UNIVERSIDAD NACIÒNAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

IMPLANTACION DE UN ESQUEMA DE SEGURIDAD Y CONFIDENCIALIDAD EN SISTEMAS DE PROCESAMIENTO Y TRANSMISION DE DATOS EN EL SECTOR FINANCIERO.

TESIS PROFESIONAL

Que para obtener el Titulo de
INGENIERO EN COMPUTACION
p r e s e n t a n

ZELLA MERCEDES BONILLA MARTINEZ
CLAUDIA ANDREA CORTE FRANCO

Director de Tesis: Ing. Alejandro Ramos Larios

México, D.F. 1989

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

TABLA

DE

CONTENIDO

INDICE

DE

FIGURAS

INTRODUCCION

En nuestros días los sistemas de cómputo juegan un papel primordial en la mayoría de las organizaciones existentes; muchas de estas no podrían realizar sus funciones si no contaran con ellos. La importancia se vuelve aún mayor en las instituciones del sector financiero pues operan casi totalmente a través de sistemas automatizados. Por este motivo se hace de vital importancia la seguridad que se les debe brindar. Cualquier falla en el sistema, pérdida de información o falta de seguridad tendría consecuencias terribles para la institución: dejar de operar por un tiempo, confundir los estados de cuenta de los clientes, perder imagen, ser objeto de grandes desfalcos e incluso podría provocar la ruina.

Teniendo en cuenta estos peligros, este tipo de organizaciones y todas en general deben tener medidas de seguridad que los protegan en contra de ellos.

Este trabajo pretende contemplar los puntos más importantes que se deben considerar para tener segura la información, es decir que es lo que hay que proteger y cómo se debe proteger.

Y finalmente aplicar esto a un caso real. Se trata de la implantación del sistema de seguridad para una red de cajeros automáticos que desea instalar la Casa de Bolsa PROBURSA S.A. de C.V. para dar mejor servicio a sus clientes. El proyecto de cajeros automáticos continúa en su etapa de evaluación.

La seguridad se puede dividir en dos tipos: física y lógica. La seguridad física se refiere a los controles y mecanismos implantados para proteger el equipo de cómputo y los datos en el centro de cómputo, sus alrededores y sus recursos remotos. La seguridad lógica se refiere a la protección de los datos y programas que se encuentran dentro del sistema.

Dentro del concepto de seguridad física se deben contemplar aspectos como ubicación del centro de cómputo, suministro de energía, equipos de detección y extinción de incendios, mecanismos de control de acceso y protección del enlace de comunicaciones.

Hay que ser muy cuidadosos al elegir el sitio donde se instalará el centro de cómputo. Se debe tratar de evitar los sótanos, plantas bajas y edificios muy altos. Debe tratar de elegirse un lugar lo más lejano posible del acceso público.

Se deben evitar las áreas con alto incide de robos o crímenes, cercanas a una planta de explosivos, gasolinerías, petroquímicas, refinerías, centros comerciales, estacionamientos y restaurantes. El centro de cómputo debe ser construido con material no combustible.

En cuanto al respaldo en el suministro de energía existen varias alternativas como son: motores, bancos de baterías y alternadores de emergencia. Cual utilizar, depende de las necesidades y capacidades de cada institución.

Como hemos mencionado anteriormente otro punto importante a tratar es el de detección y extinción de incendios, esto es porque de los desastres naturales, el más peligroso es el fuego. Primero se debe tratar de detectar el incendio de la forma más rápida posible. Para esto existen dos tipos de detectores de humo: el que funciona por el principio de reflexión de luz, y el de principio de cámara de ionización. Una vez que el fuego ha sido detectado existen varias formas de controlarlo: extinguidores de mano, sistemas de inundación de gas, rociadores automáticos, mangueras, etc. Todos estos tienen sus ventajas y desventajas pero el más usado es el sistema de inudación de gas, preferentemente los que utilizan gas halón 1211 y 1301.

El punto al cual se el presta generalmente mayor importancia es al control de acceso. Este se refiere a la protección de todos los recursos y facilidades de la computadora y las comunicaciones, en los cuales el acceso no autorizado provoque una pérdida, modificación o destrucción de los datos, alguna interrupción o falla del sistema para dar servicio a los usuarios. Para esto existen diversos mecanismos que se pueden utilizar. Algunos de ellos son: tarjetas magnéticas, dispositivos biométricos como los basados en huellas digitales, voz, geometría de la mano, firmas y letra, y patrones de retina. Estos puede ser acompañados por otro tipo de dispositivos de seguridad como: dispositivos de contacto magnético, dispositivos fotoeléctricos, sistemas opticos y de luz infraroja, circuito cerrado de televisión, etc.

En el aspecto de comunicaciones hay diferentes áreas que se deben proteger: los dispositivos de comunicación, líneas y sistemas de conmutación, cable telefónico y los sistemas de microondas y comunicación vía satélite. Para esto también hay diversos mecanismos de protección. La elección que se haga de ellos, dependerá de la importancia de la información que se tenga que proteger y de los recursos con los que cuenta la institución.

En seguridad lógica lo más importante son las claves y jerarquías de acceso. Las claves son conjuntos de números, caracteres, palabras o combinaciones a las que se les debe dar entrada en el sistema para tener acceso a éste. Existen diversas técnicas para su creación y asignación dependiendo de los sistemas de cómputo que se utilizan y de las políticas de la institución.

Una vez que se tiene acceso al sistema, el usuario cuenta con autoridades restringidas de acuerdo a su cargo dentro de la institución. Esto es manejado por una matriz de autorización que indica que es lo que puede o no hacer dicho usuario. Cada sistema maneja esto de modo particular.

En toda organización es muy importante tener en cuenta el costo de no poder usar el sistema de cómputo en un determinado momento y todas las consecuencias que esto implica. Para algunas empresas como las del sector financiero, el no contar con el sistema de cómputo significa prácticamente no poder dar servicio a su clientela. Por esto se deben tener muy claras las medidas a tomar cuando esto ocurra para poder dar un servicio normal lo antes posible. Debe existir un plan de recuperación escrito en el cual se tengan todas aquellas situaciones que pueden ser consideradas como un desastre y la manera de recuperarse de ellas. Para cuando el equipo falla se puede contar con las siguientes alternativas:

a.- Un centro de cómputo alterno, ubicado lejos del existente.
b.- Contratar los servicios de alguna compañía que ofrece servicios de procesamiento con cierto cargo a la empresa.
c.- Tener algún arreglo recíproco entre dos organizaciones independientes que proporcionen un respaldo del servicio.

Es un principio de buena seguridad el que, para cualquier recurso de información, exista el suficiente respaldo de manera que, si se perdiera o se borrara éste pudiera ser reconstruido. Esta reconstrucción debe ser capaz de realizarse en cualquier momento de acuerdo a procedimientos preestablecidos. Los procedimentos de recuperación deben ser implantados en todo programa de procesamiento de datos y se deben establecer puntos de reinicio. Esto se hace con el objeto de que si hubiera alguna falla de hardware o software o algún error en los datos o procedimientos de operación no se tuviera que regresar al inicio y volver a procesar todo, el trabajo podría reiniciarse en el punto de reinicio antes de la falla.

También es importante mantener un archivo histórico de todo archivo que vaya a ser procesado, y éste debe contener una imagen de todos los cambios que se le hayan hecho a los registros para que en caso de que ocurra alguna falla, las modificaciones a éste puedan ser reconstruidas.

Hasta aquí nos hemos referido a las medidas de seguridad que se deben tener dentro del centro de cómputo o con respecto a éste, pero debemos tener en cuenta que la información viaja a través de los medios de comunicación y en este momento debe ser protegida también. La mejor manera de llevar a cabo esto es mediante criptografía. La criptografía es el acto de transformar mensajes o textos en formas ininteligibles para todos, excepto para aquellos que conocen su transformación inversa.

Dentro de los algoritmos criptográficos modernos el más probado y aceptado es el DES (Data Encryption Standard), el cual fue aprobado en 1977 por la National Bureau of Standards de los Estados Unidos de Norteamérica como el método oficial para proteger datos no clasificados en las agencias del gobierno federal. La seguridad que provee está en la complegidad del algoritmo, las mezcla minuciosa que se aplica al bloque de datos y el tamaño del espacio de llaves (aproximadamente 7.2×10^{16}). El DES es una transformación producto de sustituciones, transposiciones y operaciones no lineales que son aplicadas iterativamente (16 iteraciones) a bloques de 64 bits para producir bloques cifrados de 64 bits.

La llave es de 56 bits más 8 de paridad. Ya que este es un algoritmo de dominio público, lo que garantiza la seguridad es la confidencialidad de sus llaves. Estas llaves deben ser impredecibles, preferentemente números aleatorios, se deben tener precauciones en su almacenamiento y ser cuidadoso en su distribución.

El tema de seguridad y protección de información es muy amplio y cada día se avanza más en él, es por esto que es imposible abarcarlo por completo. El trabajo pretende ser sólo una primera guía al tema. Pero por esto es de gran importancia y ayuda para quien desea introducirse al tema por primera vez o que desea tener una visión general de lo que es la seguridad y como se puede llevar a cabo. Es el primer peldaño de una larga escalera.

1

LA IMPORTANCIA DE LA INFORMACION Y DE SU PROTECCION EN EL SECTOR FINANCIERO

1.1 CONCEPTOS BASICOS

Generalmente los términos datos e información se usan en forma indistinta, aunque conceptualmente son cosas diferentes. A continuación mostraremos las diferencias que existen entre ellos.

James Martin, por ejemplo, se refiere a los datos como masas de hechos y cifras en bruto que acopia la computadora y, a la información, como el extracto que se ha obtenido de esa masa y es procesado por una persona dada, con un fin dado, o para satisfacer un requerimiento especifico. Dice así que la información es la resultante de la "digestión" de los datos; aunque esto es muy relativo ya que lo que son datos "digeridos" para un organismo, son datos en crudo para otro. **[15]**

Los datos son hechos aislados y en bruto, que situados en un contexto significativo mediante un procesamiento determinado, permiten obtener deducciones relacionadas con la evaluación e identificación de personas, eventos y objetos. La representación por medio de datos substituye a dichas personas, eventos y objetos. Por ejemplo, si se habla de 5 médicos, una deuda de $500,000 o de una casa, se representa por medio de datos respectivamente a las personas, sucesos u objetos.

El procesamiento y reproducción de datos se hace con la finalidad básica de producir información. El resultado del procesamiento de los datos puede tener muchas y diferentes aplicaciones, desde la elaboración de cheques para el pago de sueldos, hasta la presentacion de informes a la gerencia para toma de decisiones.

Las organizaciones reciben cantidades ilimitadas de datos de fuentes tanto internas como externas, que si fueran procesados sin una finalidad informativa especifica, serian excesivos. Para poder obtener la cantidad apropiada de datos se debe tener un sistema adecuado de información y saber claramente para que se necesitan dichos datos.

La información es un acontecimiento, o una serie de acontecimientos, que llevan un mensaje y que, al ser percibida por el receptor mediante alguno de sus sentidos amplia sus conocimientos. Sólo el destinatario puede evaluar la significación y la utilidad de la información, ya que sólo él puede saber para que la necesita y cual es el objeto final de esta.

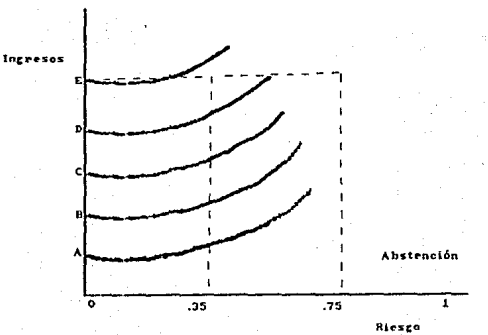
La diferencia principal entre información y datos es que los últimos son mensajes en bruto y no evaluados, mientras que la primera significa un aumento de conocimientos, obtenido por el receptor mediante la coordinación adecuada de los elementos de los datos con las variables de un problema. La información es el procesamiento de los datos, que puede proporcionar un conocimiento o el entendimiento de ciertos factores.

La función primordial de la información consiste en aumentar el conocimiento del usuario, o en reducir su incertidumbre. Se entiende por usuario a toda aquella persona que forma parte de la organización y que para desempeñar su papel dentro de ella necesita de dicha información y por lo tanto hace uso de ella. La información comunicada al usuario puede ser el resultado de la aportación de datos a un modelo de decisión, y de su procesamiento. Pero, tratándose de las decisiones más complejas, no puede hacer más que aumentar la probabilidad de la certidumbre o reducir el número de posibilidades de elección. Por ejemplo, a una persona que toma la decisión de participar o no en una inversión se le enseña la gráfica 1.1.

Esta gráfica indica la probabilidad del factor de riesgo a diferentes niveles de ingresos. La probabilidad de fracasar al nivel de ingresos D puede ser 0.75, lo cual es muy alto y el inversionista optará por abstenerse. Para el proyecto E la probabilidad de fracaso es 0.35, o sea lo suficientemente bajo para que el inversionista acepte el riesgo. Como puede verse aquí, la información hizo que la gama de soluciones se redujera.

Otra de las funciones principales de la información es la de proporcionar un conjunto de estándares, de reglas de evaluación y de reglas de decisión para la determinación y comunicación de advertencias y retroalimentación para fines de control. Esto significa que quien decide intervenir en un proyecto, necesita información que le ayude a controlar dicho proyecto.

Gráfica que indica el grado de riesgo a diferentes niveles de ingreso (Para proyectos)



GRAFICA 1.1

La información puede surgir de la observación personal, de las conversaciones sostenidas con otras personas o de las juntas de comité o de agentes externos como periódicos, informes de gobierno o del propio sistema de información. Un sistema de información es el conjunto de elementos y procedimientos intimamente relacionados que tienen como propósito el manejo de datos a fin de generar información útil para la toma de decisiones, en función de los objetivos y metas organizacionales.

El sistema de información proporciona sólo una parte de la información requerida para la toma de decisiones. El sistema de información provee al usuario, de información con respecto al estado de cosas, comunicándole un grado mayor de predictibilidad tanto en lo que se refiere a los sucesos como por lo relativo al resultado de las actividades relacionadas con la empresa.

Anteriormente mencionamos que los datos son material en bruto que se necesita manejar y situar en un contexto significativo para que pueda ser útil a quien va a recibirlo. Para poner los datos en orden y dar resultados comprensibles, es preciso efectuar alguna combinación de operaciones básicas que son las siguientes:

a.- Captación: se refiere al registro de datos hechos a partir de un evento o acontecimiento.
b.- Verificación: se refiere a la comprobación o validación de los datos, hecha con el fin de asegurarse de que fueron obtenidos y registrados en forma correcta.
c.- Clasificación: esta operación agrupa los elementos de los datos en categorías específicas que tienen un sentido para el usuario.
d.- Ordenación: los elementos de información se colocan en una secuencia específica predeterminada.
e.- Sumarización: combina o engloba los datos de dos maneras; primero, los acumula en sentido matemático y segundo, reduce los datos en el sentido lógico.
f.- Cálculo: vincula las operaciones aritméticas y lógicas de los datos.
g.- Almacenamiento: los datos se guardan en algún dispositivo, donde se pueden tener disponibles y consultarlos cuando sea necesario.
h.- Recuperación: implica buscar y obtener acceso a datos específicos, para tomarlos del dispositivo en que se encuentran almacenados.

i.- Reproducción: esta operación copia los datos de un dispositivo a otro o cambia su ubicación dentro del mismo.
j.- Distribución/Comunicación: mediante esta operación se transfieren los datos de un lugar a otro.

Los avances tecnológicos han producido muchos dispositivos diferentes que pueden usarse para realizar estas operaciones básicas. En la mayoría de las empresa, el sistema de información se compone de varios métodos: tecnológicos y manuales.

Para un manejo más efectivo, se han definido cuatro categorías generales basadas en el nivel de automatización: manuales, electromecánicos, equipo para tarjetas perforadas y computadora electrónica.

La solución del método de procesamiento más adecuado para una aplicación u organización específicas exige que el analista de sistemas conozca a fondo tanto las necesidades de procesamiento como las posibilidades de cada uno de los métodos. Las necesidades de procesamiento están determinadas por lo siguiente:

a.- Volumen de los datos involucrados.
b.- Complejidad de las operaciones.
c.- Limitaciones impuestas al tiempo de procesamiento.
d.- Demandas de cálculo.

La cuestión de que método de procesamiento elige una empresa, es en gran parte una decisión de carácter económico obviamente. De cualquier modo, se puede decir que a medida que el volumen de datos se incrementa, la complejidad aumenta, las restricciones de tiempo se hacen severas y las exigencias de cálculo se vuelven más complejas, se requiere un mayor nivel de automatización. Esto se muestra en la figura 1.2. A continuación se definen algunos factores básicos a considerar:

a.- Inversión inicial. Es el costo de adquisición de los materiales y máquinas que se requieren para el procesamiento.
b.- Preparación. Es el gasto que implica preparar inicialmente los datos obtenidos para el procesamiento.

Relación entre las necesidades de procesamiento y el nivel de automatización.

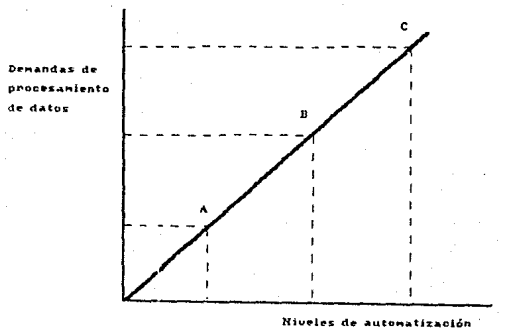


FIGURA 1.2

c.- Conversión. Es el costo único del procesamiento inicial de los datos mediante el nuevo método.
d.- Personal especializado. El nivel de conocimientos y capacitación de las personas que tendrán a su cargo el procesamiento.
e.- Costo variable. El costo de una unidad de datos en relación con los cambios ocurridos en su volumen.
f.- Modularidad. La posibilidad de aumentar o disminuir la capacidad de procesamiento de acuerdo con las necesidades.
g.- Flexibilidad. Es la posibilidad de modificar el sistema de procesamiento para hacer frente a demandas nuevas o variables.
h.- Versatilidad. Es la posibilidad de llevar a cabo muchos trabajos diferentes.
i.- Velocidad de procesamiento. El tiempo necesario para convertir los datos en información.
j.- Poder de cálculo. La posibilidad de realizar operaciones matemáticas complejas.
k.- Control del procesamiento. La posibilidad de comprobar que cada una de las tareas de procesamiento se lleva a cabo conforme a lo planeado.
l.- Detección automática de errores. La posibilidad, por parte de los componentes del sistema, de detectar errores de procesamiento.
m.- Alteración del sistema. El grado en que el sistema de procesamiento pierde eficacia debido a la descompostura o falta de uno o varios componentes.
n.- Nivel de automatización.
o.- Seguridad. Se requiere de métodos de protección tanto para el equipo como para la información que éste maneja.

1.2 LA IMPORTANCIA DE LA INFORMACION Y SU EVOLUCION

Desde hace algunos años se utilizan casi como sinónimos los términos procesamiento de datos y procesamiento con computadora. Aunque actualmente la mayoría de las organizaciones utilizan las computadoras para procesar los datos, antiguamente no sucedía esto. Desde un punto de vista histórico, la computadora se puede considerar como la última revolución dentro de la tecnología del procesamiento de datos.

La primera de estas revoluciones fue el desarrollo del lenguaje y de la notación matemática. Los historiadores no están seguros de la época en que se originaron los lenguajes hablados, pero se han encontrado formas de escritura ideográfica que se remontan a la cultura babilónica del año 3500 A.C. aproximadamente. Pero se les da a los fenicios, de 2000 años después, el crédito de haber inventado el alfabeto. También los primeros sistemas matemáticos se remontan hasta el año 3500 A.C.

Utilizando el lenguaje y las matemáticas, la humanidad ha enriquecido y difundido continuamente el conocimiento y la comprensión de sí misma y de su medio ambiente. La cantidad de conocimientos e información disponible se ha vuelto tan extensa que ninguna persona es capaz de obtenerlos todos.

La tecnología se ha desarrollado continuamente con el fin de hacer más eficiente el procesamiento de datos numéricos. El ábaco se ha usado desde el año 3000 A.C., y es tal vez el dispositivo de cálculo más antiguo.

En el siglo XVII se produjeron tres avances básicos en el desarrollo de la tecnología del procesamiento de datos: John Napier construyó un conjunto de barras numeradas que simplificaban las operaciones de multiplicación y división; Blas Pascal proyectó y construyo la primera máquina sumadora; y Leibniz construyó una calculadora que podía sumar, restar, multiplicar y dividir. En el siglo XIX se produjeron avances como el telar de tarjetas perforadas de Jacquard, la máquina diferencial y la máquina analítica de Babbage y las máquinas de tarjetas perforadas de Hollerith.

La segunda revolución se localiza en el siglo XV con la invención de la imprenta, la cual dió a la humanidad la posibilidad de registrar, almacenar, recobrar, informar y transmitir datos e información más que cualquier otro invento anterior en un lapso de casi 500 años.

En el siglo XX se presenta la tercera revolución con los medios masivos de comunicación como son la radio y televisión. Antes de que terminara esta tercera revolución, se empezó a registrar la cuarta revolución al aparecer la computadora digital. Actualmente la tendencia de los sistemas de información es tratar de utilizar la computadora y la tecnología relacionada con ella, junto con las técnicas de los medios de comunicación masiva, para producir información más conveniente en las organizaciones modernas.

Estos avances en la tecnología se comprenden mejor si se toman en cuenta las exigencias que existen para que se produzca cada vez más información.

Antes del siglo XVIII había dos razones principales para procesar datos. La primera, se relaciona con el deseo natural del hombre de llevar la cuenta de sus propiedades y riqueza. A medida que aumentó el intercambio y el comercio, los hombres necesitaron cada vez más medios para estar al tanto de los detalles y de la situación de los negocios. En el siglo XV Pacioli desarrolló el sistema de teneduría de libros de doble entrada que hizo posible que los eventos económicos se registraran en términos monetarios empleando una serie de cuentas relacionadas con los ingresos y los egresos.

La segunda razón la constituían los requerimientos gubernamentales. A medida que las tribus se transformaron en naciones, sus autoridades recopilaron investigaciones administrativas para que se emplearan en la recaudación de impuestos y en el reclutamiento de soldados.

A mediados del siglo XVIII se crearon todavía más exigencias para que se procesaran los datos de manera formal. La Revolución Industrial había trasladado a las fábricas las tareas básicas de la producción en el hogar y los pequeños talleres. El desarrollo de estas grandes organizaciones

manufactureras originó el desarrollo de otras industrias de servicios tales como la investigación de mercados y la transportación. De esta manera, el gran tamaño y la complejidad de tales organizaciones hicieron imposible que un individuo administrara de manera eficaz una organización sin algún procesamiento de datos que proporcionara información adicional. Además, con la aparición del sistema de fábricas grandes y las técnicas de producción en serie, la necesidad de medios de producción más modernos requirió de inversiones mayores. Estas grandes necesidades financieras forzaron la separación entre el inversionista y la administración. Por un lado, la administración necesitaba de más información para tomar decisiones internas, y por el otro, los inversionistas necesitaban información referente a la organización y al desempeño de la administración.

A medida que aparecían las nuevas políticas de negocios, aumentaba la necesidad del procesamiento de datos. Por ejemplo, la autorización de créditos hizo necesaria la actualización de las cuentas de cobro, las de pagos y las estadísticas de crédito. Los conceptos de la contabilidad financiera, que se siguieron perfeccionando y difundiendo a lo largo de los años, también requirieron un mayor procesamiento de datos. [2]

En nuestros días la información tiene una relación muy estrecha con el objeto que representa, casi se puede considerar como el objeto mismo. Esto se debe a que el control que se lleva de la información es tan severo que es como si se manejara el objeto. Por ejemplo, el observar que el inventario de la bodega de una industria indica que hay 50 litros de pintura blanca nos asegura que estos existen, por lo tanto es como estar viéndolos físicamente. Esto mismo sucede con el manejo de cuentas de los bancos ya que si el estado de cuenta muestra que un cliente tiene un saldo de 500,000 pesos a su favor esto es equivalente a tener los billetes físicamente ante nosotros. Esto es mucho más palpable en el sector financiero. Las transferencias electrónicas de fondos que permiten que las personas hagan transacciones mediante redes de telecomunicaciones, es un ejemplo claro de que se puede contar con el dinero sin tenerlo físicamente, manejándolo solamente como un dato en el sistema de información.

Es por esto que a la información se le atribuye tanta importancia sobre todo en el sector antes mencionado, y se dice que es indispensable en cualquier organización y por eso se la considera como un recurso.

1.3 LA INFORMACION ES UN RECURSO

La información es un recurso sumamente valioso para toda organización. La mayor parte de las empresas no podrían sobrevivir si carecieran de información formal. En muchas de ellas se observa una tendencia cada vez mayor a ampliar la efectividad y la utilización de la información más allá de la simple vigilancia de los aspectos legales y de la solución rutinaria de problemas. Esto se debe a que la información obtenida en forma oportuna permite a una empresa competir favorablemente, tener mayores oportunidades de negocio e incluso le permite mayor productividad.

El tema de usar información para obtener ventajas competitivas es uno de los puntos de mayor interes para muchos ejecutivos actualmente, pero la manera de llevar esto a cabo no es tan obvia como se desearia. En Estados Unidos se llevó a cabo una investigación en algunas organizaciones que son ejemplos sobresalientes de como lograr este objetivo. Algunas de estas son American Airlines, Federal Express, Laboratorios Marion y la Universidad de Carolina del Sur. De esta investigación se obtuvieron ciertos puntos comunes en dichas organizaciones, y por lo tanto puntos claves para llegar a usar la información como una ayuda para competir con éxito. Estos puntos son:

a.- Cambiar el papel de los sistemas de información para que se convierta en un recurso de competitividad efectivo.
b.- Hacer que los directivos crean en el papel competitivo de la información y lo hagan prioritario.

Esto significa una relación mucho más estrecha de los ejecutivos con los sistemas de información pues deben proveer su visión a largo plazo del futuro del negocio, expresar que es lo que esperan y deben vender la idea de la importancia de la información para lograrlo. Es indispensable también cambiar la mentalidad del personal, hacerles comprender que el sistema de información es realmente esencial para poder cumplir con los objetivos de la organización y que dicho personal tenga la capacidad de responder a estas nuevas necesidades. Debemos indicar que este objetivo es mucho más fácil de lograr en organizaciones que brindan servicios que en la industria.

Estas compañías más que aplicar la computadora a los factores tradicionales de competencia, han redefinido dichos factores. Se han dado cuenta que de los aspectos que pueden cambiar las reglas de competencia, el cambio tecnológico es el más importante; está claro que productos y servicios de calidad alcanzados a través de empleados altamente calificados usando métodos avanzados y tecnología innovativa da mejores oportunidades de captar el mercado. Además los sistemas de información permiten prestar mejores servicios a menor costo, ser más eficientes, tener mayor comunicación con el cliente, responder más rápidamente a nuevas oportunidades de negocios, tener sistemas de planeación, diseño y operación. [3]

Para que la información tenga realmente valor y cumpla con su objetivo, debe reunir varias características como son:

a.- Accesibilidad. Se refiere a la facilidad y rapidez con que se puede obtener la información resultante.
b.- Comprensibilidad. Se refiere a la integridad del contenido de la información.
c.- Precisión. Se refiere a que no haya errores en la información obtenida.
d.- Propiedad. Se refiere a que tan bien se relaciona la información con lo solicitado por el usuario.
e.- Oportunidad. Se relaciona con una menor duración del ciclo de acceso: entrada, procesamiento y entrega al usuario. Tiene que ver con que la información esté disponible en el momento que se la necesita.
f.- Claridad. Se refiere al grado en que la información está exenta de expresiones ambiguas.
g.- Flexibilidad. Concierne a la adaptabilidad de la información, no sólo a más de una decisión, sino a más de un responsable de la toma de decisiones.
h.- Verificabilidad. Se refiere a la posibilidad de que varios usuarios examinen la información y lleguen a la misma conclusión.
i.- Imparciabilidad. Se refiere a que no exista un intento de alterar o modificar la información con el fin de hacer llegar a una conclusión preconcebida.
j.- Cuantificable. Se refiere a la naturaleza de la información producida por un sistema formal de información.

k.- Protegida. Se refiere a que no cualquier individuo pueda tener acceso a la información, sólo el personal que la necesita debe tenerla.

El poder contar con informacion con las caracteristicas antes mencionadas implica un costo. Los costos involucrados en el funcionamiento de un sistema de información son:

a.- Costo del equipo. Esto incluye:

- Computadora y almacenamiento.
- Equipo periferico.
- Equipo de comunicaciones.
- Equipo de captura.

Además se deben de considerar los costos de tarjetas, papel, cintas, discos, etc. Esto es un costo fijo.

b.- Análisis de sistemas, diseño e implantación. Incluye la formulación de una metodología para los procesamientos de datos. Si se usa la computadora, será necesario incluir también la preparación de programas. Es un costo fijo.

c.- Costo de espacio y del control de factores ambientales. Por ejemplo sistemas de aire acondicionado, medidas de seguridad, unidades de control de energia, piso falso, limpieza, etc. Es un costo semivariable.

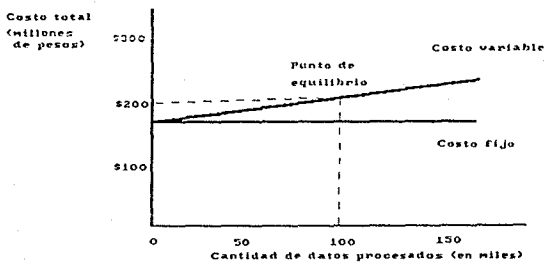
d.- Costo de conversión. Tiene que ver con convetir los sistemas antiguos, no automatizados a sistemas computarizados. Es un costo fijo.

e.- Costo de operación. Comprende el personal, la instalación y mantenimiento de sistemas, los suministros, los servcios y su conservación. Es un costo fijo.

En las gráficas 1.3 y 1.4 se pueden visualizar las caracteristicas y el comportamiento de estos costos, así como su relación con el volumen de datos procesados por dos métodos diferentes: por computadora y electromecánicos.

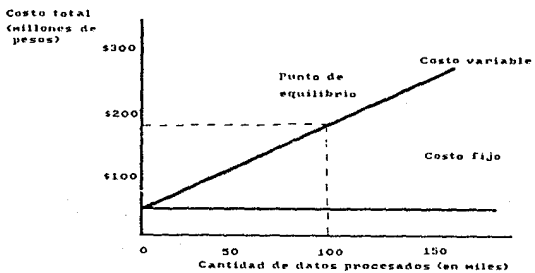
El objetivo de los sistemas de informacion es alcanzar un punto óptimo, donde el valor marginal de la información sea igual o mayor al costo marginal de su obtención. Esta relacion aparece en la figura 1.5. Con respecto al nivel de resultados pueden sentarse los siguientes principios:

Gráfica de costo, con el volumen de los datos como base para el uso de la computadora.



GRAFICA 1.3

Gráfica de costo, con el volumen de los datos como base para el método electromecánico.



GRAFICA 1.4

Relación entre el valor marginal y el costo marginal de la información

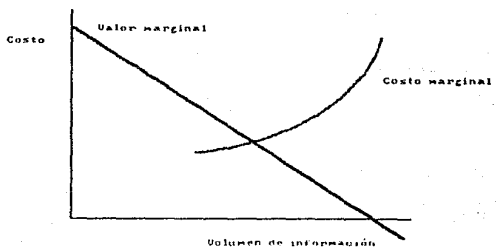


FIGURA 1.5

a.- Si el valor marginal es mayor al costo marginal: auméntese el resultado.
b.- Si el valor marginal es menor al costo marginal: limítese el resultado.
c.- Si el valor marginal es igual al costo marginal: el resultado es óptimo.

A partir de lo dicho anteriormente y como conclusión podemos obtener un modelo conceptual de una organización comercial y su relación con el sistema formal de información, el cual se muestra en la figura 1.6. [2]

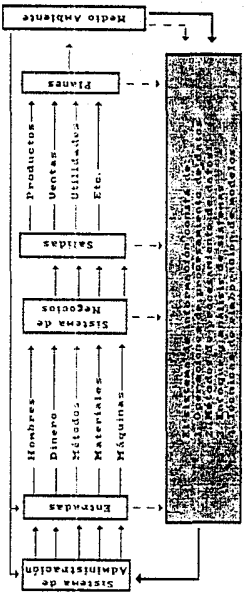


Ilustración de un sistema formal de información y su relación con el sistema total que es la empresa.

FIGURA 1.6

1.4 NECESIDAD DE PROTECCION PARA LA INFORMACION

Hasta aquí hemos tratado la importancia de la información y los beneficios que ésta presta a las organizaciones. Una vez entendida esta importancia se hace obvio que hay que cuidar y proteger este recurso tan esencial. Las organizaciones dependen de la información y los equipos que la procesan para su buen desempeño y cumplimiento de sus objetivos. Si en determinado momento una organización no cuenta con ellos, se ve prácticamente imposibilitada de llevar a cabo sus funciones en forma normal y a veces es tan crítica la situación que no puede operar del todo.

Hay que proteger la información pues está expuesta a una serie de riesgos de pérdida física y a lo que últimamente se le ha llamado el fraude electrónico y que parece ser el negocio del siglo. Por ejemplo en Estados Unidos se señalan pérdidas en sistemas de cómputo por tres billones de dólares cada año y en nuestro país se ha sabido también de varios casos de este tipo de fraude a instituciones del sector financiero.

Este último punto ha causado gran preocupación en nuestros días. Tanto así que se han desarrollado diversos congresos al respecto para tratar de encontrar algunas soluciones posibles.

Cada día, las instituciones que cuentan con algún equipo de cómputo, se hacen más concientes de los riesgos inherentes al acceso no autorizado a su información, ya que no existe forma de conocer e identificar a las personas que pueden utilizar sus conocimientos técnicos para realizar un fraude. Es por esto que muchas empresas han instalado modernos dispositivos de seguridad basados en conceptos de criptografía, control de acceso y administración de riesgos.

Pero no debemos de olvidar que existen también factores físicos de riesgo, que están fuera de nuestro control, para los cuales también se debe estar preparado. Los desastres más comunes son fallas del equipo, sabotaje, vandalismo, incendios, inundaciones y terremotos.

Es importante no sólo proteger los equipos físicos, sino que debe minimizarse también el riesgo de perder la información y cuidar que existan procedimientos para reiniciar las operaciones oportunamente.

En materia de seguridad se plantean seis controles fundamentales que conforman la administración de seguridad en redes de comunicación:

a.- Control de integridad, que evita la corrupción de los datos por accidente o a proposito, así como alteraciones, supresiones o inserción de los datos para uso fraudulento.
b.- Control de autenticidad del origen de los datos, que asegura al destinatario que la información procede del origen que se pretende.
c.- Control de confirmación, que proporciona una prueba al remitente de que el mensaje fue recibido por el destinatario y al destinatario de que el mensaje fue enviado por el remitente.
d.- Control de confidencialidad, que protege los datos contra una revelación no autorizada y asegura que sólo el remitente y destinatario pueden interpretar los datos.
e.- Control de auditoria, para probar que las transacciones con valor estén libres de errores en hora, fecha o cantidades; ciertos eventos selectivos deben ser registrados y mantenidos en un archivo para poder proporcionar, cuando se requiera, evidencias en caso de fraude.
f.- Control de autorización de acceso, que evita que terceras personas no autorizada tengan acceso a los archivos y que limita el poder de procesamiento, ejecución de programas de aplicaciones o servicos que proporciona la red.

La administración de seguridad de redes requiere además de servicios generales como son:

a.- Administracion de rendimiento e identificación de fallas.
b.- Administración de configuración de equipo.
c.- Administración de distribución de software (conjunto de instrucciones a través de las cuales queda programado el equipo de computación para la ejecución de los procesos).
d.- Administración de contabilidad.

El tener un alto grado de seguridad tanto en equipo físico como en la información es aun más importante en el sector financiero ya que es el sector más vulnerable de ser estafado en sus sistemas electrónicos. A continuación desarrollaremos con mayor detalle algunos de los tipos de control mencionados con anterioridad y trataremos las principales técnicas de seguridad.

2

SEGURIDAD FISICA Y SEGURIDAD LOGICA

2.1 SEGURIDAD DEL MEDIO AMBIENTE

La seguridad se puede dividir en dos tipos: física y lógica. La seguridad física se refiere a los controles y mecanismos implantados para proteger el hardware (estructura electromecánica de la computadora) y los datos en el centro de cómputo, sus alrrededores y sus recursos remotos. La seguridad lógica se refiere a la protección de los datos y programas que se encuentran dentro del sistema.

Las instalaciones de cómputo estan sujetas a una gran variedad de peligros por la naturaleza de su medio ambiente físico y éste tiene importancia critica en la seguridad del sistema de información. Es por esto que se le debe dar vital importancia a factores como localizacion del edificio, diseño y construcción. Esto se debe hacer durante la planeación de las instalaciones porque en esta etapa se pueden solucionar los problemas que se puedan presentar al respecto.

Las causas de daño físico pueden variar desde un fuego natural, inundaciones, hundimientos de la tierra, etc., hasta actos deliberados como explosiones, actos de sabotaje y de vandalismo.

El daño puede ser causado a varias pertenencias físicas variando desde equipo, el medio ambiente, los medios de almacenamiento, la documentación y la gente. [10]

Tanto la seguridad física como la seguridad lógica estan normalmente relacionadas y tienen una alta dependencia la una sobre la otra. Una debilidad en una puede provocar un compromiso para la otra. Las dos son igual de importantes ya que si no son seguras, el sistema no es seguro.

Muchas organizaciones implantan un alto nivel de seguridad física y de control de acceso, mucho antes de prestarle atención a la seguridad logica. Se tienen con frecuencia enormes gastos en seguridad física ya que por lo general las necesidades de este tipo son más faciles de identificar que los problemas de seguridad lógica.

Podemos decir que la seguridad física incluye tanto protección del ambiente que nos rodea como control de acceso. Las protecciones diseñadas contra las pérdidas por fuego,

explosiones, desastres naturales, fallas de energía eléctrica y hasta por la destrucción del ser humano involucran mucho estudio y grandes cantidades de gastos, al igual que los sistemas de recuperación en caso de desastre.

Los requerimientos de control de acceso pueden ser identificados inicialmente mediante una revisión sistemática de las partes vulnerables del hardware, software y sistema de comunicación de la computadora (ver figura 2.1).

Los resultados de una revisión de todos los componentes del sistema (tanto físicos como electrónicos y de procesamiento), que pueden ocasionar pérdida de potencial debido al acceso no autorizado producen un plan de acción que identifica las necesidades y requerimientos de control de acceso. El costo y la implantación de dicho plan estriba en un análisis formal y en la cantidad de recursos disponibles. [14]

Identificación de las partes vulnerables de la red de información.

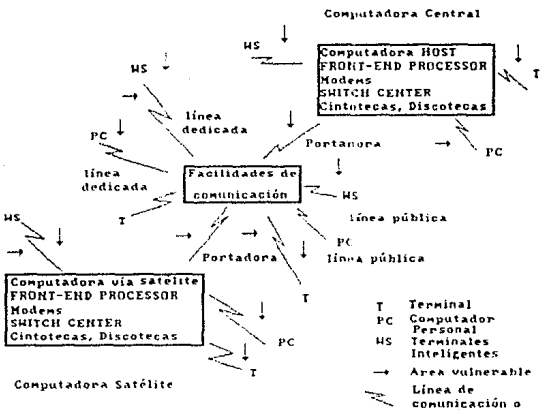


FIGURA 2.1

2.1.1 EL CENTRO DE COMPUTO

La sala de cómputo debe ser considerada como un área restringida. Unicamente se permitirá la entrada al área de cómputo, al personal autorizado. En centros pequeños, únicamente se permitirá la entrada de aquellos individuos cuyos nombres aparezcan en una lista especial. Más sin embargo se puede permitir la entrada a personas que requieran trabajar en la sala de cómputo o que deban cumplir con ciertas tareas. Un guardia de vigilancia puede o no estar asignado para llevar un control de acceso. Si no estuviera, uno de los operadores debe de ser el encargado de llevar dicho control.

Control del material en la sala de cómputo

Ningún medio de procesamiento de datos, documentación u objetos protegidos de ningún tipo deben de ser transportados hacia afuera o hacia adentro de la sala de cómputo sin la debida autorización del gerente del área. En caso de salidas y entradas normales de computadora, esta autorización será dada por alguna hoja de orden de trabajo.

Lo siguiente debe de prohibirse en todo momento en una sala de cómputo:

a.- Imanes.
b.- Equipo eléctrico o electrónico personal.
c.- Copias de documentos.
d.- Alimentos y bebidas.
e.- Abastecimieto de cigarros.
f.- Documentación no autorizada.

El acceso de equipo que esté bajo llave debe de ser restringido. Lo siguiente, así esté situado en la sala de cómputo, debe de mantenerse cerrado todo el tiempo, a menos de que requiera de reparación o de mantenimiento:

a.- Armarios.
b.- Closets de teléfono y cajas de terminales.
c.- Cajas para servicio de energía eléctrica, páneles de distribución, interruptores de transferencia manual e interruptores de control maestro. [4]

Se debe de contar dentro de la sala de cómputo con equipo de detección de líquido y de incendio.

También se debe de contar con puertas de seguridad para que en caso de incendio, todo el personal que se encuentre trabajando dentro de la sala de cómputo pueda salir sin ningún problema.

Ubicación del centro de cómputo

Los sótanos y todos los sitios bajo la tierra deben de ser evitados. Cuando esto no sea posible, debe de ser revisado el drenaje para evitar que el agua penetre al centro de cómputo. Cuando existe un alto riesgo de inundación, se debe de tener un equipo especial de bombeo.

La planta baja también debe de ser evitada, especialmente en áreas sujetas a inundaciones. Cuando esto no sea posible se deben de tomar las medidas necesarias para evitar que el agua penetre a la sala de cómputo. Además se debe de tomar en cuenta que el primer piso es más vulnerable a cualquier ataque.

Los edificios muy altos también deben de ser evitados. Cuando esto no es posible se debe de verificar la buena construcción del edificio. Se debe de garantizar un buen sistema contra incendios que cubra toda el área del centro de cómputo, este sistema debe de estar conectado directamente con el lobby del edificio para que se tomen las medidas de seguridad necesarias y se debe de prestar especial importancia al acceso al centro de cómputo.

Todo sitio a lo largo de las fallas geográficas debe de ser evitado. Cuando esto no sea posible, sólo se debe de elegir como construcción del centro de cómputo aquellos edificios cuya construcción sea a prueba de terremotos.

La ubicación ideal de todo centro de cómputo es que éste se encuentre lo más lejano del acceso público. En general es preferible que no sea un lugar muy poblado.

No es buena idea el construir un centro de cómputo en un área que tenga un alto índice de robos o de crímenes. Tampoco se debe de elegir un edificio cerca de una planta de explosivos, gasolinerías, plantas de petróleo, petroquímicas, refinerías, centros comerciales, estacionamientos o restaurantes.

Construcción del edificio

Todo centro de cómputo debe de ser construido con material no combustible. En caso de que el centro de cómputo se construyera con otro tipo de material, se debe de prestar especial importancia al sistema contra incendios que vaya a ser adquirido. También se debe de observar que éste cubra toda la sala de cómputo. [4]

El edificio debe contar con las siguientes caracteristicas:

a.- La loza del piso debe estar preferentemente soportada por una división de pilares de 720 X 840 cms. o 840 X 840 cms.
b.- Debe ser capaz de soportar el peso del equipo y construcciones adicionales.
c.- Los pisos de los corredores deben soportar el transporte de equipo.
d.- El centro de cómputo debe estar rodeado de una zona de seguridad.
e.- Se debe tener el menor número de cables, ductos y cañerías posibles que pasen por el centro de cómputo.
f.- Debe estar cerca de una pared exterior con ventanas.
g.- Las ventanas en paredes exteriores deben ser pequeñas y altas. [17]

Protección del centro de cómputo

La sala de cómputo y la cintoteca o discoteca, que son los lugares donde se almacenan cintas y discos magnéticos respectivamente, deben de estar rodeadas por el sistema contra incendios. Esto implica que todas las puertas de la sala de cómputo deben de ser puertas contra fuego. Deben de tener la capacidad de permanecer cerradas cuando haya condiciones de alarma o cuando se vaya la luz y además deben de permitir su apertura por medio de un seguro.

Es recomendable también que la cintoteca y la discoteca se encuentren dentro de un área rodeada por paredes con alta resistencia al fuego y separada de la computadora principal.

Por razones de protección contra incendios, al igual que por seguridad física, todas las paredes de la sala de cómputo deben de extenderse de pared a pared y ser de material no combustible. Es recomendable no tener ventanas y ningún tipo de ventilación externa. [4]

Es recomendable que el sistema de aire acondicionado esté localizado fuera de la sala de cómputo.

El suministro de aire acondicionado para las áreas de cómputo debe de estar completamente separado de cualquier otro sistema, de otra manera hay un grave riesgo de llevar calor, humo y gases a la sala de cómputo.

Por la misma razón los ductos que suministren a otras áreas no deben de pasar por la sala de cómputo, a menos que estén protegidos adecuadamente.

El sistema de aire acondicionado debe mantener una presión de aire positiva para el área de cómputo, esto para prevenir que los gases o humos de afuera entren a ella.

La sala de la planta de emergencia, debe de estar aparte de la sala de cómputo con una construcción que tenga como mínimo una hora de resistencia al fuego. La limpieza en este tipo de salas es esencial y deben de estar siempre cerradas para evitar el acceso no autorizado. [22]

Techo falso y piso falso

Por lo general toda sala de cómputo tiene tanto piso falso como techo falso. Las protecciones contra incendio que se deben de tener dentro de la sala de cómputo deben de preveer que el incendio pueda ser extinguido tanto en el piso falso como en el techo falso.

El piso falso se utiliza para tapar todos los cables que van de gabinete a gabinete de la computadora y de esta manera dar una buena imagen. Pero debe de permitir que sea fácil de quitar en caso de que se necesite realizar otro cableado o de que se tenga algún problema.

El techo falso también nos puede servir para tapar todo el sistema contra incendios, dejando únicamente a la vista las boquillas de salida.

Cuando menos dos puertas deben de ser proporcionadas como salidas de emergencia en caso de incendio en una sala de cómputo. El número de puertas depende de la cantidad de personal y del tamaño de las puertas. Aun cuando las demandas de seguridad indican que se tenga el menor número de puertas posibles, la sala de cómputo frecuentemente tiene que brindar salidas de emergencia en caso de incendio.
Las salidas de emergencia no deben de estar juntas, por lo general deben de estar en polos opuestos.

Toda salida de emergencia debe de estar identificada por medio de una señal y debe de tener una mínima cantidad de iluminación.

Subdivisiones internas

Es recomendable que la sala de cómputo esté subdividida por muros contra incendios.

Debe de haber un área de equipo de procesamiento que tenga que ver con papel de impresión, incluyendo impresoras de impacto, impresoras laser y desencarbonadoras. Acumulaciones de carga estática en los stocks de papel para impresoras de alta velocidad y el polvo de pequeñas partículas de papel han causado incendios. Por lo tanto deben de existir medidas preventivas tales como control de humedad, conductos para descargas a tierra y aire acondicionado.

Debe de haber un área de equipo de procesamiento de datos que requiera la frecuente intervención del personal de operación para manejo de cintas y discos.

Otro equipo de procesamiento de datos

La mayoría de las personas se imagina que en la sala de cómputo únicamente se encuentra la computadora principal, o el procesador central. Y esto no es necesariamente verdad.

La principal razón de seguridad hacia la computadora principal es que ésta representa un gran capital invertido, la cual se requiere para ejecutar las operaciones más críticas de la empresa sin ninguna interrupción y puede ser difícil si no es que imposible el sustituirla.

Por supuesto que todo el demás equipo de procesamiento de datos también posee estas características, incluyendo las computadoras personales, impresoras, equipo de microfilmación, etc. Todo este tipo de equipo debe de tener la protección equivalente a la que se le da a la computadora principal.

Actividades peligrosas

Actividades tales como fumar, comer, correr o jugar deben de estar prohibidas dentro de la sala de cómputo y cualquier otra área que contenga equipo de este tipo.

Toda operación de mantenimiento que requiera de una soldadura muy pesada debe de ser realizada fuera de la sala de cómputo. Materiales con cierto riesgo deben de ser almacenados en áreas protegidas fuera de la sala de cómputo. [4]

2.1.2 SUMINISTRO DE ENERGIA

Existen seis tipos de disturbios de energía eléctrica:

a.- Falla de energía: que se define como la interrupción de energía en cualquiera de las fases de un ciclo.
b.- Anomalías de estado uniforme: que son condiciones de bajo voltaje o de sobrevoltaje.
c.- Variaciones ciclo a ciclo: son variaciones de voltaje hacia arriba o hacia abajo.
d.- Impulsos que pueden ser de sobrecarga o de baja de voltaje alrededor de 0.5 a 100 microsegundos.
e.- Interferencias causadas por ruido electromagnético.
f.- Eventos catastróficos que son pulsos electromagnéticos muy grandes y muy rápidos.

Es esencial que todo centro de cómputo cuente con una configuración mínima de equipo para soportar cualquier tipo de falla eléctrica.

Ahora presentaremos cinco maneras de realizar un respaldo de energía:

a.- Utilización de un motor.- únicamente nos va a proporcionar 15 segundos de energía de emergencia.
b.- Un banco de baterías básico.- nos puede llegar a proporcionar hasta 45 minutos de energía de emergencia; claro que esto va a depender del tamaño del banco que se tenga.
c.- Modificación del banco de baterías.- se le incluye un interruptor de transferencia estática entre el banco de baterías y la corriente alterna.
d.- Múltiples bancos de baterías.- la utilización de varios bancos de baterías independientes permite que se tenga una operación continua de los bancos en caso de que alguno tuviera alguna falla.
e.- Alternador de emergencia.- esto es la instalación de alguna planta de emergencia tal como una planta diesel o una turbina de gas que nos proporcionará servicio hasta que el combustible se le termine.

Los interruptores de control maestro deben de ser instalados uno junto a la consola maestra de la computadora y el otro dentro de la sala de cómputo y cerca de la entrada principal. Estos interruptores deben ser marcados claramente indicando la función que realizan. Y deben de ser diseñados para activarse sin ningún esfuerzo.

Toda instalación eléctrica debe de realizarse utilizando el material apropiado de acuerdo al código eléctrico vigente. Además cualquier mantenimiento que se le deba realizar al equipo de energía eléctrica, debe ser supervisado y autorizado por el gerente del centro de cómputo.

También se debe de prestar especial atención de control a la ventilación y al aire acondicionado que debe de tener la sala de cómputo.

La temperatura y la humedad que debe de tener la sala de cómputo debe de ser la recomendada por el proveedor de la computadora que se tenga. Aunque nos debemos de asegurar que estas cantidades no tengan un rango de variacion de mas del 5% al 10%.

El sistema de aire acondicionado que se instale debe de cumplir con los requerimientos de la sala de cómputo y tener capacidad de mantener la temperatura adecuada para todos los gabinetes que se localicen dentro de ella.

Debemos de prestar especial atención al sistema de aire acondicionado ya que debido a las grandes cantidades de agua que maneja podría llegar a causar serios problemas.

En caso de que no podamos llegar a controlar la temperatura de la sala de cómputo y ésta rebace los 25° C, deberá pararse por completo la maquinaria, ya que si se continua trabajando se podrían dañar los circuitos integrados de la máquina y podríamos llegar a tener problemas de integridad de los datos en procesamiento. **[4]**

2.1.3 SISTEMA DE DETECCION Y DE EXTINCION DE INCENDIOS

De los desastres naturales el más peligroso es el fuego, por esto un equipo de detección de incendios debe estar presente en todo centro de cómputo.

Normalmente los centros de cómputo y las demás áreas asociadas tienen miles de millones de pesos invertidos en computadoras, equipo de comunicaciones y en información.

El proporcionar un adecuado nivel de notificación contra incendios para el personal del centro de cómputo como para mantener el equipo a salvo es absolutamente esencial.

Dentro de los sistemas contra incendios tenemos por ejemplo el del gas halón y sistemas de regaderas de agua. Pero la elección del equipo se debe de realizar teniendo en cuenta los siguientes puntos:

a.- El valor de la información y del equipo.
b.- Presencia de personal las 24 horas de dia.
c.- Locales remotos como bovedas de cintas, deben de tener equipo para extinción de incendios.
d.- Tiempo de respuesta del departamento de bomberos.
e.- Alternativas de costo-beneficio. [16]

Las siguientes estadisticas han reafirmado la necesidad de tener adecuados sistemas contra incendios tanto en el centro de cómputo como en todas aquellas áreas externas pertenecientes a la compañia (ver figura 2.2).

Deben ser instalados sistemas de detección, además de buenos procedimientos en la sala de cómputo. Un plan de contingencia, debe de ser puesto a prueba y aprobado. Debe de proporcionar una operación rápida de recuperación en caso de desastres mayores. [10]

Incidentes en los cuales se dañaron las computadoras.

FIGURA 2.2

Gases tóxicos y corrosivos

Este tipo de gases se puede propagar rápidamente a través de ductos a partes remotas de un edificio. Paredes sólidas y pisos con una adecuada resistencia al fuego son esenciales para evitar esto. El detener apropiadamente la propagación del fuego a través de aperturas y pasajes es vital. La propagación de estos gases tóxicos a través de ductos y techos falsos presentan un grave peligro para la gente, ya que los gases letales pueden llegar, sin ninguna medida de protección a cualquier área remota y libre de cualquier peligro de incendio. El fuego también puede propagarse rápidamente a través de un sistema de aire acondicionado. Es por ello que en el diseño de cualquier sistema de aire acondicionado se toman protecciones especiales contra el fuego.

El humo y los gases son también muy dañinos para computadoras, sistemas de oficina y todos los medios de soporte. Tanto el calor como los productos corrosivos de combustión pueden causar serios daños al equipo de computación y a los medios de almacenamiento. Temperaturas que exceden los 50° F son causa del mal funcionamiento del equipo electrónico. Los medios magnéticos de almacenamiento se pueden deformar y se tendría la pérdida de los datos. Los discos flexibles se pueden dañar en temperaturas arriba de los 52° F.

La combustión de materiales plásticos tales como el cable de aislamiento y la cinta magnética producen productos corrosivos que dañan los componentes internos, los contactos y los conectores.

El monóxido de carbono siempre ha sido un gran aniquilador. Sus características físicas, incoloro e inodoro, se producen por la combustión incompleta de materiales como textiles naturales, papel, madera, carbono y gas. Por lo tanto no hay ninguna señal de precaución en el aire. Esto puede causar que una persona llegue a tener daño irreversible en el cerebro. **[22]**

Incendios

Un incendio se desarrolla en tres etapas. Primero el fuego se encuentra en estado latente. Luego se desarrollan las llamas y se propagan por contacto directo, finalmente el fuego se hace tan fuerte y la temperatura es tan alta que el fuego se propaga por radiación del calor. Por esto se utilizan detectores de humo para localizar incendios antes de que estén fuera de control. Para evitar que el fuego se propague por contacto directo, es necesario controlar los lugares de almacenamiento de materiales inflamables y complementar esto con detectores de calor.

Los detectores de humo funcionan bajo dos principios:

a.- Principio de reflexion de luz, dependen básicamente de la propiedad de las particulas de humo de reflejar la luz. Las particulas de humo reflejan la luz emitida por una lámpara a un aparato fotoeléctrico.
b.- Principio de cámara de ionización, usan una pequeña cantidad de material radioactivo para cargar electrodos en el cuarto. Las particulas de humo reducen la conductividad pegándose a los iones, lo cual hace que baje su movilidad y como consecuencia limita la cantidad de corriente. Cuando la corriente se reduce a un valor especifico, funciona la alarma. [5]

Despues de que un incendio es detectado, se puede controlar usando:

a.- Extinguidores de mano.
b.- Sistemas de inundación de gas.
c.- Rociadores automáticos (Sprinklers).
d.- Mangueras.

Los extinguidores de mano se encuentran a simple vista en la mayoría de los edificios pero generalmente en caso de una emergencia es muy poca la gente que sabe usarlos, por lo tanto es esencial que el personal esté entrenado.

Los sistemas de agua de regadera o rociadores automáticos fueron utilizados por primera vez en 1866. Este tipo de sistema contra incendio es muy lento en comparación de los otros sistemas de protección. Tiene un tiempo de respuesta muy lento y está propenso a falsa alarma. Además no son los más adecuados para proteger una sala de cómputo, ya que si no se utiliza agua purificada las sales y minerales que pueden llegar a tener pueden dañar por completo los circuitos electrónicos que tienen las computadoras. [22]

Sistemas de inundación de gas

El dióxido de carbono y algunos gases halón son agentes muy efectivos para combatir incendios.

Los sistemas de inundación de gas deben de estar diseñados de tal manera que en cualquier evento de incendio el espacio que se tenga cubierto pueda ser llenado con una concentración suficiente de gas para extinción del fuego.

Los sistemas de inundación de gas son particularmente utilizados para techos y pisos falsos, en donde puede llegar a ser imposible apagar un incendio con extinguidores de mano. Los sistemas de inundación de gas pueden introducir el gas a través de tubos de uno o más tanques de almacenamiento.

Sistemas de dióxido de carbono

Aproximadamente un 30% de la concentración de dióxido de carbono puede extinguir casi completamente el fuego de una sala de cómputo. Desafortunadamente el dióxido de carbono es un gas asfixiante y es mortal en pequeñas cantidades que son necesarias para extinguir un incendio, aun cuando existen adecuadas cantidades de oxígeno.

Las concentraciones debajo del 7% de dióxido de carbono permiten una difícultosa respiración. Pero arriba del 10% empezamos a tener problemas de dolor de cabeza, problemas visuales, sumbido de oidos e incluso se puede llegar a perder la conciencia.

La concentración de dioxido de carbono utilizada en los sistemas de inundación de gas produce la asfixia inmediata e incluso la muerte.
En cualquier sistema de inundación de gas se deben de tomar las más seguras precauciones. Deben de existir buenos controles de seguridad de manera que antes de cualquier descarga a la sala de cómputo, ésta haya sido completamente evacuada, y después de que ocurra el suceso se debe de evitar la entrada hasta que el área haya quedado limpia de cualquier residuo de gas.

Se debe de tener mucha precaución con la temperatura que se llega a tener cuando se dispara el dióxido de carbono, ya que el cambio tan violento de la temperatura puede llegar a dañar el equipo. Este enfriamiento tan rápido del aire es a lo que le llamamos un "shock térmico".

Sistemas Halón

Dos gases de hidrocarbono halogenado, Halón 1211 y Halón 1301, son los comunmente utilizados para extinguir el fuego, tanto en sistemas de inundación de gas como en extinguidores halogenados. Halón es la abreviación de hidrocarbonos halogenados. Los halógenos son los cinco elementos químicos floruro, cloro, bromo, yodo y astato. Los halones se forman del tratamiento de compuestos de hidrocarburo con varios halógenos.

Los halones son más efectivos en concentraciones más pequeñas que el dióxido de carbono. Los sistemas típicos están diseñados para proporcionar de 5% a 8% de la concentración en los espacios protegidos.

El halón 1211 no nos proporciona ninguna señal de presencia. Pero se sugiere que la máxima concentración de éste en el aire en el cual un individuo pueda estar expuesto hasta un minuto sin tener ningún efecto que lo enferme es del 4% al 5%, lo cual es insuficiente para extinguir el fuego. Los efectos tóxicos que se tienen son falla de coordinación y reducción de la actividad mental así como una acción narcótica.

El halón 1301 es un gas un poco más amable y menos tóxico que el halón 1211. El halón 1301 es el que se utiliza más frecuentemente para salas de cómputo y es preferido por ser inherentemente más seguro. Al igual que los demás es inodoro y no da signos de presencia, pero en concentraciones arriba de 5% o 7% puede causar irritación de ojos.

También se dice que las exposiciones de poco tiempo del 6% de concentración o menos, no tienen ningún efecto en los humanos. Pero las concentraciones de 10% pueden causar serios problemas en el sistema nervioso.

El gas halón es mucho más caro que el dióxido de carbono.

La gente que trabaja dentro del espacio protegido por el sistema contra incendios debe de estar entrenada adecuadamente para tomar las acciones necesarias cuando suceda cualquier tipo de descarga. La descarga es muy ruidosa, y si nunca se ha escuchado puede llegar a causar miedo. [22]

Detección de fugas de agua

El agua también puede producir grandes daños a los sistemas de cómputo y su hardware, incluyendo cortos eléctricos, deterioramiento físico y errores en los datos. Existen detectores que censan pequeñas cantidades de humedad como por ejemplo los monitores WATER ALERT de la compañía Dorlen Products. Los aparatos detectores deben ser puestos en lugar estratégico para que la menor gotera pueda ser identificada y arreglada antes de que se transfrome en un problema mayor. Los sensores pueden operar con baterías o pueden ser conectados a una fuente de CA. Pueden operar independientemente o conectados a un sistema de alarma. [5]

2.2 CONTROL DE ACCESO

La seguridad física no es solamente el evitar que personas ajenas a la sala de cómputo tengan acceso a ella, sino que incluye protección de las áreas que rodean la sala de cómputo, de las terminales y de la comunicación de la red.

El equipo siempre ha sido una parte importante de todo programa de seguridad de la computadora. Inicialmente era utilizado para prevenir acceso físico a la sala de cómputo y para detección de incendios. Pero ahora la seguridad en el equipo de computación puede ser utilizada para prevenir el acceso a los recursos de la computadora así como para proteger los datos cuando estos se transportan por líneas de comunicación o hacia otros centros de cómputo.

El control de acceso al equipo aparentemente siempre está presente en los grandes centros de cómputo. Comienza con un equipo de seguridad en la entrada principal y continua con alarmas en la puertas de salida de emergencia. [16]

Idealmente la planeación de la seguridad física y la protección de control de acceso deben de comenzar con el diseño inicial del sistema. Esto incluye la construcción o adaptación de un edificio u oficinas para incrementar la seguridad.

El sistema, para identificar las debilidades de control de acceso puede ser implantado fácilmente si se utiliza una lista de chequeo para asegurarnos que no se nos olvido ninguna área. Dentro de las cosas que deben ser revisadas se deben incluir las siguientes:

a.- Selección para el lugar del sistema.
b.- Acceso al centro de cómputo.
c.- Acceso a las salas del centro de cómputo.
d.- Areas de terminales.
e.- Cintoteca, discoteca.
f.- Equipo de protección.
g.- Protección de los medios magnéticos, incluyendo discos flexibles.

h.- Banco de baterías.
i.- Sistema de documentación de archivos.
j.- Facilidades centrales de comunicación.
k.- Facilidades distribuidas de comunicación.
l.- Computadoras personales y terminales remotas.
m.- Aplicaciones en línea y computadora para comunicación vía satélite.
n.- Todas las facilidades de respaldo.
o.- Facilidades de mantenimiento.
p.- Sistemas de comunicación vía satélite.

El control de acceso es la protección de todos los recursos y facilidades de la computadora y las comunicaciones, en los cuales el acceso no autorizado provoque una pérdida, modificación o destrucción de los datos, alguna interrupción o falla del sistema para dar servicio a los usuarios o algun compromiso de seguridad lógica.

Los sistemas de protección más avanzados utilizan un sistema de alarma. Estos sistemas usualmente consisten de tres partes:

a.- Dispositivos sensores.- que es el proceso donde el intruso es detectado.
b.- Control de alarma.- es el mecanismo por medio del cual prendemos o apagamos una alarma.
c.- Señales de alarma.- es el proceso por medio del cual la persona responsable es notificada de que el sistema de alarmas ha sido activado.

El fondo de protección para tener una seguridad física es esencialmente la implantación de múltiples niveles de seguridad para proteger las facilidades de la computadora o algunos componentes del sistema. Esto propone que cuando menos debemos de tener tres capas de defensa para el sistema de algún acceso no autorizado.

Normalmente estas capas son clasificadas de la siguiente forma:

a.- Perímetro o protección del camino de entrada.
b.- Protección del área.
c.- Protección del objeto.

Como se muestra en la figura 2.3 el perimetro de defensa puede ser una reja o la seguridad que nos proporcionan puertas y ventanas; la protección para el área de riesgo debe ser un acceso controlado hacia esta sala; y la protección hacia el objeto (sea computadora, terminal, cinta magnética, reporte, línea de comunicación, pantallas) debe ser a través de algún tipo de sensor electrónico o alguna protección magnética que sujete al objeto.

Las herramientas o tecnologías, utilizadas para proporcionar la protección necesaria a todos los niveles, deben ser seleccionadas de una gran variedad de posibilidades (un guardia, alarmas o controles magneticos, tarjetas magnéticas, dispositivos electrónicos de control de acceso). La mayoría de los dispositivos electrónicos y de seguridad, están diseñados para proporcionar la seguridad necesaria a una o más áreas de alta vulnerabilidad. [14]

Las puertas que proporcionan el acceso a la sala de cómputo son las primeras barreras para el acceso del personal no autorizado, además deben ser lo suficientemente fuertes para evitar cualquier acceso forzado o con violencia.

Los grandes centros de cómputo deben de tener un buen equipo de seguridad a la entrada, el cual cuando menos requiera que la primera persona que desea entrar a la sala posea una tarjeta magnética o algún número de identificación. Ademas estos sistemas tienen la capacidad de restringir el acceso a personas autorizadas a entradas especificas durante horas especificas de algunos dias.

Podemos encontrar varios tipos de sistemas los cuales deben de trabajar bien si se tiene el control adecuado sobre el sistema. [16]

Los sistemas de control de acceso tienen tres funciones principales:

a.- Identificación, que incluye la información básica de un usuario como su apellido. Normalmente este es un dato conocido públicamente.
b.- La clave asociada a la identificación de un usuario es un mecanismo para confirmar o autentificar que la persona que desea hacer uso de la computadora es quien dice que es.

Esquema de Seguridad física.

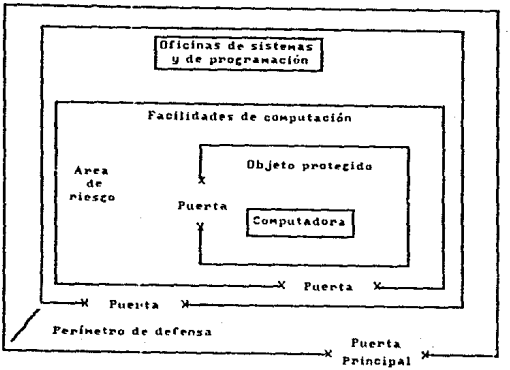


FIGURA 2.3

c.- La autorización de acceso a recursos específicos del sistema como archivos, programas o aparatos, está determinada por una comparación de la identificación del usuario y su clave con un conjunto de permisos predeterminados para usar el sistema.

Mecanismos de identificación física

Para mejorar el nivel de seguridad en el acceso lógico a la computadora se está utilizando actualmente el principio de que el usuario debe poseer algo físicamente que le permita dicho acceso, esto puede ser una tarjeta magnética, llaves, etc.

Varias puertas de una sala de cómputo son seguras con cerraduras de combinación digital. Frecuentemente estas cerraduras requieren que cada persona digite la misma secuencia de tres números entre el 0 y el 9. Desafrotunadamente los gerentes de seguridad no permiten el cambio de esta combinación. Esta falla pone a la sala de cómputo en peligro ya que es fácil de obtener la clave secreta de algún usuario. Además, personal no autorizado puede observar cuando un empleado digita la combinación y esto puede causar problemas.
Otra fuente menos obvia de compromiso es que se digiten tres números mal. Pero el intruso sólo tiene que probar con los seis permutados de los números y de esta manera lograr entrar. Esta situación puede no ser solucionada ni modificando la clave de seguridad constantemente.

Pero existen otros sistemas que nos permiten la autentificación por clave. Esto usualmente implica la ruta de algún mecanismo de digitalización como llave para una clave y algún artículo independiente de control, como una tarjeta magnética.

Estas tarjetas magnéticas no deben de tener ningún tipo de identificación visual de los privilegios de que goza la persona que la tiene. Para que de esta manera si alguien la llegara a encontrar no supiera que hacer con ella.

La elección del tipo de tarjeta magnética a utilizar, de una o dos bandas, se debe de realizar de acuerdo a los requerimientos de cada empresa. Las llamadas tarjetas inteligentes, desarrolladas en Francia, nos proporcionan una excelente alternativa. Consisten de un microcircuito empotrado en una tarjeta plástica y es del mismo tamaño que el de una tarjeta de crédito. Este mecanismo puede almacenar 8,000 bytes de información, suficientes para grabar la descripcion física y la vida de la persona que la portará.

Los dispositivos de control de acceso pueden contener una microcomputadora que puede leer de la tarjeta la información para realizar comparaciones lógicas y, de acuerdo a los resultados obtenidos permitir o no la entrada de la persona. **[4]**

MASTIFF SYSTEMS produce pequeños transmisores de baja potencia que contienen códigos específicos. Se pueden usar como sensores de proximidad para controlar acceso físico, también se pueden usar para encender terminales automáticamente cuando el usuario esta cerca y, apagarlas cuando se aleja. Se les da poca duración a sus baterías para que no funcionen después de un día si se pierden o son robadas. Los usuarios autorizados dejan los transmisores en la compañía despues del trabajo para que sean recargados.

El tipo de alternativa que se escoga dependerá del nivel de seguridad que se requiera y del costo que se desee pagar. Se deben considerar los siguientes parámetros para hacer dicha selección:

a.- La probabilidad de negar el acceso a un usuario autorizado debe ser mínima.
b.- La probabilidad de aceptar a un usuario no autorizado debe ser mínima.
c.- El tiempo necesario para pasar la barrera de acceso no debe ser excesivo.
d.- La memoria requerida por el control no debe ser excesiva.
e.- El mantenimiento debe ser fácil y rápido.
f.- La confiabilidad del sistema debe ser adecuadamente alta, si éste no funciona causa muchos problemas de operación. [5]

Identificación personal usando comparación de características físicas

Los sistemas de identificación que están basados en una comparación de una o más características físicas de una persona se llaman sistemas biométricos. Estos sistemas proporcionan otro nivel de protección de acceso usando una característica personal que prueba la identidad de la persona. Los sistemas biométricos que existen actualmente en el mercado validan la identidad de la persona por características físicas como:

a.- Huellas digitales. Compara automáticamente las huellas de dedos específicos colocados en un aparato explorador con las de la persona que se está identificando. La gran dificultad es obtener un buen registro; cortes, ampollas y suciedad pueden hacer que la comparación falle. La mayoría de los sistemas utilizan tecnología óptica para la exploración. Por ejemplo FINGERMATICS tiene un dispositivo que requiere de 512 bytes de almacenamiento y su costo es de 6,500 dólares; tiene una probabilidad de 0.37% de no aceptar personal autorizado y de 0.03% de admitir personal no autorizado.
b.- Voz. Compara el patrón de voz de una persona con una grabación previa. Se tiene la dificultad de que las gripas, laringitis y estrés emocional cambian la voz. Algunas compañías que trabajan este tipo de dispositivo son: THRESHOLD TECHNOLOGY, TURNKEY INFORMATION PROCCESING INC.

c.- Geometría de la mano. Compara la longitud y/o translucidez de los dedos apoyados en un plato especial con una imagen previa de la mano de la persona. Estos sistemas son muy confiables. Un ejemplo es el sistema de STELLAR SYSTEMS cuyo precio es de 5,000 dólares.

d.- Firmas y letra. Compara diferencias de presión y velocidad para identificar la letra de una persona con una grabación previa. El principio básico de este sistema es que las personas tienen la tendencia a escribir sus nombres en una forma única y consistente. Pero existe el problema de que si la persona ha sufrido alguna herida o está bajo presión esto se puede alterar. Algunas compañías que trabajan este tipo de productos son: SANDIA NATIONAL LABORATORIES, IBM, STANDFORD RESEARCH INSTITUTE, TRANSACTION SECURITY LTD, MICROPATD INC.

e.- Huellas de la palma de la mano. Utilizan tecnología similar a la de huellas digitales. Un ejemplo es el sistema PG2000 de PALMGUARD INC. que tiene 3 segundos de tiempo nominal de acceso, una probabilidad menor al 1% de no aceptar personal autorizado y 0.00025% de aceptar personal no autorizado, tiene memoria para 256 palmas diferentes y su precio es de 48,000 dólares.

f.- Patrones de retina. Reconoce a un individuo por su patrón de venas en su ojo. EYEDENTIFY INC. tiene aparatos cuyos precios varían desde 10,000 a 75,000 dólares. **[14],[5]**

Nuevos y altamente sofisticados mecanismos electrónicos de seguridad y otros dispositivos han sido puestos en el mercado hoy en día. Muchos de estos productos tienen cierto avance tanto científico como tecnológico, así como el hardware y el software que acompañan al sistema que requiere de protección. Computadoras especiales y facilidades de comunicación por lo general están incluidas en un sistema total de seguridad y protección de la información.

Ya que el estado del arte es tan complejo, consejos de expertos y de profesionales deben de ser utilizados para la selección del sistema y de los mecanismos de seguridad.

Ejemplos de sistemas de protección y dispositivos de seguridad incluyen:

a.- Dispositivos de contacto magnético. Para proteger puertas y ventanas. Aquí se incluyen dispositivos como tapetes o trampas de presión.
b.- Dispositivos fotoeléctricos. Utilizados para defensa en el perimetro.
c.- Luz modulada. Utiliza un haz de luz que reacciona únicamente con la luz generada por el mismo. También conocido como "luz de pared".
d.- Detección de vibraciones y de audio. Utilizado para monitorear acceso o penetración no autorizada.
e.- Circuito cerrado de televisión. Utilizado para monitorear áreas sensibles, desde una estación central de vigilancia.
f.- Detección de capacitancia. Utilizada para generar una alarma cuando un intruso se acerca a un área u objeto sensible.
g.- Detección de movimiento. Utiliza energía ultrasonica o de microondas para identificar a un intruso cuando alguna forma de movimento crea un corrimiento Doppler que es registrado por el sistema.
h.- Sistemas ópticos y de luz infraroja. Utilizado para la detección del calor generado por los movimientos del cuerpo de un intruso.
i.- Detectores de metal y magnómetros. Utilizados para detectar la entrada no autorizada de objetos metálicos peligrosos al área sensible.
j.- Dispositivos de control electrónico de entrada. Incluyen sistemas de tarjeta magnética o de llave que controlan la apertura o el cierre de puertas o de otros accesos a áreas sensibles. De este tipo de dispositvos existen diversas variaciones que incluyen requerimientos de entrada de digitos especiales o de códigos como entrada al sistema.

Además de todos los sistemas de protección antes descritos existen numerosos dispositivos de control de acceso. Estos además proporcionan información de identificación de usuarios y/o acceso lógico a los recursos de la computadora como archivos, programas y facilidades de comunicación. [14]

El control de acceso a la computadora se refiere a la combinación de protección lógica, física y administrativa que estan asociadas a la red o al sistema de la computadora.

Principio básicos de control de acceso

Como principio general, la simple posesión de algún articulo de control de acceso no debe permitir o dar autoridad de acceso a ningún bien sensible, debido a que puede existir un uso inapropiado de los articulos de control de acceso o por el alto grado de falsificacion.

Un segundo principio del control de acceso es que lo más sensible son los bienes, lo más seleccionado debe de ser el mecanismo de control de acceso.

Un tercer principio está enfocado principalmente a tener un especial cuidado de la informacion clasificada y es que ninguna persona debe de ser autorizada a accesar cualquier bien sensible o seleccionado por razones de posición en la empresa. [4]

2.3 SEGURIDAD EN EL ENLACE DE COMUNICACIONES

Comenzaremos por decir que los aficionados de la computacion, conocidos por el nombre de "hackers", inicialmente tienen acceso legal a ciertas facilidades de comunicación. Ellos rompen la ley cuando utilizan sus sistemas para lograr la entrada ilegal a otras facilidades de la computadora o de comunicaciones con el propósito de realizar ciertas actividades comprometedoras.

Por otro lado tenemos que, se asegura generalmente que la debilidad del enlace físico de varios sistemas de información se localiza en el área de comunicaciones. Una de las razones es que la mayoría de los sistemas parecen haber sido creados con la noción de que los sistemas portadores de comunicación son inviolables. Pero hasta la gente que conoce más sobre esto, ha construido redes de información que confían en las leyes federales y en el gobierno para la protección de las comunicaciones. Se ha sabido desde hace mucho tiempo que las comunicaciones son extremadamente vulnerables a intervenciones de líneas telefónicas o intercepciones de microondas. **[14]**

La figura 2.4 nos muestra un resumen de las amenazas típicas a un sistema de teleproceso y las medidas de seguridad que se deben tener para contrarestarlas.

Las terminales están localizadas en los departamentos de usuario, frecuentemente en sitios remotos con pobre o ningún control de acceso. Es por eso que se debe de prestar particular importancia al sistema de red de comunicaciones que se tiene y se debe de considerar la posibilidad de que cualquiera de los siguientes eventos ocurra:

a.- Exposición de información a una persona no autorizada para tenerla. Esto aplica particularmente a información tal como registros personales, información de sueldos, etc.
b.- Sustitución de la información, o sea, reemplazo de la información correcta por información falsa.

c.- Información retardada. La mayoría de los sistemas asumen que todos los datos recibidos vía la red de comunicaciones son correctos hasta que son modificados. En sistemas en los cuales una modificación se retrase, se tendrá una falsa imagen de la información histórica.
d.- Diversificación. Aplicaciones críticas que involucran redes de comunicación que incluyen transferencia electrónica de fondos (EFTS); otras aplicaciones críticas incluyen sistemas de correo electrónico los cuales manejan información sensible que usualmente esta ligada a sistemas de procesamiento de palabra.

En la siguiente página se presenta un esquema de las amenazas y seguridades de un sistema de teleproceso. [10]

Como se puede observar en la figura 2.5, las partes vulnerables de todo sistema de comunicaciones pueden ser identificadas en cuatro áreas:

a.- Dispositivos de comunicaciones.
b.- Líneas de comunicación y sistemas de control de línea.
c.- El cable telefónico de la central más cercana al edificio.
d.- Sistemas de microondas y comunicación vía satelite.

Dispositivos de comunicaciones

Existen áreas en donde el compromiso se puede hacer sin el contacto físico, y esta posibilidad debe de ser considerada cuando se examinan las áreas de vulnerabilidad. Por ejemplo, las transmisiones vía radiaciones electromagnéticas proporcionadas por computadoras electrónicas y por dispositivos de comunicaciones, son susceptibles de detección y grabación no autorizada, de señales generadas, por una terminal o una computadora personal de algún lugar cercano.

Todos los dispositivos de comunicaciones incluyendo terminales, computadoras personales, modems, controladores de comunicaciones y concentradores, requieren de protección física para un acceso no autorizado. Simples procedimientos y mecanismos de protección física, como guardias, puertas con llave, teclados con llave, circuitos cerrados de televisión,

Amenazas típicas y medidas de seguridad en un sistema de teleproceso.

Componente del Sistema / Evento/ Contramedida	Operador	Terminal	Línea	Procesador	Línea	Host	Almacenamiento secundario
Amenaza Accidental	Error humano	Falla	Falla/ ruido	Falla	Falla/ Ruido	Falla	Falla
Contramedida	Diseño de un diálogo para minimizar que ocurra un error	Utilización de la terminal más cercana	Rutas alternas	Ruta Alterna	Chequeo de línea	Utilización de procesador alterno	Uso de dispositivos alternos
Amenaza Deliberada	1. Tentación. 2. Hacerse pasar por otra persona 3. Acceso no autorizado a información sensible	Substitución de la terminal.	Manipulación de líneas.	Acceso no autorizado Corrupción de datos	Manipulación de líneas	Acceso al sistema operativo/ corrupción	Acceso no autorizado
Contramedida	1. Correr a la persona. 2. Romper la línea o comunicación. 3. Pared detras del usuario.	Cheques de autentificación.		Físicamente asegurar el procesador o controlador		Protección de control de acceso y de información activa	Encriptar información sensible

ENCRIPCION

Puntos vulnerables en el sistema de comunicación.

FIGURA 2.5

etc., pueden ser utilizados para proteger estos dispositivos. El tipo de protección seleccionado no debe de ser elegido de una manera arbitraria sino que se debe elegir de acuerdo a cierto diseño y a ciertos objetivos.

Líneas de comunicación y sistemas de switcheo

Los usuarios de los sistemas de comunicación por lo general no le dan la importancia debida a la protección de las facilidades de comunicación tanto las locales en las cuales solo ellos desean trabajar o en aquellas que son públicas.

La reciente introduccion de sistemas más avanzados de comunicación, tales como redes de línea privada, sistemas de comunicación via satélite o de microondas y redes de área local diseñados para integrar transmisiones de voz y datos hacen de la protección física algo esencial. El nuevo equipo no es más vulnerable que el viejo sistema telefónico, pero en estos sistemas se manejan más datos sensibles a cualquier intromisión.

Ahora debemos de tener en cuenta que la protección física para las facilidades de comunicación no ha cambiado. Ya que podemos utilizar todos los mecanismos de seguridad antes mencionados.

Generalmente las cinco areas típicas de todo sistema de comunicaciones que deben ser investigadas y que requieren de protección son:

a.- Nodos que puedan ser investigados.
b.- Dispositivos de acoplamiento que conecten lineas y entronques de la red.
c.- Lineas de distribución, entronques y enlaces.
d.- Interruptores.
e.- Dispositivos fuente y destino (computadoras, terminales, etc.).

Lo siguiente también requiere de investigación: enlaces via satelite y de microondas; determinados componentes de redes de área local; todas las facilidades de comunicación orientadas a la computadora principal o a terminales, así como procesadores de comunicaciones localizados antes del computador principal, concentradores y modems. **[14]**

Según Wong existen dos formas para interferir un sistema de computación. Los eventos anormales que incluyen eventos tales como fraude, robo, acciones industriales y otros, y los eventos normales que incluyen caída del sistema, caída del equipo, errores y omisiones.

Las estadísticas que se tienen nos indican que los fraudes cada vez van a ser mayores. Algunos casos de penetración al sistema se deben a los vacíos que este tiene. Para evitar todo este tipo de incidentes se deben de utilizar los más efectivos sistemas de seguridad, control de entrada/salida, procedimientos adecuados para autorizar la entrada al sistema, diseño estructurado y la utilización de lenguajes de alto nivel que requieran de mayor conocimiento y tengan un mayor grado de dificultad.

El buen reclutamiento para la utilización de los procedimientos aunado a revisiones continuas del desempeño, ayudarían para reducir y prevenir cualquier abuso de la instalación. [10]

Cable telefónico

El cable telefónico es una de las partes de mayor vulnerabilidad en una red de comunicaciones, ya que la mayoría de los datos que viajan de una facilidad a la otra van por ellos. Existen varios dispositivos de seguridad física que pueden solucionar este problema. Dependiendo de la vulnerabilidad del sistema se deben de implantar varios niveles de seguridad. Para los dueños de este tipo de sistema de comunicaciones se les recomienda tener los cables telefónicos bajo tierra y/o el uso de la encripción. **[14]**

Sistemas de microondas y de comunicación vía satélite

La primera vulnerabilidad de los sitemas de microondas y comunicación vía satélite es la intercepción. La solución para evitar el acceso no autorizado al mensaje es la encripción.

Un enlace de comunicaciones es necesario para conectar computadoras y terminales distantes. Las terminales pueden ser "tontas", "inteligentes", con capacidades limitadas de procesamiento, microcomputadoras o estaciones remotas de trabajo.

El enlace puede conectar la terminal directamente con el centro de cómputo. Comúnmente se utiliza cable coaxial o alambre de par torcido para realizar el enlace de las terminales con el sistema.

Después de algunos cientos de pies el enlace de comunicación se debe de realizar por alguno de los siguientes métodos:

Líneas dial-up o públicas.- Tienen el mínimo nivel de protección de seguridad. Cualquier persona con una terminal o con una microcomputadora puede colgarse a la red y lograr el acceso para consulta o modificación. Las intervenciones de líneas son posibles.

Líneas privadas.- Tienen un mayor grado de seguridad porque están conectadas físicamente al equipo y pueden ser identificadas. La intervención de líneas es posible.

Transmisiones vía satélite.- Son extremadamente vulnerables ya que cualquiera con una antena o un "plato" puede interceptar o iniciar comunicación.

Enlaces miscelaneos.- Incluyen fibras opticas y circuitos de microondas ofrecen diferentes ventajas de seguridad. Las líneas de fibras ópticas son dispositivos de mucha dificultad para un intruso y son dispositivos con un alto mejoramiento de seguridad.

Los datos en el enlace requieren de proteccion mas allá de los controles de calidad que son proporcionados por chequeo de error o prueba de la línea. El enlace debe estar libre de cualquier intervención directa de la línea o cualquier otra señal de intervención.

Si el enlace pudiera llegar a ser intervenido los datos podrían ser obtenidos por un intruso sin la autorización del propietario o se podrían llegar a realizar transacciones no autorizadas en la red. Por lo tanto si la integridad del enlace no puede ser garantizada, los datos del enlace se harían inutilizables. **[16]**

Dentro de los dispositivos de seguridad que tenemos disponibles para hacer casi imposible la entrada a la computadora por medio del teléfono estan los dispositivos "dial-back".

Los dispositivos "dial-back" se ponen en la red de telecomunicaciones del sistema. Un individuo que quiera entrar a la computadora por medio de una llamada telefonica puede colgarse o desconectar la línea telefónica.

El dispositivo de "dial-back" hace un chequeo interno de los usuarios autorizados y la hora y los días en los cuales tiene acceso al sistema. Si el usuario cumple el criterio de autorización entonces el dispositivo le permite que comience su procedimiento de entrada "log-on".

Existen también dispositivos llamados "dial-through", los cuales realizan las mismas funciones que el "dial-back" nada mas que estos, después de autentificar la identificación del usuario pasan la llamada al sistema. **[16]**

La encripción, que muchos usuarios de red desafortunadamente piensan que es sinónimo de seguridad de los datos, es una herramienta muy poderosa para proteger los datos en un enlace de comunicación. Debe de ser considerada para redes en las cuales los requerimientos de seguridad son muy altos y donde su uso no esté imposibilitado por la ley nacional.

Encripción es el "revolver" o recodificar los datos para la transmisión, de manera que los datos interceptados tengan el menor sentido para el intruso. La encripción se puede realizar tanto por hardware como por software. El dato original que ha de ser transmitido (texto original) se convierte en un texto intelegible (texto cifrado).

El texto cifrado se manda al destino en donde se traduce para ser de nuevo el texto original. Este proceso es conocido como encripción y decripción.

La encripción no es una tecnologia nueva; las computadoras sólo hacen el proceso más fácil para nosotros. El proceso de encripción está controlado por un algoritmo y una llave. El algoritmo es el método por medio del cual los datos son revueltos. La llave es la que nos indica cuando comenzar y terminar de revolver los datos en una manera que haga utilizables los datos para el usuario que tiene la llave.

La National Bureau of Standards desarrolló el estándar DES (Data Encryption Standard) que proporciona un método de encripción que no ha sido roto hasta hoy. El DES puede ser implantado tanto en software como en hadware. Más adelante se tratará este tema con mayor detalle. Otros métodos menos rigurosos han sido probados como métodos que se pueden romper.

La elección de la implantación de la encripción debe estar basada en el diseño de la red, el costo de operacion y la capacidad de procesamiento de la máquina. La encripción por medio de software requiere ciclos de CPU. En cambio la encripcion por medio de hardware utiliza su propio CPU y no tiene ningún impacto en el performance del CPU del computador principal, pero tenemos que tomar en cuenta que la implantación del método de ecripción por hardware requiere de equipo adicional con cierto costo.

Se debe de tener mucho cuidado con el manejo de la llave de encripción, su distribución y su almacenamiento, ya que es la seguridad del método de encripción utilizado. [16]

Códigos de verificación

Se debe de utilizar un mecanismo efectivo de detección de errores en la transmisión, y si fuera posible que también se realizara la corrección de ellos. Existe una gran cantidad de códigos para realizar la detección y corrección de errores debido al alto grado de interés que se tiene para realizar comunicaciones libres de errores tanto en vuelos espaciales como en comunicaciones vía satélite.

Ahora nos dedicaremos a discutir algunos de estos códigos de verificación.

Contador de paridad.- Un contador de paridad puede ser tanto de chequeo de redundancia longitudinal (LRC) como vertical (VRC). Si estos dos se utilizan simultáneamente existe la probabilidad de tener una detección de error así como su corrección. Una protección mucho mejor esta disponible si se utiliza el chequeo de redundancia cíclica (CRC).

Los codigos de computadora y de comunicaciones representan caracteres con una longitud uniforme de marcas y espacios. Paridad significa llevar un conteo de las marcas de una secuencia y determinar si existe un número par o impar de ellas. La paridad non significa que se encontró un número non de marcas y por lo tanto se agregará una marca que nos indicará el bit de paridad. Al igual que en la paridad non, en la paridad par se cuenta el número de marcas y si el número de éstas es par se agrega una marca indicando el bit de paridad. De otra forma la posición del bit de paridad estaría ocupada por un espacio.

Como ejemplo citaremos el siguiente: un bloque de mensaje consiste de una secuencia de nueve caracteres 1, 2, 3, 4, 5, 6, 7, X, Y en un código de 6 bits. La paridad par es utilizada para los códigos VRC 00X0XX0XXXX y LRC 0XXX0XX.

Los bits de paridad forman parte del bloque de mensajes, por lo tanto cuando se añade el bit de paridad y el carácter de fin de bloque (EOB) tenemos una secuencia de once caracteres de 7 bits.

La paridad es verificada cada vez que el dato es transmitido y las nuevas secuencias son comparadas con las originales.

Suponiendo que durante la transmisión se metiera ruido al dato, este ya sería diferente y por lo tanto tendríamos un error de transmisión en nuestra secuencia.
Por lo tanto nuestra secuencia nos quedaría:

```
OOXXXXOXXXO     VRC
XXXXOXO         LRC
```

diciéndonos en VRC que un error se ha introducido en el cuarto carácter y en LRC nos dirìa que se ha introducido un error en la primera posición.

El código de correccion del error ha determinado la posicion del error, ahora el mecanismo cambiará el primer bit del cuarto carácter y corregirá la paridad. En este momento la paridad que se tenía ya es igual a la del mensaje y el error causado por el ruido ha sido eliminado.

Las cintas magnéticas que tienen una densidad de 13,000 bits por pulgada o más utilizan paridad doble diagonal en lugar de paridad ortogonal.

Digito verificador.- Existen muchas formas de realizar la verificación de un digito. La que mostraremos a continuación es la más utilizada. Los digitos verificadores protegen contra transcripciones erroneas de un número. El sistema que se va a describir tiene un 100% de ser exitoso en la detección de errores cuando un digito se copia con error.

Daremos un número con longitud de 8 digitos; para realizar la verificación, multiplicaremos por 1 y por 2 como se muestra a continuación, sumaremos el resultado de las multiplicaciones y el resultado lo restaremos del número más cercano hacia arriba que sea multiplo de 10.

números	4 4 1 8 9 3 0 4
	X X X X X X X X
peso	1 2 1 2 1 2 1 2
resultado módulo 9	4+8+1+7+9+6+0+8 = 43
dígito verificador	50 - 43 = 7

El número final es 441-893-047. Cada vez que se transcriba, el digito verificador realizara una comparación contra el que tiene y el que fue transcrito para detectar los errores.

Conteo de caracteres.- El conteo de caracteres se utiliza para proteger la integridad de los datos. El bit de paridad es un caso especial de conteo.

En varios registros, el conteo se realiza por el número de agujeros que deben de ser realizados en una tarjeta para protegerse de que alguien quiera cambiar los datos añadiendo más agujeros. En archivos usualmente se tiene un registro que lleva el número de bloques de manera que se lleve un control sobre el tamaño del archivo y no se le pierdan o se le añadan partes que nos puedan ocasionar problemas.

Es costumbre realizar un conteo de caracteres en tablas para ver si alguien ha realizado algún cambio no autorizado al contenido de las mismas despues del último cambio permitido. **[4]**

2.4 CLAVES Y JERARQUIAS DE ACCESO

El control de acceso lógico, es la protección a los datos almacenados o procesados en un formato magnetizado en una computadora o en un sistema de comunicación y al sotfware y hardware asociado.

El control de acceso lógico es una de las partes principales del programa de seguridad de la computadora. La seguridad total para una computadora incluye lo siguiente: una necesidad de proteger los datos y programas almacenados, o procesados en una computadora o en una red en contra de cualquier forma de pérdida; el acceso no autorizado o de modificación; las diferentes formas que deben ser usadas para proporcionar la confidencialidad y privacidad de la información, incluyendo impresiones y protección de documentos; la necesidad de proteger al usuario en contra de cualquier falla de comunicación o de procesamiento; y la capacidad de planes de recuperación o contingencia y procedimientos de respaldo. [14]

En general la mayoria de los paquetes de software de seguridad proporcionan, en mayor o menor grado, la seguridad lógica para un sistema de computación o para una red en sus cuatro principales áreas:

a.- Identificación de usuario
b.- Autentificación
c.- Autorización
d.- Vigilancia de la seguridad y reporteo

Los dueños de los sistemas que ya tienen la protección adecuada en cada una de estas áreas, probablemente no puedan justificar un gasto adicional para añadir software adicional. La justificación de la adquisición de este software no debe ser sumamente difícil cuando hay algo inadecuado en alguna de las siguientes áreas:

a.- Identificación de usuario y autentificación de clave.
b.- Nivel de autorización de control de acceso.
c.- Control de acceso en sistemas telefónicos.
d.- Reportes de herramientas autorizados al sistema.

e.- Facilidades que limitan el número de veces que una entrada al sistema no autorizada se permite antes de desconectarse al usuario.
f.- Facilidades de llamada y respuesta en una red telefónica.

No debe de sorprendernos el que el número de paquetes que se nos ofrezca para tener una seguridad lógica varie tan considerablemente. La variedad existente se debe a:

a.- El tipo de diseño del paquete dependiendo de la arquitectura de hardware y software en el que vaya a correr.
b.- Funciones primarias del sistema tales como tiempo compartido y procesamiento de transacciones.
c.- La cantidad de gasto que va a ser permitido.
d.- Los requerimientos de tiempo de respuesta del usuario.
e.- Los controles de acceso existentes.
f.- Número de usuarios.
g.- Sensibilidad del sistema.
h.- Tipo de acceso denegado y sistema de alarmas requerido.

Un paquete de software completo que satisfaga la seguridad lógica debe de contemplar los objetivos de las cuatro áreas básicas: identificación, autentificación, autorización y vigilancia y reporteo (ver figura 2.6).

La seguridad lógica debe de ser la primera línea de defensa en contra de algún usuario o transacción no autorizada. Para completar esto, el sistema debe de contener un mínimo de las siguientes tres funciones:

a.- Prevención.
b.- Detección.
c.- Reporteo de violaciones.

Conceptualmente, la mayoría de los sistemas de control protegen el acceso por uno de los siguientes tres mecanismos:

a.- Principio de default: el acceso no está permitido sin la autorización específica.
b.- Principio de respuesta activa: un archivo no está protegido a menos que un requerimiento específico se haya submitido por una protección especial.

c.- Principio combinado; los datos y recursos que no son sensibles pueden ser accesados por todos; sin embargo los datos y recursos con alto grado de sensibilidad pueden seguir inaccesibles por default.

Paquete típico para seguridad lógica.

FIGURA 2.6

Por lo general, la mayoría de los paquetes para tener una seguridad lógica incluyen herramientas que nos proporcionan lo siguiente:

a.- Verificación de entrada al sistema y de clave de usuario.
b.- Restricción de acceso a datos y recursos sensibles por operador, día, hora y otros criterios de protección.
c.- Protección de recursos y datos que puedan ser manipulados por terminales, equipos periféricos, archivos y programas.
d.- Proteccion de los datos de salida, de estructura de datos y campos y de otros recursos definidos por el usuario.
e.- Reporteo inmediato de violaciones de seguridad al sistema y preparación de reportes de violaciones de acceso.

En resumen, las principales diferencias que podemos encontrar entre los diferentes paquetes son:

a.- Facilidad de instalación.
b.- Controles administrativos.
c.- Mantenimiento.
d.- Documentación y soporte de entrenamiento.
e.- Capacidad de modificación.

Varios de los paquetes de control de acceso o seguridad lógica han sido puestos en el mercado, aproximadamente hace 10 años, existe un aumento de los testimonios de varios compradores que previenen de las debilidades y los beneficios de estos paquetes. Por lo tanto se deben de considerar estos testimonios para realizar la adquisición del paquete más adecuado. [14]

El control de acceso también considera más que problemas de acceso no autorizado a datos, porque muchos diferentes recursos pueden estar conectados directa o indirectamente a una computadora en particular. Impresoras locales y remotas, terminales, dispositivos de cinta o disco y dispositivos de comunicación, todos bajo un control lógico pueden ser usados para comprometer o abusar de un sistema.

Dentro de la seguridad lógica debemos de prestar especial importancia a los sistemas de transacciones en línea. La seguridad de los datos en un sistema de transacciones en línea requiere de un control central de acceso a los datos y restricciones en la utilización de terminales tal como lo describe LEE:

a.- Controles para el dueño del dato.- accesos retringidos a designados dueños de datos. Todo dato que pertenezca al sistema debe de tener asignado un código que indique su dueño. Este código se utiliza para verificar que el dato solicitado pertenezca a ese usuario.
b.- Controles de operador.- restringir a un operador de manera que sólo pueda realizar funciones especificas, en ciertas terminales y a determinadas horas.
c.- Controles de aplicación.- se tiene un acceso restringido a los datos necesarios para realizar los servicios que solicita la aplicación. Cada aplicación debe de trabajar como si fuera un sistema individual de seguridad.
d.- Controles de terminales.- restringir una terminal de manera que pueda realizar sólo las transacciones permitidas.
e.- Controles de operación y mantenimiento.- acceso restringido al sistema y al uso de comandos del operador. El sistema de seguridad debe de proporcionar controles para operaciones y comandos de mantenimiento. [10]

Existen tres métodos básicos por medio de los cuales se puede autentificar la identidad de una persona para el propósito de controlar el acceso a una computadora remota:

a.- Algo que la persona sabe.
b.- Algo que la persona tiene.
c.- Algo que la persona es.

El primero incluye claves y combinaciones. Las tarjetas de identificación, llaves y gafetes pertenecen a la segunda categoría. La tercera categoría incluye caracteristicas tales como la apariencia física de la persona, su voz, huellas digitales, firma y forma de la mano.

La autentificación puede ser requerida en muchos puntos del camino para el acceso a los datos. Estos puntos pueden ser:

a.- Entrada al edificio.
b.- Entrada al cuarto de terminales.
c.- Al prender la terminal.
d.- Unidad de encripción.
e.- Al firmarse.
f.- Acceso a archivos.
g.- Acceso a datos.

Los aparatos físicos (tarjetas y llaves) son usados en los tres primeros puntos y las claves en los tres últimos.

Las técnicas que se usarán en un sistema deberán ser determinadas por un análisis de riesgo-costo. Actualmente los sistemas de claves son más baratos que los demás y se pueden usar en combinación con otras técnicas.

Las claves son conjuntos de números, caracteres, palabras o combinaciones a las que se les debe dar entrada en el sistema para tener acceso a éste.

Esquemas de claves

Estos difieren de acuerdo a:

a.- Técnica de selección.
b.- Tiempo de vida.
c.- Características físicas.
d.- Contenido de información.

a.- Las claves pueden ser escogidas por el usuario o asignados a él. Las elegidas por el usuario no son seguras pues se tiende a escoger palabras o números que tienen algún significado especial y por lo tanto son fáciles de adivinar, pero tienen la ventaja de que son fáciles de recordar y no hay que escribirlas. Pueden ser asignadas por el oficial de seguridad o por el mismo sistema; aunque estas últimas generalmente son más seguras, sus beneficios pueden ser nulificados si son escritos, extraídos de una lista o generados por un algoritmo que se puede deducir. Un ejemplo de claves generadas por el sistema es el de Multics (Honeywell).

El generador aleatorio de palabras forma sílabas pronunciables y las concatena para formar palabras. Una tabla de reglas de pronunciación se utiliza para determinar la validez de la construcción. Esto se hace con el fin de que sea fácil de recordar. El generador de palabras aleatorio puede crear palabras de cualquier longitud pero se recomiendan palabras de cinco a ocho caracteres.

Otro método es asignar números que puedan ser asociados con objetos fácilmente visualizables. Por ejemplo, se puede asignar el número 2356, donde el vigésimo tercer objeto de una lista es un balón y el quincuagésimo sexto es una llanta. El usuario podrá formarse una imagen de su clave y podrá recordarla fácilmente si se pone una lista de objetos en cada terminal. La lista debe tener objetos suficientes para que no se puedan descubrir las claves por prueba y error.

b.- Las claves pueden ser asignadas por un periodo indefinido de tiempo, por intervalos predeterminados (un mes) o para una sola vez. Las claves que son efectivas en forma indefinida son especialmente vulnerables a pruebas exaustivas. Haciendo la longitud de la clave lo suficientemente grande, y dando tiempos para su captura se hace más difícil su descubrimiento. Es deseable que se hagan cambios frecuentes de las claves. Hay sistemas como el AFDSC (Airforce Data Services Center) que obliga a hacer esto cada seis meses. Las claves que se utilizan una sola vez proveen un mayor grado de protección. Las sucesivas claves pueden ser seleccionadas por el sistema de una lista interna, generada por un programa, o seleccionada de una lista distribuida previamente a los usuario autorizados.

c.- Incluye su tamaño y forma. El número de las claves diferentes en un esquema dado se llama el espacio de claves. Si se tiene una clave de longitud l y que se forma usando las 26 letras del alfabeto inglés existen 26^l posibles claves de longitud l que se pueden generar. El espacio de claves puede ser mayor si se permiten claves de hasta l caracteres, entonces el espacio de claves S

$$\text{es } S=\sum_{i=1}^{l} N^i$$

N= número de caracteres

d.- La clave puede proveer información adicional además de la autentificación personal. El sistema de información de la universidad del oeste de Ontario (GIRS) tiene claves asignadas cuyos contenidos revelan los niveles de autorización del usuario. En particular determinan:

- Que subconjunto de las funciones de proceso existententes pueden ser ejercitadas.
- Que porción de los registros pueden ser operadas por estas funciones.
- Con que registros puede trabajar el usuario.

En la figura 2.7 se muestra un cuadro con algunos sistemas de claves existentes en el mercado y sus características.

La lista de claves debe ser encriptada en algún código irreversible y ser transmitidas encriptadas también.

Un esquema de claves fuerte debe tener las siguientes características:

a.- Se debe de utilizar una sola vez.
b.- Debe ser generada por el sistema o asignada.
c.- Debe ser única.
d.- Debe tener mínimo 6 caracteres.
e.- Debe ser generada aleatoriamente.
f.- Debe ser almacenada encriptada.
g.- Debe ser encriptada para su transmisión.
h.- No debe ser desplegada a la hora de su captura. [21]

Existen también algoritmos que pueden ser usados en lugar de las claves o además de ellas. Con esto se pretende que el usuario realice tareas preescritas que sólo el puede llevar a cabo. Una técnica es una encuesta de acceso. El sistema le pregunta al usuario datos personales que teóricamente sólo el sabe, como por ejemplo el cumpleaños de su mamá, el nombre de una mascota, etc. Las preguntas son selecionadas aleatoriamente durante el proceso de entrada al sistema.

Otro método es dar algunos números al usuario previamente y pedirle algún cálculo con dichos números. Por ejemplo se le pueden dar tres número decimales como x, y, z. Durante el proceso de entrada se le proporciona al usuario dos operadores aleatorios α y ß que se deben combinar con los tres número anteriores, es decir xαyßz donde α y ß representan suma, resta, multiplicación o división. Por ejemplo, a un usuario se le proporcionan los números 5, 1 y 8 y se le presenta lo siguiente en el momento de su entrada al sistema:

x + y − z, el sistema esperará la respuesta −2. [5]

Una vez que la autentificación se ha llevado a cabo, se puede verificar la autoridad de un usuario, terminal u otro recurso con respecto a su petición.

Si una operación deseada está permitida, se dice que el solicitante esta autorizado a utilizar cierto tipo de información. Este tipo de información puede ser un archivo, un registro, un campo, una relación o alguna otra estructura. Si el acceso es permitido o no depende de varias cosas:

a.- Los privilegios de acceso del usuario.
b.- Los privilegios de acceso de la terminal.
c.- La operación solicitada.
d.- Los datos mismos.
e.- El valor de los datos.

Generalmente no se consideran todos los puntos anteriores. El sistema de seguridad mantiene un perfil para cada usuario, terminal, procedimiento u otros recursos que accesan a los diferentes tipos de información. Estos perfiles son construidos por un programa con privilegios especiales y se pueden representar con una matriz de autorización. Cada vez que un perfil es construido y cambiado se pueden tomar las siguientes acciones dependiendo de los datos:

a.- Retrasar la construcción/cambio un día.
b.- Retrasar la construcción/cambio hasta que otro usuario autorizado trate de hacer el mismo cambio.
c.- Retrasar la construccion/cambio hasta que un usuario especifico de la orden.

Matriz de autorización

Cada entrada A_{ij} en ésta matriz determina los derechos de acceso del recurso i-ésimo al recurso j-ésimo. Un ejemplo típico es el mostrado en la figura 2.8, donde terminales especificas tienen acceso a datos especificos.

En la figura 2.8 "01" indica privilegio de lectura, "10" privilegio de escritura, "00" no se permite el acceso y "11" privilegio de lectura y escritura. Además de leer y escribir existen otros privilegios como ejecutar, borrar y agregar.

Los elementos de la matriz de autorización generalmente contienen bits que representan operaciones que pueden ser realizadas en la terminal sobre algún tipo de dato. Si se quiere, los elementos pueden tener apuntadores a procedimientos. Estos procedimientos son ejecutados en cada intento de acceso en una terminal dada a un tipo de dato determinado y toman decisiones de acceso que no pueden ser fácilmente representadas en la matriz simple. Algunos ejemplos son:

Terminales \ Tipo de datos	Nombre empleado	Dirección empleado	Número de ID del empleado	Número de SS del empleado	Salario del empleado	Información de vehículo del empleado	Proyección de ventas de la corporación	Precio de artículos
Personal	11	11	11	10	11	00	00	00
Estacionamiento	00	00	00	00	00	11	00	00
Tesorería	01	00	01	01	11	00	00	00
Mercadeo	00	00	00	00	00	00	11	01
Compras	00	00	00	00	00	00	00	11
Investigación	00	00	01	00	00	00	00	01

FIGURA 2.8

a.- La decisión de acceso está basada en la historia de acceso de otros recursos: el usuario A puede escribir en el archivo F solo si no ha leído el archivo G.
b.- La decisión de acceso está basada en el estado dinámico del sistema: el usuario B puede abrir el archivo H solo en el momento en que la base de datos en la que se encuentra está abierta.
c.- La decisión de acceso está basada en el uso preescrito del recurso. Cuando un usuario llama a una rutina de ordenamiento para ordenar un archivo en particular, sus derechos para leer son mayores que los del usuario, pero la rutina no muestra los datos al usuario.
d.- La decisión de acceso está basada en el valor actual del recurso: un usuario no puede leer el salario de ningún registro de personal si este es mayor a $20,000.
e.- La decisión de acceso está basada en el valor de algunas variables internas del sistema: no se permite ningún acceso en un grupo particular de usuarios si no es entre las siete de la mañana y las siete de la tarde excepto que se use la terminal 72.

Usualmente la matriz de autorización es almacenada como un archivo cifrado aparte, y sus renglones son llevados a memoria principal cuando se les necesita. Los renglones de la matriz no son siempre terminales y las columnas registros o archivos. Los renglones pueden ser usuarios o grupos de usuarios, programas o subsistemas que necesiten acceso a algún dato. Las columnas pueden ser tipos de solicitudes.

Niveles de autoridad

La autorización puede estar también basada en un nivel de autoridad asociado con el recurso. Las solicitudes de acceso son denegadas a menos que el nivel de autoridad de la terminal y del usuario igualen o excedan el nivel de autoridad de la operación y/o del dato solicitado.
También se pueden combinar los dos modos. Por ejemplo, suponga que hay tres niveles sucesivos con mayores privilegios: confidencial, secreto y ultrasecreto. Suponga también que existen 16 categorías distintas de datos, C1, C2,.. C16. Luego, si la franquicia de un usuario es ultrasecreta y las categorías C1, C3, C4, C7, C13 y C14, y la franquicia de la terminal usada es secreta y categoría C11 y C14, el usuario tendrá solo acceso confidencial y secreto a la categoría C14 desde esta terminal.

Utilización de rutinas de entrada/salida para autorización

La mayoría de los compiladores de propósito general, si se encuentran con una solicitud de entrada/salida en un programa de usuario, generan una llamada a una rutina de la biblioteca de subrutinas del sistema. Esta rutina del sistema realiza la operación de entrada/salida requerida. La misma rutina puede ser programada para llamar a subrutinas de seguridad. Obviamente, para que esto sea efectivo, los usuarios no deben poder crear sus propias rutinas de entrada salida (ver figura 2.9). [7]

Rutinas de entrada/salida modificadas para implantar módulos de seguridad.

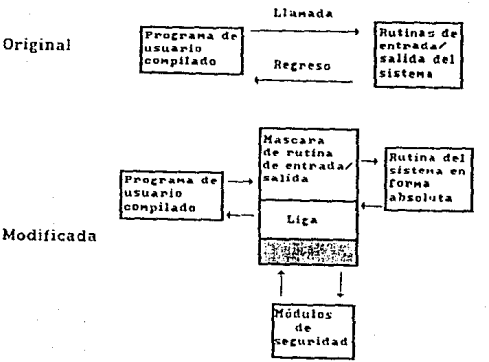


FIGURA 2.9

2.4.1 ASIGNACION DE CLAVES EN PROBURSA

En PROBURSA Casa de Bolsa, la autentificación de la identidad de una persona se realiza utilizando el método básico "Algo que la persona sabe", el cual incluye claves y combinaciónes.

Este método de autentificación es requerido a la hora de utilizar el sistema para poder tener acceso a programas, archivos y datos.

Dentro de PROBURSA Casa de Bolsa contamos con dos equipos de cómputo, el sistema 38 y el sistema 4381 de IBM. Para cada uno de estos sistemas se cuenta con un esquema especial de asignacion de claves y recursos a los que se tiene acceso, el cual será descrito a continuación.

Método de asignacion de claves para el sistema 38

La asignación de claves para los usuarios del sistema 38 la realiza la gerente de claves, de acuerdo al departamento al que pertenecen y a la jerarquia que tienen dentro de la institución, con lo cual se le asigna el menú al cual podrá tener acceso.

Por lo general cada uno de los departamentos de la institución tiene la siguiente estructura: dirección, subdirección, gerencia, auxiliares y asistentes (promotores, contadores, capturistas, analistas, programadores, etc.).

Para cada clave que se va ha asignar, se siguen los siguientes pasos:

a.- Verificar el departamento al que pertenece el usuario solicitante.
b.- Checar la jerarquía del usuario dentro de la institución para decidir a que información se le dará autoridad de lectura, escritura o borrado.
c.- Determinar a que menú se le dará acceso de acuerdo a los programas que tenga que utilizar.

Este esquema de claves no tiene un tiempo de vida determinado y su técnica de selección y asignación es departamental y jerárquica.

La composición de la clave del usuario es de una combinación de caracteres alfanuméricos que por lo general describen el área a la que pertenece. La clave con la cual tiene acceso a los programas es confidencial y entregada personalmente.

Debido a la cantidad de trabajo que tienen los ejecutivos de alto nivel jerárquico, es al personal de niveles inferiores al que se le da autoridad completa sobre los programas.

Este es el único caso en el cual se rompe todo el esquema de asignación de recursos de acuerdo a la jerarquía del usuario.

Método de asignación de claves para el sistema 4381

La asignacion de claves a los usuarios del equipo 4381, se efectúa en base a las funciones que realiza dentro de la institución.

La definición de clases y grupos se determina de acuerdo a las funciones desarrolladas por cada departamento. Y en base a esto se identificará dentro de que grupo y clase puede ser definido un usuario.

Para cada una de las clases y grupos, se desarrollan procedimientos por medio de los cuales se le da acceso a los usuarios a los recursos que pueden utilizar.

La identificacion de usuarios, de grupos y de clases se realiza de la siguiente forma:

a.- Usuario.- la identificacion para el sistema de seguridad es de 5 caracteres alfanuméricos, utilizando el siguiente estándar:

aaiii

donde

- aa = identificación del área a la que pertenece el usuario.
- iii = iniciales de nombre y apellidos del usuario.

b.- Grupo.- para la identificacion de grupos se utilizan 5 caracteres alfanumericos.

En el caso de grupos definidos por un administrador de grupo o usuario de un grupo, el nombre del grupo que se crea tiene el siguiente formato:

ggggcccc

donde

- ggggg = cualquier grupo de 6 caracteres alfanuméricos.
- ccc = número consecutivo dentro del área.

Para la asignacion y la definición de grupos, no se permiten nombres duplicados.

c.- Clase.- se utilizan 7 caracteres alfanuméricos para su definición. En caso de clases definidas por nombres genéricos, al menos el primer carácter debe ser alfabético.

La herramienta utilizada en el equipo 4381 para la asignación de claves es RACF (Resource Access Control Facility). Esta herramienta de control de acceso a los recursos nos proporciona las siguientes facilidades:

a.- Acceso al sistema por:

- Usuario.
- Area.
- Sucursal.
- Ubicación.

b.- Mantenimiento de clave de acceso.

c.- Restricción de acceso por:

- Dia y hora.
- Registro de intentos fallidos.
- Programa.
- Subsistema.
- Transacción.

d.- Autorización de acceso por subsistema:

- Utilizando TSO (Time Sharing Option) se puede tener acceso por:

  . Usuario.
  . Area.
  . Sucursal.

e.- Restricción de terminales por:

- Usuario.
- Area.
- Sucursal.

f.- Autorización para ejecución desde:

- TSO.
- Un programa en particular.
- Un grupo de programas.
- Algún plan o grupo de planes.
- CICS (Customer Information Control System).
- Una transacción o grupo de transacciones en particular.

g.- Acceso a información por:

- Volúmen.
- Grupos de volumenes.
- Archivo de CICS, TSO o DB2.
- Catálogos.
- Tablas de la base de datos.
- Bases de datos.
- Vistas de la base de datos.

2.5 AUDITORIA

Otro punto importante que se debe tener en cuenta si se quiere tener buen nivel de seguridad en una organización, es la auditoria a la gestión de informática. Esta evalúa el nivel de control interno y analiza el desarrollo de todas las actividades del centro de infromática, tanto para el desarrollo y el mantenimiento de aplicaciones, como para la explotación de su información. En la orientación actual de la auditoria a la gestión de infromática se destacan dos aspectos:

a.- El impacto que tienen las funciones de informatica y de auditoria en las organizaciones por su nivel de dependencia; asi como los recursos de que se dispone, las necesidades que se plantean y particularmente para auditoria la orientación que da a sus intervenciones en el ámbito informatico.
b.- La amplitud que constituye el horizonte de intervencion del auditor dado que los distintos ingredientes de la gestión de infromática, con las actividades y recursos que la constituyen, son susceptibles de ser auditados.

El ámbito informático, es una de las entidades de cualquier organización que más rápidamente se desarrolla modificando su estructura interna e impactando en general a la organización, por la virtud e importancia que tiene cada dia más la automatización de sistemas y los rápidos desarrollos tecnológicos que frecuentemente se van liberando.

Ello dificulta la identificación de metodologias orientadas a precisar "como" llevar a cabo la auditoria de la gestion de informática, porque su vigencia invariablemente dependerá de la permanencia del tipo de actividades y elementos informáticos a que se refiere. Sin embargo, por otro lado se hace necesario plantear el uso de estructuras que permitan la ubicación conceptual y la aplicación práctica de los distintos tipos de intervención, sus objetivos y el tipo de resultados a obtener.

Para algunos gerentes de procesamiento de datos, la auditoria en informática es la actividad que les va a identificar los problemas técnicos y eventualmente operativos, que ellos por su posición en la organización se ven limitados a observar; en ocasiones esperan que el auditor determine si los planes de acción y desarrollo de informática, se mantienen acordes a las necesidades y circunstancias por las que atraviesa la organización.

En otras ocasiones, algunos gerentes financieros o contralores consideran que bajo este tipo de auditoria se formularán diagnósticos para determinar si el manejo de información financiera y operativa, esta protegida contra errores o incongruencias, o si los sistemas estan resguardados contra malversaciones y fraudes.

En ciertos casos, los directores generales o administrativos consideran que el propósito de estas intervenciones, consiste en definir las condiciones de protección y seguridad física que guardan los recursos informáticos en los sistemas de información ante posibles contingencias de pérdidas y/o destrucciones, para restablecer el servicio de cómputo de la organización, por fallas que pudieran suspender dichos servicio, una hora, un día, un mes o permanentemente.

En los planteamientos anteriores, se observa que todas y cada una de las interpretaciones son importantes aunque disimbolas por sus distintos planos de intervención.

Este hecho, llevó a J. M. Lazcano a proponer en la decimotercera conferencia interamericana de contabilidad, un esquema de intervención que denominó "Matriz para plantear la concepción de auditoria PED" (Proceso Electrónico de Datos), con el fin de precisar y dejar sentada una estructura que permitiera ubicar la interpretación de este tipo de intervencion por parte del auditor en informática.

De esta forma, se presentó una definición matricial integrada por dos factores: uno de trazo horizontal que identifica todas las actividades tipicas que se relizan en el área de informática y en el que la amplitud queda determinada por todas las labores susceptibles de revisión; y otro factor de trazo vertical que establece gradualmente la profundidad técnica donde es factible conducir este tipo de intervenciones y que se segmentan en tres niveles, estos son: administrativo, operativo y técnico.

Respecto a la segmentación horizontal, podemos observar que el primer nivel persigue determinar la funcionalidad administrativa con que se manejan los recursos y se desarrollan las labores del centro de infromática; el segundo nivel, persigue determinar la funcionalidad operativa; y el tercero, la funcionalidad técnica, apoyándose en los siguientes elementos:

Para el primer nivel se consideran:

a.- Integración.
b.- Organización.
c.- Disposición presupuestaria.
d.- Condiciones de seguridad.
e.- Protección física de la instalación.
f.- Manejo de recursos humanos.

Para el segundo nivel, los elementos basicos se fundan en:

a.- Manuales de procedimeintos.
b.- Mecanismos de control de calidad.
c.- Registros.

Para el tercer nivel, los elementos a considerar son:

a.- Caracteristicas técnicas de funcionamiento de cada uno de los equipos.
b.- Aprovechamiento de las facilidades automáticas incorporadas en dichos equipos.

Para que esta estructura matricial logre sus beneficios, debe integrarse con los aspectos particulares existentes en la organización en el momento de la intervención , y considerar los elementos y caracteristicas del equipo con que trabaja la instalación. En la intersección de los dos trazos se obtiene la identificación de aspectos o módulos particulares que pudieran representar un enfoque único de intervención. En caso de que se deseara considerar toda una linea de trazo vertical, se podría determinar el manejo funcional de ésta, abarcando todos los aspectos adminstrativos, operativos y técnicos relativos a dicha función; por último, englobando toda una línea de trazo horizontal, se podría determinar bajo ese nivel el desempeno de la gestión informática determinada.

El resultado de esta conjunción, genera una estructura semejante al de la figura 2.10.

Matriz de auditoría en informática.

Función / Nivel	Captura de datos	Control de calidad	Operación y explotación	Soporte técnico	Diseño de sistemas	Programación y mantenimiento
Administrativo	Integración y organización de personal. Seguridad y protección. Comunicación					
Operativo	Manuales y procedimientos. Control de calidad. Registros de productividad.	Procedimientos específicos. Reg. validación y verificación. Calendarización. Distribución de información.	Procedimientos y estándares. Reg. en uso y producción. Calendarización y prioridades. Nivel de servicio.	Procedimientos y estándares. Asignación de recursos. Prioridades.	Políticas y procedimientos. Actividades y recursos. Impacto, desarrollo y operación.	Estándares y procedimientos. Documentación. Uso de compiladores. Control de presupuestos. Actividades y recursos.
Técnico	Manuales y estándares técnicos. Capacidades y crecimiento.	Respaldo por diseño y copias. Supervisión en operación.	Respaldos de procesos. Asignación de recursos.	Uso del hardware y del software.	Estándares de diseño técnico.	Uso de bibliotecas. Revisión y aceptación.

FIGURA 2.10

Redundando en las principales ventajas que la definición matricial proporciona, destaca la identificación de objetivos y enfoques con que se pueden encausar las intervenciones, principalmente en:

a.- La definición e integración de programas de auditoría enfocados directamente a aspectos de índole administrativo, operativo o técnico, con el fin de estructurar la ejecución de auditorías integrales, modulares, paralelas o específicas, presentándose casi de manera natural los alcances, elementos y procedimientos de auditoría a utilizar.

b.- La identificación de una estructura gradual para incorporar los conocimientos necesarios, que pueden ser adquiridos por el propio personal con el consiguiente plan de capacitación y asignación de tiempo para ello; o con la integración de personal que cuente con los conocimientos requeridos para la más rápida aplicación de los mismos.

c.- En aquellas ocasiones que por razones de índole económico o técnico, no se justifica la integración de conocimentos técnicos específicos de manera permanente, da lugar a identificar con más precisión la posibilidad de contratar asesorías para apoyar específicamente el ámbito de intervensión del auditor, lo que le permite a éste establecer los lineamientos que deberán dar curso a su trabajo, y al asesorado identificar el tipo de producto-servicio que habrá de recibir.

Las principales limitaciones que la definición matricial puede tener son la subestimación de recursos o labores que llegan a considerarse de bajo rango o poca trascendencia, o la sobreestimación de elementos técnicos a los que le pudiera otorgar una importancia sobrada de la que realmente tienen.

Bajo estas consideraciones, es importante revisar periódicamente la estructura definida y hacer un aprovechamiento de las experiencias logradas ya que tal no puede ser definida con criterios de permanente.

También es importante para la parte de auditoría llevar un registro de todas las operaciones que se ejecutan dentro de los sistemas de la organización así como de ser posible quien las llevó a cabo y cuando. Esto es para tener una huella a

seguir en caso de que se haga mal uso de dichos sistemas, y poder saber quien y como lo realizó. Y esto permite a su vez evitar que vuelva a suceder pues se enmienda tal falla en los sistemas. [13]

2.6 PROTECCION DE DOCUMENTOS

Una parte crítica de cualquier sistema de clasificación es el etiquetar físicamente los documentos o los medios que contengan datos sensibles. La enorme cantidad de impresiones de la computadora más el gran número de dispositivos de almacenamiento hace que la clasificación sea un verdadero reto. Un buen sistema de clasificación debe incluir también todos los datos que pueden ser observados desde una terminal o una computadora personal.

Existen muchas variaciones de las reglas para etiquetar los documentos o las impresiones para tener un control sobre su acceso. Un buen procedimiento para etiquetar debe de especificar lo siguiente:

a.- La total clasificación del documento tanto en su primera página como en la última.
b.- Notas especiales de seguridad, si se requieren.
c.- Notas especiales de acceso, si se requieren.
d.- Identificación de todos los datos clasificados y no clasificados con el documento. [14]

Medio magnético

Los medios magnéticos, discos y cintas, que contienen los archivos y programas de la organización siempre tienen riesgo. Riesgo de que se pierdan por fuego, humo, agua, contaminación y robo. Aparte de los discos y las cintas que se estén usando, debe de haber un respaldo en alguna caja de seguridad que, de preferencia, esté ubicada fuera de la sala de cómputo. El acceso tanto a la cintoteca como a la discoteca debe de estar restringido únicamente para el personal encargado. El área o sala en donde se almacenen las cintas o discos debe tener de preferencia su propio sistema de protección contra incendios.

Las copias de respaldo de los archivos deben de estar seguras dentro de alguna caja de seguridad fuera de la sala de cómputo en caso de una pérdida total del sistema.

a.- Todos los medios magnéticos deben de guardarse en la cintoteca o discoteca, según sea el caso, claramente etiquetados con su clasificación y fecha de almacenamiento.
b.- La clasificación de las etiquetas magnéticas se debe realizar internamente. [10]

Todos los demás medios tanto de salida como de entrada deben ser etiquetados debidamente. [14]
Ninguna instalación de computación puede sobrevivir por mucho tiempo sin una adecuada documentación. Toda la documentación vital debe de estar protegida para evitar su pérdida por causa de un incendio. Debe de haber operaciones adecuadas, especificaciones de programas y sistemas para cada aplicación y paquete de software.

Un método efectivo es utilizar algún sistema de documentación en una computadora de manera que toda nuestra documentación esté protegida, al igual que cualquier otro archivo en medios magnéticos.

De esta manera se puede hacer un respaldo automático de la documentación y lo que es mejor se puede modificar y tener al día. [22]

Seguridad de listados

A continuación presentaremos varias técnicas con diferentes grados de efectividad.

Ubicación de consolas e impresoras. Cualquier dispositivo que produzca una salida debe de ubicarse de manera que la información que se tenga no sea vista por personas que no tienen acceso a ella. Esto es de particular importancia cuando nuestra sala de cómputo tiene paredes de cristales.

Cajas para impresiones. No es necesario que los operadores que se encuentran en la sala de cómputo vean lo que se está imprimiendo o lo que ha sido impreso. De manera que el ir llenando una caja con los listados ya impresos e irla sellando cuando se llene puede ayudar a prevenir que accidentalmente sean vistos.

Plantilla para interpretación de la impresión. Este método es particularmente barato y efectivo para preservar la confidencialidad de las salidas de impresión, especialmente cuando los datos son numéricos. Unicamente las partes que varían de la salida, usualmente figuras y fechas, son impresas y su interpretación depende de la plantilla a utilizar. Por lo general está impresa y esto puede ser un código o alguna palabra clave. Las plantillas obviamente deben de estar guardadas bajo llave.

Una extensión de esta técnica es el imprimir caracteres seudoaleatorios en todas aquellas posiciones en las que falte algún carácter de manera de esconder los caracteres útiles. Pero para esta técnica se debe de tomar en cuenta el tiempo extra de impresión y de programa que se requiere. La protección que esta técnica nos proporciona aumentaría si se cambiaran con cierta frecuencia las plantillas. [6]

2.7 ESTANDAR DOD (DEPARTAMENTO DE DEFENSA)

El Departamento de Defensa de los Estados Unidos de Norteamérica generó el siguiente estándar que nos muestra los niveles dentro de los cuales se pueden clasificar a los sistemas de computo confiables.

El Departamento de Defensa se basa en estos niveles para certificar el tipo de seguridad que tiene cada sistema.

El aumento de seguridad va del nivel D1 al nivel A1. Este último es el nivel que tiene mayor seguridad

Niveles para sistemas de cómputo confiables:

- D1.- Incapaz de alcanzar el nivel C1.

Los niveles C1 y C2 se conocen como discrecionales

- C1.- Acceso discrecional (a elección)

    . Acceso discrecional.
    . Identificación y autentificacción.
    . Documentación (diarios).

- C2.- Protección controlada de acceso

    . Auditoria.
    . Responsabilidad de objetos.
    . Reutilización apropiada de los objetos.

Los niveles B1, B2, B3 y A1 son niveles

- B1.- Acceso mandatorio (obligatorio)

    . Etiquetas de archivos.
    . Caminos confiables al sistema.
    . No hay residuos.
    . No se tiene informe de defectos.

- B2.- Protección estructurada

  . Protección estructurada.
  . Análisis secreto de canal.
  . Recuperación confiable.
  . Modelo formal de política.

- B3.- Dominios de seguridad.

- A1.- Diseño verificado

  . Diseño verificado (Especial/Modelo).
  . Control de configuración riguroso.
  . Controles distribuidos.

Los proveedores de mecanismos de seguridad actualmente están tratando de cumplir con estos estándares en el desarrollo de sus sistemas. Ya que estos serán los niveles de seguridad que las empresas norteamericanas, el mayor mercado para este tipo de sistemas, estarán buscando de hoy en adelante.

3

RESPALDO Y RECUPERACION

3.1 GENERALIDADES

En toda organización es muy importante tener en cuenta el costo de no poder usar el sistema de cómputo en un determinado momento y todas las consecuencias que ésto implica. Para algunas empresas como por ejemplo las del sector financiero, el no contar con el sistema de cómputo significa prácticamente no poder dar servicio a su clientela, es decir no operar mientras ésto ocurra. Esto significa una gran pérdida no sólo en ganancias, si no en imagen de la empresa que es a veces tan importante como lo primero. Por ello se debe considerar con mucha seriedad el que ésto ocurra y se deben tener muy claras las medidas a tomar en esta situación.

Debe existir un plan de recuperación escrito en el cual se tengan todas aquellas situaciones que pueden ser consideradas como un desastre y la manera de recuperarse de esas situaciones para la empresa. Este plan debe ser más que un libro gordo en la biblioteca, debe contener los procedimientos diarios que se deben de utilizar para situaciones de emergencia, y los procedimientos ya probados que pueden ser utilizados si el centro de cómputo fuera destruido o si no estuviera disponible para procesar la información vital de la organización.

El crear este plan de recuperación requiere de una persona dedicada a realizarlo por un largo tiempo, al igual que especialistas de medio tiempo de varias áreas de la empresa.

Las interrupciones y los desastres pueden ser definidos en términos de daños al equipo o a ciertas facilidades, indisponibilidad del sistema, o consecuencias dañinas para la empresa. La National Bureau of Standards sugiere tres categorías:

a.- Pérdida limitada de la capacidad.
b.- Interrupción de operaciones con poca o ninguna falla de servicio.
c.- Una gran falla o destrucción del servicio y del contenido.

La pérdida limitada de la capacidad implica que sólo algunos sistemas fueron los afectados. Es decir que la falla no implica quedarnos sin el sistema, pero nuestro tiempo de respuesta puede no ser tan bueno como antes.

Como ejemplo podemos citar cuando el CPU de nuestra máquina de producción falla y es necesario que entre como respaldo nuestra máquina de desarrollo la cual es más pequeña y no ofrece el mismo tiempo de respuesta.

Este tipo de falla puede ser ocasionada por:

a.- Falla de algunas unidades de hardware como controladores de discos, impresoras.
b.- Pérdida parcial de aire acondicionado.
c.- Pérdida parcial de algún equipo de comunicación o de algunos circuitos.
d.- Pérdida temporal o falla de algunos datos o programas claves.

Interrupción de operaciones con pequeña o ninguna falla, por un periodo corto de tiempo el cual no tenga un impacto significativo para la empresa. Una interrupción, como una falla total de la fuerza eléctrica, o del aire acondicionado detiene las actividades de procesamiento.

Sin embargo una vez que se restablece el sistema de energía eléctrica o el de aire acondicionado, si no ha existido una falla significante, las operaciones se pueden reanudar dando prioridad a las aplicaciones críticas para el sistema.

Este tipo de falla puede ser ocasionada por:

a.- Falla del equipo de comunicaciones o del computador principal.
b.- Incendio pequeño.
c.- Humo, polvo o suciedad.
d.- Evacuación causada por una alarma de bomba o alguna fuga de gas.

Falla mayor de alguna facilidad o del equipo, puede ser el desastre del centro de cómputo pero no de la organización. La recuperación de las operaciones y de las aplicaciones que son críticas para la empresa son un factor que ayuda a reducir las pérdidas de la misma.

Este tipo de fallas pueden ser ocasionadas por:

a.- Incendio en la sala de cómputo.
b.- Un temblor, terremoto, tornado.
c.- Una explosión de una bomba o el choque de un avión.
d.- Contaminación por radioactividad o material tóxico.

De todo lo anterior podemos concluir que un desastre es la total indisponibilidad para el procesamiento de los datos por un período de tres o más dias, o como la total destrucción de los datos.

Una aplicación critica es aquella que sin su operación la empresa no puede sobrevivir, como un proceso batch (en lote) o algún sistema en linea. Esta puede ser utilizada para expresar las consecuencias reales para una organización cuando sus capacidades de procesamiento son interrumpidas.

El establecer e identificar prioridades en las aplicaciones criticas para la empresa puede ser una de las tareas más difíciles de desarrollar en un plan de recuperación de un desastre. Establecer prioridades para la recuperación de aplicaciones puede ser realizado después de que han sido identificados los sistemas y se han cuantificado las consecuencias de su indisponibilidad.

También existen sistemas que no es necesario ponerlos en servicio inmediatamente para asegurar la sobrevivencia de la organización (DISCRECIONALES), pero que deben de ponerse en servicio después de un periodo corto de tiempo para mantener la operación de la organización. Los sistemas NO ESENCIALES son aquellos que pueden quedarse en un anaquel por un tiempo sin tener un impacto significativo para la empresa.

El conocer que sistemas son criticos y que requerimientos de procesamiento tienen, permite a la organización evaluar varias alternativas de procesamiento en caso de algún desastre:

a.- Un centro de cómputo alterno, ubicado lejos del ya existente.
b.- Contratar los servicios de alguna compania que ofrece servicios de procesamiento con cierto cargo a la empresa.
c.- Tener algún arreglo recíproco entre dos organizaciones independientes que proporcionen un respaldo del servicio. **[16]**

Es esencial el guardar registros de manera que los principios de seguridad de todo departamento de procesamiento de datos se pongan en práctica. Los diarios proporcionan un registro cronológico de eventos a los cuales se les puede atribuir ser causantes de una violación a la seguridad. Los archivos de respaldo hacen posible la recuperación debida a errores catastróficos o algún malfuncionamiento. La documentacion también es un factor muy importante, el cual nos describe detalladamente el desarrollo de procedimientos y protecciones. [4]

3.2 DIARIOS

Los Diarios deben de contener la actividad que toma lugar en una consola de operador, en la consola del oficial de seguridad, si éste existe, de las cintotecas, de las discotecas y de los servicios prestados a terminales.

Consola del operador

Los siguientes eventos en especifico deben de ser registrados en la consola del operador:

a.- Encendido de la computadora.
b.- El ambiente de equipo que se tiene configurado y en uso.
c.- La carga inicial de programa (IPL), iniciación del sistema.
d.- Corridas de programa de mantenimiento o pruebas de rutina.
e.- Inicio de programa o serie de programas.
f.- Finalización normal o anormal de un trabajo.
g.- Fallas de paquetes de software del sistema o fallas del equipo.
h.- Caída normal o anormal de la computadora.
i.- Pérdida de tiempo de producción. Lo cual puede ser ocasionado por una reparación de hardware, mantenimiento o reconfiguración; mantenimiento de software; o desarrollo de algún programa nuevo.
j.- Mensajes de error impresos por la computadora.
k.- Consultas no usuales de archivos clasificados.
l.- Montaje de medios removibles (cintas).
m.- Intervenciones del operador en programas de usuario.
n.- Trabajos o tareas del operador.
o.- Presencia de visitas en la sala de cómputo.

Terminales y Diarios de entrada/salida

Lo siguiente es una lista de actividades que deben ser registradas en terminales remotas. En algunos casos estos eventos son registrados automáticamente por la computadora.

a.- Identificación de usuario.
b.- Procedimiento de entrada al sistema, con la clave no desplegada.
c.- Salida del sistema o finalización de algún trabajo, elevando una contabilidad de tiempo de procesamiento y de utilización de núcleo.
d.- Fecha y hora de inicio de trabajo.
e.- Fecha y hora de finalización de un trabajo.
f.- Designación de línea o cola de impresión.
g.- Designación de terminal.
h.- Rutinas de comunicación.
i.- Sistemas operativos y computadoras utilizadas para el procesamiento de un trabajo.
j.- Programas y subrutinas llamadas y la clasificación de seguridad de cada una.
k.- Archivos de datos accesados y la clasificación de seguridad de cada uno.
l.- Identificador único del trabajo con un día de inicio y clasificación.
m.- Identificación de archivos de datos o programas, creados o destruídos en la ejecución de un trabajo así como su clasificación de seguridad y su tamaño.

Diarios de bibliotecas de medios magnéticos

La persona encargada de la cintoteca o discoteca debe de estar al pendiente de que se lleve el registro en la fecha, hora y circunstancias de los siguientes eventos:

a.- Adquisición de algún artículo para la biblioteca ya sea de software o de hardware.
b.- Destrucción o borrado de medios magnéticos de procesamiento de datos o documentación.
c.- Supresión de los medios de procesamiento de datos o de documentación.
d.- Cambio del lugar de almacenamiento de medios magnéticos o de documentación.
e.- Extracción de artículos de la biblioteca y su subsecuente retorno.
f.- Cualquier cambio de dueño de algún artículo del departamento de procesamiento de datos, ya sea documentación o algún medio magnético.
g.- Cualquier cambio en la clasificación de seguridad de medios magneticos o de documentaciones.

Diarios de consola de seguridad

Si existiera la consola del oficial de seguridad, ésta debe de ser capaz de registrar cualquier evento de seguridad. Estos registros deben de incluir:

a.- Identificacion del usuario culpable.
b.- Identificacion de la terminal en la cual se cometio la infraccion.
c.- Tipo de seguridad violada.
d.- Dia y hora en que ocurrio el incidente.
e.- La identificacion y la clasificacion de seguridad de todos los programas o archivos de datos involucrados en el incidente. [4]

3.3 RESPALDO DE ARCHIVOS

Es un principio de buena seguridad el que, para cualquier recurso de información, exista el suficiente respaldo de manera que, si se perdiera o se borrara éste pudiera ser reconstruido. Esta reconstruccion debe de ser capaz de realizarse a cualquier hora de acuerdo a los procedimientos preestablecidos.

La informacion y material necesario para implantar un procedimiento de respaldo nunca debe de estar expuesta a los mismos riesgos que la información original. Debe de ser regularmente modificada, de manera que refleje el mismo estado que la original y debe de tener el mismo nivel de protección.

Respaldo especifico

Las siguientes especificaciones se deben de realizar en conjunto con el respaldo de datos, programas y archivos:

a.- Los documentos de entrada y copias de salida que vayan a ser almacenados se deben almacenar en microfichas o microfilms.

b.- Se deben de guardar dos copias de cada archivo, ya sea en cinta magnética o disco.

c.- Todos los programas y los datos almacenados en memoria secundaria, deben de ser respaldados utilizando medios removibles. [4]

3.4 REINICIO Y RECUPERACION

En todo archivo que vaya a ser procesado se deben de establecer puntos de reinicio. Los procedimientos de recuperación deben de ser implantados en todo programa de procesamiento de datos. Esto se hace con el objeto de que si hubiera alguna falla de software o hardware o algún error en los datos o procedimientos de operación no se tuviera que regresar al inicio y volver a procesar todo. El trabajo podría reiniciarse en el punto de reinicio antes de la falla. A esta operación se le llama "retroceder" o "fallback".

Se debe de mantener un archivo journal o histórico de todo archivo que vaya a ser procesado, y este debe contener una imagen de todos los cambios hechos a los registros. Se debe de guardar la imagen de los registros antes y después de ser modificados ya que esto facilita la recuperación hacia atrás "roll-back" o hacia adelante "roll-forward".

Es muy común que desde una terminal se modifiquen directamente los archivos a las bases de datos. A esta operación se le conoce con el nombre de actualización en el lugar "update-in-place". Cuando esta técnica está implantada es esencial que el correspondiente archivo histórico se mantenga y que contenga imágenes de todos los registros antes y después de ser alterados o borrados y que además contenga una copia de las que fueron creadas.

En cualquier momento en el cual un archivo es transmitido por un enlace de telecomunicaciones, se debe de mantener una copia de lo que se transmitió hasta que el receptor nos indique que ya lo recibió.

Recuperacion de una falla

Cuando el reinicio y la recuperación se inician después de una falla de hadrware o de software, se deben de tener todos los siguientes datos para que ayuden en cualquier investigación subsecuente:

a.- Se debe de tomar una copia imagen de el contenido de la memoria principal, o un "dump".
b.- Recargar el sistema operativo a manera de restablecer el servicio satisfactoriamente y registrar cuanto fue lo que se tuvo que recargar.
c.- Determinar la condición de todos los archivos.
d.- Condición de los archivos con la información clasificada y archivos protegidos.

Recuperación de una violación

Cuando el procesamiento es interrumpido debido a que se percibió una violación de la seguridad, se debe de juntar la siguiente información:

a.- Identificacion del usuario responsable.
b.- Identificación de todos los programas y archivos involucrados.
c.- Tipo de violación de seguridad.

Enseguida se debe de sacar un vaciado de la memoria para ver que espacios de direccionamiento, "address space", fueron dañados. Tomar las medidas apropiadas para prevenir que los usuarios dañados entren al sistema antes de que el coordinador de seguridad les de autorización.

Retención de registros

Una pieza de retención de registros debe de existir. Esta poliza depende del tipo de negocio o actividad que desempeñe la compañia. Cualquier registro que no entre dentro de lo establecido debe de ser marcado con la fecha en la que tiene que ser borrado o destruido.

Documentación.- Se debe de tener una documentación al dia de todo lo que tenga que ver con:

a.- Programas del sistema (sistema operativo).
b.- Programas de utilerías del sistema (ordenamientos, edición, etc.).
c.- Programas permanentes (paquetes estadisticos, etc).
d.- Programas de aplicación (nomina, contabilidad, tesoreria, etc.).

e.- Procedimientos de operación del sistema.
f.- Instrucciones para la preparación de datos.
g.- Interconexión de hardware en el sistema.

Para todo tipo de documentación, un registro de inventario perpetuo nos debe de mostrar:

a.- Identificador.
b.- Descripción.
c.- Tipo de medio utilizado.
d.- Identificación del medio utilizado.
e.- Ubicación.
f.- Gerente responsable.

Cuando menos una vez al año todo centro de cómputo debe de identificar físicamente la documentación que mantiene y verificar su registro en el inventario. La documentación que ya no tenga vigencia se debe de destruir de una manera segura. Todo documento que vaya a ser modificado debe de tener una tarjeta en la cual se puedan registrar todos los cambios realizados y el nombre de la persona que los realizó.

Listas e inventarios

Todo centro de cómputo debe de tener listas e inventarios de manera que pueda llevar una contabilidad de sus necesidades. Las listas deben estar continuamente actualizadas por el personal del centro de cómputo; de control de acceso, identificación; garantías y pólizas de seguros.

Inventarios.- Se debe de tener una continua y perpetua actualización de inventarios de todos los siguientes puntos:

a.- Cantidad de papel para imprimir.
b.- Publicaciones.
c.- Software, incluyendo sistema operativo, utilitarios, bibliotecas permanentes y programas de aplicación.
d.- Documentación, incluyendo documentación de programas, instrucciones, procedimientos, manuales de todo tipo e infromación concerniente a la interconexión de hardware.
e.- Programas y archivos de datos.
f.- Medios de procesamiento de datos.
g.- Equipo de procesamiento de datos.
h.- Medios magnéticos no utilizados y partes de repuesto.

Papel de impresión negociable.- Todo papel de impresión que sea de tipo negociable debe de llevar el número de serie consecutivo al igual que su copia. Este tipo de papel debe de ser revisado antes y después de cada impresión para efectos de inventario.

Documentos de contabilidad.- Todo documento de contabilidad debe de ser revisado ante la presencia del personal de contabilidad cuando menos una vez al día. Este tipo de verificación no debe de realizarse siempre a la misma hora, sino que debe de hacerse de manera aleatoria.

Componentes de software.- Para cada copia de todo componente de software, un registro de inventario nos debe proporcionar:

a.- Identificador.
b.- Descripción.
c.- Tipo de medio utilizado.
d.- Identificación del medio utilizado.
e.- Ubicación.
f.- Clasificación de seguridad.
g.- Gerente responsable.

Cuando menos cada seis meses se debe de realizar una identificación física del software que se tiene y verificar los registros de inventario.

Programas y archivos de datos.- Deben de ser revisados cada 3 meses observando que cumplan con todos los requerimientos.

Medios de almacenamiento.- Todo medio de almacenamiento que ya no sea utilizado debe de ser borrado de una manera segura. Además debe de ser posible el tener referencias cruzadas (en cualquier momento, entre los medios de almacenamiento y sus correspondientes programas y archivos de datos).

Se debe de ser capaz de decir que es lo que tiene cada cinta sin necesidad de vaciar la información que tiene.

Equipo de procesamiento de datos.- Cuando menos una vez al año el centro de cómputo debe de identificar físicamente todo el equipo que tiene.

Al tiempo de realizar el inventario, se debe de revisar la ubicación física y la interconexión del equipo. Esta debe de ser comparada con la última configuración que se tiene del sistema y toda diferencia debe de ser corregida y revisada.

Sistema de respaldo

Lo que se debe de hacer en caso de que ocurra una emergencia es proporcionar operacion de emergencia al lugar principal, proporcionar registros de almacenamiento y hacer todos los preparativos para utilizar un sitio alterno en caso de que el primero este destruido o dañado.

Plan de contingencia

En todo plan de contingencia se deben de considerar las siguientes condiciones de emergencia:

a.- La sobrecarga de trabajo requiere de horas extras fuera de las horas de trabajo.
b.- Fallas catastróficas de hardware o de equipo de soporte.
c.- Falla catastrófica del programa de control.
d.- La reducida carga de trabajo provoca que se reduzcan las horas de trabajo.
e.- Operación con uno o varios componentes de hardware dañados.
f.- Huelga, ausencia del personal o motín.
g.- Incendio, inundación, bomba, temblor, derrumbe del edificio.

La parte más importante de todo plan de emergencia es el designar a la persona que tiene todo el poder de decir que hay una emergencia y escoger a la persona sustituta en caso de que la persona designada no esté disponible o esté incapacitada.

Decidir que personal va a ser requerido para proporcionar un nivel mínimo de servicio esencial. Designar a estas personas como parte del personal crítico ocupando posiciones críticas y tratándolos como miembros del primer equipo. Informar a todo el personal crítico de sus tareas de emergencia y darles el entrenamiento necesario para las mismas.

Si dentro del plan de contingencia se tiene el llevar los trabajos de procesameinto de datos a otros centros de cómputo, se debe estar seguro de que estos centros tengan cuando menos el mismo nivel de seguridad que se tenia en el centro de cómputo primario. Después de esto se debe de mandar a algún empleado a que observe que los trabajos tengan la protección necesaria.

Toda la información esencial y el material que no pueda ser duplicado y almacenado fuera del centro de cómputo debe de ser etiquetado para ser evacuado en caso de una emergencia.

Cuando menos una vez al año todo centro de computo debe de realizar un simulacro en el cual el personal demuestre su capacidad para proporcionar un nivel de servicio esencial utilizando únicamente los recursos designados para propósitos de respaldo. La seguridad debe de preservarse durante el simulacro.

Medidas en el centro de cómputo primario

Todas las medidas de seguridad deben de ser diseñadas de manera que el centro de cómputo soporte hasta un 150% de incremento en la carga de trabajo sin que esto provoque disminución de la seguridad.

Si el servicio del centro de cómputo se reduce, todas las medidas de seguridad se deben de mantener, a menos que el oficial de seguridad determine que el nivel de clasificacion de la información manejada puede reducirse o se haga algún otro cambio que reduzca el nivel de seguridad.

Cuando el servicio es continuamente critico, la utilización de procesadores en espejo o "back-to-back" debe de ser considerada. Esto es que todos los trabjos realizados en el computador principal se vean reflejados en un segundo computador. Así, en caso de que uno falle se cuenta con el otro. Si esta previsión se realiza, se deben de realizar las correspondientes provisiones de dispositivos periféricos, software y servicio de soporte del medio ambiente y equipo.

Cuando la pérdida de la capacidad primaria de comunicación se ve como un riesgo creible, se deben de tener las provisiones para un respaldo de las comunicaciones. Esto debe de incluir comunicación vía satélite, líneas telefónicas, enlaces de microondas o cuando menos un enlace de voz seguro.

Todo equipo que esté designado para propósitos de respaldo únicamente, debe de ser deshabilitado para impedir su uso no autorizado, pero debe de ser probado periodicamente y tener un alto nivel de mantenimiento a manera de asegurar su disponibilidad en cualquier emergencia.

Almacenamiento fuera del centro de cómputo

Las continuas copias de software, datos y documentos esenciales para apoyo del servicio del centro de cómputo o requeridos para el mantenimiento histórico o para evidencia legal deben de ser almacenados fuera de él. Las facilidades de almacenamiento que se tengan fuera del centro de cómputo deben de estar al mismo nivel que las facilidades que proporciona el almacenamiento en él. Esto debe de incluir encripción de archivos. La mayoría de los centros de cómputo utilizan bovedas.

Un transporte seguro debe de proporcionarse para transportar los medios de almacenamiento del centro de cómputo a nuestra boveda externa de almacenamiento.

El lugar de almacenamiento externo que haya sido elegido no debe de compartir ningún riesgo con el centro de cómputo primario. Un apropiado sistema de aire acondicionado y otros equipos de soporte del medio ambiente deben de ser proporcionados.

Cuando menos cada tres meses se debe de realizar una inspección del lugar externo de almacenamiento. Parte de esta inspección debe incluir el seleccionar aleatoriamente nuestros medios de almacenamiento ahi guardados para ser vaciados y verificar que el contenido corresponda a lo que debe de ser.

Lugar de procesamiento alterno

El equipo de procesamiento de datos de cualquier sitio alterno, debe de ser compatible con el que se tenga en el centro de cómputo. Si no es así, se deben de tener los programas de emulación adecuados para cualquier posible emergencia.

Continuas copias al día de software o documentación requeridas para proporcionar un mínimo nivel esencial de servicio deben de tenerse disponibles en el centro alterno de procesamiento. La boveda externa de almacenamiento de medios de procesamiento y el sitio alterno de procesamiento deben de ser dos lugares diferentes.

Continuas copias al día de datos, documentos y formas impresas para mantener cuando menos el mínimo nivel esencial de servico deben de estar disponibles en el centro alterno de procesamiento de datos.

Los sitios de respaldo deben de tener el mismo nivel de protección que el centro de cómputo primario. Las especificaciones eléctricas del sitio de respaldo deben de ser consistentes con aquellas del centro de cómputo primario y deben de tener requerimientos continuos de servicio. Las especificaciones del sistema de tierra, aire acondicionado y otros servicios de soporte ambiental en el sitio de respaldo deben de ser consistentes con los del centro de cómputo primario. Datos, voz y registros de comunicaciones del sitio de respaldo deben de estar enlazadas con el centro de cómputo primario.

El centro de respaldo debe de tener la capacidad de acomodar a todo el personal necesario. Además se debe de tener un medio de transporte seguro entre el centro de cómputo primario y el sitio de respaldo.

Los sitios de respaldo deben de ser seleccionados de manera que no estén sujetos a los mismos riesgos ambientales que el centro de cómputo primario. Deben de ser inspeccionados cuando menos cada seis meses. [4]

Hasta aqui hemos visto diferentes medidas que se pueden tomar en caso de falla del sistema de cómputo.

A continuación veremos como está implantado el plan de respaldo y recuperación en la base de datos DataBase2 de IBM para mostrar como funciona ésto en un caso concreto.

3.5 RESPALDO Y RECUPERACION EN IBM DATABASE2

El diario

Cada conjunto de datos del diario activo es un conjunto de datos secuencial de entrada (ESDS) de VSAM (método de acceso de almacenamiento virtual). La unidad física de salida escrita en el conjunto de datos del diario activo es un intervalo de control (CI) de 4 Kbytes. Cada CI contiene un registro VSAM y 7 bytes de información de control de VSAM.

Después de aceptar la información de control de VSAM, el CI proporciona 4089 bytes para guardar información de DB2. Este espacio es llamado un registro físico. La información que se va a registrar en un momento en particular forma un registro lógico, cuya longitud varia independientemente del espacio disponible en el CI. Por lo tanto, un registro físico puede contener varios registros lógicos, uno o más registros lógicos y parte de otro, o solamente parte de un registro lógico. El registro físico debe contener también 14 bytes de información de control de DB2. Una parte de un registro lógico que cabe en un registro físico es llamado un segmento.

Cada registro lógico incluye un prefijo, llamado encabezado del registro de diario (LRH), que contiene información de control. Su contenido se muestra en la figura 3.1

El primer segmento de un registro de diario debe contener el encabezado y algunos bytes de datos. Si el registro físico actual tiene muy poco espacio para el segmento mínimo de un nuevo registro, el residuo del registro físico no es utilizado y un nuevo registro de diario es escrito en un registro físico nuevo.

El registro de diario se puede expander cuanto sea necesario. Sólo el primer segmento incluye el encabezado completo. Cuando un registro de diario específico se necesita para recuperación, todos los segmentos son presentados juntos como si fueran almacenados en forma continua.

Encabezado del registro de diario.

Desplazamiento hexadecimal	Longitud	Información
00	2	Longitud de este registro o segmento
02	2	Longitud de cualquier registro o segmento previo en el CI; 0 si es la primera entrada en el CI. Los dos bits de mayor orden nos indican el tipo de segmento: X'00' Diario de registro completo. X'01' El primer segmento. X'11' Segmento intermedio. X'10' El último segmento.
04	2	Tipo del diario de registro.
06	2	Subtipo del diario de registro.
08	1	ID del administrador de recursos del componente del DB2 que crea el diario de registro.
09	1	Reservado.
0A	6	ID de la unidad de recuperación, si este registro es relacionado con una unidad de recuperación. De otra forma es 0.
10	6	RBA de diario, del registro previo de diario, si este es relacionado con una unidad de recuperación. De otra forma es 0.

FIGURA 3.1

Cada registro de diario físico incluye un sufijo llamado definición de control de intervalo (LCID), que dice como están situados los segmentos en el intervalo de control físico.

El diario contiene la información necesaria para recuperar los resultados de la ejecución de un programa, la base de datos, y el subsistema DB2. No contiene información para contabilidad, estadísticas o evaluación de operación.

Existen tres tipos de registros de diario :

a.- Unidad de recuperación.
b.- Punto de chequeo.
c.- Registro de control de conjunto de página de la base de datos.

Cada registro tiene un encabezado que indica su tipo, el subcomponente de DB2 que hace el registro, y para registros de unidad de recuperación, el identificador de unidad de recuperación. Los registros de diario pueden ser extraidos e impresos por el programa DSN1LOGP.

El diario de DB2 puede contener hasta 2^{48} bytes. Cada byte es direccionable por su offset desde el comienzo del diario, este offset es conocido como su dirección de byte relativa (RBA).

Un registro de diario es identificable por el RBA del primer byte de su encabezado. El registro RBA es como un sello de tiempo : crece indefinidamente, sin repetirse, e identifica únicamente un registro que comienza en un punto particular en el diario siguiente.

a.- Registros de unidad de recuperación.- La mayoría de los registros de diario describen cambios a la base de datos. Todos estos cambios están hechos de unidades de recuperación.

Una unidad de recuperación es el trabajo hecho por DB2 para una aplicación, que afecta el estado de los datos de DB2 de un punto de consistencia a otro. Un punto de consistencia es un momento cuando todos los datos recuperables que accesa un programa de aplicación son consistentes con otros datos.

Por ejemplo, una transacción bancaria transfiere fondos de la cuenta A a la cuenta B. El programa, primero sustrae el monto de la cuenta A y después suma el monto a la cuenta B. Después de sustraer, las dos cuentas son inconsistentes; sólo hasta que el monto es sumado a la cuenta B son consistentes nuevamente. Cuando ambos pasos están completos, el programa puede anunciar un punto de consistencia y hacer los cambios visibles para otros programas de aplicación.
Una unidad de recuperación comienza en un punto de consistencia y termina en el siguiente. Esto se muestra en la figura 3.2. La terminación normal de un programa de aplicación causa un punto de consistencia automáticamente.

Si ocurre una falla dentro de una unidad de recuperación, DB2 quita todos los cambios a los datos, llevándolos al estado en el que se encontraban al comienzo de la unidad de recuperación.

Cuando se hace un cambio a la base de datos, DB2 genera un registro de deshacer/rehacer que describe el cambio. La información de rehacer es necesaria si el trabajo es completado y después debe ser recuperado. La información de deshacer es usada para volver al punto inicial cuando un trabajo no es completado.

Si el trabajo es revertido, el registro deshacer/rehacer es usado para remover el cambio; al mismo tiempo un nuevo registro rehacer/deshacer es creado y contiene la llamada información de compensación que revierte el cambio.

DB2 también mantiene diarios de la creación y destrucción de conjuntos de datos. Si el trabajo es revertido, las operaciones son revertidas.

La figura 3.3 sumariza la información registrada para cambios en los datos y los índices. Existen tres clases de cambios básicos a una página de datos :

- Cambios a información de control. la utilería COPY usa esta información cuando hace copias de imagen incremental.

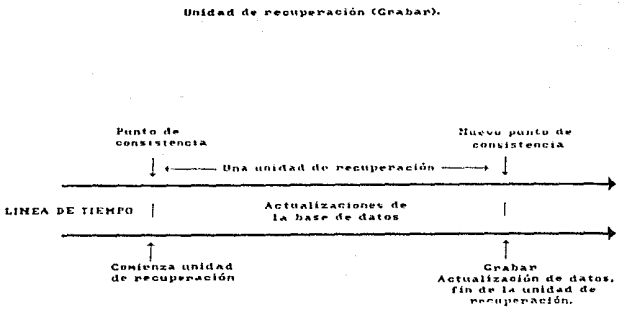

Unidad de recuperación (Grabar).
Punto de consistencia
Nuevo punto de consistencia
Una unidad de recuperación
LINEA DE TIEMPO
Actualizaciones de la base de datos
Comienza unidad de recuperación
Grabar Actualización de datos, fin de la unidad de recuperación.

FIGURA 3.2

Información registrada para los cambios de la base de datos.

Operación	Información registrada
Insertar datos	La nueva fila. Cuando se rehace, la fila es insertada en la fila RID. Cuando se borra, la fila es borrada, si ésta existe.
Borrar datos	La fila borrada. Cuando se rehace, el RID se hace disponible para otra fila. Cuando se borra, la fila es insertada nuevamente con su RID.
Actualizar datos	Cuando se rehace, el nuevo dato. Cuando se borra, el dato formado.
Insertar entrada indexada	El desplazamiento está en la página indexada, el nuevo valor de llave y el dato RID.
Borrar entrada indexada	El desplazamiento está en la página indexada, el valor de la llave borrada y el dato RID.

FIGURA 3.3

- Cambios a apuntadores de base de datos. Los apuntadores son usados en dos situaciones:

  . El catálogo y el directorio, pero no las bases de datos del usuario, contienen apuntadores que conectan renglones relacionados entre si.
  . Cuando un renglón de una base de datos de usuario se hace tan larga que no cabe en el espacio disponible, se mueve a una página nueva. Cuando esto ocurre se deja en la página original una dirección que apunta a la nueva localización.

- Cambios a los datos. En DB2, cada renglón es confinado a una sola página. Cada renglón es identificado por una identificación de registro (RID) que consiste de:

  . El número de la pagina.
  . Una identificación de un byte que identifica el renglón dentro de la página. Una página puede contener hasta 127 renglones.

El registro de diario identifica el RID, la operación (inserción, borrado o actualización) y el dato. Dependiendo del tamaño del dato y de otras variables, DB2 puede escribir un sólo registro de diario con la información de deshacer y rehacer, o puede escribir registros separados para deshacer y rehacer.

b.- Registros de punto de chequeo.- Para reducir el tiempo de recomienzo, DB2 toma puntos de chequeo periódicos durante la operación normal, en las siguientes circunstancias:

- Cuando un numero predefinido de registros de diario han sido escritos.
- Cuando se cambian de un conjunto de datos de diario activo a otro.
- Al final de un reinicio exitoso.
- En una terminacion normal.

La figura 3.4 muestra la información registrada.

c.- Registro de control de conjunto de página de base de datos. Registra varios tipos de información que se describen a continuación:

- Asignación, apertura y cierre de conjunto de página: este tipo de registro contiene principalmente la asignación, apertura y cierre de cada conjunto de página. La misma información está en el directorio de DB2, pero se registra en el diario también para que esté disponible para el reinicio.
- Estados excepcionales: también registra si cualquier base de datos, espacio de tabla, espacio de índice o partición está en un estado excepcional. Un objeto puede estar en un estado excepcional por cualquiera de las siguientes razones:

  . Fue detenido.
  . Fue iniciado para acceso de sólo lectura o sólo utilería.
  . Ocurre un error de escritura.
  . Cambios que fueron diferidos en un reinicio anterior de DB2 están todavía pendientes.
  . Una utilería de DB2 tiene control sobre él.
  . Se requiere una copia imagen para hacerlo recuperable.

- Copias imagen de tablas especiales.

El proceso de crear los diarios se muestra esquemáticamente en la figura 3.5. Los registros de diarios típicamente pasan por el siguiente ciclo:

a.- Los registros de diario son originados por los administradores de recursos de DB2.

b.- El administrador de diarios divide los registros en segmentos si es necesario.

c.- Los registros de diario son colocados secuencialmente en diarios de buffers, que son formateados como intervalos de control de VSAM. Cada registro es identificado por un RBA continuamente creciente en un rango de 0 a $2^{48} - 1$.

Contenido de los registros
de punto de chequeo.

Tipo de registro	Información registrada
Inicio de punto de chequeo.	Marca el inicio del resumen de información.
Unidad de recuperación.	Identifica una unidad incompleta de recuperación. Incluye el día y la hora de su creación, su ID de conexión, ID de autorización, el nombre del plan utilizado y su estado actual.
Resumen de juego de páginas.	Contiene información de objetos ubicados y abiertos a la hora de reinicio e identifica el punto de chequeo más reciente. Existe un registro para cada juego de páginas.
Resumen de juego de páginas de excepción.	Identifica el tipo de estado de excepción. Existe un registro para cada base de datos y juego de páginas que son estados de excepción.
Punto de final de chequeo.	Marca el final de la información sobre el punto de chequeo.

FIGURA 3.4

d.- Los CI's son escritos en un conjunto predefinido de conjuntos de datos de diario activo en un dispositivo de almacenamiento de acceso directo (DASD), que son usados secuencialmente y reciclados.

e.- A medida que cada conjunto de datos de diario activo se llena, sus contenidos son descargados automáticamente a un conjunto de datos de diario archivo nuevo.

Los registros de diario son recobrados a través de los siguientes eventos:

a.- El administrador de recursos pide un registro de diario por su RBA.
b.- El administrador de recursos busca las localizaciones listadas a continuación, en el orden dado:

- Los buffers de diario.
- Los diarios activos.
- Los diarios archivo.

Los buffers de diario son escritos en un conjunto de datos de diario activo almenos cuando se llenan, y más frecuentemente cuando hay actualizaciones frecuentes. En el último caso, el mismo CI puede ser escrito varias veces en la misma posición. Se recomienda tener diarios activos dobles como una medida de seguridad en caso de que la estructura o el diario activo falle.

El proceso de copiar diarios activos a diarios archivo se llama descarga. La relación de la descarga con otros eventos de registro se muestra esquemáticamente en la figura 3.6.

La descarga de un diario activo puede ser causada por varios eventos. Los más comunes son:

a.- Que se llene el conjunto de datos de diario activo.
b.- Dar inicio a DB2 cuando un conjunto de datos de diario activo está lleno.

La descarga también es causada cuando ocurre algún error al estar escribiendo un conjunto de datos de diario activo o el conjunto de datos es truncado antes del punto de falla, y el registro en el que ocurrió la falla se convierte en el primer registro del siguiente conjunto de datos.

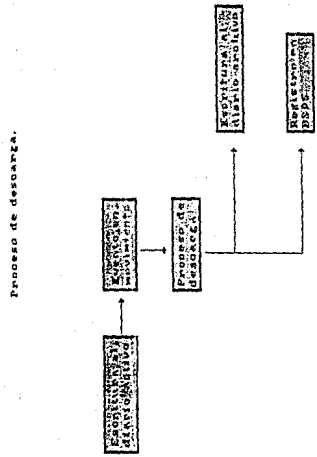


FIGURA 3.6

Durante el proceso, DB2 determina cual conjunto de datos descargar. Usando el RBA del último diario descargado, se calcula el RBA de diario en el cual empezar. También se determina el RBA en cual terminar, del RBA del último registro de diario grabado en el conjunto de datos, y registra este RBA en el BSDS (conjunto de datos de secuencia de inicio).

El proceso de descarga es automático: no hay comandos ni utilerías de DB2 relacionadas con él. De cualquier modo, cuando un diario activo está listo para ser descargado, una petición para montar una cinta o preparar un DASD puede ser enviada a la consola del operador. Los conjuntos de datos de diario archivo pueden ser almacenados en cintas etiquetadas comunes, en DADS o subsistemas de almacenamiento masivo (MSS) y pueden ser administrados por DFHSM (Administrador de Almacenamiento Jerárquico). Siempre son escritos por QSAM (Queue Sequential Access Method). El tamaño del bloque es un multiplo de 4 KB y para mayor eficiencia los registros se bloquean. Los conjuntos de datos de diario archivo de salida son posicionados automáticamente con nombres elegidos por DB2 y son especificados cuando este es instalado.

Si existe una falla cuando la descarga se está llevando a cabo, la descarga comienza nuevamente desde el RBA anterior cuando DB2 se reinicia.

Conjunto de datos de secuencia de inicio (BSDS)

El BSDS es un conjunto de datos secuencial con llave de VSAM que contiene información de los conjuntos de datos de diario y los registros que estos incluyen. Es definido con servicios de métodos de acceso cuando se instala DB2. Normalmente se mantienen copias duplicadas del BSDS. Si un error de E/S llegara a ocurrir, se desasigna la copia que está fallando y se continúa con un sólo BSDS.

Los conjuntos de datos de diario archivo son posicionados dinámicamente. Cuando uno es posicionado, el nombre del conjunto de datos es registrado en el BSDS en entradas separadas para cada volumen en los cuales se aloja el diario. La lista de conjunto de datos de diario archivo se expande a medida que se añaden archivos. El número máximo de entradas es 1000 para diarios archivos simples y 2000 para dobles.

Cada vez que un nuevo conjunto de datos de diario archivo es creado, se crea también una copia del BSDS. Si el diario archivo está en cinta, el BSDS es el primer archivo en el primer volumen de salida. Si el diario archivo está en DSAD, el BSDS es un archivo separado en el mismo volumen.

El BSDS registra el estado de un conjunto de datos de diario activo como uno de los cinco valores listados a continuación:

ESTADO	SIGNIFICADO
Nuevo	El conjunto de datos ha sido definido pero nunca ha sido usado por el administrador, el diario fue truncado en un punto anterior al conjunto de datos. En este caso, los RBA de comienzo y terminación del conjunto de datos son puestos en cero.
Reusable	El conjunto de datos es nuevo y no tiene registros, o ha sido descargado.
No reusable	El conjunto de datos contiene registros que no han sido descargados.
Detenido	El procesador de descarga encontró un error cuando leía un registro, y no pudo ser obtenido de la otra copia del diario activo.
Truncado	Uno de los siguientes casos: a.- Ocurrió un error de E/S (Entrada/Salida), y el administrador de diario ya no escribe en este conjunto de datos. La escritura continúa en el siguiente conjunto de datos de diario activo disponible. b.- El diario fue truncado por reinicio condicional en un punto dentro del rango del RBA del conjunto de datos.

Reinicio

DB2 puede trabajar con otro subsistema. Si los datos deben ser consistentes en los dos subsistemas, cualquier cambio en un sistema debe ser realizado en conjunto con un cambio en el otro. Antes de que cualquier subsistema realice un cambio en los datos, debe saber que el otro subsistema puede hacer el cambio correspondiente. Por esto los subsistemas se deben comunicar.

DB2 usa un proceso de dos fases para la comunicación entre diferentes subsistemas. En la fase 1, cada subsistema determina independientemente si ha grabado suficiente información para recuperación en su diario, y puede realizar su trabajo. Al final de la fase, los subsistemas se comunican. Si están de acuerdo, cada uno comienza la fase 2, en la cual realmente se cambian los datos. Aunque uno de los subsistemas termine anormalmente durante la fase 2, la operación se completa por un proceso de recuperación al reinicio.

Si DB2 falla cuando está conectado con otro sistema, se debe detrminar durante el reinicio si llevar a cabo los cambios o retroceder las unidades de recuperación que estaban activas al momento de la falla. Para algunas unidades de recuperación, DB2 tiene información suficiente para tomar la decisión. Para otras puede que no la tenga, y debe obtenerla del otro sistema cuando la conexión se restablezca.

El estado o estatus de una unidad de recuperación después de una falla depende del momento de la falla:

ESTATUS	DESCRIPCION Y PROCESAMIENTO
En vuelo	Falla antes de terminar la fase 1; al reinicio DB2 desecha las actualizaciones.
En duda	Falla después de terminar la fase 1 y antes de empezar la fase 2. Si la falla fue antes de llevar a cabo el cambio, DB2 debe desecharlo; si ocurrio despues, DB2 debe realizar los cambios. Al reinicio, DB2 espera información del otro sistema antes de procesar esta unidad de recuperación.
En ejecución	Falla después de que comienza su propia fase 2; realiza los cambios ejecutados.
En aborto	Falla después de que una unidad de recuperación comenzó a ser retrocedida pero antes de que el proceso fuera completado; durante el reinicio, DB2 continúa desechando los cambios.

Reinicio y recuperación normal

Para saber que recuperar al reinicio, DB2 usa su diario de recuperación y el BSDS. El BSDS identifica los conjuntos de datos activo y archivo, la localización del punto de chequeo más reciente y el calificador de alto nivel del nombre del catálogo de ICF (Catálogo integrado).

Después de que DB2 es inicializado, el proceso de reinicio atraviesa por cuatro fases:

a.- Fase 1: inicialización de diario.
b.- Fase 2: reconstrucción del estado actual.
c.- Fase 3: recuperación de diario hacia adelante.
d.- Fase 4: recuperación de diario hacia atrás.

Al finalizar la cuarta fase, la recuperacion está completa. Tiene los siguientes efectos:

a.- Los cambios realizados se reflejan en los datos.
b.- Las actividades dudosas son reflejadas en la base de datos como que se tomó la decisión de realizar la actividad, pero no se ha llevado a cabo todavia.
c.- Los cambios interrumpidos en vuelo o en aborto son removidos de la base de datos. Los datos son consistentes y pueden ser usados.

Fase 1: Inicialización de diario

Durante la fase 1, DB2 trata de localizar el último RBA del diario que fue escrito antes de la terminación. En esta fase DB2:

a.- Compara el calificador de alto nivel del nombre de catálogo de ICF, en el BSDS, con el correspondiente calificador del nombre en el módulo parámetro actual.

- Si son iguales, el proceso continúa con el paso 2.
- Si son diferentes, DB2 termina con el mensaje: DSNJ130I.

Si los nombres no coinciden, DB2 puede actualizar un catalogo completamente diferente.

b.- Verifica que los sellos de tiempo en el BSDS sean consistentes.

- Si ambas copias del BSDS son actuales, DB2 verifica si los dos sellos son iguales.
  . Si son iguales, el proceso continúa con el paso tres.
  . Si son diferentes, DB2 da el mensaje DSNJ120I y termina. Esto puede suceder cuando las dos copias del BSDS están en volúmenes de DASD separados y uno de los dos volúmenes es restaurado mientras DB2 es detenido. DB2 detecta esta situación al reinicio.

- Si una de las copias del BSDS fue desalojada, y se continuó con un sólo BSDS, se puede presentar un problema si ambas copias se mantienen en un sólo volumen, y el volumen fue restaurado, o si las dos copias de BSDS fueron restauradas en forma separada, puede suceder que DB2 no detecte la restauración.

c.- Encuentra el RBA de diario del último registro de diario escrito antes de la terminación, en el BSDS.
d.- Revisa el diario hacia adelante, comenzando en el RBA de diario de registro de diario más reciente, hasta el último CI escrito antes de la terminación.
e.- Se prepara para continuar escribiendo registros de diario en el siguiente CI en el diario.
f.- Envía el mensaje DSNJ001I, que identifica el RBA de diario en el cual se continúa la sesión actual. Señala el final de la fase.

Fase 2: Reconstrucción del estado actual

Durante esta fase, DB2 determina los estatus de los objetos al momento de la terminación. Al final de la fase, DB2 ha determinado si alguna unidad de recuperacion fue interrumpida por la terminación. En la fase 2, DB2:

a.- Revisa el BSDS para encontrar el RBA de diario del último punto de chequeo completo antes de la terminación.
b.- Lee cada registro de diario desde ese punto de chequeo hasta el final de diario e identifica:

- Todas las unidades de recuperación que están pendientes y su estatus.
- Todas las condiciones excepcionales que existen para cada base de datos y toda la información de copia imagen.
- Todos los objetos abiertos al tiempo de la terminación, y cuanto se debe retroceder en el diario para reconstruir páginas de datos que no fueron escritas en DADS.

c.- Envía el mensaje DSNR004I, que sumariza la actividad requerida al reinicio para las unidades de recuperación pendientes.
d.- Se envía el mensaje DSNR007I también, si se descubren algunas unidades de recuperación pendientes.

Durante la fase 2 no se lleva a cabo ningún cambio en la base de datos ni son completadas ninguna de las unidades de recuperación. Solamente determina que cambios son necesarios antes de que permita acceso a la base de datos.

Fase 3: Recuperacion de diario hacia adelante

Durante la fase 3, DB2 completa el proceso para todos los cambios en ejecución y las operaciones de escritura a la base de datos. En la fase 3, DB2:

a.- Revisa el diario hacia adelante comenzando en el RBA más pequeño que es:

- Requerido para completar las escrituras a base de datos.
- Está asociado con la unidad de recuperación inicial de unidades de recuperación en duda o en ejecución.

b.- Utiliza el RBA de diario del registro de diario rehacer/deshacer más cercano para cada objeto. Todos los cambios anteriores al objeto fueron escritos en DASD.
c.- Lee las páginas de datos o indices para cada registro de diario rehacer/deshacer restante. El encabezado de página registra el RBA de diario del registro del último cambio a la página.
d.- Escribe páginas a DADS a medida que se necesiten los buffers.
e.- Marca el término de cada unidad de recuperación procesada.
f.- Realiza todos los cambios a bases de datos para cada unidad de recuperación en duda y bloquea la información para prevenir su acceso después del reinicio. Cuando una unidad en duda es resuelta, el proceso es completado en una de las siguientes maneras:

- para retroceso, DB2 lee y procesa el diario revirtiendo todos los cambios.
- para ejecución DB2 lee el diario pero no procesa los registros, porque todos los cambios han sido efectuados.

g.- Termina de revisar el diario a su fin.
h.- Escribe el DADS todos los buffers modificados que no han sido escritos todavía.

i.- Envía el mensaje DSNR005I, que sumariza el número de las unidades de recuperación en duda y en ejecución restantes.
j.- Envía el mensaje DSNR007I, que identifica cualquier unidad de recuperación pendiente que todavía necesita ser procesada.

Fase 4 : Recuperación hacia atrás

durante la fase 4, DB2 completa el procesamiento revirtiendo todos los cambios hechos para unidades de recuperación en vuelo y en aborto. En esta fase, DB2 :

a.- Revisa el diario hacia atrás, comenzando del final actual. La revisión continúa hasta la primera "unidad de recuperación de comienzo" para cualquier unidad de recuperación en vuelo o en aborto pendiente.
b.- Lee la página de datos o índices para cada registro deshacer restante. El encabezado de página registra el RBA de diario del registro del último cambio a la página.
c.- Escribe información de compensación de rehacer en el diario para cada registro de deshacer del diario. los registros de rehacer revierten los cambios y facilitan la recuperación del medio.
d.- Escribe páginas en DASD a medida que se necesiten buffers.
e.- Finalmente, escribe en DASD todos los buffers modificados que no han sido escritos todavía.
f.- Envía el mensaje DSNR006I, que sumariza el número de unidades de recuperación en aborto y en vuelo restantes.
g.- Marca la completación de cada unidad de recuperación en el diario de modo que, si el proceso de reinicio termina, la unidad de recuperación no sea procesada nuevamente en el siguiente reinicio.
h.- Toma un punto de chequeo, después de que todas las escrituras a base de datos han sido completadas.

Respaldo y recuperación de bases de datos

Los principios de respaldo y recuperación de DB2 son simples. La estructura a recuperar es un espacio de tabla. Para asegurar que el espacio de tabla puede estar nuevamente en un estado estable, se debe hacer una copia de la misma. DB2 registra en el diario todos los cambios hechos al espacio de tabla. Si ocurre una falla DB2 puede usar la copia como punto de inicio y reaplicar todos los cambios grabados en el diario de recuperación.

DB2 provee un conjunto de programas de utilería que ayudan a recuperar datos. Una utilería de copia de imagen, copia el espacio de tabla. DB2 lleva control automático de los cambios hechos a las tablas en el espacio de tabla y graba estos cambios en el diario. Una utilería de recuperación construye nuevas tablas en el espacio de tabla a partir de la copia y el diario. Este proceso es conocido como recuperacion hacia adelante, porque la utilería recupera el espacio de tabla desde el último punto estable en adelante.

La figura 3.7 muestra el proceso de recuperación.

Hacer copias completas de un espacio de tabla muy grande lleva mucho tiempo, es por ésto que DB2 permite hacer copias de imagen incrementales. Se copian solamente aquellas porciones del espacio de tabla que fueron cambiadas desde que la copia imagen más reciente fue hecha. Estas copias incrementales pueden ser combinadas con una copia imagen completa para producir una copia imagen completa nueva.

El usar esta copia imagen combinada como punto de inicio, elimina la necesidad de aplicar todos los cambios grabados en el diario.

En la figura 3.7 se observa que existen dos diarios. Para prevenir que el diario sobrepase su capacidad, DB2 lleva un control sobre los conjuntos de datos del diario y mueve automáticamente conjuntos de datos de diario llenos a un diario secundario en disco o cinta. DB2 tiene diarios dobles tanto del activo como del secundario por si alguno no puede ser leído.

Ahora veremos como se pueden usar estas herramientas para recuperarse de una falla en la base de datos.

Proceso de Recuperación.

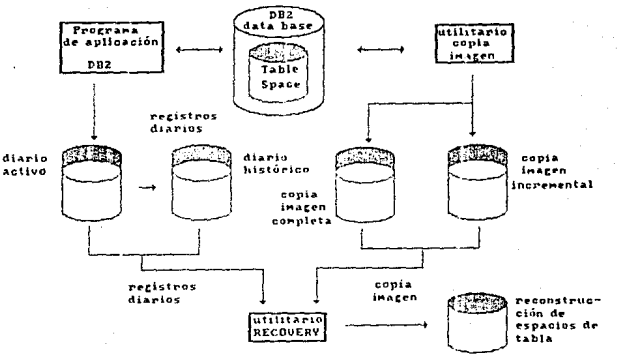


FIGURA 3.7

Imagine que usted es el administrador de la base de datos DBase1. Suponga que el espacio de tabla TSpace1 ha estado disponible toda la semana. Una escritura a un disco conteniendo datos para la tabla en ese espacio de tabla falla. Usted necesita recuperar el espacio de tabla en el último punto estable antes de que ocurriera la falla. Para hacer ésto, describiremos el proceso de recuperación completo, empezando desde que usted dio inicio a DBase1.

Inmediatamente después de darle inicio usted tomó una copia imagen completa de TSpace1 de modo que tiene un punto de reinicio estable del cual comenzar la recuperación. Para esto utilizó la utilería de copia imagen. Usted puede accesar TSpace1, incluso actualizarlo mientras la copia imagen está siendo tomada.

El día siguiente se corre la utilería de copia imagen nuevamente. Esta vez usted realizo una copia imagen incremental para registrar solo los cambios que se han hecho al espacio de tabla desde la última vez. Por los siguientes tres días, usted hizo otra copia imagen incremental cada mañana.

Al final de la semana, ocurre una escritura no exitosa y se necesita recuperar el espacio de tabla. Usted corre la utilería de recuperación para hacer esto. Esta restaura automáticamente el espacio de tabla de la copia imagen completa y de todas las copias imagen incrementales, y automáticamente incorpora todos los cambios subsecuentes del diario de recuperación de DB2.

Mientras se procesa la utilería, usted recibirá mensajes indicando el progreso de ésta. Cuando halla terminado, usted recibirá un mensaje que le indicará que el espacio de tabla ha sido recuperado exitosamente.

Para recuperar un espacio de tabla, la utilería RECOVERY utiliza lo siguiente :

a.- Una copia imagen completa; esto es una copia del espacio de tablas completo.
b.- Cualquier copia incremental posterior; cada una sumariza todos los cambios hechos al espacio de tabla desde el momento en que la copia imagen anterior fue tomada.
c.- todos los registros de diario creados desde la copia imagen más reciente.

Si el diario se ha dañado, se puede hacer una recuperación parcial limitando el rango de registros de diario que deben ser aplicados por la utilería RECOVERY.

En la planeación para la recuperación, se determina cuan seguido se deben tomar las copias imagen y cuantos ciclos completos guardar. Estos valores determinan la longitud de los registros de diario para la recuperación de base de datos.

Para decidir cuan seguido tomar las copias imagen, se debe considerar el tiempo necesario para la recuperación de un espacio de tabla. Está determinado por :

a.- La cantidad de diario a recorrer.
b.- El tiempo que toma al operador montar y desmontar volúmenes de cinta archivo.
c.- El tiempo que toma leer la parte del diario necesaria para la recuperación.
d.- El tiempo necesario para reprocesar páginas cambiadas.

En general, mientras más seguido se tomen las copias imagen menor es el tiempo que toma la recuperación; pero por supuesto, mayor el tiempo que se pierde tomando las copias.

La información necesaria para la recuperación está contenida en las siguientes localizaciones:

a.- SYSIBM.SYSCOPY, una tabla de catálogo, que contiene información sobre las copias imagen. Para cada copia imagen incremental o completa registra :

- El nombre del conjunto de datos.
- Tipo de dispositivo.
- Número serie del volumen.
- Fecha.
- Hora de finalización.
- RBA de inicio del diario para actualizaciones posteriores.

b.- SYSIBM.SYSLGRNG, una tabla de directorio, que contiene registros de los rangos de RBA de diario usados durante cada periodo de tiempo en el cual cualquier espacio de tabla recuperable fue abierto para actualización.

c.- El diario para recuperación registra copias imagen del SYSIBM.SYSCOPY.

Si la copia imagen más reciente de un objeto está dañada, la utilería RECOVERY busca una copia imagen previa y continúa buscando hasta que encuentra una copia imagen que no está dañada o hasta que no hay más copias imagen.

El DFHSM puede proporcionar administrar automáticamente la disponibilidad de espacio y datos en los dispositivos de almacenamiento del sistema. Mueve automáticamente datos desde y hacia la base de datos DB2.

El DFHSM administra el espacio de DASD en forma eficiente moviendo conjuntos de datos que no han sido usados recientemente a un medio de almacenamiento menos caro. También los hace disponibles para recuperación, copiando automáticamente a cinta, DASD o MSS conjuntos de datos nuevos o cambiados. Puede borrar conjuntos de datos o moverlos a otro dispositivo. Su operación es diaria, a una hora determinada.

Todas las operaciones del DFHSM pueden ser efectuadas manualmente. [8]

3.5 TECNOLOGIAS DE ALMACENAMIENTO

A la hora de respaldar es importante tener en cuenta que tecnología se desea utilizar de acuerdo a las necesidades de la organización. El uso de estas tecnologías de almacenamiento depende de tres factores principales:

a.- Costo por bit.
b.- Tiempo de acceso.
c.- Costo de entrada.

La reducción de costo por bit en todas las tecnologías se deriva principalmente de un incremento en la densidad del material utilizado para el almacenamiento y está asociado a un aumento en el tamaño del módulo básico de almacenamiento.

Al plasmar las diversas tecnologías en una gráfica de costo por bit contra tiempo de acceso (ver figura 3.8), se hace evidente la separación tanto de tiempo de acceso y de costo por bit entre las memorias de semiconductores y los aparatos que dependen de movimiento para hacer su acceso.

En el espectro de tiempo de acceso, las memorias de semiconductores están en un lado y los medios magnéticos de almacenamiento en el otro, con numerosas tecnologías ubicadas entre ellos. Este espacio entre ambas tecnologías es lo que ha implusado el dasarrollo de nuevos métodos de almacenamiento basados en burbujas magnéticas, haz de electrones, óptica, etc.

Memoria de burbujas y CCD

CCD (dispositivo acoplado por carga) es un diseño de memoria basado en una tecnología de silicón bien establecida. Es un registro de corrimiento derivado de RAM (memoria de acceso directo), cuyo menor costo es obtenido almacenando información en paquetes de carga en lugar de circuitería biestable. La similitud tecnológica puede retardar la aceptación de las memorias CCD porque comparadas con RAM, la reducción de dos a cuatro veces el costo, no es suficiente para opacar la disminución de mil a uno en tiempo de acceso, excepto en aplicaciones muy específicas.

Tecnologías de Almacenamiento.

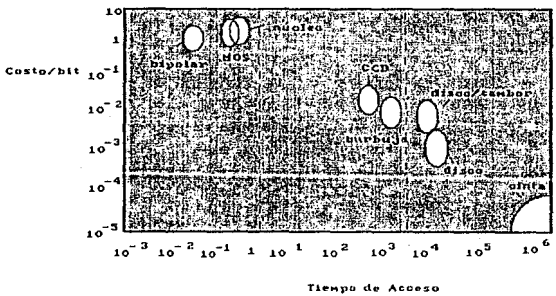


FIGURA 3.8

La MBM (memoria de burbuja magnética) también usa una organización de registro de corrimiento. Las burbujas magnéticas son pequeños dominios magnéticos de forma cilíndrica que se forman en una delgada capa magnética, cuando un campo magnético diagonal externo es aplicado en forma normal al plano de la capa. Las burbujas son magnetizadas en sentido inverso al de la capa. La información es codificada en términos de ausencia o presencia de burbujas. Estas son controladas creando un gradiente de campo magnético a través de un campo rotatorio operando en conjunto con permalloy que define la localización de la celda del bit. MBM es no volátil a diferencia de CCD. Ambas tecnologías dependen de procesos de fabricación similares.

Una mirada a la figura 3.9 sugiere que si esta proyección se mantiene, CCD será más atractivo que MBM porque la no volatilidad no es tan importante como las ventajas en tiempo de acceso. En cuanto a costo por bit no presentan ningún peligro para los discos de cabeza móvil.

Disco de video óptico

No es un dispositivo de lectura/escritura ya que la información no puede ser modificada en el mismo lugar en que está almacenada, pero proporciona mayor densidad de grabación que los dispositivos magnéticos.

Un haz brillante de luz laser modulada es enfocada hacia un disco giratorio. La información grabada puede ser recuperada posteriormente iluminando el disco con un haz menos intenso y luego detectando la modulación de la luz reflectada o transmitida por el disco.

Una separación entre pistas de aproximadamente dos micrones se usa en los discos de video y proporciona alrededor de quincemil pistas por pulgada y sistemas de 15 MHz de ancho de banda.

A pesar de que las técnicas usadas son ópticas, los retos de diseño son principalmente mecánicos y requieren de servomecanismos muy sofisticados para la grabación y enfoque. El material de grabación es un factor importante ya que cuando se necesite verificar al escribir o corregir rápidamente la información grabada, no debe ser necesario procesar el material previamente, y las continuas lecturas no lo deben degradar.

El potencial de la grabación óptica podría ser mejorado notablemente si se encontrara un material reusable y se pudieran utilizar lasers de estado sólido para grabar y leer.

Grabación magnética

Este tipo de tecnología es la dominante en el almacenamiento masivo de datos. Esto se debe a que se trata de una tecnología madura que se rehusa a envejecer, además de que cumple con las necesidades de los usuarios y las espectativas de industriales y científicos.

La grabación magnética se ha usado por más de treinta años ya que su bajo costo por bit compensa su lento tiempo de acceso.

Algunos dispositivos basados en ésta tecnología son:

a.- Floppy.
b.- Minifloppy.
c.- Cartucho.
d.- Casettes y cartuchos digitales.
e.- Discos duros de película delgada. [9]

4

CRIPTOGRAFIA

4.1 HISTORIA

La práctica de la criptografía data desde la antiguedad y se cree que los romanos fueron los primeros en la historia en preocuparse de la necesidad de mantener su información confidencial.

Etimológicamente, la criptografía significa escritura escondida y el concepto se aplica cuando surge la necesidad de enviar un mensaje de un punto a otro con un alto grado de confidencialidad, así como el mantenerlo secreto en un lugar fijo.

Nuestros antepasados utilizaron las siguientes formas para mantener su información confidencial durante el trayecto que el mensaje seguía del emisor hacia el receptor:

a.- Sobres lacrados. Procedimiento que no funcionó pues sólo bastaba con interceptar al mensajero, extraerle el sobre, abrirlo y leer el mensaje.
b.- Sistema de memorizar textos. Por medio de este procedimiento se memorizaban los textos del mensaje evitando así el escribirlo, pero tampoco funcionó ya que se interceptaba al mensajero, se le torturaba y se obtenía el mensaje.
c.- Criptografía. Finalmente se llegó a este procedimiento escondiendo el verdadero texto dentro del mismo texto.

Julio César, emperador romano, encriptaba su correspondencia confidencial con la técnica de sustitución, reemplazando cada letra del mensaje por otra cuya posición era un número de veces previamente establecido adelante en el alfabeto.

Los espartanos, para proteger su información oficial, fueron los primeros en utilizar la técnica de encripción llamada transposición o permutación, la cual consiste en cambiar de posición cada letra del mensaje reacomodándola en un orden diferente al que tiene originalmente, siendo necesario establecer previamente el orden de la permutación a utilizar.

El precisar el número de veces adelante en el alfabeto en el " Cifrado de César ", y establecer el orden de la permutación en el caso de los espartanos, constituye lo que es conocido como llave de encripción, sin la cual el receptor nunca podrá entender el mensaje.

El método de Julio Cesar de sustituir una letra por otra y la práctica de los espartanos de reacomodar las letras de un mensaje, son ejemplos de lo que en la actualidad es llamado algoritmo, es decir, un procedimiento o conjunto de reglas a seguir para lograr algo. En nuestro caso este algo es un texto o un mensaje encriptado.

La criptografía moderna empieza a evolucionar alrededor del año 1200 d.c., pero se mantuvo haciendo uso de papel y lápiz hasta después de la primera Guerra Mundial, cuando surgieron las primeras máquinas electromecánicas de cifrado de datos, las cuales no solamente produjeron sistemas criptográficos difíciles de conocer, sino también incrementando sustancialmente la velocidad a la cual la información podría encriptarse y desencriptarse. La máquina más famosa de esta época fué la " Enigma " diseñada por el Ingeniero alemán Arthur Scherbius, la cual, además sentó las bases para el diseño de las primeras máquinas digitales de criptografía.

El único sistema de encripción que a la fecha se considera "Irrompible" es el llamado ONE - TIME PAD o "Cuaderno de único uso", el cual consiste en que, tanto el emisor como el receptor tengan un cuaderno idéntico de llaves de encripción, cada página contiene una llave diferente, comúnmente es una gran secuencia de dígitos seleccionados aleatoriamente, conteniendo al menos el mismo número de letras que existan en el mensaje, una llave es utilizada solamente para encriptar un mensaje, una vez enviado y recibido éste la página que contiene la llave se desprende del cuaderno y se destruye.

El método ONE-TIME PAD es utilizado para enlaces de comunicaciones ultrasecretas, tal como la línea Washington - Moscú, donde se requiere una alta seguridad a prueba de toda falla.

Este método es impráctico para utilizarlo comercialmente debido a la dificultad de la distribución de cuadernos y el mantener la pista de cada llave en cada página.

En teoría cualquier otro sistema de encripción puede ser descubierto por los criptoanalistas, sin embargo existen algunos mejores que otros, siendo lo verdaderamente importante elegir un sistema criptográfico sólido, de manera tal que un experto criptoanalista requiera contar con recursos casi ilimitados durante periodos de tiempo prolongados para descubrir la llave y entender la información.

Un sistema criptográfico no necesita ser indescifrable para utilizarse pero si lo suficientemente difícil para ser descubierto.

4.2 CONCEPTOS GENERALES

Criptografía.- Es el acto de transformar mensajes o textos en formas ininteligibles para todos, excepto para aquellos que conocen su transformación inversa.

Criptología.- Es la ciencia de las comunicaciones secretas; incluye además de la criptografía, el criptoanálisis.

Criptoanálisis.- Son las metodologías y técnicas para transformar el texto cifrado en su original.

Un aspecto básico para proveer seguridad a los mensajes por medio de técnicas de criptografía es mantener en secreto la transformación usada o el parámetro (llave) que selecciona una transformación especifica de un grupo de ellas.

Las técnicas de criptografía se utilizan para dar seguridad a los datos y mensajes en los medios de comunicación y en las redes.

Existen dos métodos para proteger mensajes y datos:

a.- Sistemas verdaderamente secretos, en los cuales la existencia del mensaje no está escondida, pero su significado está oculto bajo una transformación.
b.- Sistemas de ocultamiento, en los cuales la existencia del mensaje está escondida, como cuando se utiliza tinta invisible, mezclar un mensaje con otro, etc.

Las transformaciones criptográficas y los códigos se encuentran entre los primeros. Un código es una transformación en donde un mensaje completo puede ser representado por una palabra en particular o por una cadena de símbolos. Generalmente se hace con ayuda de un diccionario (libro de códigos). El nivel de protección depende del control que se tenga sobre los diccionarios y en los cambios periódicos de código.

La figura 4.1 muestra un sistema de criptografía para una comunicación segura entre un transmisor S, y un receptor R. Consiste de los siguientes elementos:

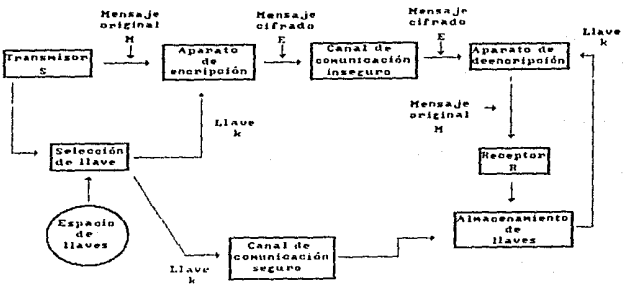

Mensaje original
M
Mensaje cifrado
E
Mensaje cifrado
E
Llave
k
Transmisor
S
Aparato de encripción
Canal de comunicación inseguro
Aparato de desencripción
Mensaje original
M
Llave
k
Selección de llave
Receptor
R
Espacio de llaves
Almacenamiento de llaves
Canal de comunicación seguro
Llave
k

FIGURA 4.1

a.- Un mensaje M, que debe ser transmitido y protegido.
b.- Una gran familia de transformación criptográficas reversibles T.

Cada transformación T_k en la familia, está determinada únicamente por un parámetro k, la llave del criptosistema. Todas las posibles llaves constituyen el espacio de llaves K del criptosistema.

c.- En el proceso de encripción se selecciona una llave y, la correspondiente transformación T_k es aplicada al mensaje para producir el correspondiente texto cifrado $E:E=(M)T_k$. E es transmitido a su destino donde el receptor aplica la transformación inversa

$$(T_k)^{-1}: (E)T_k^{-1}=M(T_kT_k^{-1})=M.$$

Este criptosistema será efectivo sólo si la llave permanece en secreto, y el espacio de llaves K es suficientemente grande para que sea muy difícil determinar el valor correcto por métodos de prueba y error. También es necesario que S y R usen la misma llave k, este valor debió haber sido intercambiado previamente por un medio de comunicación segura.

Criterios para diseño

Existe un conjunto de criterios de efectividad para un criptosistema, estos son:

a.- La transformación debe ser imposible de romper, sino teóricamente por lo menos en la práctica.
b.- El conocimiento por parte del interceptor, de la familia de transformaciones y del equipo utilizado no deben comprometer la protección otorgada.
c.- La llave debe ser capaz de proveer toda la protección: debe ser fácil de generar, aplicar, almacenar, transmitir y cambiar.
d.- El tamaño del espacio de llaves debe ser lo bastante grande para que no se pueda descubrir su valor por métodos de prueba y error.
e.- Idealmente, todas las características del lenguaje, como frecuencia relativa de letras, estructura de palabras, deben ser alteradas.

f.- La transformación debe ser lo suficientemente compleja para prevenir análisis matemático.
g.- Se debe tratar de que el tamaño del mensaje no cresca, para no alterar los requerimientos de almacenamiento y tiempo de transmisión.
h.- Debe ser suseptible a detección y/o corrección de errores.

Caracteristicas de aplicación que afectan la selección de la transformación:

a.- El valor de la información que debe ser protegida.
b.- El lenguaje usado. Se debe tener en cuenta que las caracteristicas de los lenguajes son útiles para el criptoanálisis.
c.- Dimensión y dinámica de la aplicación. El volumen de mensajes o registros que deben ser transmitidos o almacenados, tiempos de respuesta requeridos, naturaleza del proceso a realizar.

Consideraciones técnicas en la aplicación de técnicas criptográficas

a.- Capacidad de proceso. La disponibilidad de procesadores lo suficientemente rapidos para realizar la encripción y decripción dentro de los limites de tiempo de la aplicación sin degradar la capacidad del canal de transmisión.
b.- Manejo de errores. Las caracteristicas del canal de comunicación son importantes para elegir el sistema de encripción. Por ejemplo en un canal telefónico con muchos errores el uso de transformaciones que propagan errores, o que requieren sincronización continua puede llevar a muchas transmisiones inútiles.
c.- Medio ambiente operacional. La naturaleza del sistema y su control. Si es un sistema multiusuarios, una red pública; el entrenamiento de los operadores y usuarios del sistema.
d.- Distribución y administración de llaves. Las técnicas utilizadas para generar, distribuir y controlar las llaves. **[20]**

4.3 SISTEMAS CRIPTOGRAFICOS CLASICOS

A través de la historia se han inventado numerosos métodos de encripción, pero los concernientes a mensajes escritos en lenguaje natural tienden a caer en dos grandes grupos:

a.- Por substitución de caracteres o grupos de caracteres del alfabeto del mensaje por caracteres o grupos de caracteres del alfabeto de ciframiento.
b.- Por transposición de los caracteres del mensaje.

Transformaciones de estos dos tipos pueden ser combinadas para obtener transformaciones producto que son las más convenientes para la comunicación entre computadoras.

Transformaciones por sustitución

Existen dos categorías: monoalfabéticas y polialfabéticas. Cada una de estas puede ser monográfica o poligráfica. La última clasificación se refiere al número de caracteres que se sustituyen como un grupo. En sustituciones monográficas, se sustituyen caracteres individuales. En sustituciones poligráficas se sustituyen grupos de dos o más caracteres.

Un ejemplo es el método VIGENERE, que utiliza sustitución polialfabética. Utiliza M alfabetos B_1, ... B_M. La llave son las correspondientes letras de estos alfabetos para la letra "a" del alfabeto del mensaje.

Alfabeto original:

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

Alfabetos cifrados:

B_1: l m n o p q r s t u v w x y z a b c d e f g h i j k

B_2: o p q r s t u v w x y z a b c d e f g h i j k l m n

B_3: v w x y z a b c d e f g h i j k l m n o p q r s t u

B_4: c f g h i j k l m n o p q r s t u v w x y z a b c d

B_5: r s t u v w x y z a b c d e f g h i j k l m n o p q

Mensaje original:

sell all shares

Llave:

lover

Texto cifrado:

dsgp rwz nlrcol

Transformaciones por transposición

Opera sobre grupos de caracteres de un bloque del mensaje y los rearregla dentro del bloque. Una implantación clásica es escribir el mensaje en una matriz de M columnas, renglón por renglón, y después reescribirlo tomando las columnas en un orden especifico.

Transformaciones producto

Para las computadoras, ninguno de los tipos de trasnformaciones citados anteriormente provee la seguridad necesaria. Más bien se utilizan transformaciones que son combinación de las anteriores. La transformacion producto más conocida es el DES (Data Encryption Standard) que será tratado posteriormente. [20]

4.4 CLASIFICACION DE LA CRIPTOGRAFIA

Existen dos maneras en términos computacionales para encriptar la información:

a.- Por hardware.
b.- Por software.

El algoritmo D.E.S. se puede usar tanto para encriptar la información por hardware o por software.

La encripción por software aplica cuando se instalan dispositivos electrónicos para la proteccion de la información.

Podemos apreciar que la ubicación de los dispositivos en la red de comunicaciones es del lado central inmediatamente antes del equipo de comunicación de datos (generalmente un modem), y del lado remoto inmediatamente después del equipo de comunicacion de datos.

La encripción por software aplica cuando la protección de la información se logra por medio de un proceso de transformación o programa, como se muestra en la figura 4.2.

Se puede apreciar que se requieren medios fisicos (computador o microcomputador), tanto en el lado central como en el remoto para realizar la encripción/decripción.

Para tomar la decisión de encriptar por hardware o software en un sistema en línea se deben considerar los siguientes puntos:

a.- Si se cuenta con medios fisicos e inteligencia para correr un programa de aplicación capaz de encriptar y decriptar la información, lo recomendable sería hacerlo por software, en caso contrario por hardware.
b.- Si el tiempo de procesamiento para hacer la encripcion y decripción afecta en la comunicación, lo recomendable es hacerlo por hardware, en caso contrario por software.

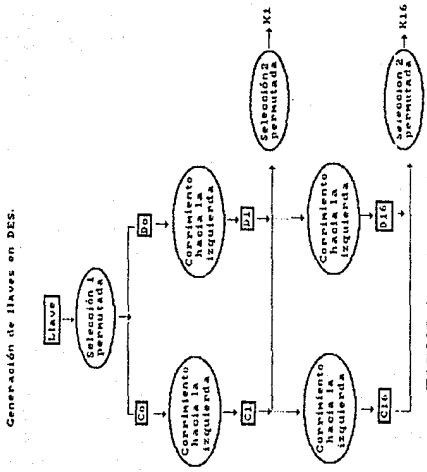

Generación de llaves en DES.
Llave
Selección 1 permutada
C0
D0
Corrimiento hacia la izquierda
Corrimiento hacia la izquierda
C1
D1
Selección2 permutada
K1
Corrimiento hacia la izquierda
Corrimiento hacia la izquierda
C16
D16
Selección 2 permutada
K16

FIGURA 4.2

En la encripción por hardware existen factores importantes que deben ser tomados en cuenta, ya que el cometer un pequeño error en la elección del sistema de encripción por hardware, llevaría a un enlace inconfiable, de baja relación de uso del canal y con una seguridad pobre. En principio se requiere el absoluto conocimiento de las características del enlace, para que sea compatible con el encriptor utilizado. Además de un adecuado manejo de las señales de control de los encriptores en las interfaces, entre los equipos de comunicación y las terminales.

4.5 DES

El algoritmo más probado y aceptado hoy en día en transmisión de datos para uso comercial es el Data Encryption Standard (D.E.S.), el cual está basado en los métodos de sustitución y transposición. Este algoritmo fue aprobado en el año de 1977 por la National Bureau of Standards de los Estados Unidos de Norteamérica como el método oficial para proteger datos no clasificados en las agencias del Gobierno Federal.

Debido a la importancia que este algoritmo representa en el ambiente actual de la criptografía, diferentes autores han desarrollado modalidades en su uso que facilitan su aplicación en la transmisión de datos y robustecen su confidencialidad.

La seguridad que provee está en la complejidad del algoritmo, la mezcla minuciosa que se aplica al bloque de datos y el tamaño del espacio de llaves (aproximadamente 7.2×10^{16}). El DES es una transformación producto de sustituciones, transposiciones y operaciones no lineales que son aplicadas iterativamente (16 iteraciones) a bloques de 64 bits para producir bloques cifrados de 64 bits. La llave es de 56 bits (mas 8 de paridad). La transformación DES se aplica de la siguiente manera:

a.- Dado el bloque de datos de 64 bits este se divide en partes izquierda y derecha de 32 bits cada una, L_0 y R_0 respectivamente. La llave de 56 bits K, se descompone también en dos partes de 28 bits cada una, C_0 y D_0.

b.- Las siguientes operaciones son repetidas 16 veces.

- La llave a ser usada K_1, es producida generando C_1 y D_1 de C_0 y D_0 recorriéndolas hacia la izquierda un número específico de lugares. Luego, K_1 de 48 bits se compone seleccionando 24 bits específicos de D_1 y C_1 como se muestra en la figura 4.2.
- Se produce L_1 haciéndola igual a R_0.
- R_1 es producida computando una función $f(R_0,K_1)$, y sumándola luego bit a bit con L_0. Al computar $f(R_0,K_1)$, como se muestra en la figura 4.3, R_0 se expande primero a una palabra de 48 bits, luego se suma con K_1, se escogen 32 bits de la suma y luego se aplica una transposicion, esto es, $R_1=L_0() f(R_0,K_1)$

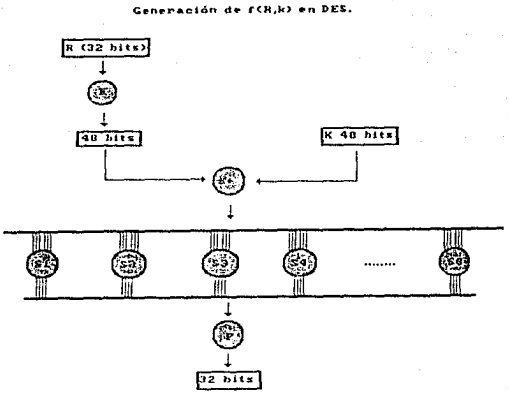

Generación de f(R,K) en DES.
R (32 bits)
48 bits
K 48 bits
S1
S2
S3
S4
S8
32 bits

FIGURA 4.3

c.- La última operación es combinar L_{16} y R_{16} y aplicar una permutación que es inversa a la permutación inicial aplicada a M antes de que fuera separada en R_0 y L_0. El resultado es el texto cifrado de 64 bits E, de M.

Existen tres métodos básicos para usar DES en un sistema de comunicaciones. El primero es un libro de código electrónico del cual, el bloque de datos de 64 bits M es transformado para producir E. El segundo método es el método de retroalimentación donde E_0 es producido de un bloque inicializador I_0, y luego G_1 es producido aplicando la transformación a E_0. E_1 corresponde a M_1, el primer bloque de datos a encriptar, es producido sumando G_1 y M_1. Por lo tanto los bloques de datos mismos no pasarán a través de la transformación DES. El tercer método es encadenamiento de bloques donde el bloque M_2 es sumado primero con el texto cifrado E_1, de transformar el bloque M_1, y luego la suma es transformada en el aparato DES. Este último da mayor protección que los dos primeros. [20]

Componentes del algoritmo

A continuación presentaremos en forma detallada los principales componentes del algoritmo DES y después continuaremos con los procesos de enciframiento y desciframiento, los cuales incorporan todas las componentes.

a.- Procedimiento de cálculo de la lista de llaves, el cual genera 16 subllaves.
b.- Operación de suma módulo-2
c.- Función enciframiento, la cual comprende las principales operaciones en la transformación producto.
d.- Transposición de bloque; que produce un bloque "presalida", que sirve como entrada a la permutación inversa inicial.
e.- Permutación inicial, que se describe como una tabla de selección.
f.- Permutación inicial inversa; descrita como una tabla de selección.

Cálculo de la lista de llaves

El objetivo de este componente es el de generar 16 subllaves, referidas como K_n, requeridas para los procesos de encriframiento y desciframiento. Cada K_n tiene una longitud de 48 bits y proviene del uso de operaciones de permutación, selección y corrimiento. Los bits de la llave de 64 bits están numerados del 1 al 64, de izquierda a derecha. Sin embargo, todos los bits de la llave no son utilizados en el cálculo de la lista de llaves. Recordando también que la llave de 64 bits representa 8 bytes de 8 bits, un bit de cada byte es utilizado para guardar la paridad impar y no es utilizado en el cálculo de la lista de llaves. Los bits de paridad son 8, 16, 24, 32, 40, 48, 56 y 64, dejando los siguientes bits para los cálculos de la lista de llaves:

1 al 7
9 al 15
17 al 23
25 al 31
33 al 39
41 al 47
49 al 55
57 al 63

Los cálculos para la lista de llaves son ejecutados de la siguiente forma:

a.- Los bits que no son de paridad en la llave van a través de una operación de permutación produciendo dos bloques de 28 bits denotados por C_0 y D_0. Este es el punto inicial para el cálculo de las subllaves.
b.- C_0 y D_0 son recorridas circularmente hacia la izquierda un lugar produciendo C_1 y D_1.
c.- Bits seleccionados de C_1 y D_1 son extraídos produciendo la subllave K_1.
d.- C_1 y D_1 son recorridos circularmente hacia la izquierda un lugar produciendo C_2 y D_2.
e.- Bits seleccionados de C_2 y D_2 son extraídos produciendo la subllave K_2.
f.- El proceso continúa para las subllaves K_3 hasta K_{16}. Cada C_i y D_i se obtiene del valor anterior después de un número preescrito de corrimientos circulares a la izquierda.

Los cálculos de la lista de llaves están resumidos en la figura 4.2. Cada subllave, denotada por K_i, es obtenida a través de una operación seleccionada de C_i y D_i. C_i y D_i se obtienen de C_{i-1} y D_{i-1}, respectivamente y a través de operaciones de corrimiento.

Inicialmente C_0 y D_0 se obtienen de la llave de 64 bits a través del uso de la permutación elegida 1, la cual es resumida en la tabla de la figura 4.4. Recordando que los bits en la llave de enciframiento están numerados del 1 al 64, de izquierda a derecha, la permutación elegida 1 especifica que los bits de C_0 son respectivamente, los bits 57, 49, 41,...,9,1,58,50,..., 18, 10, 2, 59,..., 27, 19, 11,..., 36 de la llave de enciframiento. De igual forma, los bits de D_0 son respectivamente los bits 63, 55, 47,..., 15, 7, 62, 54,..., 22, 14, 6, 61,..., 29, 21, 13, 5,..., 4 de la llave de enciframiento.

La permutación elegida 2 es utilizada para seleccionar una llave en particular K_n de una concatenación de C_n y D_n. C_n y D_n, cada una de 28 bits de longitud por lo que C_nD_n combinadas tienen bits que van del 1 hasta el 54. La permutación elegida 2 está resumida en la figura 4.5. Los bits en la subllave K_n están numerados del 1 al 48, de izquierda a derecha y son respectivamente los bits 14, 17,..., 5, 3, 28,..., 10, 23, 19,..., 8,..., 46, 42,..., 32 de C_nD_n. Debe de notarse que la permutación elegida 2 es utilizada en el cálculo de cada una de las subllaves K_1 hasta K_{16}.

En la implantación del algoritmo DES, se anticipa que los cálculos de la lista de llaves van a ser realizados como procedimeintos iterativos, donde la iteración 1 genera K_1, la iteración 2 genera K_2 y así sucesivamente. El número de corrimientos circulares hacia la izquierda, para cada iteración de cálculo se resume en la siguiente tabla.

Segunda Permutación, utilizada en el cálculo de la subllave Ki.

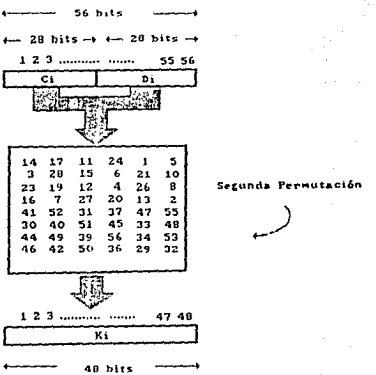


FIGURA 4.5

Número de iteración	Número de corrimientos circulares hacia la izquierda
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Suma módulo-2

La operación suma módulo-2 bit a bit es utilizada en varios pasos del algoritmo DES. La operación denotada por $\oplus$ se define de la siguiente manera:

$\oplus$	0	1
0	0	1
1	1	0

Así que el siguiente ejemplo será válido:

$$\begin{array}{r} 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0 \\ \oplus\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1 \\ \hline 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1 \end{array}$$

La operación suma modulo-2 es la misma que la operación de OR-exclusiva.

Función de enciframiento

La función de enciframiento abarca las operaciones principales de la transformación producto. Esta función es utilizada en cada iteración de la transformación producto y está definida por:

$$f(A, K_n)$$

Donde A es una cadena de 32 datos representando R_i para encripción y L_i para decripción, y K_n es una subllave de 48 bits determinada del cálculo de la lista de llaves.

La figura 4.6 nos presenta un panorama de la funcion de enciframiento la cual combina las siguientes operaciones:

a.- Una operación de selección E que opera en el argumento A de 32 bits y produce un resultado de 48 bits.
b.- Una suma módulo-2 que suma, el resultado de la operación de selección E y la llave K_n de 48 bits, bit a bit para producir un resultado de 48 bits.
c.- Un juego único de funciones de seleccion S_i que convierte el resultado de 48 bits de la suma modulo-2 en un juego de 32 bits.
d.- Una operación de permutación P que opera en el resultado de 32 bits de la operación previa y produce un resultado de 32 bits.

La operación de selección E descrita en la figura 4.7, produce un resultado de 48 bits donde los bits de resultado son respectivamente los bits 32, 1, 2,..., 5, 4, 5,..., 9, 8, 9,..., 13, 12, 13,..., 17, 16, 17,..., 21, 20, 21,..., 25, 24, 25,..., 29, 28, 29,..., 1 del argumento simbólico A, que representa R_i o L_i, para encriptar o decriptar respectivamente.

El juego único de funciones de selección S_i se muestra conceptualmente en la figura 4.3 en donde S_i toma un bloque de 6 bits como entrada y produce un resultado de 4 bits. La función de selección está representada como una matriz de números de 4 X 16 utilizada en una manera preestablecida.

Función de enciframiento.

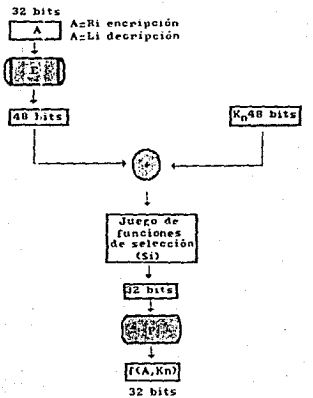


FIGURA 4.6

La operación de selección E para la función de encriptamiento.

FIGURA 4.7

La entrada al juego único de funciones de selección, de S_1 hasta S_8 es un bloque de 48 bits, denotados simbólicamente como $B_1B_2B_3B_4B_5B_6B_7B_8$. Cada B_i contiene 8 bits. S_1 va a ser utilizada con B_1; S_2 con B_2; y así sucesivamente. Si S_i es una función de selección y B_i es su argumento entonces el resultado de 4 bits de la función de selección es $S_i(B_i)$.

El resultado de la función de selección S_i en el argumento B_i, se define simbólicamente por $S_i(B_i)$ y es calculada como sigue:

a.- El primero y el último bit de B_i representan un número binario en el rango de 0 a 3, denotado por m.
b.- Los cuatro bits intermedios de B_i representan un número binario en el rango de 0 a 15, denotado por n.
c.- Utilizando indexación de origen cero, el número ubicado en la m-ésima fila y en la n-ésima columna de la S_i-ésima matriz es seleccionado como un bloque binario de 4 bits.
d.- El resultado del paso c es la salida de la función de selección S_i.

La salida del juego completo de funciones de selección por lo tanto, es la cadena $S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$ que denota simbólicamente la salida S_1 de cuatro bits, seguida de la salida S_2 de cuatro bits y así sucesivamente.

La figura 4.8 contiene un ejemplo del uso de la función de selección S_1. La entrada a la función es la siguiente cadena de 6 bits: 101100. El primero y el último bit de la entrada son 1 y 0, respectivamente, que es la representación binaria del número 2. Esta es la fila indexada. Los cuatro bits intermedios de la entrada son: 0110, que es la representación binaria del numero 6. Esta es la columna indexada. Utilizando indexación de origen cero, el valor localizado en la fila dos y columna 6 de la matriz S_1 es el valor 2. El valor dos entonces es convertido a su valor binario de cuatro bits correspondiente 0010, que es la salida de cuatro bits de la función de selección S_1 para la entrada dada.

La siguiente tabla nos da las matrices correspondientes de S_1 hasta S_8.

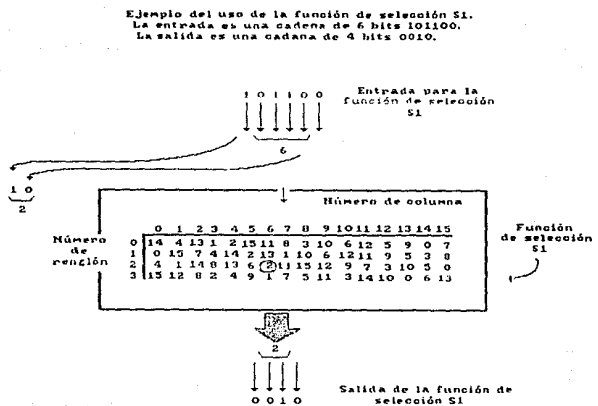

Ejemplo del uso de la función de selección S1.
La entrada es una cadena de 6 bits 101100.
La salida es una cadena de 4 bits 0010.
1 0 1 1 0 0
Entrada para la función de selección S1
6
1 0
2
Número de columna
Número de renglón
Función de selección S1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
1 0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8
2 4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
3 15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13
4
2
0 0 1 0
Salida de la función de selección S1

FIGURA 4.8

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

La salida del juego de ocho funciones de selección, S_1 a S_8, es una cadena de 32 bits, mostrada en la figura 4.3. Esta salida de 32 bits va a través de una operación de permutación P que produce un resultado de 32 bits y completa la función de encíframiento, esta permutación final en la función de encíframiento se muestra en la figura 4.9. La operación de permutación P produce un resultado de 32 bits donde los bits de resultado son respectivamente, 16, 7, 20, 21, 29,..., 17, 1,..., 26, 5,...., 10, 2,...., 14, 32,..., 9, 19,..., 6, 22,...., 25 del resultado de 32 bits del juego de funciones de selección.

Bloque "presalida"

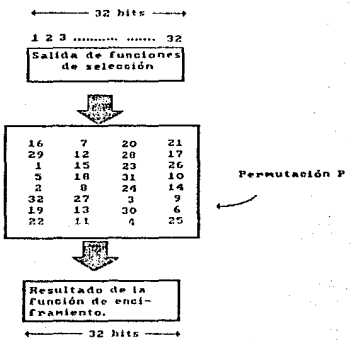
La salida de la última iteración en la transformación producto va a través de un bloque de transformación produciendo un resultado de 64 bits denominado bloque "presalida". En el bloque de transformación se realiza un simple intercambio de R_{16} y L_{16}, como se representa en la figura 4.10. El bloque "presalida" está formado de los bits de R_{16} seguido de los bits de L_{16} y constituye un bloque de 64 bits los cuales están numerados del 1 al 64 de izquierda a derecha.

Permutación inicial

La permutación inicial es el primer paso en el algoritmo DES y es la permutación llave independiente dada en la figura 4.11. La salida de la permutación inicial es respectivamente los bits 58, 50,..., 2, 60, ..., 4, 62,..., 61, 53,..., 5, 63,..., 7 del texto completo de entrada al algoritmo DES.

El resultado de la permutación inicial (PI) es un bloque de 64 bits. Los 32 bits de la izquierda constituyen L_0; los 32 bits de la derecha constituyen R_0. L_0 y R_0 son los bloques iniciales de entrada a la transformación producto.

La operación de permutación P en la función de enciframiento.



FICURA 4.9

Bloque de transformación para producir el bloque presalida.

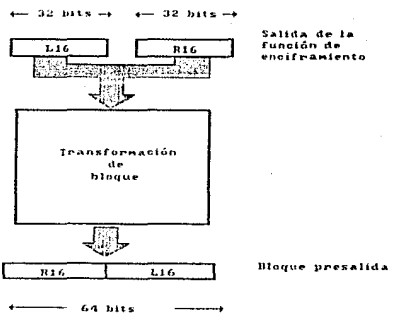


FIGURA 4.10

Permutación inicial (PI).

FIGURA 4.11

Permutación inicial inversa

La salida de la transformación producto es el bloque "presalida" que está sujeto a una permutacion que es el inverso de la permutacion inicial. La permutación inicial inversa (PI^{-1}) se muestra en la figura 4.12. La salida de la PI^{-1}, que es sinónimo del texto de enciframiento de salida del algoritmo es, respectivamente, los bits 40, 8,..., 32, 39,..., 31, 38,..., 34, 2,..., 26, 33, 1,..., 25 del bloque "presalida".

El texto de enciframiento de salida de 64 bits del algoritmo DES, puede ser utilizado como una cadena de datos para transmisión o almacenamiento, o puede ser convertido en caracteres BCD para subsecuentes procesamientos de datos.

El proceso de enciframiento

El proceso de enciframiento se puede resumir de la siguiente manera. Dados dos bloques L y R y utilizando la regla de que LR denota el bloque formado de los bits de L seguido de los bits de R, la permutación inicial (PI) se define como:

$$L_0R_0 \leftarrow PI(<\text{bloque de entrada de 64 bits}>)$$

Entonces si KS denota el cálculo de la lista de llaves donde la funcion KS produce una subllave K_n de 48 bits para los argumentos de entrada n y LLAVE, donde LLAVE es la llave de enciframiento de 64 bits, donde

$$K_n \leftarrow KS(n, LLAVE)$$

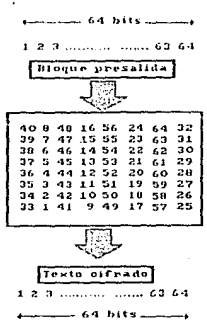
denota el cálculo de la subllave K_n.

Las 16 iteraciones en la transformación producto que utilizan la función de enciframiento son representadas simbólicamente por:

$$L_n \leftarrow R_{n-1}$$

$$R_n \leftarrow L_{n-1} \oplus f(R_{n-1}, K_n)$$

Permutación inicial inversa (PI^{-1}).



Permutación inicial inversa.

FIGURA 4.12

donde f es la función de enciframiento y $\oplus$ denota suma módulo-2 bit a bit. L_n y R_n son calculados a medida que n va desde 1 a 16. El bloque "presalida" es $R_{16}L_{16}$ y el resultado del algoritmo es especificado como:

$$\text{<texto encifrado de 64 bits>} \leftarrow PI^{-1}(R_{16}L_{16})$$

El proceso de descifrar un bloque de texto cifrado de 64 bits involucra el mismo algoritmo de enciframiento. Esto se debe a que la permutación inicial y la permutación inicial inversa son por definición inversas entre sí.

Aplicando la notación anterior, el resultado de la permutación inicial (PI) está dada por:

$$R_{1A}L_{1B} \leftarrow PI(\text{<texto cifrado de 64 bits>})$$

donde la expresión toma la transformación del bloque final en consideración. Las 16 iteraciones en la transformación producto está representadas simbólicamente como:

$$R_{n-1} \leftarrow L_n$$

$$L_{n-1} \leftarrow R_n \oplus f(L_n, K_n)$$

donde L_0 y R_0 son calculadas a medida que n varía de 16 a 1. El resultado del deciframiento es especificado como:

$$\text{<texto original de 64 bits>} \leftarrow PI^{-1}(L_0R_0).$$ **[11]**

4.6 APLICACION DE CRIPTOGRAFIA A REDES

Las técnicas de criptografía pueden ser implantadas en una red de comunicaciones en tres formas básicas:

a.- Encripción enlace-a-enlace. Cada enlace de comunicación de un centro de conmutación a su centro de conmutación vecino tiene su propia llave de encripción. Dentro de los centros de conmutación, los mensajes que llegan son decriptados, y luego encriptados otra vez usando la llave para el siguiente enlace.

b.- Encripcion nodo-a-nodo. Es una variación de la enripción enlace-a-enlace donde cada enlace usa una llave única, pero la traducción de una llave a otra se lleva a cabo en un módulo especial de seguridad en el centro de conmutacion o el nodo.

c.- Encripción fin-a-fin. El transmisor encripta el mensaje y este permanece así mientras es transmitido a través de la red, hasta que es recivido y decriptado por el receptor.

d.- Super-encripción. Se utiliza encripcion enlace-a-enlace (o nodo-a-nodo) y encripción fin-a-fin para mayor seguridad. [20]

Técnica de encripción enlace-a-enlace.

FIGURA 4.13

Técnica de encripción nodo-a-nodo.

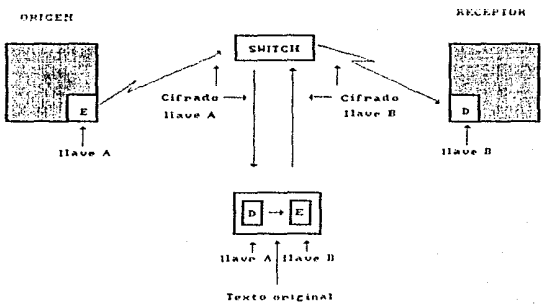


FIGURA 4.14

4.7 ADMINISTRACION DE LLAVES

Es obvio que la seguridad que puede dar un sistema de criptografía depende de la seguridad en sus llaves. Esto se hace más evidente en el algoritmo DES ya que es un algoritmo de dominio público. Lo que garantiza la seguridad del mensaje encriptado bajo este algoritmo es la confidencialidad de sus llaves. Esto hace pensar que se les debe dar mayor protección a las llaves que a los datos mismos. Por esto, es prudente mantener en secreto los procedimientos de administración de llaves. Las lleves deben ser impredecibles, preferentemente números aleatorios. Se deben tener precauciones en su almacenamiento; deben ser encriptadas también con una llave maestra y se debe ser cuidadoso en su distribución.

Hay tres métodos esenciales para su distribución: por correo certificado, correo diplomático o por medio de la red de comunicaciones del sistema de cómputo. El último requiere el desarrollo de protocolos, facilidades especiales y un poco de sentido común. Por ejemplo, no se debe usar la llave actual para encriptar las llaves que están siendo distribuidas. Para esto existe una jerarquía de llaves:

a.- Llave de sesion, establecida para una interacción fin-a-fin entre transmisor y receptor. Esta llave es temporal y será desechada cuando la sesión termine.
b.- Llave submaestra, usada para encriptar las llaves de sesión cuando son almacenadas en archivos de llaves o transmitidas a través de la red.
c.- Llave maestra, usada para proteger las llaves submaestras cuando están almacenadas en archivos. Debe estar físicamente segura pues no tiene protección de encripción. [20]

Deben tomarse muy en cuenta los siguientes puntos para fortalecer la seguridad:

a.- La generación de la llave debe hacerse en forma aleatoria, secreta y sin que intervenga el factor humano.
b.- Deben de existir dos tipos de llaves: una maestra y una de sesión de trabajo.
La función de la llave maestra es la de encriptar la llave de sesión.

La función de la llave de sesión es la de encriptar los datos.

c.- Las llaves maestras nunca deben viajar en el medio de comunicación , su transportación deberá ser en un dispositivo confiable e inviolable.

d.- El cambio de las llaves de sesión se deberá realizar en forma secreta y aleatoriamente en el tiempo.

e.- Los cambios de las llaves maestras deberán ser bajo una política impuesta por la institución correspondiente.

4.8 OTROS SISTEMAS CRIPTOGRAFICOS

Criptosistemas con llaves públicas

La necesidad de protección sobre las llaves se deriva de que se debe usar la misma llave para encriptar y decriptar un mensaje. Hace poco se descubrió que si existían dos llaves diferentes, K_E para encriptar y K_D para decriptar, ambas generadas al mismo tiempo pero con la propiedad de que dada K_E no se puede derivar K_D, entonces K_E se puede hacer pública sin comprometer la seguridad del sistema. Esto se conoce como un criptosistema con llave pública. No se requiere de distribución de llaves, ya que cada usuario genera su propio par K_E y K_D, hace K_E pública pero guarda K_D en secreto.

Estos sistemas deben tener las siguientes características:

a.- Decripción revierte a encripción
$$T_D(T_E M)=M$$

b.- Decripción no puede ser posible sin K_D
$$T_E(T_E M)<>M$$

c.- Se puede generar el par (K_E,K_D) en forma fácil
d.- No se puede obtener K_D de K_E
e.- Encripción revierte a decripción
$$T_E(T_D M)=M$$

Actualmente se está trabajando con sistemas que cumplan con estas características pero son difíciles de llevar a cabo. Uno de los más conocidos actualmente funciona de la siguiente manera:

a.- El mensaje M es representado como un entero positivo.
b.- Las llaves de encripción y decripción se diseñan así:

- Dos números primos grandes, p y q, se escogen y se forman dos cantidades
  $n=pq$ y $r=(p-1)(q-1)$

- Se selecciona un entero F en forma aleatoria de modo que 3<F<r y que no tenga factores comunes con r. Luego se halla otro entero D que es el inverso de F módulo r.
- La llave de encripción K_E, consiste del par (F,n) y la de decripción K_D, es el par (D,n).

c.- Dado un mensaje M, que es un entero entre 1 y n-1, la encripción produce el texto cifrado E de la siguiente manera:

$$E=M^F \bmod(n)$$

d.- La decripción se lleva a cabo mediante la operación

$$M=E^D \bmod(n) \qquad [20]$$

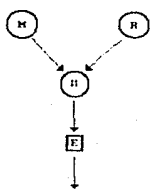
Técnicas de encripción aleatorias

Un procedimiento de encripción aleatoria cifra un texto escogiendo aleatoriamente un texto cifrado de un conjunto de ellos que corresponden a un mensaje bajo la actual llave de encripción. Produce un texto cifrado vía una función no determinística del mensaje a encriptar y de la llave de encripción. Para cada llave, un mensaje dado puede ser encriptado de muchas maneras; el procedimiento de encripción hace una selección aleatoria para elegir cual manera usar. Se asume que para cada llave, cada texto cifrado corresponde a lo más a un mensaje.

Este tipo de esquema requiere una fuente generadora de bits aleatorios. Estas fuentes pueden ser construidas usando tubos de descarga de neón, diodos de ruido, deshechos radioactivos, u otras fuentes naturales de aleatoriedad.

Como para cada llave, cada mensaje corresponde a varios textos cifrados y cada texto cifrado corresponde a lo mas a un mensaje, el espacio de textos cifrados sera mayor que el espacio del mensaje. Esto requiere de una expansión del ancho de banda en el canal de comunicaciones porque se deben transmitir mayor número de bits para especificar el texto cifrado. Este es le mayor costo de usar encripción aleatoria y es inevitable. En la figura 4.15 se muestra un diagrama de bloques del proceso. [18]

Método "RELLENO ALEATORIO".



M: Mensaje
R: Secuencia aleatoria
E: Encripción determinística
||: Concatenación

FIGURA 4.15

Una de las técnicas es concatenar una secuencia aleatoria a un blogue del mensaje y encriptar el resultado. La unidad de decripción aplica la función de decripcion y desecha la secuencia aleatoria. Este método se llama "Relleno Aleatorio"

Por lo menos 28 compañías tienen en el mercado hardware para encripción; 14 de ellas utilizan DES. Las características de funcionamiento de este hardware varían ampliamente en parámetros como velocidad de encripción, seguridad física, administración de llaves, costo, complejidad de operación y configuración física:

a.- La velocidad de encripción varía entre 9.6 Kbps a 10 Mbps. La mayoría opera cerca del límite inferior, los aparatos de alta velocidad son generalmente los más costosos.
b.- El precio por unidad (se necesitan dos para un enlace) varía entre 300 y 10,000 dólares.
c.- Todos menos los más simples proporcionan protección extra como retroalimentación.
d.- El consumo de energía varía entre 100 W y 10 W.

El futuro de la encripción de datos en informática no se presenta del todo claro, ya que los especialistas en seguridad siguen considerando válida la utilización del algoritmo D.E.S. para fines comerciales pero sugieren que para aplicaciones específicas se desarrollen algunos otros que pudieran ser más efectivos. [5]

5

ANALISIS E IMPLANTACION DE UN ESQUEMA DE SEGURIDAD Y CONFIDENCIALIDAD EN UNA EMPRESA DEL SECTOR FINANCIERO

5.1 INTRODUCCION

El propósito del presente documento es proporcionar una panorámica del análisis e implantacion del esquema de seguridad para el sistema de atención a clientes de PROBURSA S.A. DE C.V. a través de cajeros automáticos.

Se presentará una descripción del problema y se definirán los objetivos que se buscan cubrir con este nuevo servicio. También se presentará el proceso del cajero automático y una descripción de los programas que se ejecutarán en el computador principal para atender el cajero.

PROBURSA S.A. de C.V. tiene como uno de sus objetivos ofrecer nuevos servicios a sus clientes a traves de cajeros automáticos.

Dentro de los servicos que se desean ofrecer encontramos los siguientes:

a.- Retiro en efectivo. Un cliente podrá retirar efectivo del cajero automático a traves de la venta de titulos de las emisoras PROGRESA o PRODUCE, o retirarlo del efectivo disponible que tenga.
b.- Consulta de titulos. Por medio de este servicio, un cliente obtendrá el detalle del monto de efectivo al que equivalen los titulos que tiene en las diferentes emisoras.
c.- Consulta de los últimos movimientos. Con este servicio, el cliente obtendrá detalles de sus últimas operaciones realizadas.
d.- Transferencia entre emisoras. El cliente podrá realizar la venta de titulos de una emisora, y con el importe obtenido comprar titulos en otra.

5.2 DESCRIPCION DEL MEDIO AMBIENTE OPERACIONAL

El medio ambiente de hardware y de software en donde deben operar las aplicaciones que atenderán los servicios del sistema de cajeros automáticos son:

a.- Ambiente de cómputo en PROBURSA:

- Procesador central IBM 4381 con sistema operativo MVS/XA (Memory Virtual Storage/Extended Architecture).
- Método de acceso a disco VSAM.
- Método de acceso a teleproceso VTAM (Virtual Telecommunications Access Method).
- Monitor de teleproceso CICS.
- Procesador de comunicaciones IBM 3725 trabajando en ambiente SNA (System Network Architecture) con NCP (Network Control Program).
- Método de transmisión SDLC (Synchronous Data Link Control).
- Manejador de base de datos DB2.
- Lenguaje para desarrollo de aplicaciones CSP (Cross System Product) con acceso a SQL (Structured Query Language).

b.- Ambiente del VS/6E

- Minicomputador WANG VS/6E con sistema operativo VS versión 7.13.
- Dos líneas de comunicaciones multipunto programables.
- Programa desarrollado en lenguaje COBOL. Es un programa de conversión de protocolo el cual, al entrar en funcionamiento queda como una terminal virtual bajo CICS en el computador principal.

c.- Equipo interface

- Cajero automático de WANG modelo 8160.
- Teclado.
- Video de 560 caracteres.

- Lectora de tarjetas con banda magnética.
- Impresora de auditoria.
- Impresora de 40 columnas para comprobante a clientes.
- Línea de comunicación hacia la VS con protocolo asincrono POLL/SELECT.

d.- Ambiente de software

En la actualidad PROBURSA, Casa de Bolsa ofrece los servicios de atención a clientes en su casa matriz y sucursales a través de un promotor. El retiro de efectivo no existe en este momento. En su lugar, PROBURSA emite cheques a veinticuatro horas a solicitud del cliente apoyados en la venta de titulos correspondientes al monto solicitado por el cliente.

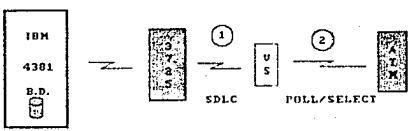
Las aplicaciones computacionales están orientadas a un promotor; es decir que, un cliente siempre interactúa con un promotor para obtener un servicio.

Las aplicaciones están actualmente implantadas en un sistema IBM 38 y se están rediseñando y reimplantando en un sistema IBM 4381.

El objetivo a nivel sistema es crear y/o modificar las aplicaciones que sean necesarias, tanto en el computador principal como en la VS/6E para que el cajero automático pueda brindar los servicios que se desean ofrecer.

La figura 5.1 nos muestra el diagrama a bloques del sistema de cajeros automáticos así como su conexión al sistema 4381.

Diagrama a bloques del sistema de cajeros automáticos
en PROBURSA S.A. de C.V.



1 Comunicación con eliminador de modem porque el 3725 requiere de un reloj.
2 Utilización de línea telefónica y dos modems configurados para protocolo POLL/SELECT.

FIGURA 5.1

5.3 OBJETIVOS Y DESCRIPCION DE LOS SERVICIOS A OFRECER

Los objetivos específicos que se buscan son:

a.- Brindar al cliente los servicios de retiro, consultas y transferencia a través del cajero automático.
b.- Implantar estos servicios cumpliendo los siguientes requisitos:

- Los programas de aplicación que atiendan las solicitudes del cajero automático estén en el computador principal. Los programas deberán desarrollarse con las herramientas que se tienen actualmente.
- Que el manejo del cajero y su interacción con el computador principal sea lo más eficiente posible; tanto en recursos de consumo de hardware como de software. Esto involucra evitar en la medida de lo posible duplicidad de archivos, consumo excesivo de memoria en el computador principal, facilidad para el mantenimiento y desarrollo de nuevos requerimientos.
- Que las aplicaciones que están en el computador principal, que van a servir como parte de atención del nuevo servicio, no sean modificadas en más de un 5%.
- Que las nuevas aplicaciones que se tengan que desarrollar se adapten perfectamente a las actuales de forma tal que no se tengan que hacer cambios al diseño actual del sistema.

Descripción de los servicos a ofrecer

Un cliente de PROBURSA, debidamente autorizado, podrá llegar a un cajero automático y realizar las siguientes operaciones:

a.- Retiro de efectivo de las emisoras PROGRESA o PRODUCE o de su disponible. El cliente deberá insertar su tarjeta de uso del cajero, éste le solicitará su número de identificación personal. Si el acceso es autorizado el cliente deberá proporcionar el monto a retirar. El

sistema deberá verificar que el usuario esté autorizado para retirar efectivo del cajero y que exista la suficiente cantidad de títulos en su cuenta para cubrir el monto solicitado. En caso de que el retiro sea del disponible, el sistema verificará que exista suficiente disponible, para cubrir el monto solicitado.

Al momento de pasar esta verificación, el sistema realizará la venta de los títulos correspondientes al monto solicitado o se entrega el disponible de la cuenta del cliente, se afecta la cartera correspondiente a las transacciones, se genera un número de folio para marcar las transacciones realizadas y se envía un código de retorno al cajero para que entregue el dinero al cliente.

Si el cajero no tiene suficiente disponible para cubrir el monto solicitado, o alguna otra causa no le permite entregar el dinero, el cajero envía al sistema un mensaje para que se revierta la transacción.

Si el cajero puede terminar la transacción, entonces entregará el dinero y un comprobante al cliente. Enseguida enviará un código de fin de transacción al sistema.

b.- Consulta de títulos y último movimiento. El cliente insertará su tarjeta y el cajero le solicitará su número de identificación personal. El sistema deberá verificar que el cliente esté autorizado para realizar este tipo de transacción.

Para la consulta de títulos el sistema consultará el archivo maestro de cartera. Clasificará la cartera por emisora, calculará su valor de acuerdo al precio del día y obtendrá un total por emisora y un total final. El sistema enviará esta información al cajero y este emitirá una salida impresa para que el cliente la recoja.

c.- Transferencia entre emisoras (PROGRESA y PRODUCE). El cliente insertará su tarjeta y el cajero le solicitará su número de identificación personal. El sistema deberá verificar que el cliente esté autorizado para realizar este tipo de transacción. Si esta verificación es

satisfactoria, el sistema deberá generar la venta de títulos de la emisora origen, y a su vez realizar la compra de títulos por el mismo monto, en la emisora destino. El sistema actualizará la cartera, enviará código de retorno y detalles de la transacción al cajero. Con esta información el cajero procederá a emitir un comprobante de la transacción para que lo retire el cliente.

5.4 CAJEROS AUTOMATICOS

5.4.1 LOS CAJEROS AUTOMATICOS Y SUS SERVICIOS

Los controles utilizados en un cajero automático (ATM; Automated Teller Machine) nos proporcionan un ejemplo de controles que cumplen con prevenir que ocurra un evento no deseado y/o el poder contener el impacto del evento no deseado hasta un cierto límite de tolerancia.

Para hacer uso de un cajero automático el usuario debe tener tanto una tarjeta válida como un número de identificación personal válido.

Este usuario del ATM puede ser el dueño de una cuenta de alguna institución financiera o pudo haber obtenido tanto la tarjeta como el número de identificación personal de una manera fraudulenta.

Como el cajero automático no tiene la capacidad de distinguir entre estas dos posibilidades, se programa al cajero automático para no proporcionar o despachar más de cierto límite de dinero durante cualquier periodo de 24 hrs.

Los controles del programa de computadora tampoco pueden detectar a un usuario no autorizado que tiene tanto la tarjeta válida como el número de identificación personal, a menos de que se hubiese reportado la tarjeta.

Lo que sí puede detectar es cuando se quiere retirar más dinero del que se tiene disponible. Y también puede ser diseñado para detectar atentados físicos a su circuitería para lo cual utiliza un sistema de alarmas.

El ATM no proporciona el dinero sino hasta que se válida la identificación del usuario, así como la cantidad de dinero disponible, por lo tanto si se detectó algo no deseado el evento fraudulento se puede prevenir.

d.- Una alta atención y disponibilidad hacia los clientes, obteniendo una mejor imagen y realización comercial de los productos ofrecidos.

Todos los cajeros automáticos están integrados por los elementos siguientes:

a.- Pantalla de salida de datos.
b.- Teclado de acceso de la información.
c.- Dispositivo lector de tarjetas magnéticas.
d.- Mecanismo emisor de billetes.
e.- Unidad de recepción de los depósitos.
f.- Caja blindada que protege las áreas de almacenamiento de depósitos y del dinero.

Existen productos derivados de esta nueva tecnología y que son variantes del cajero automático. Entre los ya existentes en el mercado, se encuentran:

a.- Terminales que sólo proporcionan consulta de saldos e información, así como traspaso entre cuentas.
b.- Los denominados "dispensadores de efectivo", que a excepción de los depósitos ofrecen los demás servicios de cajero automático.

Así mismo, ya existen en el mercado, cajeros automáticos que cuentan con las innovaciones siguientes:

a.- Pantalla de salida de datos policromática.
b.- Selección digital de opciones en la pantalla, logrando una mejor claridad para el cliente, y la eliminación de teclas.
c.- Incremento en el tipo de billetes que pueden manejarse, ofreciendo al cliente la selección hasta de 5 denominaciones distintas.

En el contexto del sistema financiero mexicano, las instituciones que lo conforman han procurado implantar el sistema de cajeros automáticos, con objeto de mejorar su servicio para sus clientes y descongestionar sus sucursales.

Como producto de la flexibilidad de los cajeros automáticos que ya se encuentran operando, así como de la alta creatividad que han mostrado las instituciones financieras para ofrecer más y mejores servicios, es probable que en un plazo breve se implanten otras facilidades en sus sistemas respectivos.

5.4.2 SISTEMA DE CAJEROS AUTOMATICOS

Un sistema de cajeros automáticos es el compuesto por todos los elementos requeridos para que los cajeros automáticos sean atendidos por una computadora y puedan proporcionar las facilidades previstas para los clientes. Estos elementos pueden clasificarse en los siguientes tipos:

Físicos

a.- Uno o varios equipos de computo.
b.- Equipos periféricos: unidades de disco y cintas, impresoras de alta velocidad.
c.- Equipos de teleproceso: controladores de teleproceso, controladores de proceso distribuido.
d.- Sistema de telecomunicaciones: líneas telefónicas, modems, conmutadores de señal, controladores de telecomunicaciones, equipos especiales para transmisión vía satélite o microondas.
e.- Los cajeros automáticos y su equipo complementario: cartuchos contenedores de dinero, de disgnóstico y de mantenimiento.
f.- Requeridos para su operación: terminales, impresoras.

De programación

a.- Del sistema operativo y ambiente de teleproceso.
b.- De los programas en línea.
c.- De los programas batch que procesan cada sistema: cheques, valores, etc.
d.- De los programas de cajeros automáticos.

De operación del sistema

a.- De los procesos generales del sistema: arranque, terminación, reinicio.
b.- Detección y control de condiciones anormales:

- Agotamiento del dinero disponible.
- Vandalismo.
- Funcionamiento incorrecto.

c.- De la operación de la red de cajeros automáticos.
d.- De la ejecución de los procesos batch.

Administrativos

Procedimientos y áreas que controlen:

a.- Aclaraciones a clientes.
b.- Aclaraciones internas.
c.- Operación.
d.- Mantenimiento de equipos.
e.- Instalación de nuevas facilidades.
f.- Manejo y uso de reportes.
g.- Papelería y accesorios complementarios.
h.- Generación y control de tarjetas magnéticas y claves de acceso personales.
i.- Consulta e impresión de información en tiempo real.
j.- Reportes de sistemas asociados obtenidos vía batch.
k.- Reportes y controles específicos de auditoría.
l.- Reportes estadísticos de volumen de operaciones y errores.

De seguridad

a.- Relacionados con la ubicación y segura instalación de cada cajero automático.
b.- Procedimientos y estructuras que permitan la segura ejecución del sistema:

- Archivos maestros en línea de cada aplicación y un respaldo de cada uno de fácil puesta en operación.
- Archivos de registro de transacciones normal y espejo para evitar pérdida de las transacciones operadas.
- Agil reinicio y recuperación del sistema.
- Acceso físico restringido al equipo de operación
- Niveles de control de acceso (password) y funciones en terminales de operación.

Inherentes al sistema de cajeros automáticos

a.- Acceso controlado a clientes basados en tarjeta magnética y clave de acceso (número de identificación personal).
b.- Protección de la información a través del sistema de telecomunicaciones por medio de técnicas de reacomodo y recodificación de los datos (cifrado).
c.- Contadores de transacciones efectuadas y de billetes procesados por cada emisor.
d.- Mensajes de alerta enviados al computador que indica apertura de puertas de seguridad, atoramiento o error en los dispositivos, así como el estado operativo.
e.- Estructura blindada y chapas de combinación.
f.- Dispositivos detectores integrados de detección de:

- Apertura de puertas.
- Calor.
- Movimiento.

g.- Dispositivo de activación de cámara fotográfica por cada acceso de clientes.

5.4.3 DESCRIPCION DEL PROCESO

Como sucede en la mayoría de sistemas en tiempo real, un sistema de cajeros automáticos consta de dos subsistemas principales:

a.- De servicio en línea.
b.- De procesos en lote (batch).

a.- De servicio en línea

La mayoría de estos sistemas funcionan con los archivos siguientes:

- Archivos maestros del sistema de cajeros automáticos.
- Archivos maestros por cada tipo de cuenta.
- Archivos de registro de transacciones efectuada (diarios).
- Archivos de auditoría y de recuperación del sistema.
- Archivos de consulta en tiempo real.

Así mismo, se acostumbra que en forma diaria se inicie un ciclo de operaciones, debiendo de existir procesos de inicio y terminación.

Procesos de operación del ciclo operativo

Dependiendo de la institución, en algunos casos se efectúa la baja del sistema en su totalidad. En otros casos, se efectúa la suspensión total del servico mientras se desconectan los archivos usados y se reconectan los nuevos archivos. Para los archivos se preveen los procesos siguientes:

- Se verifica que los archivos maestros estén debidamente actualizados, aplicando las transacciones operadas a una copia de los archivos maestros generados en el ciclo anterior.

- Se sacan copias de los archivos de registro de transacciones y se procesan para que queden sin ninguna información, o en su defecto se reconectan nuevos archivos vacios.
- Para los archivos de auditoria y recuperación del sistema, se efectúa la misma acción del inciso anterior.
- Los archivos de consulta en tiempo real, casi siempre son regenerados para que no tenga informacion alguna.

Proceso de inicio del ciclo

Ya habiendo concluido los procesos que se ejecutan durante la terminación, se procede a efectuar la alta total del sistema en algunas instituciones. En otras, se procede a efectuar la reconexión de los archivos previamente verificados e inicializados.

Reinicio y recuperación del sistema

Como un punto especial, cabe mencionar que los sistemas en línea bajo situaciones esporádicas y urgentes tienen necesidad de suspensión y, para ello efectuan su terminación, sin embargo, en estos casos no se efectúan los procesos de archivos relacionados con la terminación del ciclo de operaciones.

Bajo esta condición, de acuerdo a las facilidades técnicas de cada sistema deberán preveerse los elementos que a continuación se citan:

- Actualización forzada de áreas de entrada/salida del sistema de los archivos.
- Vaciado de áreas de control del sistema en medios magnéticos para un correcto reinicio del sistema.
- Procedimientos especiales de operación y administrativos para información y atención al cliente.

Al corregirse la situación que originó la suspensión del servicio, el sistema se iniciará de una forma similar al inicio de un nuevo ciclo, excepto que los archivos y condicionamientos del sistema deben conservar el estado operativo que se tenía al suspenderse las operaciones.

b.- Relacionado con procesos en lote (batch)

En todo sistema se aplican un conjunto de procesos para cada ciclo diario de operaciones, los cuales tienen por objeto la actualización y control de los sistemas relacionados con cada tipo de cuenta, que denominaremos como aplicaciones.

De un modo general, puede indicarse que se efectúan procesos que satisfacen los siguientes objetivos:

- Integrar en los bancos de datos de cada aplicación los movimientos efectuados:
  - De cajeros automáticos.
  - De otros sistemas en línea, vía terminales.
  - De sistemas de captura.
  - De otras aplicaciones, como son las remesas de otros bancos, traspasos de fondos y los originados en el interior de la república.
- La obtención de reportes impresos para aclaraciones control de las operaciones efectuadas y auditoría del sistema, así como los relacionados con las aplicaciones.
- Generar en medios magnéticos, los archivos previstos para sistemas externos y para procesos periódicos, así como para fines estadísticos.

5.4.4 PROCESO DE UNA TRANSACCION EN UN SISTEMA DE CAJEROS AUTOMATICOS

a.- El cliente inserta su tarjeta e introduce su clave de acceso para poder hacer uso del cajero automatico.

b.- Se le solicita que tipo de transacción requiere efectuar, a lo que el cliente digita los datos siguientes:

- Tipo de transacción.
- Tipo de cuentas.
- Importe (excepto en consultas).

En este momento, algunas transacciones son rechazadas con base a la tarjeta magnética.

c.- Se cifran los datos y la transacción es enviada al computador para su proceso.

d.- El computador recibe la transaccion, la interpreta y válida en primera instancia que provenga de un cajero reconocido en su red.

e.- Se procesa el mensaje recibido y se accesa el archivo maestro de clientes, verificándose las condiciones siguientes:

- Que la tarjeta sea valida y se encuentre vigente en el sistema:
  - Que no tenga fecha vencida.
  - Que no tenga condicionamientos de retención.
- Que la transaccion solicitada sea factible de ejecutarse de acuerdo a las politicas vigentes por tipo de tarjeta, y así el cliente tiene acceso al sistema con respecto a la transacción.
- Si la transacción es de retiro en efectivo, se verifica que el importe solicitado no exceda de los limites asignados según el tipo de cliente.

f.- Se efectúa el acceso a los archivos de los sistemas relacionados con cada cuenta, verificándose que la transacción sea válida para las políticas de cada aplicación y que existan los fondos suficientes. En este momento, se graban en los archivos de registro de transacciones (diarios), el intento de transacción.

g.- Si la transacción fue autorizada por el sistema se efectúan los procesos siguientes:

- Se enviará un mensaje de regreso al cajero automático, indicando al cliente que su transacción fue ejecutada correctamente.
- Se guarda información de control para el proceso relacionado con archivos por cuenta y el maestro de clientes.

h.- Si la transacción no fue autorizada por no existir fondos o excederse de las políticas establecidas se envía al cajero automático un mensaje en el cual se indican las causas de rechazo.

i.- El cajero automático recibe el mensaje de rechazo o autorización, indicando al cliente cual fue el resultado de su solicitud. Si la transacción fue autorizada, en la mayoría de los casos procede a emitir un comprobante de la operación efectuada y de ser un retiro en efectivo, procede a emitir el dinero solicitado.

j.- El cajero automático envía al computador un mensaje de terminación del proceso, en el cual se describe como concluyó la transacción. En el caso de retiros en efectivo, es sumamente importante debido a que indica si el dinero se proporcionó al cliente.

k.- El computador recibe el mensaje, efectuando los siguientes procesos:

- Si la transacción fue autorizada la graba en los archivos de transacciones, actualiza los archivos por cuenta y el maestro de clientes.
- Actualiza los archivos de consulta de auditoría en tiempo real del sistema.
- Informa sobre la transacción efectuada en los medios de control y registros existentes en el sistema (impresoras y/o terminales). **[1]**

5.5 ELEMENTOS DE SEGURIDAD Y AUDITORIA

5.5.1 GENERALIDADES

Tarjeta magnética

Con base a una tarjeta magnética se habilita que solo los clientes que la posean puedan accesar un sistema de cajeros automáticos. La información comunmente grabada es:

a.- Tipo de tarjeta.
b.- Cuenta del cliente.
c.- Plaza geográfica.
d.- Versión de la tarjeta.
e.- Fecha de expiración.

Desde el momento en que la tarjeta es leida por el cajero automático, su programación verificará si es válida y en caso contrario la rechazará.

De acuerdo a la tarjeta se le permitirá el acceso al cliente para las transacciones que le son permitidas efectuar.

Clave de acceso

Para poder dar inicio a sus operaciones, cada cliente de un sistema de cajeros automáticos, posterior a la aceptación de su tarjeta deberá digitar una clave secreta de identificación. Exclusivamente a través de la clave correcta el cliente podrá accesar el servicio.

Esta clave de acceso a diferencia de la metodología usada tradicionalmente en los sistemas de terminales ofece las características de seguridad que a continuación se citan:

a.- Es calculada en forma local por la tecnología del propio cajero automático con base a ciertos datos de control que sólo puede interpretar la electrónica de este equipo.

b.- La obtención de estas claves de acceso para su envío a clientes, se efectúa por medio de procesos especiales de alta seguridad que tienen las siguientes características:

- Los módulos de carga y datos de control se generan exclusivamente al inicio del sistema bajo una mecánica integral de seguridad, la cual impide su conocimiento e interpretación por programadores y operadores.
- El documento que se envía a cada cliente para hacer de su conocimiento la clave de acceso, se genera en un papel especial que consta de dos partes o elementos de seguridad que son:

  . Una que sirve de cubierta, impidiendo que sea visible la impresión.
  . Otra en donde el cliente tiene impresa su clave.

  El papel especial usado tiene por objeto que ninguna persona se entere de la clave de acceso y que sólo el cliente al cortar este documento se entere de la clave asignada.

c.- Con el uso conjunto de tarjeta magnética y clave de acceso se logra un mejor nivel de seguridad pues si se cuenta con sólo uno de los elementos citados no es posible hacer uso de los cajeros automáticos.

Cifrado

Esta facilidad permite que la información que fluye a través del sistema de telecomunicaciones y teleproceso se encuentre protegida respecto a interpretación para fines no autorizados.

La técnica de cifrado es de uso general en los sistemas de cajeros automáticos pues la mayoría de éstos cuentan con facilidades electrónicas que efectúan automáticamente el cifrado de los datos. Como medida de seguridad, los programadores de estos sistemas sólo conocen una porción de datos que se cifran y los parámetros que requiere este tipo de electrónica para operar. Sin embargo, carecen de los elementos de control que por características integrales, son incluso desconocidos para los que fueron responsables de instalar el sistema.

Es importante mencionar que la información se cifra y descifra por medio de programas que cumplen este propósito en el computador. Las complicaciones se presentan al llegar a requerir el acceso a la información en su forma natural para atender fallas del sistema o verificar su contenido.

Es casi imposible alterar la información que fluye en las telecomunicaciones debido a los requerimientos siguientes:

a.- Se requiere la posibilidad y el equipo para interceptar el sistema de telecomunicaciones.
b.- Se requiere el equipo de decodificado de señal electrónica de comunicaciones a la señal electrónica del cajero correspondiente.
c.- Se necesita que el equipo de cómputo, programas y parámetros de control que permitan modificar la información.
d.- Se requieren programas de alta técnica y amplios conocimientos del sistema específico, y aun así no sería factible forzar a un cajero automático o al computador a efectuar procesos no contemplados en sus políticas y controles de operación.

Controles del sistema

Los cajeros automáticos cuentan con un conjunto de medios electrónicos integrados que proporcionan control sobre la correcta continuidad de los procesos efectuados por cada cajero automático. Los más comunes son:

a.- Número consecutivo de las transacciones operadas.
b.- Cantidad de billetes emitidos por cada tipo de denominación.
c.- Verificación de la cantidad que el cajero prevee será emitida contra la cantidad ordenada por el sistema.
d.- Lógica encadenada de mensajes de diferentes tipos y formatos que se debe procesar en un orden especifico (protocolo de proceso).
e.- Indicación de mensajes especificos de la terminación del proceso.

Con los medios anteriores, un sistema de cajeros automáticos puede detectar un intento no autorizado y proceder a ejecutar una acción preprogramada para evitarlo.

Estos medios se encuentran en forma preestablecida en la electrónica del cajero automático y su control debe estar implantado en los programas del computador.

En adición a los medios citados, pueden existir:

a.- Contadores de depósitos recibidos.
b.- Contadores de lecturas de tarjeta magnética y de impresiones efectuadas.
c.- Contadores de billetes procesados para su emisión.
d.- Contadores de tarjetas retenidas.
e.- Contadores de errores y mal funcionamiento por cada tipo de dispositivo:

- Pantalla.
- Lectora de tarjetas.
- Teclado.
- Receptor de depósitos.
- De cada cartucho o casette contenedor de billetes.
- De la impresora de comprobantes.
- De la impresora de operaciones efectuadas.

f.- Registros electronicos de fallas en la lógica de proceso.
g.- Registros electrónicos del estado operativo del cajero.
h.- Registros indicativos de la configuración de proceso con la que opera el cajero.

- Es más difícil para las personas el recordar un número que ellos no han elegido y por lo tanto tendrían que escribirlo en un papel.
- El cliente nunca podrá cambiar su NIP aun cuando este haya sido violado.
- El único camino para obtener un nuevo NIP es cambiando el número de cuenta de la institución (Cancelar contrato viejo, abrir número de contrato nuevo).
- Todos los miembros de una cuenta deberán utilizar el mismo NIP.

b.- Si se le permite al cliente la elección del NIP, se obtendrán los siguientes beneficios:

- El cliente puede asociar su NIP con alguna fecha fácilmente recordable.
- El NIP puede ser cambiado en cualquier momento. Lo único que se necesita es proporcionar una tarjeta nueva.
- Los miembros de una sola cuenta pueden tener su propio NIP.
- Si la tarjeta de algún miembro de una cuenta se pierde, o el NIP es violado, únicamente hay que proporcionar una tarjeta para ese cliente y los otros miembros no requieren el cambio de tarjeta.
- El NIP nunca es registrado en la institucion y no es conocido por ninguna otra persona.
- El cliente tiene la opción de utilizar el NIP natural si así lo desea, estando advertido de las consecuencias que esto implica.

Producción de las tarjetas magnéticas

a.- Se sugiere pedirle al fabricante una docena de tarjetas que tengan las especificaciones de la institución, para realizar pruebas en el sistema de cajeros automáticos de PROBURSA, antes de emitir el total de la orden. Ya que esta es la única manera de estar seguros que las especificaciones están perfectamente entendidas.

b.- Si uno elige la opción de que el cliente eliga su NIP se tendrá lo siguiente:

- Se le debe proporcionar al fabricante de tarjetas la llave del NIP y una lista que contenga los números de cuenta incluyendo el nombre del cliente y el NIP elegido; enseguida el fabricante calculará el DES NIP offset y lo codificará en las posiciones 27 a 30 de la pista II de la tarjeta. Después de esto las tarjetas estan listas para distribuirlas a los clientes.
- El segundo método proporciona mayor seguridad tanto para la institución como para el cliente.

Proceso de codificación de tarjetas magnéticas

A continuación daremos una breve explicación del proceso de codificación que se utilizará para las tarjetas magnéticas de PROBURSA, Casa de Bolsa.

Independientemente del tipo de método de producción de tarjetas magnéticas que se elija se deberán seguir los siguientes pasos:

1.- Proporcionar los datos válidos. La longitud de los datos deberá tener las siguiente estructura:

0000787741999999

De la primera a la décima posicion deberá estar el número de cuenta del cliente, el cual debe ir alineado a la derecha.

2.- Proporcionar al proveedor de tarjetas magnéticas la llave de encripción para el NIP.

Para este punto se requiere contar con mucha seguridad. Es recomendable que la llave de encripción se divida en dos partes. Estas partes se le deben de proporcionar a diferentes personas de la institución financiera, las cuales desconocen que alguien más tiene parte de la llave de encripción.

3.- Enseguida se debe de utilizar algun algoritmo de encripción. Para el sistema de cajeros automáticos se decidió utilizar el algoritmo de encripción DES. Este algoritmo como lo vimos en el capitulo anterior es el más utilizado y lo que lo hace único es la llave de 64 bits que utiliza.

5.5.2.3 DIARIO ESTADISTICO Y TIRA DE AUDITORIA

Diario Estadistico

El diario estadístico es un programa desarrollado en COBOL. Fue desarrollado por el personal de la empresa proveedora. El programa se encuentra en la VS/6E y su objetivo principal, es el de proporcionar el estado en el que se encuentran cada uno de los cajeros automáticos conectados a la red, generar estadísticas; para el mantenimiento y el autoservicio; e ir generando un diario histórico. Es un programa básico dentro de la seguridad del sistema de cajero automáticos.

Con la información que proporciona este diario, la institución financiera puede planear la frecuencia con la que se debe de dar mantenimiento a los cajeros automáticos y de esta manera mejorar el servicio a los clientes.

La información que queda registrada en el diario estadístico es la siguiente:

a.- Entrada y salida de una sesión de mantenimiento.- cuando algún cajero automático se encuentra en modo de mantenimiento, el diario estadistico nos proporciona:

- La dirección del cajero automatico que se encuentra en mantenimiento.
- Nos indica la fecha y la hora tanto de entrada como de salida de la sesión de mantenimiento.
- Informa el tipo de mantenimiento que se le está realizando al cajero.
- Proporciona la clave del usuario que está realizando el mantenimiento.

b.- Reemplazo de cassettes de efectivo y rechazos.- cuando se realiza este tipo de mantenimiento la información que se graba en el diario es muy especial, ya que nos informa que la actividad que se está realizando tiene que ver directamente con el efectivo que maneja el cajero automático.

El cajero automático es programado para reconocer cuando su dotación de efectivo es baja y requiere el reemplazo de algún cassette. En éste caso el cajero manda un mensaje que queda registrado en el diario. Este mensaje contiene la dirección del cajero, la fecha y la hora en la que solicitó el mantenimiento.

c.- Prueba de cassettes de despacho.- despues de haber realizado el reemplazo de cassettes de efectivo, la persona de mantenimiento debe de realizar la prueba de cassettes de despacho. Esto es muy importante que quede registrado en el diario estadístico, ya que a la hora de correr esta prueba la persona de mantenimiento recibe un billete de cada cassette.

d.- Procedimiento de mantenimiento del lector de tarjetas magnéticas.- cada vez que el cajero automático retiene una tarjeta magnética, graba en el diario estadístico un registro el cual se va incrementando cada vez que éste se ejecute. Cuando el operador corre las estadísticas que proporciona el diario y se da cuenta que un cajero ha llegado a su capacidad máxima de tarjetas magnéticas retenidas (este parámetro puede ser fijado por la institución), debe de llamar al personal de mantenimiento para que este cambie el cassette de tarjetas retenidas.

En el diario estadístico queda grabada la información de la fecha y la hora en la cual se realizó el reemplazo del cassette, la clave del usuario que realizó el reemplazo y automáticamente se limpia el contador o registro de tarjetas magnéticas retenidas que se tenía.

e.- Procedimiento para dotar al cajero automático de rollos para la impresión de recibos.- de la misma manera que para el reemplazo de cassettes de efectivo, el cajero automático es programado para mandar un mensaje cuando su dotación de rollo de impresión es baja. Es muy importante estar al pendiente de este tipo de mensaje, ya que un descuido en el procedimeinto de dotación, daría una mala imagen de la institución.

Algo que en el diario histórico no se registra es el reemplazo de cartuchos de cinta entintadora. Este reemplazo se debe realizar al mismo tiempo que se haga la dotación de los rollos de impresión de recibos, aun cuando la cinta no esté muy desgastada.

Como podemos observar, en el diario histórico queda registrado todo tipo de información referida al funcionamiento del cajero automático y al mantenimiento que se le realice. Además es de este diario de donde la institución va a ir adquiriendo experiencia para poder mejorar el servicio a sus clientes. También podrá observar que tipo de lugares son los más concurridos y en cuales se retira mayor efectivo.

Tira de auditoria

La seguridad de datos cubre tanto la integridad como la recuperación de los mismos.

Mientras el cajero automático atiende a un cliente, cada cambio que afecta los totales de auditoria es registrado en la tira de auditoria. La integridad de los datos durante la comunicación se logra con el uso de números de transmisión diferentes para cada mensaje.

Cada movimiento realizado por un cliente tiene su propio número de transmisión con el cual es identificado en caso de haber algún problema con los movimientos del cliente. La tira de auditoria se le entrega a los responsables del departamento de auditoria de la institución.

La tira de auditoria no es un papel explicito ya que su contenido lo constituyen números y claves que identifican la acción realizada. Dentro de la tira de auditoria encontramos datos como los siguientes:

a.- Número de cuenta que utilizo el servicio de cajeros automáticos.
b.- Hora de entrada y de salida del sistema.
c.- Fecha en la cual se realizó la acción
d.- Clave de la acción efectuada.

En caso de haber realizado un retiro de efectivo, en la tira de auditoria queda grabada la cantidad y la denominación de los billetes que se le entregaron al cliente.

En caso de que el cajero automático entregara al cliente más dinero del solicitado, esta cantidad quedará registrada en la tira de auditoria. Por lo tanto no puede haber ningún error.

e.- Código de falla.- en caso de que hubiera alguna falla del sistema o del cajero automático, ésta quedaria registrada en la tira de auditoria. Los códigos de falla definidos corresponden a los siguientes módulos:

- Alarmas.
- Cámara.
- Lector de tarjetas.
- Despachador.
- Comunicación con el 4381 de IBM.
- Impresora de recibos para el cliente.
- Impresora de auditoria.

5.6 PROGRAMAS PARA EL SISTEMA DE CAJEROS AUTOMATICOS

La solución propuesta se ubica dentro del siguiente medio ambiente:

a.- VS/6E

Esta computadora manejará los siguientes programas que son específicamente para el manejo, control y administración del cajero automático.

- AIS.- programa utilizado para el manejo de comunicaciones entre la VS/6E y el cajero automático. Está desarrollado en microcódigo.
- DOWNLOAD.- programa utilizado para la carga de parámetros de configuración y pantallas de la VS/6E al cajero automático. Este programa está desarrollado en COBOL y BASIC.
- ATM-VS/6E-IBM.- es un programa desarrollado en COBOL, por medio del cual se realiza la interfase de envío de mensajes entre las solicitudes del cajero automático y las aplicaciones en el IBM 4381.
- UTILITARIOS.- los utilitarios nos ayudan para el desarrollo, la administración y mantenimiento de aplicaciones para el cajero automático. Dentro de estos contamos con los siguientes:

  . EZFORMAT.- que es un generador dinámico de pantallas.
  . SCRENVT.- es un validador de pantallas y convertidor a formato cajero automático.
  . ESTADOS.- es un generador de tabla de estados para manejo del cajero automático.
  . SCRFLOW.- este utilitario es un emulador del cajero automático en la VS/6E para pruebas y desarrollos.

Cabe mencionar que de todas estas aplicaciones en la única que se tuvo participación fue en la aplicación ATM-VS/6E-IBM. Las demás fueron desarrolladas por gente de Panamá y de Estados Unidos de Norteamérica.

b.- IBM 4381

Dentro del 4381 se desarrollaron todos los programas de aplicación que atenderán las solicitudes del cajero automático y realizan las transacciones en la base de datos.

- VXC0200.- este programa es el núcleo del sistema de toda la casa de bolsa. El programa ejecuta diferentes transacciones de compra/venta de títulos, solicitudes de cheques, autorizaciones, cancelaciones e impresiones.
- VXC0230.- programa de captura de datos para atender solicitudes de retiro en efectivo. Este programa transfiere parámetros al VXC0200 para que realice la operación.
- VIC0900.- programa que procesa la consulta de títulos.
- VIC0950.- programa para la opción de consulta de los últimos movimientos de un cliente.
- VOC0330.- programa que realiza la transferencia de títulos entre emisoras.

Los programas en los cuales se tuvo participación en el 4381 son: VXC0230, VIC0900, VIC0950 y VOC0330. Debido a su confidencialidad únicamente se presentan en este trabajo algunas partes de ellos.

PROGRAMAS

MSL CONCATENATION SEQUENCE

	MSL ACCESS ORDER	MSL FILE NAME
READ/WRITE MSL:	1	MCAPIMSL
READ-ONLY MSL(S):	2	DESARMSL
	3	
	4	
	5	
	6	

APPLICATION NAME: VIC0950
TYPE OF APPLICATION: MAIN TRANSACTION
WORKING STORAGE: VIW0950I
MAP GROUP NAME: VIC095
HELP MAP GROUP NAME:
HELP MAP PF KEY:
BYPASS EDIT PF KEYS:
PF1-12,PF13-24: YES
ALLOW IMPLICITS: YES
MESSAGE FILE: SIMC
MSL: DESARMSL

PROLOGUE

INSTALACION: CASA DE BOLSA PROBURSA, S.A.
CREACION: AGOSTO DOE 1988.
OBJETIVO: OBTENER LOS ULTIMOS 5 MOVIMIENTOS REALIZADOS POR UN CLIENTE.

TABLE AND ADDITIONAL RECORDS LIST

SQLCA	RECORD

```
VIE095P  ************************************************************                2
         *          PROCESO PRINCIPAL                  DESARMSL *
         ************************************************************
         OPTION -    EXECUTE                 OPTION                                  5

                     ;************************************************************  7
                     ;                    EXECUTE: VIE095P                        8
                     ;                    PROCESO PRINCIPAL                       9
                     ;************************************************************ 10
                     MOVE 1 TO EZECNVCM                ; LIBERA RECURSOS          11
                     MOVE 1 TO EZEFEC                  ; LIBERA RECURSOS          12
                     SET MIO1 EMPTY                    ; LIMPIA MAPA MIO1         13
                     PERFORM VIN095A                   ; DESPLIEGA MAPA MIO1      14
                     PERFORM VII095A                   ; INQ DE LA TABLA CUENTA   15
                     MOVE CUENTA.NOMBRE TO VIW09501.NOMBRE;                       16
                     MOVE CUENTA.NAPELL1 TO VIW09501.NAPELL1;                     17
                     IF CUENTA NOT NRF                 ; EXISTE CLIENTE           18
                       IF CUENTA.SVIGEN NE 'B'         ; VIGENCIA ALTA            19
                         PERFORM VIT095A               ; SETINQ DE TARJETA        20
                         PERFORM VIE095A               ; CONSULTA DE ULTIMOS MOVIMIENTOS 21
                       ELSE ;                                                     22
                         MOVE 61 TO EZEMNO;                                       23
                       END ;                                                      24
                     ELSE ;                                                       25
                       MOVE 18 TO EZEMNO;                                         26
                     END ;                                                        27
                     PERFORM VIN095B                   ; DESPLIEGA MAPA MIO2      28
```

ADDITIONAL PERFORMED PROCESSES

```
VIN090A  ********************************************************                30
         *       DESPLIEGA MAPA MIO1                DESARMSL *
         ********************************************************
         OPTION -  CONVERSE MIO1                MAP                             33
VII090A  ********************************************************                35
         *       INQ CUENTA                         DESARMSL *
         ********************************************************
                   ;*************************************************************  38
                   ;                INQUIRY: VII090A                             *  39
                   ;*************************************************************  40
                   MOVE MIO1.ICUENTA TO CUENTA.ICUENTA;                            41
         OPTION -  INQUIRY  CUENTA          RECORD          VRC0250              42

                   SQL SELECTION CONDITIONS MODIFIED:              YES

                   SELECT
                     SVIGEN, ICUENTA,
                     NOMBRE, NAPELL1
                   INTO
                     :SVIGEN, :ICUENTA,
                     :NOMBRE, :NAPELL1
                   FROM
                     CUENTA T1
                   WHERE
                     ICUENTA = :ICUENTA
                   ;** INSERT ORDER BY CLAUSE HERE **

VIT090A  ********************************************************                44
         *       SETINQ CARTERA PRECIO              DESARMSL *
         ********************************************************
                   ;*************************************************************  47
                   ;                  SETINQ: VIT090A                            *  48
                   ;*************************************************************  49
                   MOVE MIO1.ICUENTA TO VIJ09001.ICUENTA;                          50
                   MOVE MIO1.WTODOFOR TO VIJ09001.FPRECIO.                         51
         OPTION -  SETINQ   VIJ09001        RECORD          VRC0250              52

                   SQL SELECTION CONDITIONS MODIFIED.              YES

                   SELECT
                     T1.ICUENTA, T1.IEMISORA, T1.ISERIE, T1.ICUPON,
                     T1.CTITULOS, T2.IEMISORA, T2.ISERIE, T2.ICUPON,
                     T2.MPRECOMP, T2.ICONCEPT, T2.FPRECIO,
                     T2.HPRECIO
                   INTO
```

```
                    :ICUENTA, :IEMISORA1, :ISERIE1, :ICUPON1, :CTITULOS,
                    :IEMISORA, :ISERIE, :ICUPON, :MPRECOMP, :ICONCEPT,
                    :FPRECIO, :MPRECIO
                  FROM
                    CARTERA T1,
                    PRECIO T2
                  WHERE
                    T1.ICUENTA = :ICUENTA AND T1.IEMISORA = T2.IEMISORA AND
                    T1.ISERIE = T2.ISERIE AND T1.ICUPON = T2.ICUPON AND
                    T2.FPRECIO = (SELECT MAX(FPRECIO)
                    FROM     PRECIO PR1    WHERE
                     T2.IEMISORA = PR1.IEMISORA AND
                     T2.ISERIE = PR1.ISERIE AND
                     T2.ICUPON = PR1.ICUPON) AND
                     T2.MPRECIO = (SELECT MAX(MPRECIO)
                    FROM     PRECIO PR2    WHERE
                     T2.IEMISORA = PR2.IEMISORA AND
                     T2.ISERIE = PR2.ISERIE AND
                     T2.ICUPON = PR2.ICUPON AND
                     T2.FPRECIO = PR2.FPRECIO)
                  ;** INSERT ORDER BY CLAUSE HERE **

VIE090A   ************************************************************                    54
          -       REALIZA CALCULO TOT CART.          DESARROL *
          ************************************************************
          OPTION -    EXECUTE                  OPTION                                     57

                      ;************************************************************      59
                      ;                EXECUTE: VIE090A                                  60
                      ;************************************************************      61
                      PERFORM VIS090A                  ;SCAN A CARPRE                    62
                      SET MIO2 EMPTY                   ;LIMPIA MAPA                      63
                      MOVE 0 TO WI090AUX               ;LIMPIA                           64
                      MOVE 0 TO AI090I                 ;LIMPIA                           65
                      WHILE VIJ09001 NOT NRF;                                            66
                        IF VIJ09001.IEMISORA = 'PROGRES';                                67
                          OR VIJ09001.IEMISORA = 'PRODUCE';                              68
                          IF VIJ09001.IEMISORA = 'PROGRES';                              69
                            MOVE 1 TO AI090I;                                            70
                          END ;                                                          71
                          IF VIJ09001.IEMISORA = 'PRODUCE';                              72
                            MOVE 2 TO AI090I;                                            73
                          END ;                                                          74
                          WI090TOT(AI090I) = VIJ09001.CTITULOS * VIJ09001.MPRECOMP;      75
                          MOVE VIJ09001.IEMISORA TO WI090EMI(AI090I);                    76
                          MOVE VIJ09001.CTITULOS TO WI090TIT(AI090I);                    77
                          MOVE VIJ09001.MPRECOMP TO WI090PRE(AI090I);                    78
                          WI090TOC = WI090TOC + WI090TOT(AI090I);                        79
                          PERFORM VIS090A                ;SCAN CARPRE                    80
                        ELSE ;                                                           81
                          WI090AUX = VIJ09001.CTITULOS * VIJ09001.MPRECOMP;              82
                          WI090TOT(3) = WI090TOT(3) + WI090AUX;                          83
```

```
                    MOVE "OTROS" TO WI090EMI(3);                                  84
                    WI090TOC = WI090TOC + WI090TOT(3);                            85
                    PERFORM VIS090A             ;SCAN CARPRE                      86
                  END ;                                                           87
                END                           ;WHILE NRF                        88
                MOVE VIW09001.WI090NOM TO MI02.WI090NOM;                          89
                PERFORM VII090B               ; INQ CARTERA                     90
                IF CARTERA.ICONCEPT = 1;                                          91
                  WI090TOT(3) = WI090TOT(3) + CARTERA.CTITULOS;                   92
                  WI090TOC = WI090TOC + CARTERA.CTITULOS;                         93
                END ;                                                             94

VIS090A  ********************************************************                 96
         *          LEE EL RENGLON DE CARPRE            DESARMSL *
         ********************************************************
         OPTION -  SCAN    VIJ09001      RECORD        VRC0250                    99

                   SQL SELECTION CONDITIONS MODIFIED:          NO

                   FETCH EZL_CURSOR_NNN USING DESCRIPTOR SQLDA

VII0908  ********************************************************                101
         *          INQ CARTERA                         DESARMSL *
         ********************************************************
                   MOVE MI01.ICUENTA TO CARTERA.ICUENTA;                          104
                   MOVE 1 TO CARTERA.ICONCEPT;                                    105
         OPTION -  INQUIRY  CARTERA      RECORD        VRC0250                    106

                   SQL SELECTION CONDITIONS MODIFIED:          YES

                   SELECT
                     ICUENTA, ICONCEPT,
                     CTITULOS
                   INTO
                     :ICUENTA, :ICONCEPT,
                     :CTITULOS
                   FROM
                     CARTERA T1
                   WHERE
                     T1.ICUENTA = :ICUENTA AND
                     T1.ICONCEPT = :ICONCEPT

VIN0908  ********************************************************                108
         *                                              DESARMSL *
         ********************************************************
         OPTION -  CONVERSE MI02          MAP                                     111
```

STATEMENT GROUPS

```
VRC0250  ************************************************************                113
         *          MANEJO DE ERRORES DE SQL            DESARMSL *
         ************************************************************
                  IF EZESQCOD < 0;                                                   116
                    OR EZESQCOD = 100;                                               117
                    OR EZESQCOD = -803;                                              118
                  ELSE ;                                                             119
                    CALL EZEROLLB;                                                   120
                    MOVE EZESQLCA TO SQLCA.SQLCASCA;                                 121
                    MOVE EZESQCOD TO SQLCA.SQLCACOD;                                 122
                    MOVE EZESQRRM TO SQLCA.SQLCAHRM;                                 123
                    MOVE EZESQRD3 TO SQLCA.SQLCARD3;                                 124
                    MOVE EZESQWN1 TO SQLCA.SQLCAWN1;                                 125
                    MOVE EZESQWN6 TO SQLCA.SQLCAWN6;                                 126
                    ; IF WAM01 NE 'B';                                               127
                    CALL VRC0300 SQLCA            ; ON-LINE                          128
                    ; ELSE ;                                                        129
                    ;   CALL VRC0750 SQLCA          ; BATCH                        130
                    ; END ;                                                         131
                    EZECLOS;                                                         132
                  END ;                                                              133
```

APPLICATION STRUCTURE

NAME	LVL	OPTION	OBJECT	ERROR	DESCRIPTION	LINE
VIE090P	001	EXECUTE			PROCESO PRINCIPAL	2
VIN090A	002	CONVERSE	MIO1		DESPLIEGA MAPA MIO1	30
VII090A	002	INQUIRY	CUENTA	VRC0250	INQ CUENTA	35
VRC0250	003	GROUP			MANEJO DE ERRORES DE SQL	113
VII090A	002	SETINQ	VIJ09001	VRC0250	SETINQ CARTERA PRECIO	44
VRC0250	003	GROUP			MANEJO DE ERRORES DE SQL	113
VIE090A	002	EXECUTE			REALIZA CALCULO TOT CART.	54
VIS090A	003	SCAN	VIJ09001	VRC0250	LEE EL RENGLON DE CARPRE	96
VRC0250	004	GROUP			MANEJO DE ERRORES DE SQL	113
VII090B	003	INQUIRY	CARTERA	VRC0250	INQ CARTERA	101
VRC0250	004	GROUP			MANEJO DE ERRORES DE SQL	113
VIN090B	002	CONVERSE	MIO2			108

GENERATION OPTIONS

LOAD LIBRARY	=	DESARALF
CREATE REFERENCE FILE	=	NO
PRINT STATEMENT LISTING	=	NO
FOLD PRINT	=	NO
VALIDATE SQL STATEMENTS	=	YES
EXECUTION MODE	=	SEGMENTED
SEGMENTED TRANSACTION	=	109A
CLIST FOR DPPX/SP	=	YES

MAP GROUPS

GENERATE	NAME
YES	VIG090

DB2 STATIC MODULE

GENERATE	NAME
YES	VIC09005

RECORD DEFINITIONS

RECORD NAME: VIW09001

ORGANIZATION: WORKING STORAGE
LENGTH IN BYTES: 100
MSL: DESARMSL

NO PROLOGUE

NAME	LVL	OCCURS	TYPE	LENGTH	DEC	BYTES	START	MSL	DESCRIPTION
ICLIENTE	10		CHA	16		16	1	MCAPIMSL	ICLIENTE
ICUENTA	10		PACK	7		4	17	MCAPIMSL	ICUENTA
WI090FOP	10		CHA	10		10	21	DESARMSL	FECHA DE LA TRANSACCION
WI090AUX	10		PACK	15	2	8	31	DESARMSL	VARIABLE AUXILIAR WI090TOT
AI090I	10		PACK	3		2	39	DESARMSL	CONTADOR
WI090NOM	10		CHA	60		60	41	DESARMSL	NOMBRE DEL CLIENTE
NOMBRE	15		CHA	20		20	41	MCAPIMSL	NOMBRE
NAPELL1	15		CHA	40		40	61	MCAPIMSL	NAPELL1

RECORD DEFINITIONS

RECORD NAME: SQLCA

ORGANIZATION: WORKING STORAGE
LENGTH IN BYTES: 216
MSL: DESARMSL

NO PROLOGUE

NAME	LVL	OCCURS	TYPE	LENGTH	DEC	BYTES	START	MSL	DESCRIPTION
SQLCASCA	10		CHA	136		136	1	MCAPIMSL	
SQLCACOD	10		BIN	9		4	137	MCAPIMSL	
SQLCARRM	10		CHA	70		70	141	MCAPIMSL	
SQLCARD3	10		BIN	9		4	211	MCAPIMSL	
SQLCAWN1	10		CHA	1		1	215	MCAPIMSL	
SQLCAWNG	10		CHA	1		1	216	MCAPIMSL	

RECORD NAME: CUENTA

ORGANIZATION: SQL ROW
DEFAULT KEY ITEM:
LENGTH IN BYTES: 738
MSL: MCAPIMSL

SQL TABLE NAME(S)

USER ID TABLE NAME TABLE LABEL

CUENTA T1

```
DEFAULT SELECTION CONDITIONS
SELECT
  SVIGEN, ICTAGLO, ICUENTA, ITIPOCTA, IPERJUR,
  IRFC, ITASAFIS, INACIO, IPROM, ICCOSTO,
  IUSUARIO, IPROGRAM, FALTA, FALTAANT, FBAJA,
  FULTCAMB, FULTMOV, IENVDOC, NPROF, NABREV,
  NOMBRE, NAPELL1, NAPELL2, DCALLE, DCOLON,
  DPOBLA, IPOS, DESTADO, DCALLEP, DCOLONP,
  DPOBLAP, IPOSP, DESTADOP, ITEL1, IEXT1, ITEL2,
  IEXT2, ICAPTA, IFIRMA, IRUTA, SCOMPNAC, SDOCUM,
  SLIQUID, SOPER12, PCOMCTA, MABOANO, MABOMES,
  MCGOANO, MCGOMES, MCARACT, MCARIMES, APREFMAR,
  FDEBEDES, XSEG
INTO
  :SVIGEN, :ICTAGLO, :ICUENTA, :ITIPOCTA, :IPERJUR,
  :IRFC, :ITASAFIS, :INACIO, :IPROM, :ICCOSTO,
  :IUSUARIO, :IPROGRAM, :FALTA, :FALTAANT, :FBAJA,
  :FULTCAMB, :FULTMOV, :IENVDOC, :NPROF, :NABREV,
  :NOMBRE, :NAPELL1, :NAPELL2, :DCALLE, :DCOLON,
  :DPOBLA, :IPOS, :DESTADO, :DCALLEP, :DCOLONP,
  :DPOBLAP, :IPOSP, :DESTADOP, :ITEL1, :IEXT1, :ITEL2,
  :IEXT2, :ICAPTA, :IFIRMA, :IRUTA, :SCOMPNAC, :SDOCUM,
  :SLIQUID, :SOPER12, :PCOMCTA, :MABOANO, :MABOMES,
  :MCGOANO, :MCGOMES, :MCARACT, :MCARIMES, :APREFMAR,
  :FDEBEDES, :XSEG
FROM
  CUENTA T1
WHERE
:** INSERT DEFAULT SELECT CONDITIONS HERE **
```

NO PROLOGUE

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
SVIGEN	CHA	1	1	5	NO		SVIGEN	453	MCAPIMSL	SVIGEN
ICTAGLO	PACK	7	4	10	NO		ICTAGLO	485	MCAPIMSL	ICTAGLO
ICUENTA	PACK	7	4	18	YES		ICUENTA	485	MCAPIMSL	ICUENTA
ITIPOCTA	CHA	1	1	26	YES		ITIPOCTA	453	MCAPIMSL	ITIPOCTA
IPERJUR	CHA	2	2	31	NO		IPERJUR	453	MCAPIMSL	IPERJUR
IRFC	CHA	13	13	37	NO		IRFC	453	MCAPIMSL	
ITASAFIS	CHA	1	1	54	NO		ITASAFIS	453	MCAPIMSL	ITASAFIS
INACIO	CHA	2	2	59	NO		INACIO	453	MCAPIMSL	INACIO
IPROM	PACK	4	3	65	YES		IPROM	485	MCAPIMSL	IPROM
ICCOSTO	PACK	5	3	72	YES		ICCOSTO	485	MCAPIMSL	ICCOSTO
IUSUARIO	CHA	8	8	79	NO		IUSUARIO	453	MCAPIMSL	IUSUARIO
IPROGRAM	CHA	8	8	91	NO		IPROGRAM	453	MCAPIMSL	IPROGRAM
FALTA	CHA	10	10	103	NO		FALTA	453	MCAPIMSL	FALTA
FALTAANT	CHA	10	10	117	NO		FALTAANT	453	MCAPIMSL	FALTAANT
FBAJA	CHA	10	10	131	NO		FBAJA	453	MCAPIMSL	FBAJA
FULTCAMB	CHA	10	10	145	NO		FULTCAMB	453	MCAPIMSL	FULTCAMB
FULTMOV	CHA	10	10	159	NO		FULTMOV	453	MCAPIMSL	FULTMOV
IENVDOC	PACK	2	2	173	NO		IENVDOC	485	MCAPIMSL	IENVDOC
NPROF	CHA	5	5	179	NO		NPROF	453	MCAPIMSL	NPROF
NABREV	CHA	25	25	188	NO		NABREV	453	MCAPIMSL	NABREV
NOMBRE	CHA	20	20	217	NO		NOMBRE	453	MCAPIMSL	NOMBRE
NAPELL1	CHA	40	40	241	NO		NAPELL1	453	MCAPIMSL	NAPELL1
NAPELL2	CHA	20	20	285	NO		NAPELL2	453	MCAPIMSL	NAPELL2

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
DCALLE	CHA	25		25	309	NO	DCALLE	453	MCAPIMSL	DCALLE
DCOLON	CHA	25		25	338	NO	DCOLON	453	MCAPIMSL	DCOLON
DPOBLA	CHA	30		30	367	NO	DPOBLA	453	MCAPIMSL	DPOBLA
IPOS	PACK	5		3	401	NO	IPOS	485	MCAPIMSL	IPOS
DESTADO	CHA	25		25	408	NO	DESTADO	453	MCAPIMSL	DESTADO
DCALLEP	CHA	25		25	437	NO	DCALLEP	453	MCAPIMSL	DCALLEP
DCOLONP	CHA	25		25	466	NO	DCOLONP	453	MCAPIMSL	DCOLONP
DPOBLAP	CHA	30		30	495	NO	DPOBLAP	453	MCAPIMSL	DPOBLAP
IPOSP	PACK	5		3	529	NO	IPOSP	485	MCAPIMSL	IPOSP
DESTADOP	CHA	25		25	536	NO	DESTADOP	453	MCAPIMSL	DESTADOP
ITEL1	PACK	7		4	565	NO	ITEL1	485	MCAPIMSL	ITEL1
IEXT1	PACK	4		3	573	NO	IEXT1	485	MCAPIMSL	IEXT1
ITEL2	PACK	7		4	580	NO	ITEL2	485	MCAPIMSL	ITEL2
IEXT2	PACK	4		3	588	NO	IEXT2	485	MCAPIMSL	IEXT2
ICAPTA	CHA	1		1	595	NO	ICAPTA	453	MCAPIMSL	ICAPTA
IFIRMA	CHA	1		1	600	NO	IFIRMA	453	MCAPIMSL	IFIRMA
IRUTA	CHA	3		3	605	NO	IRUTA	453	MCAPIMSL	IRUTA
SCOMPNAC	CHA	1		1	612	NO	SCOMPNAC	453	MCAPIMSL	SCOMPNAC
SDOCUM	CHA	1		1	617	NO	SDOCUM	453	MCAPIMSL	SDOCUM
SLIQUID	CHA	1		1	622	NO	SLIQUID	453	MCAPIMSL	SLIQUID
SOPER12	CHA	1		1	627	NO	SOPER12	453	MCAPIMSL	SOPER12
PCOMCTA	PACK	5	4	3	632	NO	PCOMCTA	485	MCAPIMSL	PCOMCTA
MABOANO	PACK	15		8	639	NO	MABOANO	485	MCAPIMSL	MABOANO

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
MABOMES	PACK	15		8	651	NO	MABOMES	485	MCAPIMSL	MABOMES
MCGOANO	PACK	15		8	663	NO	MCGOANO	485	MCAPIMSL	MCGOANO
MCGOMES	PACK	15		8	675	NO	MCGOMES	485	MCAPIMSL	MCGOMES
MCARACT	PACK	15		8	687	NO	MCARACT	485	MCAPIMSL	MCARACT
MCARIMES	PACK	15		8	699	NO	MCARIMES	485	MCAPIMSL	MCARIMES
APREFMAR	PACK	9	5	5	711	NO	APREFMAR	485	MCAPIMSL	APREFMAR
FDEBEDES	CHA	10		10	720	NO	FDEBEDES	453	MCAPIMSL	FDEBEDES
XSEG	CHA	5		5	734	NO	XSEG	453	MCAPIMSL	XSEG

RECORD NAME: VIJ09001

ORGANIZATION: SQL ROW
DEFAULT KEY ITEM:
LENGTH IN BYTES: 117
MSL: DESARMSL

SQL TABLE NAME(S)

USER ID	TABLE NAME	TABLE LABEL
	CARTERA	T1
	PRECIO	T2

DEFAULT SELECTION CONDITIONS

```
SELECT
  T1.ICUENTA, T1.IEMISORA, T1.ISERIE, T1.ICUPON,
  T1.CTITULOS, T2.IEMISORA, T2.ISERIE, T2.ICUPON,
  T2.MPRECOMP, T2.ICONCEPT, T2.FPRECIO,
  T2.HPRECIO
INTO
  :ICUENTA, :IEMISOR1, :ISERIE1, :ICUPON1, :CTITULOS,
  :IEMISORA, :ISERIE, :ICUPON, :MPRECOMP, :ICONCEPT,
  :FPRECIO, :HPRECIO
FROM
  CARTERA T1,
  PRECIO T2
WHERE
```

```
T1.ICUENTA = :ICUENTA AND T1.IEMISORA = T2.IEMISORA AND
T1.ISERIE = T2.ISERIE AND T1.ICUPON = T2.ICUPON AND
T2.FPRECIO = (SELECT MAX(FPRECIO)
FROM
 STECNSVT.PRECIO PR1
WHERE
 T2.IEMISORA = PR1.IEMISORA AND
 T2.ISERIE = PR1.ISERIE AND
 T2.ICUPON = PR1.ICUPON) AND
 T2.HPRECIO = (SELECT MAX(HPRECIO)
FROM
 STECNSVT.PRECIO PR2
WHERE
 T2.IEMISORA = PR2.IEMISORA AND
 T2.ISERIE = PR2.ISERIE AND
 T2.ICUPON = PR2.ICUPON AND
 T2.FPRECIO = PR2.FPRECIO)
```

NO PROLOGUE

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
ICUENTA	PACK	7		4	5	YES	T1.ICUENTA	485	MCAPIMSL	ICUENTA
IEMISOR1	CHA	7		7	13	YES	T1.IEMISORA	453	DESARMSL	IEMISORA
ISERIE1	CHA	5		5	24	YES	T1.ISERIE	453	DESARMSL	ISERIE
ICUPON1	PACK	3		2	33	YES	T1.ICUPON	485	DESARMSL	ICUPON
CTITULOS	PACK	15		8	39	YES	T1.CTITULOS	485	MCAPIMSL	CTITULOS
IEMISORA	CHA	7		7	51	YES	T2.IEMISORA	453	MCAPIMSL	IEMISORA
ISERIE	CHA	5		5	69	YES	T2.ISERIE	453	MCAPIMSL	ISERIE
ICUPON	PACK	3		2	71	YES	T2.ICUPON	485	MCAPIMSL	ICUPON
MPRECOMP	PACK	15	5	8	77	YES	T2.MPRECOMP	485	MCAPIMSL	MPRECOMP
ICONCEPT	PACK	5		3	89	YES	T2.ICONCEPT	485	MCAPIMSL	ICONCEPT
FPRECIO	CHA	10		10	96	YES	T2.FPRECIO	453	MCAPIMSL	FPRECIO

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
HPRECIO	CHA	8		8	110	YES	T2.HPRECIO	453	MCAPIMSL	HPRECIO

RECORD NAME: CARTERA

ORGANIZATION: SQL ROW
DEFAULT KEY ITEM:
LENGTH IN BYTES: 175
MSL: MCAPIMSL

SQL TABLE NAME(S)

USER ID	TABLE NAME	TABLE LABEL
	CARTERA	T1

DEFAULT SELECTION CONDITIONS

```
SELECT
  ICUENTA, SCUENTA, ICONCEPT, SCONCEPT, IEMISORA,
  ISERIE, ICUPON, FCARTERA, FULTCOMP, ITIPOCAR,
  ITIPOSDO, ITIPOTEN, IREF, AREND, FVEN, CDIAPZO,
  CTITULOS, MVALMERC, MCPROEXI, ICONCEXP
INTO
  :ICUENTA, :SCUENTA, :ICONCEPT, :SCONCEPT, :IEMISORA,
  :ISERIE, :ICUPON, :FCARTERA, :FULTCOMP, :ITIPOCAR,
  :ITIPOSDO, :ITIPOTEN, :IREF, :AREND, :FVEN, :CDIAPZO,
  :CTITULOS, :MVALMERC, :MCPROEXI, :ICONCEXP
FROM
  CARTERA T1
WHERE
,** INSERT DEFAULT SELECT CONDITIONS HERE **
```

NO PROLOGUE

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
ICUENTA	PACK	7		4	5	YES	ICUENTA	485	MCAPIMSL	ICUENTA
SCUENTA	CHA	1		1	13	NO	SCUENTA	453	MCAPIMSL	SCUENTA
ICONCEPT	PACK	5		3	16	YES	ICONCEPT	485	MCAPIMSL	ICONCEPT
SCONCEPT	CHA	1		1	25	NO	SCONCEPT	453	MCAPIMSL	SCONCEPT
IEMISORA	CHA	7		7	30	NO	IEMISORA	453	MCAPIMSL	IEMISORA
ISERIE	CHA	5		5	41	NO	ISERIE	453	MCAPIMSL	ISERIE
ICUPON	PACK	3		2	50	NO	ICUPON	485	MCAPIMSL	ICUPON
FCARTERA	CHA	10		10	56	YES	FCARTERA	453	MCAPIMSL	FCARTERA
FULTCOMP	CHA	10		10	70	NO	FULTCOMP	453	MCAPIMSL	FULTCOMP
ITIPOCAR	CHA	1		1	84	YES	ITIPOCAR	453	MCAPIMSL	ITIPOCAR
ITIPOSDO	CHA	1		1	89	YES	ITIPOSDO	453	MCAPIMSL	ITIPOSDO
ITIPOTEN	CHA	1		1	94	YES	ITIPOTEN	453	MCAPIMSL	ITIPOTEN
IREF	PACK	9		5	99	NO	IREF	485	MCAPIMSL	IREF
AREND	PACK	8	4	5	108	NO	AREND	485	MCAPIMSL	AREND
FVEN	CHA	10		10	117	NO	FVEN	453	MCAPIMSL	FVEN
CDIAPZO	PACK	3		2	131	NO	CDIAPZO	485	MCAPIMSL	CDIAPZO
CTITULOS	PACK	15		8	137	NO	CTITULOS	485	MCAPIMSL	CTITULOS
MVALMERC	PACK	15	2	8	149	NO	MVALMERC	485	MCAPIMSL	MVALMERC
MCPROEXI	PACK	15	5	8	161	NO	MCPROEXI	485	MCAPIMSL	MCPROEXI
ICONCEXP	PACK	5		3	173	NO	ICONCEXP	485	MCAPIMSL	ICONCEXP

MAP GROUP NAME : VIG090 (NO MAPGROUP MEMBER DEFINED)

NUMBER OF SUPPORTED DEVICES 1

TOTAL MAPS 2

* = SUPPORTED, S = SIZE ERROR

3278-2

MAP: NAME	LINE	COLUMN	DEPTH	WIDTH	MSL	
MIO1	1	1	24	79	DESARMSL	*
MIO2	1	1	24	79	DESAPMSL	*

SPECIFICATION FOR FOLLOWING DEVICE TYPES

3278-2

MAP CHARACTERISTICS

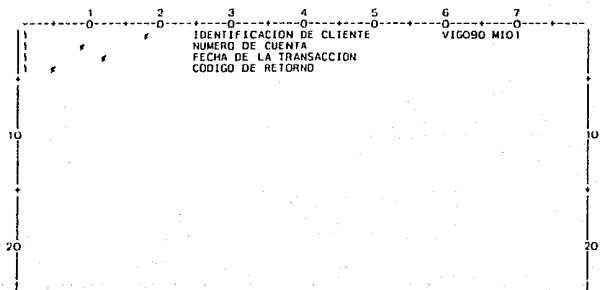
MAP SIZE: DEPTH = 24
WIDTH = 79

MAP POSITION: LINE = 1
COLUMN= 1

CURSOR FIELD = ICLIENTE

FIELD AND ATTRIBUTE DEFINITION

CONSTANT FIELD CODE: ¢
VARIABLE FIELD CODE: \
SPACER CHARACTER: /



APPLICATION NAME: VIC090O CSP/AD DATE: 05/12/89 TIME: 17:48:24 PAGE: 020
MAPGROUP: VIG090 MAP: MIO1 MSL: DESARMSL

FIELD ATTRIBUTE CHARACTERS

LINE	COLUMN	FIELD NAME	ATTRIBUTES
1	1	ICLIENTE	UNPROTECT CURSOR
2	1	ICUENTA	UNPROTECT NUMERIC
3	1	WIO90FOP	UNPROTECT
4	1	WIO90COD	UNPROTECT NUMERIC

MAP ITEM DEFINITIONS

	OCCURS	TYPE/ERR	LENGTH	DEC	JUS	FOLD	FIL	ZERO	MIN/ERR	SIGN	SEP	MONY	REQ/ERR	EDIT RTN/ERR	MIN	MAX	ERR	HEX
ICLIENTE	IDENTIFICACION DE CLIENTE																	
		CHA	16		LEF	MAP	N	NO		NO	NO	NO	NO					NO
ICUENTA	ICUENTA																	
		NUM	7		RIG	MAP	N	NO		LEA	NO	NO	NO					NO
WIO90FOP	FECHA DE LA TRANSACCION																	
		CHA	10		LEF	MAP	N	NO		NO	NO	NO	NO					NO
WIO90COD	CODIGO DE RETORNO																	
		NUM	3		LEF	MAP	N	NO		NO	NO	NO	NO					NO

SPECIFICATION FOR FOLLOWING DEVICE TYPES

3278-2

MAP CHARACTERISTICS

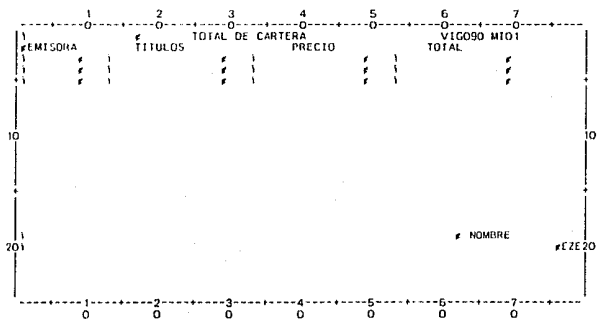
MAP SIZE: DEPTH = 24
WIDTH = 79

MAP POSITION: LINE = 1
COLUMN= 1

CURSOR FIELD - WIO90TOC

FIELD AND ATTRIBUTE DEFINITION

CONSTANT FIELD CODE: #
VARIABLE FIELD CODE: \
SPACER CHARACTER: /



MAP ITEM DEFINITIONS

	OCCURS	TYPE/ERR	LENGTH	DEC	JUS	FOLD	FIL	ZERO	MIN/ERR	SIGN	SEP	MONY	REQ/ERR	EDIT RTN/ERR	MIN	MAX	ERR	HEX
WI090I0C		TOTAL DE CARTERA NUM	15	2	RIG	MAP	N	NO		NO	YES	NO	NO					NO
WI090EM1		EMISORAS CHA	7		LEF	MAP	N	NO		NO	NO	NO	NO					NO
WI090TIT	3	TITULOS NUM	15		LEF	MAP	N	NO		NO	YES	NO	NO					NO
WI090PRE	3	PRECIO NUM	15	2	RIG	MAP	N	NO		NO	YES	NO	NO					NO
WI090I0T	3	TOTAL NUM	15	2	RIG	MAP	N	NO		NO	YES	NO	NO					NO
WI090NOM		NOMBRE DEL CLIENTE CHA	60		LEF	MAP	N	NO		NO	NO	NO	NO					NO
LZEMSG		MENSAJE DE RETORNO CHA	74		NO	MAP	N	NO		NO	NO	NO	NO					

ITEM	GROUP	TYPE	CROSS REFERENCE
AIO90I		ITEM	DEFINED IN VIW09001(RECD P9) USED IN VIE090A(PROC 65* 70* 73* 75 76 77 78 79)
APPLEMAN		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
ARENO		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
CARTERA		RECD P16	VIE090A(PROC 91 92 93) VII090B(PROC 104 105 106)
CDIAPZO		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
CTITBLOS		ITEM	DEFINED IN CARTERA(RECD P17) VIJ09001(RECD P15) USED IN CARTERA(RECD P16) VIE090A(PROC CARTERA 92 93) VIE090A(PROC VIJ09001 75. 77 82) VII090B(PROC CARTERA 106*) VIJ09001(RECD P15) VIT090A(PROC VIJ09001 52*)
CUENTA		RECD P11	VIE090P(PROC 16 17 18 19) VII090A(PROC 41 42)
DCALLE		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
DCALLEP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DCOLON		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DCOLONP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DESTADO		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DESTADOP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DPOBLA		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DPOBLAP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
EZECLOS			USED IN VAC0250(SGAP 132)
EZECNVCM			USED IN VIE090P(PROC 11*)

ITEM	GROUP	TYPE	CROSS REFERENCE		
EZEFEC			USED IN	VIE090P(PROC 12*)	
EZEMNU			USED IN	VIE090P(PROC 23* 26*)	
EZEMSG		ITEM	DEFINED IN	MIO2(MAP VIG090 P23)	
EZEROLLB			USED IN	VRC0250(SGRP 120)	
EZESQCOD			USED IN	VRC0250(SGRP 116 117 118 122)	
EZESQLCA			USED IN	VRC0250(SGRP 121)	
EZESQRD3			USED IN	VRC0250(SGRP 124)	
EZESQRRM			USED IN	VRC0250(SGRP 123)	
EZESQWN1			USED IN	VRC0250(SGRP 125)	
EZESQWN6			USED IN	VRC0250(SGRP 126)	
FALTA		ITEM	DEFINED IN	CUENTA(RECD P12)	
			USED IN	CUENTA(RECD P11)	
FALTAANT		ITEM	DEFINED IN	CUENTA(RECD P12)	
			USED IN	CUENTA(RECD P11)	
FBAJA		ITEM	DEFINED IN	CUENTA(RECD P12)	
			USED IN	CUENTA(RECD P11)	
FCARTERA		ITEM	DEFINED IN	CARTERA(RECD P17)	
			USED IN	CARTERA(RECD P16)	
FDEBEDES		ITEM	DEFINED IN	CUENTA(RECD P14)	
			USED IN	CUENTA(RECD P11)	
FPRECIO		ITEM	DEFINED IN	VIJ09001(RECD P15)	
			USED IN	VIJ09001(RECD P15)	VIT090A(PROC 51* 52*)
FULTCAMB		ITEM	DEFINED IN	CUENTA(RECD P12)	
			USED IN	CUENTA(RECD P11)	
FULTCOMP		ITEM	DEFINED IN	CARTERA(RECD P17)	
			USED IN	CARTERA(RECD P16)	
FULTMOV		ITEM	DEFINED IN	CUENTA(RECD P12)	
			USED IN	CUENTA(RECD P11)	
FVEN		ITEM	DEFINED IN	CARTERA(RECD P17)	
			USED IN	CARTERA(RECD P16)	
HPRECIO		ITEM	DEFINED IN	VIJ09001(RECD P16)	
			USED IN	VIJ09001(RECD P15)	VIT090A(PROC 52*)

ITEM	GROUP	TYPE	CROSS REFERENCE	
ICAPTA		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
ICCOSTO		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
ICLIENTE		ITEM	DEFINED IN	MIO1(MAP VIG090 P20) VIW09001(RECD P9)
ICONCEPT		ITEM	DEFINED IN	CARTERA(RECD P17) VIJ09001(RECD P15)
			USED IN	CARTERA(RECD P16) VIE090A(PROC CARTERA 91) VII0908(PROC CARTERA 105*. . 106*) VIJ09001(RECD P15) VIT090A(PROC VIJ09001 52*)
ICONCEXP		ITEM	DEFINED IN	CARTERA(RECD P17)
			USED IN	CARTERA(RECD P16)
ICTAGLO		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
ICUENTA		ITEM	DEFINED IN	CARTERA(RECD P17) CUENTA(RECD P12) MIO1(MAP VIG090 P20) VIJ09001(RECD P15) VIW09001(RECD P9)
			USED IN	CARTERA(RECD P16) CUENTA(RECD P11) VII090A(PROC CUENTA 41 42*) VII090A(PROC MIO1 41) VII0908(PROC CARTERA 104* 106*) VII090B(PROC MIO1 104) VIJ09001(RECD P15) VIT090A(PROC VIJ09001 50) VIT090A(PROC VIJ09001 50* 52*)
ICUPON		ITEM	DEFINED IN	CARTERA(RECD P17) VIJ09001(RECD P15)
			USED IN	CARTERA(RECD P16) VIJ09001(RECD P15) VIT090A(PROC VIJ09001 52*)
ICUPON1		ITEM	DEFINED IN	VIJ09001(RECD P15)
			USED IN	VIJ09001(RECD P15) VIT090A(PROC 52*)
IEMISORA		ITEM	DEFINED IN	CARTERA(RECD P17) VIJ09001(RECD P15)
			USED IN	CARTERA(RECD P16) VIE090A(PROC VIJ09001 67 68 69 72 76) VIJ09001(RECD P15) VIT090A(PROC VIJ09001 52*)
IEMISOR1		ITEM	DEFINED IN	VIJ09001(RECD P15)
			USED IN	VIJ09001(RECD P15) VIT090A(PROC 52*)
IENVDOC		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
IEXT1		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
IEXT2		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
IFIRMA		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
INACIO		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)

ITEM	GROUP	TYPE	CROSS REFERENCE
IPERJUR		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IPOS		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
IPOSP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
IPROGRAM		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IPROM		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IREF		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
IRFC		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IRUTA		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
ISERIE		ITEM	DEFINED IN CARTERA(RECD P17) VIJ09001(RECD P15) USED IN CARTERA(RECD P16) VIJ09001(RECD P15) VIT090A(PROC VIJ09C01 52*)
ISERIE1		ITEM	DEFINED IN VIJ09001(RECD P15) USED IN VIJ09001(RECD P15) VIT090A(PROC 52*)
ITASAFIS		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
ITEL1		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
ITEL2		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
ITIPOCAR		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
ITIPOCTA		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
ITIPOSDO		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
ITIPOTEN		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
IUSUARIO		ITEM	DEFINED IN CUENTA(RECD P12)

ITEM	GROUP	TYPE	CROSS REFERENCE
			USED IN CUENTA(RECD P11)
MABOANO		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
MABOMES		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
MCARACT		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
MCARIMES		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
MCGOANO		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
MCGOMES		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
MCPROEXI		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
MI01	VIG090	MAP	P20 VII090A(PROC 41) VII090B(PROC 104) VIN090A(PROC 33) VIT090A(PROC 50 51)
MI02	VIG090	MAP	P23 VIE090A(PROC 63* 89) VIE090P(PROC 13*) VIN090B(PROC 111)
MPRECOMP		ITEM	DEFINED IN VIJ09001(RECD P15) USED IN VIE090A(PROC 75 78 82) VIJ09001(RECD P15) VIT090A(PROC 52*)
MVALMERC		ITEM	DEFINED IN CARTERA(RECD P17) USED IN CARTERA(RECD P16)
NABREV		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
NAPELL1		ITEM	DEFINED IN CUENTA(RECD P12) VIW09001(RECD P9) USED IN CUENTA(RECD P11) VIE090P(PROC CUENTA 17) VIE090P(PROC VIW09001 17*) VII090A(PROC CUENTA 42*)
NAPELL2		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
NOMBRE		ITEM	DEFINED IN CUENTA(RECD P12) VIW09001(RECD P9) USED IN CUENTA(RECD P11) VIE090P(PROC CUENTA 16) VIE090P(PROC VIW09001 16*) VII090A(PROC CUENTA 42*)
NPROF		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
PCOMCTA		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)

ITEM GROUP TYPE CROSS REFERENCE

SCOMPNAC ITEM
DEFINED IN CUENTA(RECD P13)
USED IN CUENTA(RECD P11)

SCONCEPT ITEM
DEFINED IN CARTERA(RECD P17)
USED IN CARTERA(RECD P16)

SCUENTA ITEM
DEFINED IN CARTERA(RECD P17)
USED IN CARTERA(RECD P16)

SDOCUM ITEM
DEFINED IN CUENTA(RECD P13)
USED IN CUENTA(RECD P11)

SLIQUID ITEM
DEFINED IN CUENTA(RECD P13)
USED IN CUENTA(RECD P11)

SOPER12 ITEM
DEFINED IN CUENTA(RECD P13)
USED IN CUENTA(RECD P11)

SQLCA RECD P10 VRC0250(SGRP 121 122 123 124 125 126 128)

SQLCACOD ITEM
DEFINED IN SQLCA(RECD P10)
USED IN VRC0250(SGRP 122*)

SQLCARD3 ITEM
DEFINED IN SQLCA(RECD P10)
USED IN VRC0250(SGRP 124*)

SQLCARRM ITEM
DEFINED IN SQLCA(RECD P10)
USED IN VRC0250(SGRP 123*)

SQLCASCA ITEM
DEFINED IN SQLCA(RECD P10)
USED IN VRC0250(SGRP 121*)

SQLCAWN1 ITEM
DEFINED IN SQLCA(RECD P10)
USED IN VRC0250(SGRP 125*)

SQLCAWN6 ITEM
DEFINED IN SQLCA(RECD P10)
USED IN VRC0250(SGRP 126*)

SVIGEN ITEM
DEFINED IN CUENTA(RECD P12)
USED IN CUENTA(RECD P11) VIE090P(PROC 19) VIIQ90A(PROC 42*)

VIE090A PROC 54 VIE090P(PROC 21)

VIE090P PROC 2

VIIQ90A PROC 35 VIE090P(PROC 15)

VIIQ90B PROC 101 VIE090A(PROC 90)

VIJO9001 RECD P15 VIE090A(PROC 66 67 68 69 72 75 76 77 78 93) VIS090A(PROC 99)
VIIQ90A(PROC 50 51 52)

ITEM	GROUP	TYPE	CROSS REFERENCE
VIN090A		PROC	30 VIE090P(PROC 14)
VIN090B		PROC	108 VIE090P(PROC 28)
VIS090A		PROC	96 VIE090A(PROC 62 80 86)
VIT090A		PROC	44 VIE090P(PROC 20)
VIW09001		RECD	P9 VIE090A(PROC 89) VIE090P(PROC 16 17)
VRC0250		SGRP	113 VIT090A(PROC 42) VIT0905(PROC 106) VIS090A(PROC 93) VIT090A(PROC 52)
VRC0300	*EXTERNAL		USED IN VRC0250(SGRP 128)
WIO90AUX		ITEM	DEFINED IN VIW09001(RECD P9) USED IN VIE090A(PROC 64* 82* 83)
WIO90COD		ITEM	DEFINED IN MIO1(MAP VIG090 P20)
WIO90EMI		ITEM	DEFINED IN MIO2(MAP VIG090 P23) USED IN VIE090A(PROC 75* 84*)
WIO90FOP		ITEM	DEFINED IN MIO1(MAP VIG090 P20) VIW09001(RECD P9) USED IN VIT090A(PROC MIO1 51)
WIO90NOM		ITEM	DEFINED IN MIO2(MAP VIG090 P23) VIW09001(RECD P9) USED IN VIE090A(PROC MIO2 89*) VIE090A(PROC VIW09001 89)
WIO90PRE		ITEM	DEFINED IN MIO2(MAP VIG090 P23) USED IN VIE090A(PROC 78*)
WIO90TIT		ITEM	DEFINED IN MIO2(MAP VIG090 P23) USED IN VIE090A(PROC 77*)
WIO90TOC		ITEM	DEFINED IN MIO2(MAP VIG090 P23) USED IN VIE090A(PROC 79* 85* 93*)
WIO90TOT		ITEM	DEFINED IN MIO2(MAP VIG090 P23) USED IN VIE090A(PROC 75* 79 83* 85 92*)
XSEG		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)

MSL CONCATENATION SEQUENCE

	MSL ACCESS ORDER	MSL FILE NAME
READ/WRITE MSL:	1	MCAPINSL
READ-ONLY MSL(S):	2	DESARMSL
	3	
	4	
	5	
	6	

APPLICATION NAME: VIC0900
TYPE OF APPLICATION: MAIN TRANSACTION
WORKING STORAGE: VIW09001
MAP GROUP NAME: VIC090
HELP MAP GROUP NAME:
HELP MAP PF KEY:
BYPASS EDIT PF KEYS:
PF1-12+PF13-24: YES
ALLOW IMPLICITS: YES
MESSAGE FILE: SIVC
MSL: DESARMSL

PROLOGUE

INSTALACION: CASA DE BOLSA PROBURSA, S.A.
CREACION: AGOSTO DE 1988.
OBJETIVO: OBTENER LA POSICION DEL CLIENTE.
OBTENER EL MONTO DE LOS TITULOS
Y UN GRAN TOTAL DE:
PROGRESA
PRODUCE
OTROS (TODAS AQUELLAS EMISORAS QUE NO SEAN
PROGRESA Y PRODUCE)

TABLE AND ADDITIONAL RECORDS LIST
SQLCA RECORD

```
VIEO90P  ************************************************************                2
         *            PROCESO PRINCIPAL                  DESARMSL *
         ************************************************************
         OPTION -    EXECUTE                 OPTION                                  5

                     ;************************************************************   7
                     ;              EXECUTE: VIEO90P                                8
                     ;              PROCESO PRINCIPAL                               9
                     ;************************************************************  10
                     MOVE 1 TO EZECNVCM              ; LIBERA RECURSOS              11
                     MOVE 1 TO EZEFEC                ; LIBERA RECURSOS              12
                     SET MIO2 EMPTY                  ; LIMPIA MAPA MIO1             13
                     PERFORM VINO90A                 ; DESPLIEGA MAPA MIO1          14
                     PERFORM VIIO90A                 ; INQ DE LA TABLA CUENTA       15
                     MOVE CUENTA.NOMBRE TO VIWO9001.NOMBRE;                         16
                     MOVE CUENTA.NAPELL1 TO VIWO9001.NAPELL1;                       17
                     IF CUENTA NOT NRF               ; EXISTE CLIENTE               18
                       IF CUENTA.SVIGEN NE 'B'       ; VIGENCIA ALTA                19
                         PERFORM VITO90A             ; SETINQ DE CARTERA JOIN PRECIO 20
                         PERFORM VIEO90A             ; CALCULO TOTAL DE CARTERA     21
                       ELSE ;                                                       22
                         MOVE 61 TO EZEMNO;                                         23
                       END ;                                                        24
                     ELSE ;                                                         25
                       MOVE 18 TO EZEMNO;                                           26
                     END ;                                                          27
                     PERFORM VINO90B                 ; DESPLIEGA MAPA MIO2          28
```

ADDITIONAL PERFORMED PROCESSES

```
VIN095A  ************************************************************                    30
         *  DESPLIEGA MAPA MIO1                          DESARMSL *
         ************************************************************
         OPTION -  CONVERSE MIO1                MAP                                      33
VII095A  ************************************************************                    35
         *  INQ CUENTA                                   DESARMSL *
         ************************************************************
                   ;************************************************************       38
                   ;                    INQUIRY: VII095A                                39
                   ;                    INQ CUENTA                                      40
                   ;************************************************************       41
                   MOVE MIO1.ICUENTA1 TO CUENTA.ICUENTA.                                42
         OPTION -  INQUIRY  CUENTA          RECORD          VRC0250                      43

                   SQL SELECTION CONDITIONS MODIFIED:              YES

                   SELECT
                     SVIGEN, ICUENTA,
                     NOMBRE, NAPELL1
                   INTO
                     :SVIGEN, :ICUENTA,
                     :NOMBRE, :NAPELL1
                   FROM
                     CUENTA T1
                   WHERE
                     ICUENTA = :ICUENTA
                   ;** INSERT ORDER BY CLAUSE HERE **

VIT095A  ************************************************************                    45
         *  SETINQ OPERA                                 DESARMSL *
         ************************************************************
                   ;************************************************************       48
                   ;                    SETINQ: VIT095A                                 49
                   ;                    SETINQ OPERA                                    50
                   ;************************************************************       51
                   MOVE MIO1.ICUENTA1 TO OPERA.ICUENTA1.                                52
         OPTION -  SETINQ   OPERA           RECORD          VRC0250                      53

                   SQL SELECTION CONDITIONS MODIFIED:              YES

                   SELECT
                     ITRANS,
                     EOPERA, ICONCEP1, CANT1,
                     ICONCEP2, CANT2,
                     FLIQUIDA
```

```
                    INTO
                      :ITRANS,
                      :EOPERA, :ICONCEP1, :CANT1,
                      :ICONCEP2, :CANT2,
                      :FLIQUIDA
                    FROM
                      OPERA T1
                    WHERE
                      ICUENTA1 = :ICUENTA1
                    ORDER BY
                      FLIQUIDA DESC

VIEO95A ********************************************************                                    55
        *       CONSULTA DE ULTIMOS MOV.          DESARMSL *
        ********************************************************
        OPTION -    EXECUTE                OPTION                                                   58

                    ;*************************************************                               60
                    ;*************************************************                               61
                    ;                  EXECUTE: VIEO95A                                           62
                    ;*************************************************                               63
                    PERFORM VISO95A                 ; SCAN A OPERA                                  64
                    SET MIO2 EMPTY                  ; LIMPIA MAPA                                   65
                    MOVE 1 TO AIO951                ; INICIALIZA VARIABLE                           66
                    WHILE AIO951 <= 5               ; CONSULTA ULTIMOS 5 MOVIMIENTOS                67
                      IF OPERA NOT NRF;                                                             68
                        IF ITRANS = 'R';                                                            69
                          OR ITRANS = 'O';                                                          70
                          OR ITRANS = 'T';                                                          71
                          MOVE ICONCEP1 TO CONCEPT.ICONCEPT;                                        72
                          PERFORM VII095B           ; INQ CONCEPT                                   73
                        END ;                                                                       74
                        IF ITRANS = 'C';                                                            75
                          MOVE ICONCEP2 TO CONCEPT.ICONCEPT;                                        76
                          MIO2.WIO95PRE(AIO951) = OPERA.CANT1 / OPERA.CANT2;                        77
                          PERFORM VII095B           ; INQ CONCEPT                                   78
                        END ;                                                                       79
                        MOVE OPERA.FLIQUIDA TO MIO2.WIO95FOP(AIO951),                               80
                        MOVE OPERA.EOPERA TO WIO95OPE(AIO951);                                      81
                        MOVE CONCEPT.IEMISORA TO WIO95EMI(AIO951),                                  82
                        MOVE OPERA.CANT2 TO WIO95TIT(AIO951);                                       83
                        MOVE OPERA.CANT1 TO WIO95IMP(AIO951);                                       84
                        PERFORM VISO95A             ; SCAN A OPERA                                  85
                      END ;                                                                         86
                      AIO951 = AIO951 + 1           ; INCREMENTA CONTADOR                           87
                    END ;                                                                           88
                    MOVE VIW095O1.WIO95NOM TO MIO2.WIO95NOM;                                        89

VISO95A ********************************************************                                    91
        *       LEE EL RENGLON DE OPERA           DESARMSL *
        ********************************************************
        OPTION -    SCAN    OPERA       RECORD      VRCO25O                                         94
```

```
                    SQL SELECTION CONDITIONS MODIFIED:            NO

                    FETCH E2E_CURSOR_NNN USING DESCRIPTOR SQLDA

VII0958 ********************************************************                 96
        *          INQ CONCEPT                          DESARMSL *
        ********************************************************
        OPTION -    INQUIRY  CONCEPT        RECORD        VRC0250                99

                    SQL SELECTION CONDITIONS MODIFIED:            YES

                    SELECT
                      ICONCEPT, ISERIE, ICUPON,
                      IEMISORA
                    INTO
                      :ICONCEPT, :ISERIE, :ICUPON,
                      :IEMISORA
                    FROM
                      CONCEPT T1
                    WHERE
                      ICONCEPT = :ICONCEPT
                    ;** INSERT ORDER BY CLAUSE HERE **

VIN0958 ********************************************************                101
        *                                               DESARMSL *
        ********************************************************
        OPTION -    CONVERSE M102              MAP                             104
```

STATEMENT GROUPS

```
VRC0250 ************************************************************                106
        *          MANEJO DE ERRORES DE SQL                  DESARMSL *
        ************************************************************
                IF EZESQCOD < 0;                                                    109
                  OR EZESQCOD = 100;                                                110
                  OR EZESQCOD = -803;                                               111
                ELSE ;                                                              112
                  CALL EZEROLLB;                                                    113
                  MOVE EZESQLCA TO SQLCA.SQLCASCA;                                  114
                  MOVE EZESQCOD TO SQLCA.SQLCACOD;                                  115
                  MOVE EZESQRRM TO SQLCA.SQLCARRM;                                  116
                  MOVE EZESQRD3 TO SQLCA.SQLCARD3;                                  117
                  MOVE EZESQWN1 TO SQLCA.SQLCAWN1;                                  118
                  MOVE EZESQWN6 TO SQLCA.SQLCAWN6;                                  119
                  . IF WAMB1 NE 'B';                                                120
                  CALL VRC0300 SQLCA              ; ON-LINE                         121
                  ; ELSE ;                                                          122
                  ;   CALL VRC0750 SQLCA          ; BATCH                           123
                  ; END ;                                                           124
                  EZECLOS;                                                          125
                END ;                                                               126
```

APPLICATION STRUCTURE

NAME	LVL	OPTION	OBJECT	ERROR	DESCRIPTION	LINE
VIE095P	001	EXECUTE			PROCESO PRINCIPAL	2
VIN095A	002	CONVERSE	MIO1		DESPLIEGA MAPA MIO1	30
VII095A	002	INQUIRY	CUENTA	VRC0250	INQ CUENTA	35
VRC0250	003	GROUP			MANEJO DE ERRORES DE SQL	106
VIT095A	002	SETINQ	OPERA	VRC0250	SETINQ OPERA	45
VRC0250	003	GROUP			MANEJO DE ERRORES DE SQL	106
VIE095A	002	EXECUTE			CONSULTA DE ULTIMOS MOV.	55
VIS095A	003	SCAN	OPERA	VRC0250	LEE EL RENGLON DE OPERA	91
VRC0250	004	GROUP			MANEJO DE ERRORES DE SQL	106
VII095B	003	INQUIRY	CONCEPT	VRC0250	INQ CONCEPT	96
VRC0250	004	GROUP			MANEJO DE ERRORES DE SQL	106
VIN095B	002	CONVERSE	MIO2			101

GENERATION OPTIONS

LOAD LIBRARY	DESARALF
CREATE REFERENCE FILE	NO
PRINT STATEMENT LISTING	NO
FOLD PRINT	NO
VALIDATE SQL STATEMENTS	YES
EXECUTION MODE	SEGMENTED
SEGMENTED TRANSACTION	IO9F
CLIST FOR DPPX/SP	YES

MAP GROUPS

GENERATE	NAME
YES	VIG095

DB2 STATIC MODULE

GENERATE	NAME
YES	VIC095OS

RECORD DEFINITIONS

RECORD NAME: VIW0950I

ORGANIZATION: WORKING STORAGE
LENGTH IN BYTES: 85
MSL: DESARMSL

NO PROLOGUE

NAME	LVL	OCCURS	TYPE	LENGTH	DEC	BYTES	START	MSL	DESCRIPTION
ICLIENTE	10		CHA	16		16	1	MCAPIMSL	ICLIENTE
ICUENTA	10		PACK	7		4	17	MCAPIMSL	ICUENTA
AI0951	10		PACK	3		2	21	DESARMSL	CONTADOR
WI095NOM	10		CHA	60		60	23	DESARMSL	NOMBRE DEL CLIENTE
NOMBRE	15		CHA	20		20	23	MCAPIMSL	NOMBRE
NAPELL1	15		CHA	40		40	43	MCAPIMSL	NAPELL1
ICONCEPT	10		PACK	5		3	83	MCAPIMSL	ICONCEPT

RECORD DEFINITIONS

RECORD NAME: SQLCA

ORGANIZATION: WORKING STORAGE
LENGTH IN BYTES: 216
MSL: DESARMSL

NO PROLOGUE

NAME	LVL	OCCURS	TYPE	LENGTH	DEC	BYTES	START	MSL	DESCRIPTION
SQLCASCA	10		CHA	136		136	1	MCAPIMSL	
SQLCACOD	10		BIN	9		4	137	MCAPIMSL	
SQLCARRM	10		CHA	70		70	141	MCAPIMSL	
SQLCARD3	10		BIN	9		4	211	MCAPIMSL	
SQLCAWN1	10		CHA	1		1	215	MCAPIMSL	
SQLCAWNG	10		CHA	1		1	216	MCAPIMSL	

RECORD NAME: CUENTA

ORGANIZATION: SQL ROW
DEFAULT KEY ITEM:
LENGTH IN BYTES: 738
MSL: MCAPIMSL

SQL TABLE NAME(S)

USER ID	TABLE NAME	TABLE LABEL
	CUENTA	T1

DEFAULT SELECTION CONDITIONS

```
SELECT
  SVIGEN, ICTAGLO, ICUENTA, ITIPOCTA, IPERJUR,
  IRFC, ITASAFIS, INACIO, IPROM, ICCOSTO,
  IUSUARIO, IPROGRAM, FALTA, FALTAANT, FBAJA,
  FULTCAMB, FULTMOV, IENVDOC, NPROF, NABREV,
  NOMBRE, NAPELL1, NAPELL2, DCALLE, DCOLON,
  DPOBLA, IPOS, DESTADO, DCALLEP, DCOLONP,
  DPOBLAP, IPOSP, DESTADOP, ITEL1, IEXT1, ITEL2,
  IEXT2, ICAPTA, IFIRMA, IRUTA, SCOMPNAC, SOOCUM,
  SLIQUID, SOPER12, PCOMCTA, MABOANO, MABOMES,
  MCGOANO, MCGOMES, MCARACT, MCARIMES, APREFMAR,
  FDEBEDES, XSEG
INTO
  :SVIGEN, :ICTAGLO, :ICUENTA, :ITIPOCTA, :IPERJUR,
  :IRFC, :ITASAFIS, :INACIO, :IPROM, :ICCOSTO,
  :IUSUARIO, :IPROGRAM, :FALTA, :FALTAANT, :FBAJA,
  :FULTCAMB, :FULTMOV, :IENVDOC, :NPROF, :NABREV,
  :NOMBRE, :NAPELL1, :NAPELL2, :DCALLE, :DCOLON,
  :DPOBLA, :IPOS, :DESTADO, :DCALLEP, :DCOLONP,
  :DPOBLAP, :IPOSP, :DESTADOP, :ITEL1, :IEXT1, :ITEL2,
  :IEXT2, :ICAPTA, :IFIRMA, :IRUTA, :SCOMPNAC, :SOOCUM,
  :SLIQUID, :SOPER12, :PCOMCTA, :MABOANO, :MABOMES,
  :MCGOANO, :MCGOMES, :MCARACT, :MCARIMES, :APREFMAR,
  :FDEBEDES, :XSEG
FROM
  CUENTA T1
WHERE
;** INSERT DEFAULT SELECT CONDITIONS HERE **
```

NO PROLOGUE

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME
SVIGEN	CHA	1		1	5	NO	SVIGEN
ICTAGLO	PACK	7	4	10	10	NO	ICTAGLO
ICUENTA	PACK	7	4	10	18	YES	ICUENTA
ITIPOCTA	CHA	1		1	26	YES	ITIPOCTA
IPERJUR	CHA	2		2	31	NO	IPERJUR
IRFC	CHA	13		13	37	NO	IRFC
ITASAFIS	CHA	1		1	54	NO	ITASAFIS
INACIO	CHA	2		2	59	NO	INACIO
IPROM	PACK	4		3	65	YES	IPROM
ICCOSTO	PACK	5		3	72	YES	ICCOSTO
IUSUARIO	CHA	8		8	79	NO	IUSUARIO
IPROGRAM	CHA	8		8	91	NO	IPROGRAM
FALTA	CHA	10		10	103	NO	FALTA
FALTAANT	CHA	10		10	117	NO	FALTAANT
FBAJA	CHA	10		10	131	NO	FBAJA
FULTCAMB	CHA	10		10	145	NO	FULTCAMB
FULTMOV	CHA	10		10	159	NO	FULTMOV
IENVDOC	PACK	2		2	173	NO	IENVDOC
NPROF	CHA	5		5	179	NO	NPROF
NABREV	CHA	25		25	188	NO	NABREV
NOMBRE	CHA	20		20	217	NO	NOMBRE
NAPELL1	CHA	40		40	241	NO	NAPELL1
NAPELL2	CHA	20		20	285	NO	NAPELL2

SQL DATA CODE	MSL	DESCRIPTION
453	MCAPIMSL	SVIGEN
485	MCAPIMSL	ICTAGLO
485	MCAPIMSL	ICUENTA
453	MCAPIMSL	ITIPOCTA
453	MCAPIMSL	IPERJUR
453	MCAPIMSL	
453	MCAPIMSL	ITASAFIS
453	MCAPIMSL	INACIO
485	MCAPIMSL	IPROM
485	MCAPIMSL	ICCOSTO
453	MCAPIMSL	IUSUARIO
453	MCAPIMSL	IPROGRAM
453	MCAPIMSL	FALTA
453	MCAPIMSL	FALTAANT
453	MCAPIMSL	FBAJA
453	MCAPIMSL	FULTCAMB
453	MCAPIMSL	FULTMOV
485	MCAPIMSL	IENVDOC
453	MCAPIMSL	NPROF
453	MCAPIMSL	NABREV
453	MCAPIMSL	NOMBRE
453	MCAPIMSL	NAPELL1
453	MCAPIMSL	NAPELL2

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
DCALLE	CHA	25		25	309	NO	DCALLE	453	MCAPIMSL	DCALLE
DCOLON	CHA	25		25	338	NO	DCOLON	453	MCAPIMSL	DCOLON
DPOBLA	CHA	30		30	367	NO	DPOBLA	453	MCAPIMSL	DPOBLA
IPOS	PACK	5		3	401	NO	IPOS	485	MCAPIMSL	IPOS
DESTADO	CHA	25		25	408	NO	DESTADO	453	MCAPIMSL	DESTADO
DCALLEP	CHA	25		25	437	NO	DCALLEP	453	MCAPIMSL	DCALLEP
DCOLONP	CHA	25		25	466	NO	DCOLONP	453	MCAPIMSL	DCOLONP
DPOBLAP	CHA	30		30	495	NO	DPOBLAP	453	MCAPIMSL	DPOBLAP
IPOSP	PACK	5		3	529	NO	IPOSP	485	MCAPIMSL	IPOSP
DESTADOP	CHA	25		25	536	NO	DESTADOP	453	MCAPIMSL	DESTADOP
ITEL1	PACK	7		4	565	NO	ITEL1	485	MCAPIMSL	ITEL1
IEXT1	PACK	4		3	573	NO	IEXT1	485	MCAPIMSL	IEXT1
ITEL2	PACK	7		4	580	NO	ITEL2	485	MCAPIMSL	ITEL2
IEXT2	PACK	4		3	588	NO	IEXT2	485	MCAPIMSL	IEXT2
ICAPTA	CHA	1		1	595	NO	ICAPTA	453	MCAPIMSL	ICAPTA
IFIRMA	CHA	1		1	600	NO	IFIRMA	453	MCAPIMSL	IFIRMA
IRUTA	CHA	3		3	605	NO	IRUTA	453	MCAPIMSL	IRUTA
SCOMPNAC	CHA	1		1	612	NO	SCOMPNAC	453	MCAPIMSL	SCOMPNAC
SDOCUM	CHA	1		1	617	NO	SDOCUM	453	MCAPIMSL	SDOCUM
SLIQUID	CHA	1		1	622	NO	SLIQUID	453	MCAPIMSL	SLIQUID
SOPER12	CHA	1		1	627	NO	SOPER12	453	MCAPIMSL	SOPER12
PCOMCTA	PACK	5	4	3	632	NO	PCOMCTA	485	MCAPIMSL	PCOMCTA
MABOANO	PACK	15		8	639	NO	MABOANO	485	MCAPIMSL	MABOANO

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
MABOMES	PACK	15		8	651	NO	MABOMES	485	MCAPIMSL	MABOMES
MCGOANO	PACK	15		8	663	NO	MCGOANO	485	MCAPIMSL	MCGOANO
MCGOMES	PACK	15		8	675	NO	MCGOMES	485	MCAPIMSL	MCGOMES
MCARACT	PACK	15		8	687	NO	MCARACT	485	MCAPIMSL	MCARACT
MCARIMES	PACK	15		8	699	NO	MCARIMES	485	MCAPIMSL	MCARIMES
APREFMAR	PACK	6	5	5	711	NO	APREFMAR	485	MCAPIMSL	APREFMAR
FDEBEDES	CHA	10		10	720	NO	FDEBEDES	453	MCAPIMSL	FDEBEDES
XSEG	CHA	5		5	734	NO	XSEG	453	MCAPIMSL	XSEG

RECORD NAME: OPERA

ORGANIZATION: SQL ROW
DEFAULT KEY ITEM:
LENGTH IN BYTES: 279
MSL: MCAPIMSL

SQL TABLE NAME(S)

USER ID	TABLE NAME	TABLE LABEL
	OPERA	T1

DEFAULT SELECTION CONDITIONS

```
SELECT
  IOPERA, IREF, ISEC, ITRANS, IDOCTO, IUSUARIO,
  EOPERA, ETRANS, ICUENTA1, ICONCEP1, CANT1,
  ICUENTA2, ICONCEP2, CANT2, ACOSCASA, ACOSFPRO,
  ACOSPROM, MCPKOEXI, FREG, FOPERA, FVENC,
  FLIQUIDA, IRUTA, SLIQUID, SESTATUS, MPRECIO
INTO
  :IOPERA, :IREF, :ISEC, :ITRANS, :IDOCTO, :IUSUARIO,
  :EOPERA, :ETRANS, :ICUENTA1, :ICONCEP1, :CANT1,
  :ICUENTA2, :ICONCEP2, :CANT2, :ACOSCASA, :ACOSFPRO,
  :ACOSPROM, :MCPKOEXI, :FREG, :FOPERA, :FVENC,
  :FLIQUIDA, :IRUTA, :SLIQUID, :SESTATUS, :MPRECIO
FROM
  OPERA T1
```

RECORD DEFINITIONS

WHERE
;** INSERT DEFAULT SELECT CONDITIONS HERE **

NO PROLOGUE

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME
IOPERA	PACK	5		3	5	NO	IOPERA
IREF	PACK	9		5	12	YES	IREF
ISEC	PACK	2		2	21	YES	ISEC
ITRANS	CHA	1		1	27	NO	ITRANS
IDOCTO	PACK	7		4	32	NO	IDOCTO
IUSUARIO	CHA	8		8	40	NO	IUSUARIO
EOPERA	CHA	15		15	52	NO	EOPERA
ETRANS	CHA	15		15	71	NO	ETRANS
ICUENTA1	PACK	7		4	90	NO	ICUENTA1
ICONCEP1	PACK	5		3	98	NO	ICONCEP1
CANT1	PACK	15		8	105	NO	CANT1
ICUENTA2	PACK	7		4	117	NO	ICUENTA2
ICONCEP2	PACK	5		3	125	NO	ICONCEP2
CANT2	PACK	15		8	132	NO	CANT2
ACOSCASA	PACK	8	4	5	144	NO	ACOSCASA
ACOSFPRO	PACK	8	4	5	153	NO	ACOSFPRO
ACOSPROM	PACK	8	4	5	162	NO	ACOSPROM
MCPROEXI	PACK	15	5	8	171	NO	MCPROEXI
FREG	CHA	26		26	183	NO	FREG

SQL DATA CODE	MSL	DESCRIPTION
485	MCAPIMSL	IOPERA
485	MCAPIMSL	IREF
485	MCAPIMSL	ISEC
453	MCAPIMSL	ITRANS
485	MCAPIMSL	IDOCTO
453	MCAPIMSL	IUSUARIO
453	MCAPIMSL	EOPERA
453	MCAPIMSL	ETRANS
485	MCAPIMSL	ICUENTA1
485	MCAPIMSL	ICONCEP1
485	MCAPIMSL	CANT1
485	MCAPIMSL	ICUENTA2
485	MCAPIMSL	ICONCEP2
485	MCAPIMSL	CANT2
485	MCAPIMSL	ACOSCASA
485	MCAPIMSL	ACOSFPRO
485	MCAPIMSL	ACOSPROM
485	MCAPIMSL	MCPROEXI
453	MCAPIMSL	FREG

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
FOPERA	CHA	10		10	213	NO	FOPERA	453	MCAPIMSL	FOPERA
FVENC	CHA	10		10	227	NO	FVENC	453	MCAPIMSL	FVENC
FLIQUIDA	CHA	10		10	241	NO	FLIQUIDA	453	MCAPIMSL	FLIQUIDA
IRUTA	CHA	3		3	255	NO	IRUTA	453	MCAPIMSL	IRUTA
SLIQUID	CHA	1		1	262	NO	SLIQUID	453	MCAPIMSL	SLIQUID
SESTATUS	CHA	1		1	267	NO	SESTATUS	453	MCAPIMSL	SESTATUS
MPRECIO	PACK	15	5	8	272	NO	MPRECIO	485	MCAPIMSL	MPRECIO

RECORD NAME: CONCEPT

ORGANIZATION: SQL ROW
DEFAULT KEY ITEM:
LENGTH IN BYTES: 254
MSL: MCAPIMSL

SQL TABLE NAME(S)

USER ID	TABLE NAME	TABLE LABEL
	CONCEPT	T1

DEFAULT SELECTION CONDITIONS

```
SELECT
  ICONCEPT, ECONCEPT, ITIPOCON, MVALNOM,
  ICONCEXP, IEMISORA, ISERIE, ICUPON, ICONTAB,
  ICTAPROV, ICORRO, ITIPOVAL, IVALBM, FALTA,
  FBAJA, FCOLOCA, FVENC, CLOTEMIN, ABURSA, AISR,
  PCOMIS1, MLIMCOM, PCOMIS2, SCOLOCA, SCUBMAR,
  MPUJAMIN
INTO
  :ICONCEPT, :ECONCEPT, :ITIPOCON, :MVALNOM,
  :ICONCEXP, :IEMISORA, :ISERIE, :ICUPON, :ICONTAB,
  :ICTAPROV, :ICORRO, :ITIPOVAL, :IVALBM, :FALTA,
  :FBAJA, :FCOLOCA, :FVENC, :CLOTEMIN, :ABURSA, :AISR,
  :PCOMIS1, :MLIMCOM, :PCOMIS2, :SCOLOCA, :SCUBMAR,
  :MPUJAMIN
FROM
  CONCEPT T1
```

```
WHERE
** INSERT DEFAULT SELECT CONDITIONS HERE **

NO PROLOGUE
```

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
ICONCEPT	PACK	5		3	5	YES	ICONCEPT	485	MCAPIMSL	ICONCEPT
ECONCEPT	CHA	20		20	12	NO	ECONCEPT	453	MCAPIMSL	ECONCEPT
ITIPOCON	CHA	1		1	36	NO	ITIPOCON	453	MCAPIMSL	ITIPOCON
MVALNOM	PACK	15	5	8	41	NO	MVALNOM	485	MCAPIMSL	MVALNOM
ICONCEXP	PACK	5		3	53	NO	ICONCEXP	485	MCAPIMSL	ICONCEXP
IEMISORA	CHA	7		7	60	NO	IEMISORA	453	MCAPIMSL	IEMISORA
ISERIE	CHA	5		5	71	NO	ISERIE	453	MCAPIMSL	ISERIE
ICUPON	PACK	3		2	80	NO	ICUPON	485	MCAPIMSL	ICUPON
ICONTAB	PACK	5		3	86	NO	ICONTAB	485	MCAPIMSL	ICONTAB
ICTAPROV	PACK	7		4	93	NO	ICTAPROV	485	MCAPIMSL	ICTAPROV
ICORRO	PACK	7		4	101	NO	ICORRO	485	MCAPIMSL	ICORRO
ITIPOVAL	PACK	3		2	109	NO	ITIPOVAL	485	MCAPIMSL	ITIPOVAL
IVALBM	PACK	6		4	115	NO	IVALBM	485	MCAPIMSL	IVALBM
FALTA	CHA	10		10	123	NO	FALTA	453	MCAPIMSL	FALTA
FBAJA	CHA	10		10	133	NO	FBAJA	453	MCAPIMSL	FBAJA
FCOLOCA	CHA	10		10	151	NO	FCOLOCA	453	MCAPIMSL	FCOLOCA
FVENC	CHA	10		10	165	NO	FVENC	453	MCAPIMSL	FVENC
CLOTEMIN	PACK	11		6	179	NO	CLOTEMIN	485	MCAPIMSL	CLOTEMIN
ABURSA	PACK	8	4	5	189	NO	ABURSA	485	MCAPIMSL	ABURSA

RECORD DEFINITIONS

NAME	TYPE	LENGTH	DEC	BYTES	START	READ ONLY	SQL COLUMN NAME	SQL DATA CODE	MSL	DESCRIPTION
AISR	PACK	8	4	5	198	NO	AISR	485	MCAPIMSL	AISR
PCOMIS1	PACK	8	7	5	207	NO	PCOMIS1	485	MCAPIMSL	PCOMIS1
MLIMCOM	PACK	15		8	216	NO	MLIMCOM	485	MCAPIMSL	MLIMCOM
PCOMIS2	PACK	8	4	5	228	NO	PCOMIS2	485	MCAPIMSL	PCOMIS2
SCOLOCA	CHA	1		1	237	NO	SCOLOCA	453	MCAPIMSL	SCOLOCA
SCUBMAR	CHA	1		1	242	NO	SCUBMAR	453	MCAPIMSL	SCUBMAR
MPUJAMIN	PACK	15	5	8	247	NO	MPUJAMIN	485	MCAPIMSL	MPUJAMIN

MAP GROUP NAME: VIG095 (NO MAPGROUP MEMBER DEFINED)

NUMBER OF SUPPORTED DEVICES 1

TOTAL MAPS 2

* = SUPPORTED, S = SIZE ERROR

3278-2

MAP. NAME	LINE	COLUMN	DEPTH	WIDTH	MSL	
MI01	1	1	24	79	DESARMSL	*
MI02	1	1	24	79	DESARMSL	*

SPECIFICATION FOR FOLLOWING DEVICE TYPES

3278-2

MAP CHARACTERISTICS

MAP SIZE: DEPTH = 24
WIDTH = 79

MAP POSITION: LINE = 1
COLUMN= 1

CURSOR FIELD = ICLIENTE

FIELD AND ATTRIBUTE DEFINITION

CONSTANT FIELD CODE: ¢
VARIABLE FIELD CODE: \
SPACER CHARACTER: /

```
          1         2         3         4         5         6         7
----+----0----+----0----+----0----+----0----+----0----+----0----+----0----+----
|\              ¢       IDENTIFICACION DE CLIENTE          VIG095 M001
|\       ¢              NUMERO DE CUENTA
|\          ¢           FECHA DE LA TRANSACCION
|\   ¢                  CODIGO DE RETORNO
+                                                                            +
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
10                                                                           10
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
|                                                                            |
20                                                                           20
|                                                                            |
|                                                                            |
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----
          0         0         0         0         0         0         0
```

FIELD ATTRIBUTE CHARACTERS

LINE	COLUMN	FIELD NAME	ATTRIBUTES
1	1	ICLIENTE	UNPROTECT CURSOR
2	1	ICUENTA1	UNPROTECT NUMERIC
3	1	WIO95FOP	UNPROTECT
4	1	WIO95COD	UNPROTECT NUMERIC

MAP ITEM DEFINITIONS

	OCCURS	TYPE/ERR	LENGTH	DEC	JUS	FOLD	FIL	ZERO	MIN/ERR	SIGN	SEP	MONY	REQ/ERR	EDIT RTN/ERR	MIN	MAX	ERR	HEX
ICLIENTE	IDENTIFICACION DEL CLIENTE																	
		CHA	16		LEF	MAP	N	NO		NO	NO	NO	NO					NO
ICUENTA1	NUMERO DE CUENTA																	
		NUM	7		RIG	MAP	N	NO		LEA	NO	NO	NO					NO
WIO95FOP	FECHA DE LA TRANSACCION																	
		CHA	10		LEF	MAP	N	NO		NO	NO	NO	NO					NO
WIO95COD	CODIGO DE RETORNO																	
		NUM	3		LEF	MAP	N	NO		NO	NO	NO	NO					NO

SPECIFICATION FOR FOLLOWING DEVICE TYPES

3278-2

MAP CHARACTERISTICS

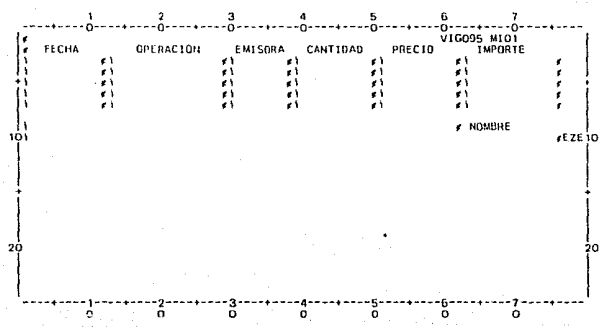
MAP SIZE: DEPTH = 24
WIDTH = 79

MAP POSITION: LINE = 1
COLUMN= 1

CURSOR FIELD = WIG095FOR(1)

FIELD AND ATTRIBUTE DEFINITION

CONSTANT FIELD CODE: ¢
VARIABLE FIELD CODE: ¡
SPACER CHARACTER: /



FIELD ATTRIBUTE CHARACTERS

LINE	COLUMN	FIELD NAME	ATTRIBUTES
3	1	WIO95FOP(1) ...	UNPROTECT CURSOR
3	13	WIO95OPE(1) ...	UNPROTECT
3	30	WIO95EMI(1) ...	UNPROTECT
3	39	WIO95TIT(1) ...	UNPROTECT NUMERIC
3	51	WIO95PRE(1) ...	UNPROTECT NUMERIC
3	63	WIO95IMP(1) ...	UNPROTECT NUMERIC
4	1	WIO95FOP(2) ...	UNPROTECT
4	13	WIO95OPE(2) ...	UNPROTECT
4	30	WIO95EMI(2) ...	UNPROTECT
4	39	WIO95TIT(2) ...	UNPROTECT NUMERIC
4	51	WIO95PRE(2) ...	UNPROTECT NUMERIC
4	63	WIO95IMP(2) ...	UNPROTECT NUMERIC
5	1	WIO95FOP(3) ...	UNPROTECT
5	13	WIO95OPE(3) ...	UNPROTECT
5	30	WIO95EMI(3) ...	UNPROTECT
5	39	WIO95TIT(3) ...	UNPROTECT NUMERIC
5	51	WIO95PRE(3) ...	UNPROTECT NUMERIC
5	63	WIO95IMP(3) ...	UNPROTECT NUMERIC
6	1	WIO95FOP(4) ...	UNPROTECT
6	13	WIO95OPE(4) ...	UNPROTECT
6	30	WIO95EMI(4) ...	UNPROTECT
6	39	WIO95TIT(4) ...	UNPROTECT NUMERIC
6	51	WIO95PRE(4) ...	UNPROTECT NUMERIC
6	63	WIO95IMP(4) ...	UNPROTECT NUMERIC
7	1	WIO95FOP(5) ...	UNPROTECT
7	13	WIO95OPE(5) ...	UNPROTECT
7	30	WIO95EMI(5) ...	UNPROTECT
7	39	WIO95TIT(5) ...	UNPROTECT NUMERIC
7	51	WIO95PRE(5) ...	UNPROTECT NUMERIC
7	63	WIO95IMP(5) ...	UNPROTECT NUMERIC
9	1	WIO95NOM	UNPROTECT
10	1	EZEMSG	ASKIP

MAP ITEM DEFINITIONS

	OCCURS	TYPE/ERR	LENGTH	DEC	JUS	FOLD	FIL	ZERO	MIN/ERR	SIGN	SEP	MONY	REQ/ERR	EDIT RTN/ERR	MIN	MAX	ERR	HEX
WI095FOP		FECHA DE LA TRANSACCION																
	5	CHA	10		LEF	MAP	N	NO		NO	NO	NO	NO					NO
WI095OPE		OPERACION REALIZADA																
	5	CHA	15		LEF	MAP	N	NO		NO	NO	NO	NO					NO
WI095EMI		EMISORA																
	5	CHA	7		LEF	MAP	N	NO		NO	NO	NO	NO					NO
WI095TIT		CANTIDAD DE TITULOS																
	5	NUM	10		LEF	MAP	N	NO		NO	YES	NO	NO					NO
WI095PRE		PRECIO DEL TITULO																
	5	NUM	10	2	RIG	MAP	N	NO		NO	YES	NO	NO					NO
WI095IMP		IMPORTE DE LA OPERACION																
	5	NUM	12	2	RIG	MAP	N	NO		NO	YES	NO	NO					NO
WI095NOM		NOMBRE DEL CLIENTE																
		CHA	60		LEF	MAP	N	NO		NO	NO	NO	NO					NO
EZEMSG		MENSAJE DE RETORNO																
		CHA	74		NO	MAP	N	NO		NO	NO	NO	NO					

ITEM GROUP TYPE CROSS REFERENCE

```
ABURSA                  ITEM          DEFINED IN  CONCEPT(RECD P17)
                                        USED IN  CONCEPT(RECD P17)

ACOSCASA                ITEM          DEFINED IN  OPERA(RECD P15)
                                        USED IN  OPERA(RECD P15)

ACOSFPRO                ITEM          DEFINED IN  OPERA(RECD P15)
                                        USED IN  OPERA(RECD P15)

ACOSPROM                ITEM          DEFINED IN  OPERA(RECD P15)
                                        USED IN  OPERA(RECD P15)

AISR                    ITEM          DEFINED IN  CONCEPT(RECD P18)
                                        USED IN  CONCEPT(RECD P17)

AIO95I                  ITEM          DEFINED IN  VIW0950I(RECD P9)
                                        USED IN  VIE095A(PROC 66* 67 77 80 81 82 83 84 87*)

APREFMAR                ITEM          DEFINED IN  CUENTA(RECD P14)
                                        USED IN  CUENTA(RECD P11)

CANT1                   ITEM          DEFINED IN  OPERA(RECD P15)
                                        USED IN  OPERA(RECD P15)  VIE095A(PROC 77 84)  VIT095A(PROC 53*)

CANT2                   ITEM          DEFINED IN  OPERA(RECD P15)
                                        USED IN  OPERA(RECD P15)  VIE095A(PROC 77 83)  VIT095A(PROC 53*)

CLOTEMIN                ITEM          DEFINED IN  CONCEPT(RECD P17)
                                        USED IN  CONCEPT(RECD P17)

CONCEPT                 RECD    P17   VIE095A(PROC 72 76 82)  VII095B(PROC 99)

CUENTA                  RECD    P11   VIE095P(PROC 16 17 18 19)  VII095A(PROC 42 43)

DCALLE                  ITEM          DEFINED IN  CUENTA(RECD P12)
                                        USED IN  CUENTA(RECD P11)

DCALLEP                 ITEM          DEFINED IN  CUENTA(RECD P13)
                                        USED IN  CUENTA(RECD P11)

DCOLON                  ITEM          DEFINED IN  CUENTA(RECD P13)
                                        USED IN  CUENTA(RECD P11)

DCOLONP                 ITEM          DEFINED IN  CUENTA(RECD P13)
                                        USED IN  CUENTA(RECD P11)

DESTADO                 ITEM          DEFINED IN  CUENTA(RECD P13)
                                        USED IN  CUENTA(RECD P11)
```

ITEM	GROUP	TYPE	CROSS REFERENCE
DESTADOP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DPOBLA		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
DPOBLAP		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
ECONCEPT		ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17)
EOPERA		ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15) VIE095A(PROC 81) VIT095A(PROC 53*)
ETRANS		ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15)
EZECLOS			USED IN VRC0250(SGRP 125)
EZECNVCM			USED IN VIE095P(PROC 11*)
EZEFEC			USED IN VIE095P(PROC 12*)
EZEMNO			USED IN VIE095P(PROC 23* 26*)
EZEMSG		ITEM	DEFINED IN MIO2(MAP VIG095 P24)
EZEROLLB			USED IN VRC0250(SGRP 113)
EZESQCOD			USED IN VRC0250(SGRP 109 110 111 115)
EZESQLCA			USED IN VRC0250(SGRP 114)
EZESQRD3			USED IN VRC0250(SGRP 117)
EZESQRRM			USED IN VRC0250(SGRP 116)
EZESQWN1			USED IN VRC0250(SGRP 118)
EZESQWNG			USED IN VRC0250(SGRP 119)
FALTA		ITEM	DEFINED IN CONCEPT(RECD P17) CUENTA(RECD P12) USED IN CONCEPT(RECD P17) CUENTA(RECD P11)
FALTAANT		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
FBAJA		ITEM	DEFINED IN CONCEPT(RECD P17) CUENTA(RECD P12) USED IN CONCEPT(RECD P17) CUENTA(RECD P11)
FCOLOCA		ITEM	DEFINED IN CONCEPT(RECD P17)

ITEM	GROUP	TYPE	CROSS REFERENCE
			USED IN CONCEPT(RECD P17)
FDEBEDES		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
FLIQUIDA		ITEM	DEFINED IN OPERA(RECD P16) USED IN OPERA(RECD P15) VIE095A(PROC 80) VIT095A(PROC 53*)
FOPERA		ITEM	DEFINED IN OPERA(RECD P16) USED IN OPERA(RECD P16)
FREG		ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15)
FULTCAMB		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
FULTMOV		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
FVENC		ITEM	DEFINED IN CONCEPT(RECD P17) OPERA(RECD P16) USED IN CONCEPT(RECD P17) OPERA(RECD P15)
ICAPTA		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
ICCOSTO		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
ICLIENTE		ITEM	DEFINED IN MIO1(MAP VIC095 P21) VIW09501(RECD P9)
ICONCEPT		ITEM	DEFINED IN CONCEPT(RECD P17) VIW09501(RECD P9) USED IN CONCEPT(RECD P17) VIE095A(PROC CONCEPT 72* 76*) VIT095B(PROC CONCEPT 99*)
ICONCEP1		ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15) VIE095A(PROC 72) VIT095A(PROC 53*)
ICONCEP2		ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15) VIE095A(PROC 76) VIT095A(PROC 53*)
ICONCEXP		ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17)
ICONTAB		ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17)
ICORRO		ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17)
ICTAGLO		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)

ITEM GROUP	TYPE	CROSS REFERENCE
ICTAPROV	ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17)
ICUENTA	ITEM	DEFINED IN CUENTA(RECD P12) VIW09501(RECD P9) USED IN CUENTA(RECD P11) VII095A(PROC CUENTA 42* 43*)
ICUENTA1	ITEM	DEFINED IN MIO1(MAP VIC095 P21) OPERA(RECD P15) USED IN OPERA(RECD P15) VII095A(PROC MIO1 42) VIT095A(PROC MIO1 52) VIT095A(PROC OPERA 52* 53)
ICUENTA2	ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15)
ICUPON	ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17) VII095B(PROC 99*)
IDOCTO	ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15)
IEMISORA	ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17) VIE095A(PROC 82) VII095B(PROC 99*)
IENVDOC	ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IEXT1	ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
IEXT2	ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
IFIRMA	ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
INACIO	ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IOPERA	ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15)
IPERJUR	ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
IPOS	ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
IPOSP	ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
IPROGRAM	ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)

ITEM	GROUP	TYPE	CROSS REFERENCE	
IPROM		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
IREF		ITEM	DEFINED IN	OPERA(RECD P15)
			USED IN	OPERA(RECD P15)
IRFC		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
IRUTA		ITEM	DEFINED IN	CUENTA(RECD P13) OPERA(RECD P16)
			USED IN	CUENTA(RECD P11) OPERA(RECD P15)
ISEC		ITEM	DEFINED IN	OPERA(RECD P15)
			USED IN	OPERA(RECD P15)
ISERIE		ITEM	DEFINED IN	CONCEPT(RECD P17)
			USED IN	CONCEPT(RECD P17) VI1095B(PROC 99*)
ITASAFIS		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
ITEL1		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
ITEL2		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
ITIPOCON		ITEM	DEFINED IN	CONCEPT(RECD P17)
			USED IN	CONCEPT(RECD P17)
ITIPOCTA		ITEM	DEFINED IN	CUENTA(RECD P12)
			USED IN	CUENTA(RECD P11)
ITIPOVAL		ITEM	DEFINED IN	CONCEPT(RECD P17)
			USED IN	CONCEPT(RECD P17)
ITRANS		ITEM	DEFINED IN	OPERA(RECD P15)
			USED IN	OPERA(RECD P15) VIE095A(PROC 69 70 71 75) VIT095A(PROC 53*)
IUSUARIO		ITEM	DEFINED IN	CUENTA(RECD P12) OPERA(RECD P15)
			USED IN	CUENTA(RECD P11) OPERA(RECD P15)
IVALBM		ITEM	DEFINED IN	CONCEPT(RECD P17)
			USED IN	CONCEPT(RECD P17)
MABOANO		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
MABOMES		ITEM	DEFINED IN	CUENTA(RECD P13)
			USED IN	CUENTA(RECD P11)
MCARACT		ITEM	DEFINED IN	CUENTA(RECD P14)

ITEM	GROUP	TYPE	CROSS REFERENCE
			USED IN CUENTA(RECD P11)
MCCCUNES		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
MCGUANO		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)
MCGOMES		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)
MCPROEXI		ITEM	DEFINED IN OPERA(RECD P15) USED IN OPERA(RECD P15)
MIO1	VIG095	MAP P21	VIE095P(PROC 13*) VII095A(PROC 42) VIN095A(PROC 33) VIT095A(PROC 52)
MIO2	VIG095	MAP P24	VIE095A(PROC 65* 77 80 89) VIN095B(PROC 104)
MLIMCOM		ITEM	DEFINED IN CONCEPT(RECD P18) USED IN CONCEPT(RECD P17)
MPRECIO		ITEM	DEFINED IN OPERA(RECD P16) USED IN OPERA(RECD P15)
MPUJAMIN		ITEM	DEFINED IN CONCEPT(RECD P18) USED IN CONCEPT(RECD P17)
MVALNOM		ITEM	DEFINED IN CONCEPT(RECD P17) USED IN CONCEPT(RECD P17)
NABREV		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
NAPELL1		ITEM	DEFINED IN CUENTA(RECD P12) VIW095O1(RECD P9) USED IN CUENTA(RECD P11) VIE095P(PROC CUENTA 17) VIE095P(PROC VIW09501 17*) VII095A(PROC CUENTA 43*)
NAPELL2		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
NOMBRE		ITEM	DEFINED IN CUENTA(RECD P12) VIW095O1(RECD P9) USED IN CUENTA(RECD P11) VIE095P(PROC CUENTA 16) VIE095P(PROC VIW09501 16*) VII095A(PROC CUENTA 43*)
NPROF		ITEM	DEFINED IN CUENTA(RECD P12) USED IN CUENTA(RECD P11)
OPERA		RECD P15	VIE095A(PROC 68 77 80 81 83 84) VIS095A(PROC 94) VIT095A(PROC 52 53
PCOMCTA		ITEM	DEFINED IN CUENTA(RECD P13) USED IN CUENTA(RECD P11)

ITEM / GROUP	TYPE	CROSS REFERENCE	
PCOMIS1	ITEM	DEFINED IN	CONCEPT(RECD P18)
		USED IN	CONCEPT(RECD P17)
PCOMIS2	ITEM	DEFINED IN	CONCEPT(RECD P18)
		USED IN	CONCEPT(RECD P17)
SCOLOCA	ITEM	DEFINED IN	CONCEPT(RECD P18)
		USED IN	CONCEPT(RECD P17)
SCOMPNAC	ITEM	DEFINED IN	CUENTA(RECD P13)
		USED IN	CUENTA(RECD P11)
SCUBMAR	ITEM	DEFINED IN	CONCEPT(RECD P18)
		USED IN	CONCEPT(RECD P17)
SDOCUM	ITEM	DEFINED IN	CUENTA(RECD P13)
		USED IN	CUENTA(RECD P11)
SESTATUS	ITEM	DEFINED IN	OPERA(RECD P16)
		USED IN	OPERA(RECD P15)
SLIQUID	ITEM	DEFINED IN	CUENTA(RECD P13) OPERA(RECD P16)
		USED IN	CUENTA(RECD P11) OPERA(RECD P15)
SOPER12	ITEM	DEFINED IN	CUENTA(RECD P13)
		USED IN	CUENTA(RECD P11)
SQLCA	RECD	P10	VRC0250(SGRP 114 115 116 117 118 119 121)
SQLCACOD	ITEM	DEFINED IN	SQLCA(RECD P10)
		USED IN	VRC0250(SGRP 115*)
SQLCAR03	ITEM	DEFINED IN	SQLCA(RECD P10)
		USED IN	VRC0250(SGRP 117*)
SQLCARRM	ITEM	DEFINED IN	SQLCA(RECD P10)
		USED IN	VRC0250(SGRP 116*)
SQLCASCA	ITEM	DEFINED IN	SQLCA(RECD P10)
		USED IN	VRC0250(SGRP 114*)
SQLCAWN1	ITEM	DEFINED IN	SQLCA(RECD P10)
		USED IN	VRC0250(SGRP 118*)
SQLCAWN6	ITEM	DEFINED IN	SQLCA(RECD P10)
		USED IN	VRC0250(SGRP 119*)
SVIGEN	ITEM	DEFINED IN	CUENTA(RECD P12)
		USED IN	CUENTA(RECD P11) VIE095P(PROC 19) V1109SA(PROC 43*)
VIE095A	PROC	55	VIE095P(PROC 21)

ITEM	GROUP	TYPE	CROSS REFERENCE
VIE095P		PROC	2
VII095A		PROC	35 VIE095P(PROC 15)
VII095B		PROC	96 VIE095A(PROC 73 78)
VIN095A		PROC	30 VIE095P(PROC 14)
VIN095B		PROC	101 VIE095P(PROC 28)
VIS095A		PROC	91 VIE095A(PROC 64 85)
VIT095A		PROC	45 VIE095P(PROC 20)
VIW09501		RECD	P9 VIE095A(PROC 69) VIE095P(PROC 16 17)
VRC0250		SGRP	106 VII095A(PROC 43) VII095B(PROC 99) VIS095A(PROC 94) VIT095A(PROC 53)
VRC0500	*EXTERNAL		USED IN VRC0250(SGRP 121)
WIO095COD		ITEM	DEFINED IN MIO1(MAP VIG095 P21)
WIO095EMI		ITEM	DEFINED IN MIO2(MAP VIG095 P24) USED IN VIE095A(PROC 82*)
WIO095FOP		ITEM	DEFINED IN MIO1(MAP VIG095 P21) MIO2(MAP VIG095 P24) USED IN VIE095A(PROC MIO2 80*)
WIO095IMP		ITEM	DEFINED IN MIO2(MAP VIG095 P24) USED IN VIE095A(PROC 84*)
WIO095NOM		ITEM	DEFINED IN MIO2(MAP VIG095 P24) VIW09501(RECD P9) USED IN VIE095A(PROC MIO2 89*) VIE095A(PROC VIW09501 89)
WIO095OPE		ITEM	DEFINED IN MIO2(MAP VIG095 P24) USED IN VIE095A(PROC 81*)
WIO095PRE		ITEM	DEFINED IN MIO2(MAP VIG095 P24) USED IN VIE095A(PROC 77*)
WIO095TIT		ITEM	DEFINED IN MIO2(MAP VIG095 P24) USED IN VIE095A(PROC 83*)
XSEG		ITEM	DEFINED IN CUENTA(RECD P14) USED IN CUENTA(RECD P11)

CONCLUSIONES

Debido a la importancia que los sistemas de cómputo tienen en la actualidad, el presente trabajo pretende ser una herramienta de consulta para toda organización que opere total o parcialmente a través de sistemas automatizados.

A lo largo del presente trabajo encontramos que:

1.- Cada vez más se reconoce a la información como un recurso importante para la toma de decisiones oportunas, esto es: "el poder lo tiene quien tiene la información". Por lo tanto hay que ofrecerle todo la protección posible para que no sufra ningún tipo de daños.

2.- En la práctica existen grandes deficiencias en cuanto a la seguridad física y lógica de todo centro de cómputo. Es por esto que se plantean diversos mecanismos de seguridad, así como temas sobre protección del centro de cómputo, sistemas de protección contra incendios, sistemas de suministro de energía eléctrica, control de acceso, seguridad en las comunicaciones, claves y protección de documentos.

3.- Al planear la construcción de un centro de cómputo se debe tener en cuenta su ubicación, diseño y construcción pues de esto depende el grado de riesgo a que éste puede estar sujeto.

4.- Se debe tener un sistema de respaldo del suministro de energía. Si el sistema principal llegase a fallar, el de emergencia entra en funcionamento mientras que el primero es reparado y así no se suspende el servicio.

5.- Los sistemas de detección y extinción de incendios son indispensables en cualquier centro de cómputo ya que el fuego es el más peligroso y frecuente de los desastres naturales que pueden afectarlo.

6.- El control de acceso es decir, la protección de todos los recursos y facilidades de la computadora y las comunicaciones en contra de accesos no autorizados es sumamente importante ya que evita que la información sea utilizada en forma inadecuada. Este tipo de control se puede llevar a cabo de muchas maneras que dependen de las necesidades y posibilidades de cada organización.

7.- En cuanto al acceso lógico o sea, el acceso a los datos y programas que se encuentran dentro del sistema, es necesario el uso de claves de acceso y junto con ellas el limitar las autoridades de uso de la información de acuerdo a las funciones de cada usuario.

8.- Es de vital importancia que toda organización cuente con un buen plan de respaldo y recuperación en caso de falla o caida del sistema, ya que el volver a la normalidad lo antes posible y con las menores repercuciones depende de él.

9.- Todo centro de cómputo debe tener un plan de recuperación escrito en el cual se consideren todas las situaciones de desastre y la manera de recuperarse de ellas.

10.- Es muy importante que se cuente con algún mecanismo que sirva de apoyo en caso de que el sistema principal falle. Esto puede ser: un centro de procesamiento alterno, sistemas en espejo, tener algún arreglo con otra organización que cuente con un equipo similar, etc.

11.- Siempre se debe tener un respaldo adecuado de todos los archivos que utiliza la organización para que en caso de que alguno se dañe se cuente con alguna copia.

12.- El uso de diarios es una ayuda con la que se debe contar de ser posible, pues permite una mucho mayor facilidad de recuperación en caso de falla del sistema.

13.- Cuando la información viaja por los sistemas de comunicación y ésta debe preservar su confidencialidad, se deben utilizar las técnicas de encripción para que nadie ajeno a la organización pueda interpretarla. Al usar encripción se debe ser muy cuidadoso en el manejo de las llaves a utilizar pues de ellas depende en gran medida su éxito.

14.- Resulta difícil que una organización logre un buen sistema de seguridad y confiabilidad ya que esto implica invertir grandes cantidades de dinero, con las que a veces no se cuenta.

En cuanto a la aplicación desarrollada para PROBURSA, Casa de Bolsa debemos de mencionar que:

1.- Las medidas de seguridad que se tomaron para la instalación de la red de cajeros automáticos fueron analizadas y estudiadas cuidadosamente.

2.- Para el sistema de cajeros automáticos la criptografía es uno de los aspectos más importantes, al igual que la utilización del algoritmo DES (Data Encryption Standard) para la codificación de las tarjetas magnéticas.

3.- Tanto el diario estadístico como la tira de auditoria son elementos de seguridad de mucha importancia, además de que ayudan a incrementar la confiabilidad del sistema.

Creemos que es indispensable la utilización de medidas o técnicas de seguridad en cualquier institución que utilice equipos de cómputo para prevenir cualquier tipo de ataque, o mal uso de la información y fraudes a la institución.

BIBLIOGRAFIA

1.- Bancomer, S.N.C., Grupo Auditoría. División de Auditoría en Informática.
Seguridad en Cajeros Automáticos
Seminario de Seguridad en Informática
Toluca México, Junio 1988.

2.- Burch, John G. Jr., Strater, Felix R. Jr.
Sistemas de Información. Teoría y Práctica
Limusa.

3.- Callon, Jack D.
Using Information Systems to Compete
1987.

4.- Carroll, John Millard
Computer Security
Butterworths, 1987.

5.- Cooper, James A.
Computer Security Technology
Lexington Books, 1984.

6.- Farr, M.A.L., Wong, K.K.
Security for Computer Systems
1973.

7.- Hoffman, Lace J.
Modern Methods for Computer Security and Privacy
Prentice-Hall Inc., 1977.

8.- IBM Corp.
IBM Operation and Recovery Guide
San José, California, Fourth Edition, May 1987.

9.- IBM Corp., IBM Research Laboratory
Storage Technologies: Capabilities and Limitations
San José, California, 1979.

10.- Infotech, State of The Art Report
Computer System Security
Series 9 Number 5, 1981.

11.- Katzan, Harry
The Standard Data Encription Algorithm.

12.- Lane, V. P.
Security of Computer Based Information Systems
Macmillan, 1985.

13.- Lazcano, Juan Manuel
Rivas, Enrique
Auditoría e Informática Estructuras en evolución.
Instituto Mexicano de Contadores Públicos, A.C., 1988.

14.- Lobel, Jerome
Foiling the System Breakers.
Computer Security and Access Control
Mc Graw-Hill, 1986.

15.- Martin, James
Las Telecomunicaciones y La Computadora
Diana.

16.- Mouiton, Rolf
Computer Security Handbook Strategies and Techiques for Preventing Data Loss or Theft
1986.

17.- Mustonen, Antero
Security Threats and Planning of Computer Centers
Computer Security: A Global Challenge
North-Holland, 1984. pp. 331-376.

18.- Rivest, Ronald L., Sherman, Alan T.
Randomized Encription Techniques
MIT-LCS. Enero 1983.

19.- Sweeney, G.P. Editor
Information and The Transformation of Society
North-Holland.

20.- Turn, Rein
Application of Cryptography
Advances in Computer Security Managment, Vol. I
Heyden, 1980. pp. 168-198.

21.- Wood, Helen M.
A Survey of Computer-Based Password Techiques
Advances in Computer Security Managment, Vol. I
Heyden, 1980. pp. 141-161.

22.- Wood, Michel B.
Fire Precautions in Computer Installations
NCC Publications, 1986. pp. 28-75.