobreprotegiendo información innecesariamente, se debe realizar una clasificación de la información que se utiliza dentro de la organización, tomando en cuenta el tipo de información como puede ser contable, financiera, administrativa o legal, áreas donde se maneja, consecuencias que provocaría para un solo individuo o a la organización su exposición o destrucción e información sensible para cometer fraude.

Una clasificación de información podría ser la que se ilustra en el siguiente cuadro:

ARCHIVO	**NIVEL DE CLASIFICACION**	**AREAS QUE LO PUEDEN CONSULTAR**
ARCHIVO DE NOMINA	RESTRINGIDA	NOMINA
ARCHIVO DE AGENTES	RESTRINGIDA	VENTAS
ARCHIVO DE POLITICAS DE CONTRATACION	CONFIDENCIAL	RECURSOS HUMANOS
ARCHIVO DE SERVICIOS QUE OFRECE LA COMPAÑIA	PUBLICA	TODAS

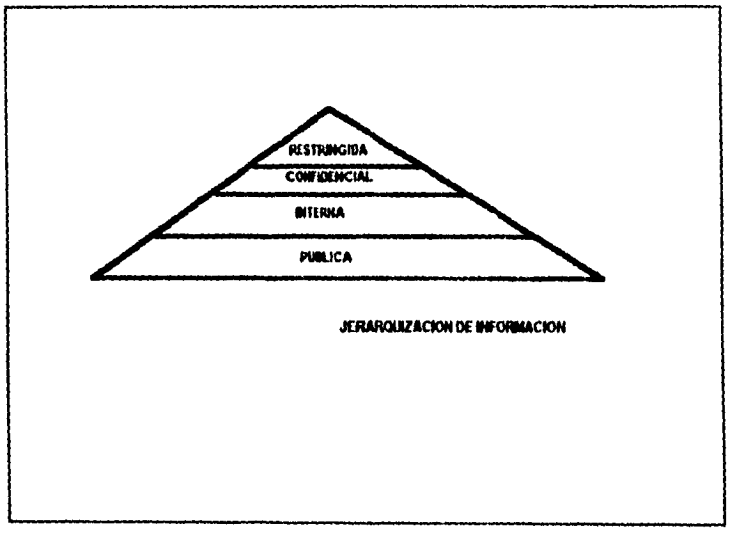
Clasificación de la información por nivel

- **Restringida**. Esta información es altamente privada y sensitiva. Su destrucción o exposición tendría un gran impacto en la operación de la organización. Normalmente la utilizan los funcionarios (planes estratégicos de negocios, planeación de recortes).

- **Confidencial**. Esta información es privada y sensitiva. Su destrucción o exposición afectaría primordialmente a un área o individuo. La utilizan departamentos específicos (nómina, historiales de personal o clientes y/o proyectos).

- **Uso Interno**. Ee tipo de información no es privada para un individuo o área específica, puede ser consultada por cualquier persona que labore en la organización. Su destrucción no tiene impacto (prestaciones, días de descanso o contrato laboral).

- **Pública o general**. Al igual que la anterior su destrucción no tiene ningún impacto. Puede ser fácilmente conocida fuera de la organización (precios de los servicios o productos que ofrece la organización).



La clasificación de la información no se realiza una vez y se deja tal cual al paso del tiempo, requiere una revisión periódica a fin de que siempre cumpla con su objetivo: proteger conjuntos de información, dando acceso a quien lo requiera y al nivel que deba accesarlo. Tan malo es dejar las puertas abiertas a quien no debe entrar como cerrárselas a quien por sus actividades debe tener autorización de acceso.

Utilización de estándares

El uso de una nomenclatura predefinida puede ayudar a la implementación y mantenimiento de una estructura de seguridad. Dependiendo de los estándares se podrá identificar fácilmente el tipo de recurso así como sus características. La nomenclatura debe ser clara, flexible y fácil de recordar, además permite mantener una eficiente administración de recursos no solo en el aspecto de la seguridad sino en cualquier otro tipo de control. Así mismo la utilización de nomenclaturas a través de prefijos puede ayudar a definir grupos de recursos en lugar de definir recursos aislados, con lo que se logra una organización más adecuada que ayuda a mantener una seguridad más flexible. A falta de estos no se puede mantener un control adecuado ya que no permite la rápida identificación de recursos, su contabilización, organización y depuración.

Por ejemplo se puede establecer un estandar para la definición e identificación de archivos; un formato para los primeros cuatro calificadores del archivo podría ser el siguiente:

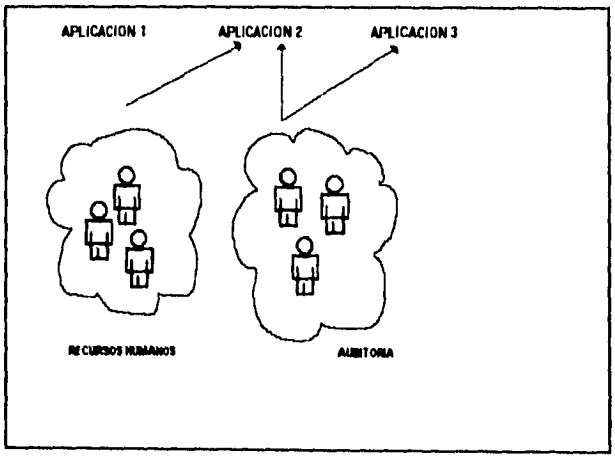
P NO X
D NO X

donde:

P o D Es una constante que identifica si es un archivo productivo o de desarrollo
NO Es una variable que identifica el sistema al que pertenece (en este caso nómina)
X Es una variable que identifica si es un archivo secuencial, particionado o VSAM.

División de tareas

Es importante definir los alcances y límites de las actividades que realiza la gente. De hecho el control de accesos refuerza ésta división de tareas entre aquellos que accesan el sistema, además de establecer responsabilidades y obligaciones, claramente permite formar grupos de usuarios que tienen las mismas necesidades de acceso al sistema, de forma que el administrador de seguridad no tiene que definir un acceso específico para cada usuario sino solo asigna los atributos de un grupo en especial.



Tipos de usuarios

Debido a que los usuarios cuentan con diferentes necesidades de acceso al sistema es conveniente agruparlos para permitir una mejor, más fácil y flexible administración de los recursos informáticos que da como resultado un adecuado y bien definido control que cubra las necesidades de seguridad del centro de cómputo ya que estas no siempre son las mismas dentro de una u otra organización. Para efectos de esta tesis mencionaré los siguientes grupos de usuarios:

- USUARIO FINAL
- PERSONAL DE DESARROLLO DE SISTEMAS
- INGENIEROS DE SISTEMAS
- ADMINISTRADOR DE LA SEGURIDAD (SA)
- ADMINISTRADOR DE BASE DE DATOS (DBA)
- OPERADORES

Usuario Final

Desde el punto de vista en análisis y desarrollo de sistemas el usuario final es aquella persona externa al área de sistemas que especifica un serie de requerimientos que serán cubiertos a través de la automatización de la información. Desde el punto de vista operativo el usuario final es aquella persona que utiliza comúnmente cualquier recurso informático. El usuario final no debe tener atributos especiales y debe tener una completa restricción de acceso a la programación y funciones del sistema. Dentro de este grupo podemos encontrar varios subgrupos formados por gerentes, consultores, capturistas, cotizadores y personal ajeno a la compañía.

Personal de desarrollo de sistemas

Este grupo de usuarios se encarga de diseñar, desarrollar y probar nuevos sistemas aplicativos para satisfacer las necesidades de automatización de la información. Deben tener acceso a algunas funciones y facilidades del sistema como reporteadores o utilerias que permiten respaldar y/o restaurar información así como a sus propios archivos de trabajo, además de trabajar en un ambiente de pruebas separado al ambiente de producción en donde no deben tener ningún acceso. Así también deben tener restringido el acceso a otros programas y archivos de desarrollo que no competan a su área. Este grupo puede estar formado por analistas, programadores, líderes de proyecto y/o gerentes.

Ingeniero de sistemas

Su función es instalar, probar y mantener el sistema operativo del host, los subsistemas y productos. Sólo deben tener acceso a algunas librerías del sistema o productos a los cuales dan mantenimiento, en cuanto a restricciones no deben tener acceso a datos y programas en desarrollo o productivos.

Administrador de seguridad o SA (Security Administrator)

Esta persona es responsable de la implantación, modificación y monitoreo de una estrategia de seguridad. Tiene la habilidad y "autorización" de cambiar las opciones del sistema, cambiar user ids y sus atributos, cambiar la autorización de acceso a recursos, leer cualquier archivo y auditar el sistema. No debe estar involucrado en tareas de programación y/o sistemas aplicativos así como a las descripciones de éstos últimos.

Administrador de la base de datos o DBA (Data Base Administrator)

El DBA es el responsable de diseñar las estructuras lógicas de la base de datos así como mantener su integridad y estructura. Valida la definición conceptual que tiene el programador de la base de datos, diseña la estructura, la conserva y le da mantenimiento. Los DBA's deben tener acceso a algunas funciones y facilidades del sistema, a los datos y base de datos de todo el ambiente de desarrollo, exceptuando los programas.

Auditor

En general esta persona verifica los estados financieros, operaciones, procedimientos y políticas de la organización a través de técnicas y herramientas que le permitan encontrar problemas, riesgos y/o prácticas erróneas. Busca revelar las ineficiencias y algunas veces ofrecer propuestas para su corrección. Sin embargo, para efectos de esta descripción podemos identificar dos tipos de auditores: el operativo y el de sistemas. El auditor operativo solo debe tener acceso de lectura a los sistemas aplicativos a fin de verificar su uso y funcionamiento. Por otro lado el auditor de sistemas puede tener todo tipo de acceso al sistema, principalmente a productos, subsistemas o utilitarios con la finaliddad de revisar el uso de recursos, intentos de violaciones, además de las políticas y procedimientos establecidos en un centro de cómputo.

Operador

Los operadores son los encargados de ejecutar los jobs indicados por el administrador del centro de cómputo, notar anomalías y reportarlas inmediatamente al personal indicado o en su defecto tomar las acciones correctivas adecuadas. Debe estar al pendiente de la consola, impresoras, cartucheras y otros dispositivos del centro de cómputo.

TIPO DE USUARIO / *RECURSO*		**USUARIO FINAL**	**DESARROLLO**	**ING**	**SA**	**DBA**	**AUDITOR**	**OPERADOR**
DATOS	PRODUCCION	SI	NO	NO	NO	NO	SI	NO
	OESARROLLO	NO	SI	NO	NO	NO	NO	NO
PROGRAMAS	PRODUCCION	NO	NO	NO	NO	NO	NO	NO
	OESARROLLO	NO	SI	NO	NO	NO	NO	NO
UTILERIAS		NO	SI	SI	SI	SI	NO	NO
LIBRERIAS DEL SISTEMA		NO	NO	SI	SI	NO	NO	NO

La división de tareas permite una mejor clasificación de usuarios que comparten las mismas necesidades de acceso.

Finalmente algunos de los cuestionamientos que se pueden realizar una vez que se ha implementado una eficiente agrupación de usuarios los menciono en el siguiente checklist:

- ☐ Asignar responsabilidades y necesidades de acceso a la información de cada grupo de usuarios
- ☐ Asegurar la existencia formal de una política que establezca el rol del administrador de seguridad
- ☐ Asegurar que los nuevos empleados conozcan las políticas y procedimientos de seguridad

- Verificar de que las políticas de seguridad son comunicadas a los distintos tipos de usuarios
- Asegurar que reciban recordatorios periódicos sobre las políticas y procedimientos de seguridad
- Evitar la duplicidad de tareas, especialmente entre distintos grupos de usuarios
- Controlar el acceso a las instalaciones en horario distinto al especificado en la jornada de trabajo dependiendo del área y tipo de usuario

DISPOSITIVOS DE AUTENTICIDAD

La utilización de passwords para dispositivos de autenticidad es la más comúnmente usada por ser la más económica. Sin embargo hay otras formas de validar la identidad de un usuario a través de la combinación de:

- Conocimiento de algo que solo sabe el usuario como un password
- Posesión de algo como una llave o tarjeta magnética
- Unidades lectoras de características físicas como huellas digitales y geometría de la mano
- Reconocimiento de voz
- Reconocimiento de formas como el cuerpo de una persona o su firma

Estos métodos de identificación de usuario sólo se utilizan en lugares donde es justificable llevar un control de accesos muy estricto por la naturaleza de las actividades y/o información que se manejan.

SEGURIDAD DE ACCESO LOGICO

Para proteger la información de destrucción deliberada o accidental y accesos no autorizados, se han implementado métodos de acceso lógico. Dichos métodos restringen la utilización de recursos del centro de cómputo así como la forma de acceso por parte de los usuarios. Actualmente existen en el mercado efectivos métodos de acceso tanto en hardware como en software que generalmente consisten en user ids y passwords, que se caracterizan por ser un método práctico que ayuda a disminuir el riesgo de actividad no autorizada por medio de la identificación (user id) y verificación (password) durante el inicio de sesión o entrada al sistema, además de ser uno de los controles funcionales más económicos.

User ID

Los user ids también llamados cuentas permiten firmarse al sistema así como permitir o negar el acceso a algún recurso o dirigir la ejecución automática de un programa. En algunos sistemas establecen la contabilidad del usuario, que permite determinar quién acceso que y para qué, establecer el uso ilícito de user ids, conocer el consumo de recursos del sistema como tiempo de procesamiento, utilización de espacio y memoria. Esta identificación de usuario puede formarse con las iniciales del nombre y/o número de empleado o una combinación de su primer nombre y apellidos, dependiendo del número de usuarios y complejidad del sistema.

Los user ids pueden funcionar solos o en combinación con passwords que es la práctica más común, ya que conservando el user id y password confidencialmente permiten implementar un buen nivel de seguridad ya que es más difícil descubrir los dos.

Para una mayor seguridad se deben asignar user ids y passwords únicos para cada usuario en lugar de asignarios a grupos de personas. Esto permite tener bien identificados a los recursos del sistema, entre elios los usuarios, y limita los efectos colaterales que se pudieran tener cuando alguna persona del grupo es promovida de puesto o deja la compañía, ya que se tendría que cambiar inmediatamente el password y dar aviso a los demás compañeros; por otro lado no se puede determinar exactamente quién accesó algún recurso por lo que no se pueden establecer los límites de responsabilidad de un usuario al haber accesado el sistema.

Passwords

El password permite verificar la identificación provista por algún usuario al checar que el password corresponda al usuario ingresado previamente. Los passwords están formados por cadenas de caracteres que en combinación con un user id o cuenta permiten el acceso a alguna aplicación o lugar físico del centro de cómputo. Básicamente se distinguen dos tipos de passwords, passwords de user ids y passwords de recursos. Los primeros siempre están ligados al user id; los segundos protegen el acceso a recursos como consulta de subsistemas, ejecución de programas, lectura de archivos o ejecución de comandos entre otros.

Para el uso y administración de passwords se deberán tomar en cuenta algunas características que permitirán que su uso sea eficiente a fin de mantener un buen nivel de seguridad.

Características

Dificultad de adivinar. Para ser difíciles de adivinar los passwords deberían tener una longitud enorme; sin embargo nadie va a perder el tiempo aprendiendolos o tecleandolos, para evitar ésto, la dificultad de adivinarlos se debe reforzar con su composición y longitud, tomando en cuenta que deben ser fáciles de recordar.

Composición. Deben estar formados por cadenas de caracteres, en algunos casos sólo alfabéticos o numéricos, una combinación de éstos o cualquier otro caracter.

Longitud. Los passwords de longitud más grande son más seguros pero toma mayor tiempo ingresarlos y es más fácil cometer errores. La longitud mínima que se recomienda son cuatro caracteres, aunque puede tomar un rango mayor o menor. Sin embargo la organización mundial de estándares establece que el password debe tener una longitud de ocho caracteres.

Expiración. La expiración del password es la característica que obliga al usuario a cambiarlo por uno nuevo que sólo sea de su conocimiento. Normalmente los passwords que se asignan por primera vez son pre-expirados así como cuando se habilita de nuevo algún user id. La expiración puede tener definido un período de tiempo determinado como rango, de esta forma al cumplirse dicho lapso se obliga al usuario a teclear y confirmar un nuevo password que a partir de ese momento solo será conocido por él.

Políticas

Los passwords pueden ser adivinados y en algunos casos pueden ser susceptibles de ser conocidos durante su almacenamiento o transmisión. Para evitar el riesgo de que ésto ocurra se debe tomar en cuenta lo siguiente:

- No utilizar passwords fáciles de adivinar, como las iniciales del nombre, del mes, fechas o palabras que pueden relacionarse fácilmente con el usuario.

- No escribirlos en papeles o documentos que son suceptibles de ser observados por otra persona o que se pueden perder.

- No imprimirlos en reportes o registros aún cuando éstos son confidenciales.

- Considerar los procedimientos para firmarse (sign-on), estos procedimientos deben ser amigables para el usuario sin contradecir los procedimientos de seguridad. Deben proporcionar la fecha y hora del último acceso.

- Considerar el número de intentos fallidos permitidos para accesar el sistema, que puede ser desde 1 hasta n veces dependiendo de las necesidades de seguridad y características del software de seguridad. Es recomendable que al tercer o quinto intento fallido se cierre el acceso para ese user id.

- Considerar el intervalo de tiempo para cambiar el password. Igualmente dependiendo de las características y necesidades de seguridad se debe establecer el período de tiempo en que estará activo un user id antes de solicitar automáticamente su cambio de password. Este intervalo puede ser variable, abarcando un rango de 1 a 365 días, aunque también se puede determinar que el password nunca expire, es decir que nunca solicite cambiarlo dejando a criterio del usuario el cambiarlo en cualquier momento. Es recomendable que el password expire cada mes, excepto cuando los user ids están en bats y no pueden ser cambiados, en este caso se debe especificar que no expire el password.

- Cambiar el password inmediatamente si por alguna razón de emergencia se prestó el user id.

- Forma de distribución del password a los usuarios correspondientes para constatar que reciban su propio password, ya sea vía telefónica, fax, correo electrónico o en persona.

Consideraciones administrativas

Como mencioné anteriormente la implantación de user ids y passwords es un control eficaz y muy económico, sin embargo se deben tomar en cuenta sus características y principalmente determinar y seguir las políticas establecidas alrededor de estos controles.

Algunos lineamientos que se pueden establecer para una mejor administración de user ids son los siguientes:

1. Establecer el procedimiento para la alta, modificación y depuración de user ids.

2.Concientizar al usuario de que los user ids y passwords son personales e intransferibles, cada uno tiene un acceso autorizado hasta cierto nivel en aplicación y consulta en los diferentes sistemas que accese, por lo que no deben prestarse por ningún motivo, ya que el titular es totalmente responsable del uso que se le dé.

3.Realizar auditorías periódicas y al azar, del uso que se le está dando a determinados user ids y en caso de encontrar alguna anomalía se deberá notificar al usuario y a su superior inmediato.

4.Establecer un período de tiempo, en el cual si un user id no es utilizado se dará de baja.

5.Realizar cruces contra nómina y proceder a dar de baja aquellos user ids de personal que ya no labore en la compañía. De esta forma no es necesario esperar la notificación por parte de personal de la liquidación o retiro de algún empleado ya que se puede aunar la clave de empleado al user id; hacer un match con el archivo de empleados periódicamente y borrar automáticamente aquellos que ya no se encuentren en dicho archivo.

SEGURIDAD EN BASE DE DATOS

Una base de datos es un conjunto de información homogénea interrelacionada entre sí para uno o varios fines previamente establecidos. En estas residen los datos e información de los que depende el buen funcionamiento de cualquier organización. Es por esto de suma importancia mantener la integridad de la información a través de medidas de seguridad aplicadas en un ambiente de base de datos conformado por el ambiente productivo y el ambiente de desarrollo.

Los riesgos a que está expuesta una base de datos pueden provocar:

-Corrupción de datos como consecuencia de un error en el programa o por la mezcla de versiones distintas de programas o archivos.
-Pérdida de información, al borrarse accidental o deliberadamente.
-Daño a la base de datos provocado por una falla en el disco.
-Extracción de información no autorizada con el objeto de causar algún daño a la compañía o utilizarla para fines personales.

Estos riesgos se pueden limitar a través de:

-La existencia de un control de acceso adecuado al equipo de cómputo.
-La protección de los recursos como discos, cintas, cartuchos, archivos, programas y utilerías.
-La detección de usuarios con privilegios excedidos.
-Monitorear la actividad y privilegios de usuarios con altos conocimientos técnicos.
-Proveer mantenimiento a los dispositivos de almacenamiento de acceso directo donde residen las bases de datos.
-La definición y delimitación de los ambientes productivo y de desarrollo.

-La implantación de políticas concernientes a la extracción de información fuera de la compañía.
-Proveer protección propiamente de la base de datos a través del diccionario de datos.

Diccionario de datos

El diccionario de datos es una base de datos que sirve como repositorio central que contiene las definiciones de datos, las relaciones de éstos entre recursos de procesamiento, módulos y documentación. Su propósito es el de centralizar las definiciones lógicas (descripción del significado de datos, quién los genera, relación con otros recursos, criterios de validación) y físicas (formato de datos, dispositivo de almacenamiento) de la base de datos a fin de organizar, controlar y documentar la información del ambiente de procesamiento de la base de datos. De igual forma el diccionario de datos provee seguridad para las definiciones del diccionario y acceso a datos.

Como vemos es importante proteger el diccionario a fin de controlar el acceso a las definiciones del sistema, base de datos y el uso de herramientas. Para limitar el acceso a un diccionario se pueden proteger los productos, tareas, programas y entidades. Esto se puede realizar asignando una clase de seguridad, por ejemplo a una tarea o programa y automáticamente se previene que un usuario accese dicha tarea o programa.

Al proteger el diccionario de datos se centraliza la administración de las bases de datos, por lo que dicha administración recae en el DBA. Además de sus actividades habituales el DBA es responsable de establecer procedimientos regulares de backup para salvaguardar la integridad de la base de datos en caso de fallas del programa, del sistema o del hardware. La realización de

backups se hará en función del tipo de información de que se trate, ya sea restringida, confidencial, interna o pública tomando en consideración los tipos de backup y aspectos administrativos mencionados anteriormente.

Archivo de Journal

El journal es el nombre del archivo que normalmente define el DBA con el objeto de grabar parcial o totalmente la actividad de la base de datos. Generalmente se utiliza pra conocer el momento y lugar donde ocurre alguna falla y de esta forma restaurar o recuperar información.

Básicamente el journal de la base de datos cuenta con dos tipos de información: entries en el registro del journal y checkpoints.

Entries en el registro del journal. Contiene los cambios de los datos en la base de datos, crea dos imágenes por cada ocurrencia en la base de datos que haya sido agregada, borrada o modificada, una imágen antes de la actualización y otra después de la actualización.

Checkpoints. Describen el estatus de programas accesando la base de datos, ya que marcan el principio, final o una terminación anormal durante la ejecución de un programa. Se usan para controlar el proceso de recuperación en el caso de una falla del programa, sistema o hardware.

Debido a que el journal consume muchos recursos se debe determinar que información es más sensitiva y relevante para la organización, o aquella que es imprescindible pra la generación de otros procesos importantes a fin de generar registros en el journal de las modificaciones a este tipo de información

y solo cuando dicha actualización es on-line; para el caso de procesos batch no se justifica el tener un archivo de journal ya que si surge la necesidad de recuperar la base de datos sólo se tendrán que reprocesar los procedimientos.

Proceso de recuperación

En el caso de presentarse una de las fallas antes mencionadas básicamente se deberá:

1. Restaurar la base de datos con el backup más reciente

2. Actualizar la copia del backup utilizando los archivos del journal en el caso de actualización on-line

3. Actualizar la copia del backup reprocesando los procesos cuando la actualización se realiza via batch

La recuperación se hará automáticamente o manualmente dependiendo del modo de acceso a la base de datos así como el ambiente de base de datos y utilierías que se tengan.

Respecto a los backups se deberán considerar las políticas y procedimientos de estos como mencioné anteriormente.

La protección se puede realizar a través de facilidades que proporcione un sistema manejador de base de datos o por software desarrollado dentro de la misma organización.

CARACTERISTICAS GENERALES DE UN SOFTWARE DE SEGURIDAD

Además del software de seguridad diseñado, desarrollado e implementado por la propia organización, existen actualmente en el mercado una serie de productos de software de seguridad diseñados para acoplarse a las necesidades de seguridad de un centro de cómputo, sirviendo como herramienta básica para una eficiente administración de la seguridad en conjunción con la implantación y seguimiento de una serie de políticas y procedimientos a fin de garantizar el buen control lógico a los recursos informáticos.

Independientemente de la diversidad de productos de este tipo que ofrecen algunos proveedores, todos ellos tienen características en común que los convierten en sistemas de seguridad.

Para equipos mainframe los sistemas de control de acceso lógico más conocidos son RACF, TOP SECRET y ACF2, los cuales comparten características muy similares siendo su funcionamiento casi igual. Para efectos de esta tesis mencionaré las características generales del software de control de accesos lógico RACF (RESOURCE ACCESS CONTROL FACILITY) que es un sistema de seguridad desarrollado por IBM en la década de los 70's para correr en ambientes MVS o VM y que actualmente funciona en empresas como Grupo Nacional Provincial, IBM, Bancomer, Pedro Domeq, Nissan y Mexicana de aviación.

En general las características que posee son las siguientes:

- Controla el acceso al sistema a través de USER IDs en combinación de passwords
- Controla el acceso a recursos protegidos
- Permite funciones de loggin y monitoreo
- Tiene una base de datos con todas las definiciones de los recursos
- Permite el uso de EXITS

Control de acceso a través de user ids y passwords

La entrada al sistema puede ser a través de subsistemas on-line como TSO o CICS o a través de un ambiente batch al enviar un job ya sea remoto o local.

Remoto. En este modo de conexión una terminal se conecta a un nodo sobre la red.

Local. Es el modo de conexión desde una terminal conectada directamente al procesador central o desde un servidor también conectado al procesador central.

Este software provee controles sobre la entrada inicial al sistema a través de la identificación y verificación de usuarios que intentan accesar el sistema. Dichos controles se desarrollan a través del uso de user ids y passwords que se almacenan en perfiles de usuario en la base de datos de seguridad.

También pueden determinar si un usuario que intenta accesar el sistema está autorizado a:

1. Accesarlo en determinado día
2. Firmarse on-line o batch
3. Firmarse desde una terminal específica
4. Accesar un aplicación específica
5. Accesar un recurso específico

Control de acceso a recursos protegidos

Una vez que el sistema de control de acceso lógico identifica y verifica la entrada de un usuario al sistema puede controlar la habilidad de los usuarios a accesar archivos y recursos generales como discos, cintas, terminales, programas y CICS.

RACF determina el acceso a archivos utiilizando la información contenida en registros llamados perfiles de archivos almacenados en la base de datos de seguridad. El control de acceso a los recursos generales se realiza a través del uso de la información contenida en otros registros llamados perfiles de recursos generales, igualmente almacenados en la base de datos de seguridad. Tanto los perfiles de archivos como los perfiles de recursos generales contienen una lista de los usuarios o grupos de usuarios autorizados a utilizar el recurso. Cuando un usuario solicita accesar un recurso el sistema de control de acceso lógico compara la información del usuario con la información del perfil de archivo o del recurso general, verificando si el nivel de autoridad solicitado por el usuario es igual o menor al especificado en el perfil del archivo o del recurso general.

Al controlar el acceso a archivos y recursos generales, se puede hacer uso de un acceso universal y un indicador de warning.

El acceso universal especifica por default el tipo de acceso que tendrá cualquier usuario o grupo de usuarios al accesar el recurso, independientemente de los atributos que tenga y que no esté definido en la lista de acceso. Este acceso puede afectar significativamente la seguridad de acceso asociada con un archivo o recurso general específico. En el caso de información confidencial se debe tener un acceso universal de none (es decir que nadie lo puede accesar) y una lista de acceso sólo con aquellos usuarios que deban accesar el recurso.

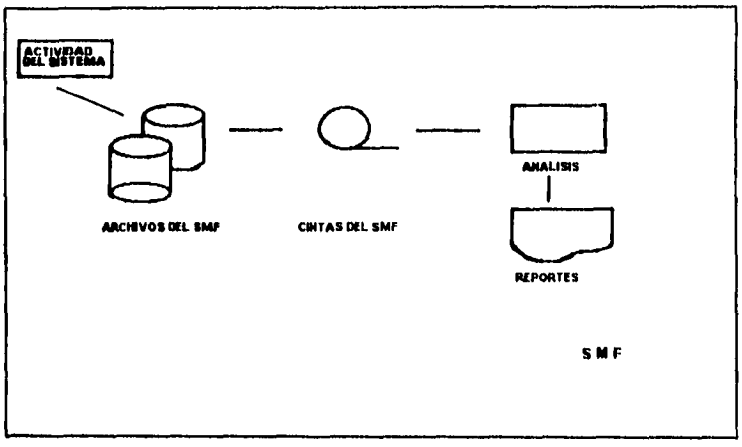
En el caso de activar el indicador de warning sobre un perfil de archivo o de recurso general, cualquier usuario puede accesar ese recurso, es decir que no se limita su acceso y solo se emite un mensaje de warning donde indica que el acceso permitido es temporal. Esta facilidad es recomendable usarla cuando se acaba de implementar el software de seguridad y aún no se establece con claridad quién y cómo accesará determinados recursos.

Por otro lado también provee la facilidad de brincarse (bypass) el proceso de chequeo de autorización para archivos y recursos generales que son accesados frecuentemente permitiendo un procesamiento más eficiente. Esta facilidad puede implementarse para algún usuario de procesos productivos y de esta forma evitar operaciones de I/O a la base de datos de seguridad que pueden ser muy significativas.

Logging y monitoreo

El logging es una facilidad que permite grabar en disco la actividad del sistema el cual sirve de base para monitorear dicha actividad y detectar posibles desviaciones o problemas.

Además permite a la organización especificar si solo determinados eventos o toda la actividad del sistema se grabará. Dicha actividad se graba en los registros del SMF (SYSTEM MANAGEMENT FACILITY) en ambientes con sistema operativo MVS o en los registros del CMS (CONVERSATIONAL MONITOR SYSTEM) para ambientes VM.



A través de la utilización de estos registros se pueden obtener reportes con información acerca de:

-Intentos de acceso a un archivo específico por determiandos usuarios, tareas o procedimientos
-Comandos emitidos por un usuario
-Intentos de logon fallido
-Intentos de violaciones de lectura, actualizaciones o borrado a archivos o recursos generales

-Listado de todos los usuarios

-Accesos permitidos a recursos como consecuencia de tener activado el indicador de warning

Base de datos de seguridad

RACF cuenta con dos bases de datos de seguridad, la base de datos primaria que es la que está activa y el backup que reside en otro disco y que se puede actualizar simultáneamente.

Esta base de datos de seguridad contiene toda la información necesaria para que el sistema de seguridad pueda realizar sus funciones. Toda la información se almacena en registros llamados perfiles. Dichos perfiles pueden ser de usuario, de grupo, de archivos, o de recursos generales.

Perfil de usuario. La información acerca de un usuario se encuentra definida en un registro de la base de datos de seguridad llamado perfil de usuario o user id. El cual contiene información propia de un usuario, como grupo al que pertenece, atributos que posee, características del password, o su nombre, entre otros datos.

```
USER=IBMUSER      NAME=                    OWNER=IBMUSER
CREATED=87.266
DEFAULT=GROUP=SYS1      PASSDATE=94.245 PASS-INTERVAL=N/A
ATTRIBUTES=NONE
REVOKE DATE=NONE        RESUME DATE=NONE
LAST-ACCESS=95.031/14:09:33
NO-INSTALLATION-DATA
LOGON ALLOWED    (DAYS)         (TIME)
-------------------------------------------------------------------------
ANYDAY                   ANYTIME
GROUP SYS1          USER CONNECTION NOT INDICATED
        GROUP=SYS1       AUTH=NONE       CONNECT-OWNER=IBMUSER
CONNECT-DATE=87.266
        CONNECTS= 312            LAST-CONNECT=95.031/14:09:33
        CONNECT ATTRIBUTES=NONE
        REVOKE DATE=NONE         rESUME DATE=NONE
NO TSO INFORMATION
```

EJEMPLO DE PERFIL DE USUARIO EN RACF DE IBM

Perfil de grupo. Este perfil contiene información acerca de un grupo de usuarios definidos en la base de datos de seguridad y que comparten las mismas necesidades de acceso.

Perfil de archivos y recursos generales

Todos los archivos y recursos generales como volúmenes, cintas, terminales, programas y transacciones definidos pueden protegerse a través de la definición en la base de datos de seguridad de perfiles discretos o genéricos.

Los perfiles discretos son máscaras que protegen únicamente un archivo o recurso genérico. Por ejemplo el perfil discreto del archivo NOMINA.SRCE sería NOMINA.SRCE, es decir que el nombre del perfil es el mismo que el del archivo. Estos perfiles se utilizan para la protección singular de algún recurso muy sensible e importante. Por otro lado los perfiles genéricos son máscaras generales que protegen más de un archivo o recurso genérico. Por ejemplo si se tienen los archivos NOMINA.ACTUAL y NOMINA.BACKUP el perfil genérico que los protegería sería NOMINA.*. Este tipo de perfil se debe usar para controlar el acceso a grupos de archivos o recursos generales que tienen requerimientos de acceso similares. Además para proteger archivos o recursos con perfiles genéricos se debe tener una nomenclatura similar, por otro lado se reduce el número de registros en la base de datos de seguridad al definir perfiles genéricos en lugar de discretos. Por lo que de igual forma se reduce el número de perfiles que deben ser administrados.

El tipo de información que contienen tanto los perfiles discretos como los genéricos incluyen entre otra información:

Lista de acceso. Que contiene los user ids y grupos que pueden o no tener acceso al recurso que protege.

Autoridad de acceso. Que define la capacidad de acceso que tendrá un usuario al accesar el recurso. Este nivel de acceso se debe especificar por cada usuario o grupo y puede ser uno de los siguientes:

Alter. Proporciona al usuario o grupo de usuarios un control total sobre archivos, lo que incluye la habilidad para modificar, borrar y renombrar el archivo. Para el caso de recursos generales este acceso permite igualmente un control total, pudiendo crear o destruir etiquetas de volúmenes por ejemplo; además de modificar cualquier perfil de los recursos generales que incluye las listas y tipos de acceso.

Update. Para el caso de archivos solo se pueden leer y/o sobreescribir. En el caso de recursos generales permite escibir en discos, aunque es igual que un READ para accesar cualquier otro recurso general.

Read. Solo permite al usuario o grupo de usuarios abrir un archivo para su lectura. En el caso de recursos generales solo se pueden leer.

Execute. Solo se aplica a los recursos generales y no a los archivos. Permite ejecutar un programa pero sin leerlo o copiarlo.

None. No permite que un usuario o grupo de usuarios accese un archivo o recurso general.

INFORMATION FOR DATASET PCAB.EAPE*(G)

LEVEL	OWNER	UACC	WARNING	ERASE
00	BASEDATO	NONE	NO	NO

NOTIFY

TT1JAI

YOUR ACCESS	CREATION GROUP
ALTER	ADMONREC

NO INSTALLATION DATA

CREATION DATE	LAST REFERENCE
165 91	NOT APPLICABLE FOR GENERIC PROFILE

ID	ACCESS
NOMINA	UPDATE
SOPROD	READ
TO2LES	READ
TA3RRS	ALTER

DATA SETS AFFECTED BY PROFILE CHANGE

PCAB.EAPE0101

PCAB.EAPE0201

PCAB.EAPE0301

PCAB.EAPE0401

PCAB.EAPE0501

PCAB.EAPE0601

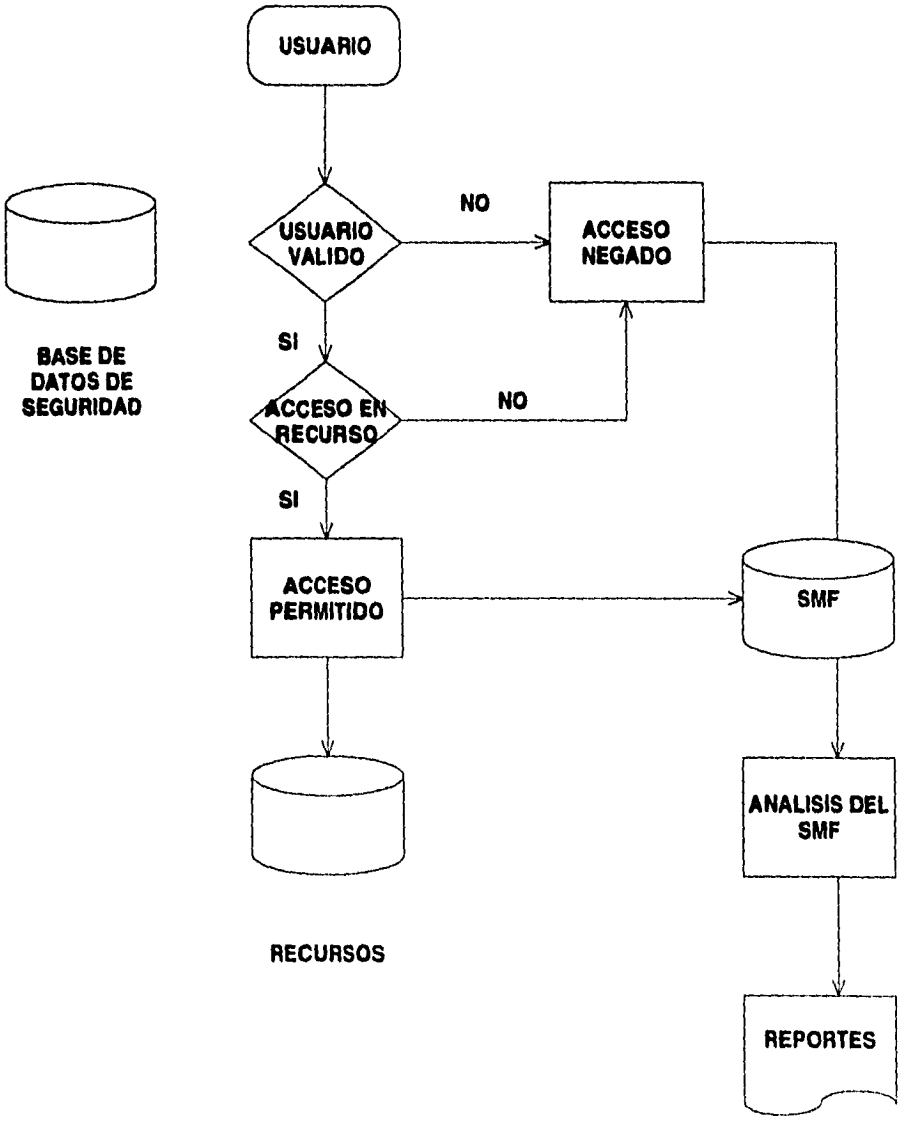
EJEMPLO DE PERFIL GENERICO DE ARCHIVO EN RACF DE IBM

Uso de exits

Una exit es un punto donde el programa normal deja de ejecutarse para procesarse un "código propio" especificado por la instalación a fin de proveer chequeos de seguridad adicionales o brincárselos. Mediante el uso adecuado de exits el software de seguridad puede acoplarse de la mejor manera a las características y necesidades de control de acceso lógico a los recursos informáticos de la organización.

Recordemos que cada sistema operativo cuenta con su propio sistema de seguridad, sin embargo no cuenta con las facilidades que provee un software diseñado exclusivamente para satisfacer las necesidades y requerimientos de seguridad de alguna instalación de procesamiento de datos. El adquirir o no una herramienta de este tipo dependerá del tamaño, importancia y necesidades del centro de procesamiento, aunque hablando de ambientes mainframe sería una falta el pensar no necesitarla ya que generalmente esos ambientes de procesamiento manejan grandes e importantes cantidades de información en donde se involucran muchos recursos.

FUNCIONAMIENTO GENERAL DE RACF

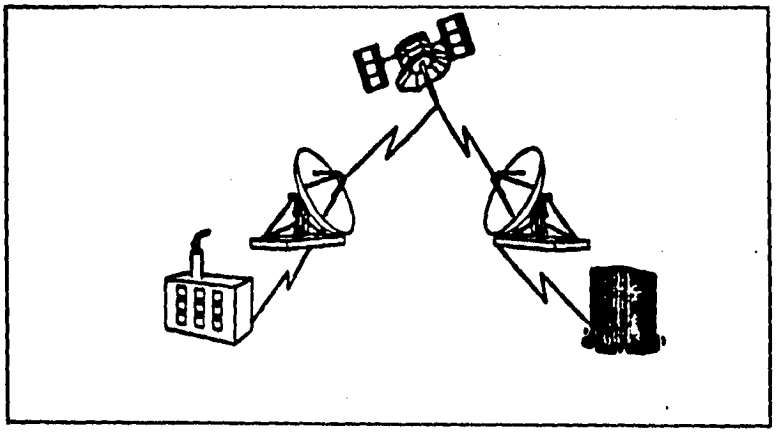


SMF Storage Management Facility

SEGURIDAD EN COMUNICACIONES

Como es sabido las computadoras almacenan y procesan datos, sin embargo actualmente también comparten esos datos y procesos con otras computadoras, lo que implica una actividad más interrelacionada con el almacenamiento y procesamiento de datos, ésta actividad se refiere a las telecomunicaciones.

Por telecomunicaciones podemos entender "la transmisión electrónica de cualquier clase de información por radio, cable, fibra óptica, microondas, láser, o cualquier otro sistema electromagnético"



De hecho, actualmente el 90 % de todas las instalaciones de procesamiento de datos utilizan alguna forma de procesamiento basada en redes de telecomunicaciones, las cuales pueden ser usadas para controlar el acceso a las facilidades de la computadora, aunque también incrementan el riesgo, por lo que se deben adoptar ciertas medidas de

seguridad física en líneas y equipo así como llevar un control de acceso lógico a fin de preservar la confidencialidad de los datos que pasan a través de canales de comunicación, es decir que se debe asegurar que el mensaje es inalterado durante su transmisión o en caso de ser así debe ser inmediatamente detectada dicha alteración. Sin embargo es bueno tener en mente el buscar un balance entre la función del negocio y el esfuerzo de seguridad con cierto riesgo aceptado de acuerdo a costos y beneficios.

Transmisión en datos

En sistemas computacionales los datos se representan como cadenas de dígitos binarios (ceros y unos). Dichas cadenas se transmiten entre dispositivos computacionales a través de señales que representan esos ceros y unos. Tradicionalmente la liga entre estos dispositivos es entre el procesador central y las terminales remotas, en estos casos el método de transmisión de datos depende del medio y el modo de transmisión. Como sabemos los medios de transmisión pueden ser entre otros el par trenzado, el cable coaxial y la fibra óptica. Haciendo referencia al modo de transmisión este puede ser simplex, half duplex o full duplex. Sin embargo las definiciones y características de estos medios y modos de transmisión no se definirán en este tema, ya que es un tópico meramente de comunicaciones y no de seguridad.

Interceptores de telecomunicaciones

Por interceptores de telecomunicaciones entendemos aquellos sujetos que accidental o deliberadamente se conectan a las líneas de comunicación interceptando los datos que viajan por estas con un fin bien definido o como mero hobby.

Dentro de los interceptores humanos de comunicaciones, básicamente podemos distinguir dos tipos:

- Los intrusos pasivos y
- Los intrusos activos

Intrusos pasivos. Son aquellos individuos que interceptan datos en una línea de comunicación por simple curiosidad o por analizar el tráfico de datos como hobby, sin ni siquiera tratar de modificar o borrar algún mensaje.

Intrusos activos. Estos individuos realizan algunas actividades a fin de interferir de una u otra forma los datos que se están transmitiendo. Estas actividades pueden:

- Modificar deliberadamente el contenido del mensaje
- Rerutear el mensaje de forma que llegue a un lugar distinto
- Enviar mensajes falsos
- Borrar mensajes de forma que nunca lleguen a su destino
- Interrumpir la línea entre dos comunicaciones y conducir dos conversaciones, una con cada parte, mientras convence a cada uno que están hablando entre ellos, (esto se conoce con el término piggy-in-the-middle).

Además de los ataques que pueden existir por parte de intrusos pasivos y activos, pueden darse accidentalmente, causando la pérdida de mensajes, duplicación de mensajes, reruteado de mensajes así como su alteración. Para evitar lo anterior es necesario contar con medidas de protección física y lógica sobre los componentes de una red de telecomunicaciones.

Componentes de una red de telecomunicaciones

Terminales. Como mencioné anteriormente las terminales son el enlace tradicional con el HOST o procesador central. De forma que son dispositivos de entrada y salida en una red de teleproceso. En cuanto a la seguridad en terminales sería prácticamente imposible y además demasiado costoso implementar medidas de seguridad física para

cada una de ellas, por lo que es mucho más conveniente usar un software que prevenga el acceso y uso de terminales dentro y fuera de la intalación, a través de la identificación de terminales por medio de passwords y especificación de horarios para su uso.

Modems. El modem es un dispositivo que permite convertir las señales digitales que envía una computadora en señales analógicas. En el lado de transmisión los pulsos provenientes de la computadoras son convertidos a tonos y transmitidos por el canal telefónico, en el lado de recepción los tonos se reconvierten a pulsos y se transmiten a la computadora. Físicamente es imposible proteger los modems ya que cualquier persona puede adquirir alguno y conectarse desde su casa, sin embargo se les pueden adaptar dispositivos para criptografiar la información a fin de conservar la integridad de la información que permiten transmitir.

Multiplexores y concentradores. Un multiplexor es un dispositivo que conecta varios dispositivos de comunicaciones a un mismo canal de comunicaciones. Típicamente liga varias líneas de baja velocidad a un línea de gran velocidad.

El concentrador hace exactamente lo mismo que un multiplexor a diferencia que puede ser programado para manejar dispositivos que transmiten a diferentes velocidades por lo que es mas flexible.

Los multiplexores y concentradores se encuentran físicamente dentro del centro de cómputo, por lo que cuentan con las características de seguridad física mencionadas anteriormente.

Líneas de comunicación. Los sistemas computacionales se pueden ligar a otros sistemas a través de líneas privadas, públicas, nacionales e internacionales.

En el caso de cableado se debe tener un diagrama de la red que se evaluará y actualizará periódicamente, así mismo se debe procurar no etiquetar los cables que identifiquen si transmiten voz o datos. Una forma de protección física más sofisticada consiste en colocar los cables en un estuche presurizado de forma que si alguien intenta meterse causan una fuga o salida de presión, lo que puede accionar una alarma visual y/o auditiva, sin embargo éste último esquema no se justifica para instalaciones comerciales. Actualmente es empleado en el servicio de inteligencia de Estados Unidos así como en cuestiones militares o secretas de Estados Unidos y países europeos.

Controladores. Son dispositivos que conectan todas las líneas de comunicación al computador central. Igualmente se encuentran dentro del centro de cómputo, por lo que cuenta con las características de seguridad física de un centro de cómputo.

CPU. Lleva a cabo la mayor parte de las tareas de procesamiento de la computadora, contando con las medidas de seguridad físicas del centro de cómputo.

Dispositivos de teleproceso. Sólo identifican las terminales no verifican

Además de las medidas de seguridad físicas para estos componentes es importante mantener procedimientos de instalación. Igualmente se pueden equipar estos dispositivos con "DISPOSITIVOS DE AUTO-IDENTIFICACION" que son circuitos que transmiten un código de identificación que puede identificar el tipo de dispositivo o únicamente una unidad individual, en otras palabras identifica el dispositivo pero no quién lo usa. Además de éste tipo de seguridad técnica, opcionalmente se utilizan métodos de protección criptográficos cuyo objetivo es preservar la integridad de la información transmitida entre computadoras locales y remotas.

CRIPTOGRAFIA

Una de las técnicas más poderosas para implementar seguridad en la transmisión de datos es la encriptación, entendiéndose por ésta el desarrollo de transformaciones matemáticas complejas que hacen inteligible cualquier dato. Esta transformación se puede hacer a través de algoritmos y del uso de llaves secretas que son necesarias para criptografiar y descifrar el contenido de la información.

El estudio y desarrollo de la criptología surgió después de la invención del telégrafo, así como durante la Primera y Segunda Guerras Mundiales con la finalidad de proteger la transmisión de datos o su almacenamiento.

Dentro de las clases de criptografía más comunes podemos mencionar dos: la transposición y la substitución.

El método de transposición se caracteriza por cambiar el orden original del mensaje de entrada. Un ejemplo muy común de éste método es el escribir un mensaje al revés, por ejemplo la palabra "requerimiento" resultaría como "otneimireuqer". Una variante de éste método es llamado "RAIL FENCE", en este método el mensaje 4pm london av quedaria como la siguiente secuencia:

4 m o d n v
p l n o a

posteriormente se toman bloques de cinco caracteres quedando finalmente como:

4MODN VPLNO A

En el método de substitución los elementos del mensaje de entrada conservan su posición relativa siendo reemplazados por letras o símbolos. Uno de los métodos de

substitución más conocidos es el sistema "César", el cual reemplaza cada letra del alfabeto por la tercera letra siguiente en la secuencia del alfabeto. El alfabeto correspondiente sería:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

En este método el mensaje de entrada HOLA quedaría como KROD.

De igual manera el método César tiene algunas variantes. una variación de dicho método es la utilización de un alfabeto cifrado al revés de la secuencia original del alfabeto.

Otra variación adicional a este método es la utilización de una palabra llave al inicio de la secuencia del alfabeto cifrado seguida de la secuencia del orden alfabético sin repetir letras que se encuentren en la palabra llave.

Obviamente este tipo de técnicas tradicionales de criptografía fueron desarrolladas muchísimo tiempo atrás al advenimiento de las computadoras por lo que no son particularmente apropiadas a éstas. Por otro lado las cantidades de información que se manejan han variado considerablemente. Actualmente la utilización de criptografía computacional se basa en operaciones aritméticas y/o lógicas.

ALGORITMO DE ENCRIPTACION-DES

Uno de los algoritmos disponibles más importantes es el DES (Data Encryption Standard) desarrollado por IBM en la década de los 70's y aprobado como un estandar federal en Estados Unidos. Este algoritmo es simétrico, lo que significa que usa la misma llave

secreta para encriptar y descifrar los datos. El proceso de este algoritmo es lento y caro y sólo puede ser realizado por procesadores con microchips. Del mismo modo las transmisiones deben criptografiarse a través de equipos cuyo hardware esté destinado a ésto.

CODIGO DE AUTENTICIDAD

Muchas computadoras de servicios financieros están involucradas con la transferencia de dinero, en las cuales el mensaje de instrucción de pago se transmite de una computadora a otra y no necesariamente dentro de la misma organización. En este punto es importante la seguridad en las transacciones de tal forma que no puedan ser alteradas sin que dicha alteración sea detectada. Para esto se pueden tomar medidas que aseguren que tales cambios se detectan en ese momento automáticamente.

Esto se hace a través de la generación con el mensaje fuente de un campo de datos especial (una etiqueta) llamada MAC (código de autenticidad del mensaje). Este código se produce por el procesamiento del mensaje entero a través de un algoritmo DES; cada bloque de 64 bits del mensaje se procesa usando una llave secreta. Nadie que altere el mensaje podrá alterar este MAC a menos que posea la llave secreta. Cuando el mensaje se recibe del otro lado, el MAC que fue generado en el emisor se recibe con él. La máquina receptora desarrolla el mismo proceso de generación de MAC en el mensaje completo, y compara su resultado con el MAC recibido. Se observa un match satisfactorio como una verificación de que el mensaje no ha sido camblado. Naturalmente la protección de la llave secreta es primordial.

MENSAJE FUENTE + DES + LLAVE SECRETA = MAC

PLAN DE RECUPERACION DE SERVICIOS EN CASO DE DESASTRE (DRP O BRP)

Actualmente existen muchas organizaciones que cada día son más dependientes del procesamiento electrónico de datos, en estos casos la reducción o pérdida parcial o total de las facilidades de procesamiento de datos puede resultar en consecuencias financieras, de mercado o legales para la organización. Para minimizar estos riesgos se realizan esfuerzos enfocados al establecimiento de controles y medidas de seguridad, sin embargo el riesgo no se puede eliminar por completo por lo que es de suma importancia desarrollar e implementar un plan de recuperación que permita el restablecimiento de las operaciones de procesamiento de datos.

Este plan de recuperación tiene como objetivo responder a problemas críticos o catastróficos de forma que permitan una pronta recuperación de la operación normal del centro de cómputo. También es conocido como DRP (DISASTER AND RECOVERY PLAN), y actualmente en Estados Unidos como BRP (BUSSINESS RECOVERY PLAN).

DESARROLLO DE UN PLAN DE RECUPERACION

El plan de recuperación dependerá de la naturaleza de la organización e inevitablemente incurrirá en un costo muy alto. Es importante tener en mente que la importancia del DRP no dependerá de la probabilidad de ocurrencia de un desastre, sino del efecto de tal desastre sin importar que tan remota sea su probabilidad. Igualmente se deberá considerar que la pérdida parcial o total de las facilidades de procesamiento puede causar entre otros:

- Pérdida de ventas
- Pérdida de ingresos
- Reducción en la capacidad de operación

- Implicaciones legales
- Incremento en el costo de operación
- Pérdida de introducción en el mercado
- Mala imagen

Dicho lo anterior el plan de recuperación debe cubrir la restauración de sistemas prioritarios o la totalidad de las operaciones de procesamiento, para lo cual durante el desarrollo e implementación del plan de recuperación se deberán seguir las siguientes etapas:

- Identificar las aplicaciones críticas o sistemas prioritarios

- Establecer responsables del DRP

- Establecer procedimientos de restauración

- Identificar sitios alternos de operación

- Establecer planes de backups

Identificación de aplicaciones críticas

A nivel dirección se deberá realizar un análisis de las aplicaciones que son cruciales para la operación continua de la organización, tomando en cuenta el costo y tiempo que implicaría el no restablecer las operaciones de procesamiento así como su importancia.

Así mismo la dirección deberá tomar en cuenta el nivel de impacto sobre las aplicaciones cruciales, es decir el tiempo que se requiera para restablecer la operación normal y cubrir los daños.

La escala de tiempo de tales implicaciones puede expresarse en tres niveles de impacto, según el tiempo que se requiera para restablecer la operación normal y cubrir los daños.

Impacto limitado. El restablecimiento de la operación normal se puede efectuar durante un día de trabajo.

Impacto Severo. El restablecimiento de la operación normal se puede efectuar durante una semana de trabajo.

Impacto Mayor. El restablecimiento de la operación normal puede tomar más de una semana de trabajo y requiere esfuerzos y recursos considerables.

Responsables

Se deberán establecer él o los responsables del plan de recuperación así como todas aquellas personas que se involucren durante la ejecución del plan. Dependiendo de la complejidad y tamaño del centro de procesamiento de datos se establecerá la responsabilidad de cada integrante paso a paso, y se considerará el tener un backup por cada integrante. Es importante que cada integrante cuente con una copia del plan de recuperación, además estas copias deberán guardarse en bóvedas de seguridad y asegurar su disponibilidad en caso de ser necesario.

Procedimientos de restauración

Se deberá especificar paso a paso los comandos de operación y los mensajes que se visualizarán a fin de levantar las aplicaciones prioritarias, comenzando con sistema operativo, y posteriormente con susbsistemas como JES2, TSO y VTAM. Igualmente se definirá el número máximo de usuarios que accesara sólo determinadas aplicaciones

mientras se restaura y normaliza el ambiente de procesamiento.

Durante los procedimientos de recuperación no debe levantarse el susbsistema de seguridad o deben definirse procedimientos que se brinquen los controles de seguridad. Al finalizar los procedimientos de recuperación los controles de seguridad se deberán restablecer así como monitorear toda la actividad que se realizó durante el período de recuperación.

Sitios Alternos de operación

El centro de cómputo cuenta con características muy específicas que no pueden ser remplazadas fácilmente como el CPU o el sistema operativo. Una buena estrategia considerará el contar con lugares alternos donde las operaciones del centro de cómputo puedan continuar. Aquí podemos identificar básicamente cuatro opciones:

- Out Sourcing
- Acuerdos con proveedores
- Acuerdos recíprocos
- Backup de instalaciones

"Out Sourcing". Se refiere a la existencia de empresas que se dedican a la renta de tiempo de CPU, lo que permite procesar datos de distintas organizaciones. Aquí la seguridad depende por completo de las políticas y procedimientos de seguridad propios del out sourcing.

Acuerdos con proveedores. Se puede acordar con los proveedores de hardware y software el que se provea o remplacen las facilidades de procesamiento en un determinado lapso de tiempo, sin embargo puede ocurrir que el proveedor no cumpla con lo establecido o no cuente con la capacidad para procesar la información en ese período de tiempo.

Acuerdos recíprocos. Se pueden realizar acuerdos entre compañías que operan bajo el mismo ambiente de procesamiento de datos como es hardware y software, las cuales aceptan continuar con el procesamiento de las aplicaciones críticas de la otra organización mientras restablece su operación normal. Aquí el acuerdo puede que no sea formal aunque también sin ningún costo.

Backup de instalaciones. Se puede tener un centro de cómputo adicional en otra localidad a fin de ser utilizado en caso de desastre del centro de cómputo base, sin embargo esto implicaría un costo elevadísimo.

Planes de backups

Dependiendo de la naturaleza e importancia de la información se establecerá el tipo de backup así como su periodicidad de realización y conservación además de otras medidas administrativas como mencioné en capítulos anteriores.

Además de preparar el plan de recuperación y considerar los puntos anteriores se debe tener en mente que este plan debe ser actual, entendible, factible, probado y documentado.

Actual. Nada permanece estático dentro de las operaciones de procesamiento del centro de cómputo, por lo que cualquier plan de recuperación debe ser actualizado por la persona que se haya establecido para este fin, con el objeto de mantener al día todas las implicaciones de recuperación de las facilidades de procesamiento.

Entendible. El plan de recuperación 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 recuperación 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 DRP debe formalizarse a través de un plan escrito que deberá estar disponible en cualquier momento.

El esfuerzo que implique la realización de un plan de recuperación 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.

CENTRALIZACION O DESCENTRALIZACION DE LA SEGURIDAD

La centralización de las funciones de seguridad informática permiten tener un control más homogéneo y eficiente. Esta función puede recaer en una sola persona o área dependiente de la dirección de informática o a nivel staff en la dirección general; este criterio de selección dependerá del tamaño y necesidades de seguridad de la organización, en empresas muy pequeñas una sola persona se podrá encargar de las funciones de seguridad a diferencia de empresas de gran tamaño en donde las actividades de administración de seguridad exigen una o más personas de tiempo completo encargadas de esta función. Independientemente del número de personas involucradas en esta labor es necesario separar las funciones de seguridad física de las funciones de seguridad lógica ya que aunque las dos buscan el mismo objetivo conllevan actividades muy distintas, como se puede apreciar al leer los temas de seguridad física y lógica. El tener centralizada las funciones de seguridad física no tiene desventajas, sin embargo en la administración de la seguridad lógica una gran desventaja es que el administrador no es experto en todos y cada uno de los sistemas o aplicaciones que maneja la compañía por lo que no puede precisar con exactitud quién deberá tener acceso a qué y a qué nivel.

Por otro lado cuando la función de seguridad informática se tiene descentralizada esta no es homogénea y hay muchos criterios de administración, lo que provoca en muchos casos un control ineficiente así como duplicidad de labores. Referente a la seguridad físcia no es nada recomendable que este descentralizada, ya que es un todo que protege algo físico pero con una sola visión global, no debe haber un responsable de seguridad física por edificio u oficina por ejemplo, sino de todo el corporativo. En el caso de una administración lógica descentralizada el responsable de cada aplicación siendo un experto sabe quienes deben o no accesar dicha aplicación y a qué nivel, esta persona puede determinar sus políticas de acceso y perfiles de aplicaciones por usuario, es decir que lleva su propia administración aunque se debe basar en las políticas y

procedimientos de seguridad de la empresa.

El decidir implantar una administración de la seguridad centralizada o descentralizada estará en función del tamaño de la organización como mencioné anteriormente y necesidades de seguridad ya que ambas incurrirán en costos para la empresa. La dirección general deberá decidir el tipo de administración de la seguridad que se implementará, igualmente deberá estar de acuerdo y apoyar todas las políticas y procedimientos del área de seguridad. Por otro lado el área de recursos humanos deberá dar a conocer todas las políticas y procedimientos de seguridad al personal de nuevo ingreso y el área de seguridad deberá enviar circulares para su reforzamiento, independientemente del tipo de estructura con que cuente la empresa.

CONCLUSIONES

Conceptualizando todo un esquema de seguridad informática aplicable en un ambiente "mainframe" podemos llegar a las siguientes conclusiones:

- El auge en el procesamiento electrónico de datos aunado a una gran proliferación y diversificación de computadoras conectadas a un host incrementó los riesgos a que está expuesto cualquier centro de procesamiento de datos, que pueden ser internos, externos o naturales, lo que dio origen a una necesidad de seguridad informática que antes no había sido necesaria.

- Cualquier organización que esté involucrada con la automatización de información tiene el riesgo de sufrir desde daños materiales a sus instalaciones o equipo causadas por riesgos naturales hasta el mal uso o daño de su información accidental o deliberadamente, causando grandes pérdidas de dinero, mala imagen, falta de confianza, pérdida de mercado o implicaciones legales.

- La implementación de medidas de seguridad física tienen la finalidad de preservar las instalaciones físicas y equipo de procesamiento de cualquier riesgo externo, interno o natural que pudiera afectar la operación normal del centro de cómputo como pudiera ser el caso de sabotajes, alborotos, inundaciones, terremotos, o incendios.

- La implementación de medidas de seguridad lógica permiten controlar y garantizar la integridad y confiabilidad de la información, previniendo que esta se dañe o altere accidental o deliberadamente.

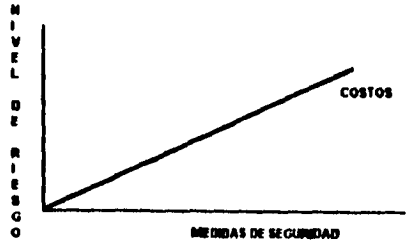
- Generar una estructura de seguridad informática a través de medidas establecidas para controlar y permitir o negar el acceso a recursos utilizados en el procesamiento electrónico de datos debe ser una prioridad para cualquier ambiente de procesamiento electrónico de datos. Sin embargo antes de decidir la implantación de cualquier tipo de seguridad se deberá hacer un análisis del costo-beneficio que esto implicaría tomando en cuenta la magnitud del centro de procesamiento de datos, los riesgos a que está expuesto y sus requerimientos de seguridad.

RIESGO	MEDIDAS DE SEGURIDAD
INCENDIO	PROCEDIMIENTOS DE SEGURIDAD CONTRA INCENDIO PROCEDIMIENTOS DE SEGURIDAD CONTRA INUNDACION BACKUPS BRP
TERREMOTO	PROCEDIMIENTOS DE SEGURIDAD CONTRA INCENDIO PROCEDIMIENTOS DE SEGURIDAD CONTRA INUNDACION BAKUPS BRP
INUNDACION	PROCEDIMIENTOS DE SEGURIDAD CONTRA INUNDACION BACKUPS BRP
OAÑO EN DISPDSITIVOS OE ALMACENAMIENTO	CONTROL OE ACCESO A LAS INSTALACIONES EQUIPO ALTERNO BACKUPS
DAÑO A LA INFORMACION	CONTROL DE ACCESO LOGICO SEGURIDAD EN BASE DE DATOS BACKUPS
ERROR HUMANO	DOCUMENTACION DE PROCEOIMIENTOS CAPACITACION BACKUPS
FRAUDE	CONTROL DE ACCESO A LAS INSTALACIONES CONTRDL DE ACCESO LOGICO SEGURIDAD EN COMUNICACIONES
SABOTAJE	CONTROL DE ACCESO A LAS INSTALACIONES CONTROL DE ACCESO LOGICO SEGURIDAD EN COMUNICACIONES
ESPIONAJE	CONTROL DE ACCESO A LAS INSTALACIONES CONTROL OE ACCESO LOGICO SEGURIDAD EN COMUNICACIONES
SOBORNO	CONTROL DE ACCESO LOGICO SEGURIOAD EN COMUNICACIONES

- Igualmente se deberá evaluar la factibilidad de implementar un software de seguridad que se acople al equipo y necesidades de seguridad. Actualmente dentro de los más conocidos en ambientes mainframe destacan RACF, TOP SECRET y ACF2 que funcionan bajo distintos sistemas operativos.

- Se debe contar con un plan de recuperación de servicios en caso de desastre con el fin de minimizar los riesgos a que está expuesto cualquier centro de procesamiento de datos, sin importar que tan remota sea la probabilidad de desastre; y de esta forma garantizar la operación continua y minimizar las posibles pérdidas que se pudieran tener.

- El marco de seguridad informática debe acompañarse de una serie de políticas y procedimientos encaminados a reforzar los sistemas de seguridad ya que por si solos no pueden cumplir eficientemente su objetivo.



A medida que el nivel de riesgo en un centro de cómputo se incrementa se deben implementar mayor número de medidas de seguridad que igualmente se reflejarán en mayores costos para la compañía.

GLOSARIO

ACCESO	Características o atributos para obtener el uso de un recurso protegido
AUTORIDAD	Derecho a accesar recursos informáticos protegidos
CICS	(Customer Information Control Systme) Monitor de transacciones interactivo
GRUPO	Conjunto de usuarios o aplicaciones con las mismas necesidades de acceso
JES2	(Job Entry Subsystem) Controla la entrada, salida y provee los recursos necesarios para el proceso de programas
JOURNAL	Archivo donde se graban los eventos del sistema de base de datos
LOG	Registro de eventos del sistema
LOGIN	Acciones que realiza un usuario para proveer su identificación cuando accesa el sistema
MVS	(Multiple Virtual Storage) Sistema operativo de IBM para correr en plataformas de equipo mainframe
PASSWORD	Cadena de caracteres que el usuario provee al momento de firmarsse para validar su identificación
PERFIL	Conjunto de elementos que describen los requerimientos de acceso a un recurso o los derechos de acceso de los usuarios
PROTECCION	Atributos de un objeto que limitan el tipo de acceso disponible a usuarios
SMF	(Storage Management Facility) Log del MVS
TSO	(Time Sharing Option) Subsistema manejador de transacciones en linea
VTAM	(Virtual Telecomunication Access Method) Software que permite el acceso entre usuarios y aplicaciones residentes en un CPU

BIBLIOGRAFIA

A handbook of computer security
keith Hearnden
Kogan Page, London, 1987

Audit, Control, and Security of RACF
International Business Machines (IBM)
ERNST & YOUNG, USA, 1992

Commonsence Computer Security: your practical guide to preventing accidental and deliberate electronic data loss
Martin R. Smith
Mc Graw-Hill, England (UK), 1989

Computer Security Handbook
Richard H. Baker
Mc Graw-Hill, USA, 1991, 2nd. Edition

Computer Security Management
Van Tassel, Dennis
Prentice Hall, USA, 1972

Computer User's Dictionary
Bryan Pfaffenberger, Ph.D.
Que Coorporation, Indiana, 1990.

EDP Auditing Conceptual Foundations and Practice
Ron Weber
Mc Graw-Hill, Singapore, 1985, 2nd Edition

Enciclopedia Universal Ilustrada Europeo Americana
Espasa-Calpe S.A., Madrid, 1927, Tomo LIV

Diccionario de Procesamiento de Datos
Jeff Maynard
Diana, México, 1978

Diccionario Mc Graw-Hill de Compuración
Sybil P. Parker
Mc Graw-Hill, México, 1989, Tomo II

Handbook of EDP Auditing
Michael A. Murphy
Xenia Ley Parker
Coopers & Librand, USA, 1989, 2nd. Edition

IDMS/R
Concepts and Facilities
Release 10.0
Cullinet Software, USA, 1986

International Technical Support Centers
CICS/MVS Security Guidelines using RACF
IBM, California, 1989.

Open VMS Guide to System Security
Digital Equipment Corporation
Digital, Massachusetts, 1994

Pequeño Larousse de Ciencias y Técnicas
Tomás de Galiana Mingot
Larousse, México, 1979

Audit, Control and Security of RACF
ERNST & YOUNG, USA, 1992.

Security, Accuracy and Privacy in Computer Systems
James Martin
Prentice-Hall, INC., Englewood Cliffs, New Jersey, 1973

Webster's World Dictionary of Computer Terms
Laura Darcy and Louise Boston
Prentice Hall Press, New York, 1988, 3ra. Edición