83
2 ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

ANALISIS Y DESARROLLO DE UN SISTEMA EXPERTO ENFOCADO A LA AUDITORIA DE CENTROS DE COMPUTO

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO EN COMPUTACION
P R E S E N T A N :
CLAUDIA MARIA RODRIGUEZ CHAN
GERARDO GABRIEL CARRASCO ZUÑIGA

DIRECTOR DE TESIS ING. SALVADOR PEREZ VIRAMONTES

MEXICO, D. F. 1992

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

CONTENIDO.

CAPITULO 1

INTRODUCCION

AUDITORIA EN CENTROS DE COMPUTO.

La Auditoría Informática es el proceso de recolectar y evaluar evidencias para determinar si un centro de cómputo mantiene en óptimas condiciones los componentes que lo conforman siendo estos los activos, la integridad de los datos, si se realizan las metas organizacionales y se consumen recursos de manera efectiva (Figura 1.1).

Es necesario controlar y auditar las a computadoras, puesto que la demanda y el mal uso de éstas está a la orden del día.

Son cinco las razones para establecer una función que examine los controles en el procesamiento de datos:

- Reducir la pérdida de información.
- Decisiones correctas.
- Menor abuso en el manejo de la información.
- Privacidad en la información.
- Control en la evolución tecnológica.

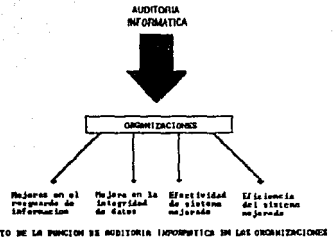


Figura 1.1 Función de Auditoría Informática.

Activos

Los activos de una instalación de cómputo incluyen equipo (hardware), sistemas y paquetería (software), personal, archivos de datos, documentación de sistemas (manuales) y suministros. Como todo capital y activo deben ser protegidos por un sistema de control interno.

Integridad de la información

Este es un concepto fundamental en auditoría de centros de cómputo. Implica que la información sea: completa, firme, pura y veraz.

Efectividad del sistema

Un sistema de procesamiento de información efectivo cumple sus objetivos. Evaluar la efectividad implica conocer las necesidades de los usuarios.

Eficiencia del sistema

Un sistema de procesamiento de información eficiente utiliza un mínimo de recursos para realizar los procesos requeridos. Estos recursos son: Tiempo de máquina, periféricos, canales, paquetería para el sistema, trabajo. La eficiencia es importante cuando una computadora ha excedido su capacidad, la ejecución de algunos sistemas de aplicación se degradan, provocando tiempos de respuesta muy altos.

EFECTOS DEL PROCESAMIENTO DE SISTEMAS EN EL CONTROL INTERNO

El resguardo de activos, la integridad de la información, y la efectividad y eficiencia del sistema pueden ser realizados solo si la alta gerencia de la organización instala un sistema de control interno.

Tradicionalmente, la mayoría de los componentes de un sistema de control interno incluyen: separación de obligaciones, clara delegación de autoridad y responsabilidad, contratación y entrenamiento de personal de alta calidad, supervisión de la gerencia, un sistema de autorizaciones, acceso limitado a activos y comparación de contabilidad registrada en activos.

Separación de obligaciones

En un sistema manual, una persona debería ser responsable de iniciar transacciones, otra sería responsable de registrarlas y otra de cuidar los activos. Como control básico, ayuda a prevenir o detectar fraudes y transacciones incompletas o erróneas.

En un sistema de cómputo no siempre existe la idea tradicional la de separación de obligaciones. Es ineficiente un programa, por ejemplo, que compara una factura de venta con un documento en una base de datos e imprime un recibo por la cantidad; a menos que éstas funciones se separen en diferentes programas.

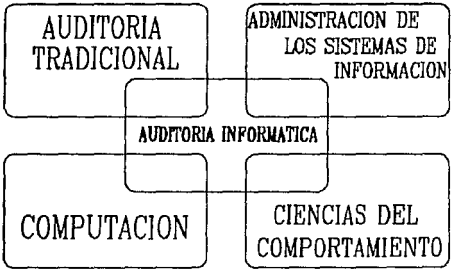
Acceso a activos

Como unidades organizacionales, las instalaciones de cómputo son algo único en la manera de concentrar los activos de la organización. Se puede perpetrar un fraude por un cambio no autorizado en un programa o archivo de datos que últimamente afecte el desembolso de fondos. Además, los programas y archivos pueden constituir valiosos activos.

FUNDAMENTOS DE AUDITORIA EN CENTROS DE COMPUTO

La auditoría a centros de cómputo (EDP audit. Electronic Data Processing) viene de dos direcciones: La primera, los auditores observaron el impacto causado por el empleo de las computadoras en cuanto a su habilidad para realizar la tarea de auditar; y segundo, la alta gerencia y la gerencia del departamento de procesamiento de información reconocen que las computadoras son recursos valiosos que necesitan ser controladas como cualquier otro recurso valioso para la organización.

La auditoría en centros de cómputo se alimenta de cuatro áreas fundamentales:



Auditoría Tradicional

La auditoría tradicional dió a la auditoría de centros de cómputo riqueza en conocimientos y experiencia en cuanto a técnicas de control interno. También impactó a los componentes de las computadoras de un sistema de cómputo.

Administración de centros de cómputo

Los primeros años de la computación muestran algunos desastres espectaculares cuando se han implantado los sistemas de cómputo. Recientemente investigadores han estado estudiando mejores maneras de desarrollar e implantar sistemas de información y han obtenido algunos avances. Se han desarrollado algunas técnicas de administración de proyectos en el área de sistemas de información.

Ciencia del comportamiento

En 1975, Henry Lucas hizó un estudio de dos mil usuarios en 16 diferentes organizaciones, y se llegó a la conclusión que la mayoría de las razones por las que fallan los sistemas de cómputo es porque ignoran el comportamiento organizacional en el diseño e implantación de sistemas de información.

Computación

Algunos científicos en computación han estado estudiando sobre el resguardo de activos, integridad de información, efectividad y eficiencia del sistema, no solo los auditores están preocupados por éstos aspectos.

El conocimiento técnico de alto nivel en computación provee beneficios y problemas para la auditoría en centros de cómputo. Por un lado, permite que el auditor se preocupe menos acerca de la confiabilidad de ciertos componentes en el sistema de procesamiento de datos. Pero por otro lado, si se abusa del conocimiento de la materia, será mas difícil para el auditor detectar tal abuso.

"Un fraude perpetrado por un programador de sistemas experto es casi imposible ser detectado por un auditor que no tiene el nivel de conocimiento técnico correspondiente"

GENERALIDADES DE LA AUDITORIA A CENTROS DE COMPUTO

Todas las instalaciones de cómputo, excepto las pequeñas, son casi imposibles de auditar detalladamente. A continuación se describe una aproximación general para realizar una auditoría en centros de cómputo.

El sistema de controles internos y auditoría

Una manera de que el auditor evalúe las aplicaciones en cuanto a resguardo de activos, integridad de información, efectividad y eficiencia del sistema, sería examinar directamente los productos finales de los sistemas: Información producida, su uso por quién toma las decisiones y los recursos consumidos por los sistemas. Obviamente esto requiere tiempo. Generalmente es menos costoso para el auditor examinar el sistema de controles internos establecido por el gerente para asegurar que éstas aplicaciones realizan sus objetivos. Si el sistema de control interno está intacto, el auditor puede tener mayor confianza en la calidad de las aplicaciones que están siendo evaluadas.

Controles y el potencial de pérdida

La gerencia establece un sistema de control interno para reducir la pérdida en potencia. El valor de un control puede ser medido en términos de su costo y el grado en la cual, éste reduce las pérdidas estimadas. Se pueden reducir las pérdidas estimadas de dos maneras: a) Reducción de la probabilidad de que ocurra la pérdida, y b) Reduciendo la cantidad de pérdida si ésta ocurre.

LA NATURALEZA DE LOS CONTROLES DE COMPUTO

La evaluación del sistema de controles internos también es facilitado si el auditor conceptualiza los controles sobre el procesamiento de información en una computadora de diferentes maneras. Las siguientes secciones establecen dos tipos de controles de la computadora.

Controles gerenciales y de aplicaciones

La clasificación de los controles de cómputo en controles gerenciales y controles de aplicaciones son útiles por tres razones: Primero, frecuentemente es más eficiente para el auditor evaluar los controles gerenciales antes de los controles de aplicación. Segundo, con la mayoría de las categorías de controles gerenciales y de aplicación, los controles de cómputo pueden ser organizados, además de proveer una base ordenada para conducir la auditoría. Tercero, se volverá aparente la discusión de que la conceptualización de controles en una instalación de cómputo es como una "cebolla" donde las capas constituyen los diferentes niveles de gerencia y aplicaciones (Figura 1.2).

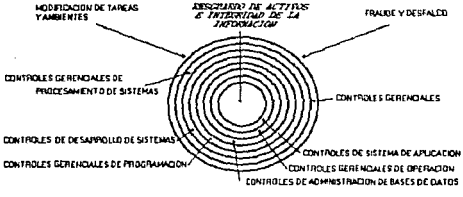


Figura 1.2 Niveles de Gerencia y Aplicaciones

Control gerencial

Los controles gerenciales intentan asegurar el desarrollo, implementación y operación de sistemas de información que proceden de manera planeada y controlada.

Nivel de Control Gerencial	Descripcion
Gerencia Superior	Asegura que la instalacion de computo sea bien administrada
Gerencia del Centro de Computo	Tiene, sobre todo, responsabilidad para la planeacion y control todas las actividades computacionales.
Gerencia de Sistemas en desarrollo	Responsable del diseno, implementacion y mantenimiento de los sistemas de aplicacion individuales.
Gerencia de Programacion	Responsable de la programacion de nuevos sistemas y proveerlos de paqueteria (Software).
Gerencia de Base de datos	Responsable del control y uso de la base de datos organizacional
Gerencia de Operaciones	Controla las operaciones diarias de los sistemas de computo. Responsable de la preparacion de informacion, del flujo de informacion a traves de la instalacion, mantener el equipo, etc.

Los controles gerenciales son fundamentales, se realizan a través de los sistemas de aplicación, por lo tanto, la omisión de alguno es un serio asunto para el auditor. No valdría la pena revisar y evaluar controles de aplicación si existe alguna debilidad en el marco de control gerencial.

Control de aplicaciones

El sistema de control de aplicaciones intenta asegurar que las aplicaciones individuales resguardan activos del centro de cómputo, mantengan integra la información y la procesen eficientemente. Los controles de aplicaciones son empleados en varias etapas en el flujo de datos a través de un sistema de cómputo:

Edo de Control de Aplicacion	Descripcion de los controles
Captura de Informacion	Asegura que todas las transacciones sean registradas y autorizadas, completas y exactas.
Preparacion de Informacion	Asegura que toda la informacion es convertida a una forma legible por la maquina y autorizada, completa y exacta.
Acceso	Aseguran que unicamente personas autorizadas obtengan acceso a los recursos de computo tales como archivos y programas del sistema de aplicacion.
Entrada	Asegura que los datos introducidos a la computadora son autorizados, exactos y completos. Detecta errores y corrige.
Transmision	Asegura que la informacion enviada entre dos puntos de un sistema de computo es autorizada, exacta y completa.A
Procesamiento	Asegura que se procese toda la informacion y que el proceso este autorizado y completo.
Salida	Asegura que la salida producida por la computadora es autorizada, exacta y completa. Distribuida al personal responsable.
Seguimiento de auditoria	Asegura que la informacion puede ser trazada a traves del sistema desde su fuente hasta su destino final.
Respaldo y Recuperacion	Asegura que la existencia fisica de la informacion puede ser restablecida si la informacion es perdida o su integridad es corrompida.

Los controles de aplicaciones también son ejemplos de controles horizontales. Estos siguen el flujo de datos a través de la organización y cortan a través de las líneas organizacionales de autoridad y responsabilidad. Los controles gerenciales, por otro lado, tienden a ser ejemplos de controles verticales; controles que siguen las líneas jerárquicas de autoridad en un organigrama.

PASOS A SEGUIR EN LA AUDITORIA INFORMATICA.

Considerando lo visto anteriormente acerca de como podría llevarse al cabo una auditoría; veremos ahora los pasos para realizar la auditoría a centros de cómputo.

Fase de revisión preliminar

El primer paso de la auditoría es la revisión preliminar de la instalación de cómputo. El objetivo es que el auditor pueda decidir la manera de proceder con la auditoría.

La conclusión de ésta fase es que el auditor puede proceder de tres maneras:

1. Retirarse de la auditoría. Puede haber problemas debido a la falta de capacidad técnica del auditor.

2. Realizar una revisión detallada del sistema de control interno esperando confiar en dicho sistema de control interno para que las pruebas de auditoría se reduzcan en lo posible.

3. Decidir en no confiar en el sistema de control interno. La primera razón es que puede ser más costosa una auditoría realizada directamente y segundo, los controles del centro de cómputo pueden duplicar los controles existentes en el área del usuario.

La revisión de los controles gerenciales permite que el auditor entienda las prácticas de organización y administración usados en cada nivel jerárquico de la instalación de cómputo

Durante la revisión de los controles de aplicaciones, el auditor intenta entender los controles aplicados a la mayoría de los tipos de transacciones que fluyen a través de los sistemas de aplicación más importantes.

Fase de revisión detallada

El objetivo es recabar la información necesaria para que el auditor tenga un entendimiento profundo de los controles empleados en una instalación de cómputo. Nuevamente, se debe decidir por alguna de las tres maneras de proceder antes mencionadas. Para algunas aplicaciones el auditor puede decidir en confiar en el sistema de control interno; para otras, algunos procedimientos de auditoría alterna puede ser más adecuado. Aquí, nuevamente, se revisan tanto controles gerenciales como controles de aplicación.

Esta fase es importante para identificar las causas de pérdida existentes en la instalación y los controles establecidos para reducir los efectos de éstas pérdidas. La conclusión de esta fase es si los controles funcionan. Debido a que el auditor conoce como trabajan los controles, se asume que funcionan confiablemente, a menos que ya haya evidencia de lo contrario.

Fase de la prueba de controles

El objetivo de ésta fase es determina si el sistema de control interno opera como éste debe hacerlo. El auditor investiga para determinar si los supuestos controles existen como tales y si trabajan confiablemente.

Un ejemplo de esta fase es cuando se evalúa un programa que lee información de un archivo; para tal efecto, se introduce un archivo con toda una gama de errores para poder conocer los datos producidos por el programa.

Revisión y prueba de los controles de usuario.

En algunos casos, el auditor podría decidir en no confiar en los controles internos debido a que los usuarios aplican controles para compensar cualquier debilidad en el sistema de control interno.

Fase de auditoría

Aquí, se debe obtener la suficiente evidencia para que el auditor pueda realizar un juicio final acerca de si se podrían presentar pérdidas materiales o si han ocurrido durante el procesamiento de la información.

ORGANIZACION Y ADMINISTRACION DE LA AUDITORIA EN CENTROS DE COMPUTO

La auditoría a centros de cómputo es parte de la auditoría tradicional, sin embargo, existe la necesidad de una sección de auditoría a centros de cómputo separada y la necesidad de especialistas en auditoría informática.

Papel del auditor en centros de cómputo.

El secreto de ser un buen auditor de centros de cómputo es el de ser capaz de combinar los controles fundamentales y las metodologías de auditoría a centros de cómputo de una manera apropiada para una instalación de cómputo específica, siendo ésta, un simple sistema de procesamiento en lote o un complejo sistema administrador de base de datos.

NECESIDAD DE UN DEPARTAMENTO DE AUDITORIA INFORMATICA

La pregunta más frecuente que surge cuando se organiza y administra la auditoría en centros de cómputo es si un grupo separado de especialistas en auditoría informática debería existir o no para realizar ésta función.

Necesidad de especialistas en auditoría informatica.

Existen tres motivos para tener especialistas en auditoría informática en una posición creada en la jerarquía de auditoría en las organizaciones. La primera, alguien debe estar técnicamente preparado para realizar las auditorías informáticas. La segunda, la independencia de la auditoría se incrementa si los

auditores están técnicamente preparados en computadoras. Y tercero, pueden existir mejores relaciones entre el personal de auditoría y el personal del centro de cómputo.

Consideraciones de la preparación técnica.

Un requisito fundamental de cualquier auditoría es que el auditor este técnicamente preparado para realizar la auditoría.

Consideraciones de la independencia de la auditoría.

Uno de todos los argumentos en cuanto a tener la auditoría de cómputo separada, es que ésta incrementará la independencia del grupo de auditoría.

Relación con el personal del centro de cómputo.

En ocasiones el respeto del personal del centro de cómputo por el auditor depende de la capacidad técnica de éste en cuanto a computadoras.

Recursos de personal en Auditoría en centros de cómputo.

Debido a que pocas personas se preparan en Auditoría y contabilidad y a la vez en conocimientos de computadoras, además de que no son muchas las instituciones que proporcionan estos conocimientos en una sola carrera, se llega a la pregunta: ¿Que se debe hacer; a un auditor entrenarlo en sistemas de cómputo o a un especialista de sistemas de cómputo entrenarlo en auditoría?.

Existe quien argumenta que los conocimientos de computación requeridos para la auditoría a centros de cómputo son mayores que los conocimientos de auditoría, y existen otros argumentos de lo contrario. Pero la mayoría de las organizaciones prefieren que los profesionales de la computación sean entrenados en auditoría.

CONOCIMIENTO DE COMPUTACION REQUERIDO PARA LOS DIFERENTES NIVELES DE AUDITORIA A CENTROS DE COMPUTO.

AREA DE CONOCIMIENTO	HABILIDAD DEL AUDITOR		
	BASICO	INTERMEDIO	AVANZADO
Principios y conceptos de procesamiento de datos	ELEMENTAL	SUSTANCIAL	SUSTANCIAL
Estructura de los sistemas de aplicacion	ELEMENTAL	SUSTANCIAL	SUSTANCIAL
Controles y procedimientos de los sistemas de aplicacion	ELEMENTAL	ELEMENTAL	SUSTANCIAL
Administracion de datos	ELEMENTAL	ELEMENTAL	SUSTANCIAL
Controles de Centros de servicio	ELEMENTAL	ELEMENTAL	SUSTANCIAL
Controles de desarrollo de sistemas de aplicacion	NO	ELEMENTAL	SUSTANCIAL
Programacion de aplicacion	NO	ELEMENTAL	SUSTANCIAL

La pregunta ahora es: ¿En que nivel jerárquico debe situarse a los auditores informáticos?

Auditoría a centros de cómputo, como función separada.

Argumentos:

1. Mejor uso de los recursos de auditoría informática
2. Mayor satisfacción de trabajo para el auditor de informática
3. Organización de la auditoría informática como departamento.
4. Facilita la coordinación y control.
5. Incrementa la especialización para competir con la tecnología más compleja.

Auditoría informática como una línea de función:

Si se tiene este enfoque, los especialistas auditores de computadoras serán asignados a cualquier auditoría, incluyendo sistemas simples, como miembros del equipo de auditoría. Por lo tanto, las responsabilidades del especialista encerrarán funciones tanto de auditoría a sistemas de cómputo como de auditoría tradicional. Los tres argumentos para tener este tipo de organización son:

1. Mayor congruencia en las metas. Como miembro del equipo que tiene grandes responsabilidades, el especialista debería tener un mejor entendimiento de todos los objetivos de la auditoría y asumir la responsabilidad para realizarlos.

2. Facilita la comunicación. Los especialistas en la auditoría informática consideran que, los auditores son deficientes, técnicamente hablando; y los auditores ven a los especialistas faltos de interés en cumplir los objetivos de la auditoría por el interés que tienen en la tecnología. Por lo tanto, teniendo a los especialistas como miembros del mismo equipo de trabajo facilita la comunicación entre ellos.

3. Mejora la experiencia en sistemas de cómputo de los auditores. Los auditores especialistas como miembros del equipo toman decisiones que los auditores respaldan y viceversa, por lo cual, los auditores adquieren más experiencia en sistemas de cómputo así como los especialistas mejoran sus conocimientos en auditoría.

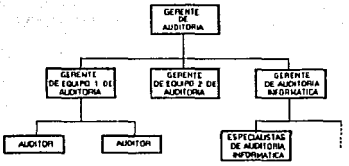


Figura 1.4 Auditoría Inform. como personal de función.

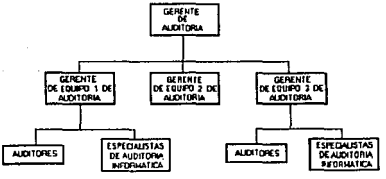


Figura 1.5 Auditoría Inform. como una línea de función

CAPITULO 2

ELEMENTOS DE AUDITORIA A CENTROS DE COMPUTO

SEGURIDAD DE LOS SISTEMAS.

Alcance del término.

La seguridad de los sistemas se refiere de manera principal a la seguridad del equipo de cómputo, é incluye:

El equipo.

Los programas de uso general, los sistemas de comunicaciones o redes, las terminales y los programas asociados a estos elementos, excepto los programas de aplicación específica.

Cada uno de estos aspectos se presentan ahora por separado. El área clave que se debe considerar en cada caso es la existencia de debilidades, las cuales exponen al sistema a la amenaza o abuso.

En general, éstas debilidades en el equipo sólo son relevantes en las instalaciones que requieren alta seguridad. Se deben identificar y determinar la manera de como eliminarlas.

Por ejemplo, los malos manejos en la operación del equipo crean el riesgo de negligencia o accidente. Estos se deben definir e incluir en un manual práctico de operaciones para el personal. Donde sea posible, estas prácticas se deben vigilar en todo el equipo por medio de pruebas sorpresa u observación.

Los programas.

El número de debilidades en los programas es considerable, por no decir infinito. No se ha diseñado todavía un sistema operativo completamente seguro. Por lo general, la seguridad se considera posteriormente y, en consecuencia, en las medidas que se toman se tienen que imponer sobre una estructura ya existente. Esto reduce de manera natural el nivel de efectividad de la seguridad.

La seguridad de la programación pretende:

1. Restringir el acceso a los programas y archivos.

2. Asegurar que los operadores puedan trabajar sin la supervisión minuciosa y no modificar los programas ni los archivos.

3. Asegurar que se estén utilizando los datos, archivos y programas correctos en el procesamiento.

El método que se debe seguir consiste en:

1. Elaborar un inventario de las debilidades identificadas.

2. Elaborar un inventario de las debilidades que no se han identificado todavía, pero que si se han mencionado.
3. Probar las debilidades existentes y potenciales para verificar su existencia.

4. Definir alguna forma de seguimiento o control para cada área de debilidad.

5. Elaborar un plan de acción para realizar tales controles.

Es muy importante comprometer al personal clave de los proveedores correspondientes en esta actividad, a fin de hacerla independiente. El nivel general de conocimiento acerca de éstas debilidades dentro de las instituciones proveedoras es bajo, y puede ser necesario contar con asesoría para ésta evaluación. Por razones obvias, la cantidad de publicaciones, tanto de proveedores como de otros, es prácticamente nula en esta área.

Redes.

Este término pretente describir los sistemas de comunicación y los programas de manejo asociados a éstos. Así como en la programación, ésta constituye un área muy complicada donde sólo un pequeño grupo de especialistas maneja los conocimientos correspondientes. El mayor riesgo reside en el acceso no autorizado a las redes, con el propósito de obtener información confidencial o de hacer uso indebido de las instalaciones de procesamiento. Se han dado casos de ambos tipos de abuso en esta área.

El aspecto del acceso a información confidencial merece especial atención en las intituciones de alta seguridad. Como en el caso de la línea de teléfono, no es muy difícil rastrear una línea de transmisión. Así como éste, existe el método de encriptación.

Terminales.

En la actualidad, muchas terminales equivalen por si solas a poderosas computadoras. Por ello, al revisar la seguridad de las terminales, éstas se deben tratar como pequeñas computadoras. Aquí, se deben revisar los siguientes aspectos:

1. La ubicación de las terminales, el conocimiento general de ello y el acceso físico a la terminal misma.

2. El control sobre la operación no autorizada de la terminal por medio de palabras clave, códigos u otro método de identificación.

3. El equipo, los programas y otras verificaciones que permitan garantizar que los controles mencionados anteriormente se reforzarán.

Aunque recientemente los programas para la red y el computador principal para el control de terminales ha mejorado en forma notable, todavía no se conoce un sistema de seguridad de terminales completamente eficaz. Así, resulta muy importante garantizar el máximo control en las siguientes áreas:

- Verificaciones físicas e informales acerca del uso de la terminal.
- Vigilancia e informes sobre los intentos de acceso no autorizado.
- Cambios sorpresa de las claves del usuario.
- Auditoría sorpresa llevadas al cabo como parte del procesamiento de datos.
- Pruebas sorpresa para las prácticas de operación.

SEGURIDAD DE LAS APLICACIONES.

Alcance del término.

El término "seguridad de las aplicaciones" abarca tanto a los componentes de la computadora como a los que no lo son en cada aplicación. Por parte de la computadora se comprende datos, programas y archivos que se procesan en el sistema. Los elementos que no son de la computadora incluyen recolección y entrega de datos e información del archivo maestro para el procesamiento, así como el control de dicha información para garantizar que se procese en forma correcta y su distribución al usuario. Las etapas clásicas de cada sistema implican:

- Recolección y Captura de datos.

- Procesamiento.

- Distribución de los resultados.

Relación computadora - usuario.

En muchas instalaciones se presta atención a los controles tanto de los departamentos usuarios como los controles de los sistemas de cómputo. Sin embargo, debido la revisión de éstos controles los realizan distintas personas en cada área, existen vacíos respecto a los controles entre las dos áreas.

Los controles de rutina en éstas áreas han sido frecuentes y son ahora efectivos en términos generales. La debilidad siempre surge cuando la disciplina no es lo suficientemente rigurosa.

Un gran problema en todos los sistemas de cómputo es el control de los errores. Existen ciertos puntos clave:

- Todos los errores se deben corregir.

- Los errores sólo se deben corregir por el personal autorizado.

- La separación de responsabilidades se debe mantener cuando se asigne la autoridad para la corrección de errores.

En el terreno práctico, todos estos aspectos presentan dificultades. Se requiere un enfoque metódico y muy riguroso.

Otro punto importante dentro de la relación hombre-máquina es la distribución de los datos. La seguridad al respecto debe cubrir lo siguiente:

1. La responsabilidad e identificación del personal autorizado para el acceso a los informes.

2. El control sobre los resultados tanto para las operaciones válidas como las frustradas.

3. El control sobre las que fueron copias carbón de los informes corregidos.

Controles del usuario.

El usuario tiene la responsabilidad primaria de asegurar que los datos recolectados para el procesamiento estén completos y sean precisos; también se debe asegurar de que todos los datos se procesen y se incluyan en los informes que le regresan. En el análisis final, no es aceptable culpar a la computadora por las decisiones que se basen en datos imprecisos.

Controles de procesamiento.

Se trata de los controles que se mantienen dentro del departamento de cómputo. Son el reflejo de aquellos que se mantienen en los departamentos de usuarios pero, en algunos aspectos, son más minuciosos:

- División de la responsabilidad entre captura de datos y operación.
- División de la responsabilidad entre operaciones y archivo.
- Registro de evidencias que reflejan la transferencia de registros y datos entre las diferentes funciones.

SEGURIDAD DE LOS ARCHIVOS.

Un elemento importante y tradicional que se debe considerar en el control del procesamiento es la seguridad de los archivos, la cual abarca lo siguiente:

Almacenamiento de las copias de seguridad.

De preferencia, la ubicación para el almacenamiento de estos archivos debe estar muy distante de la computadora. En las instalaciones de alta seguridad se deben tomar medidas especiales.

Revisión periódica de los controles de aplicación.

La revisión de los controles, tanto de la computadora como de los que no lo son, es una parte importante de la función de auditoría interna. Tal revisión es una tarea compleja y estricta que requiere mucho tiempo. No es raro que se necesiten tres o cuatro meses para las aplicaciones grandes y complicadas. Este tipo de trabajo no se acepta como de rutina en muchas instalaciones, aún en aquéllas de alto riesgo. Sin embargo, la práctica va en aumento.

Estándares de programación y operación.

Cuando se incorporan los estándares como una parte de cualquier método de seguridad, surgen varios problemas. El problema principal proviene del hecho de que no se percibe, por lo general, la relación que existe entre los estándares y la documentación con el aspecto de la seguridad en computación.

En realidad, no se requiere prácticamente ningún esfuerzo adicional cuando se aplican buenos estándares, prácticas y documentación dentro de un departamento de cómputo.

Se puede concluír que; el aspecto fundamental no es la seguridad, sino el compromiso con los buenos estándares de trabajo, lo cual todavía es un punto por tratar en muchos departamentos de cómputo. Con frecuencia el área de estandarización es también, la que causa más reacción ante cualquier estudio formal de la seguridad en computación.

La seguridad, a su vez, se debe considerar en dos niveles:

- Seguridad en la instalación.

- Seguridad en las aplicaciones específicas.

La consideración de seguridad para la instalación requiere una planificación a largo plazo para garantizar la seguridad de las aplicaciones. Esto es, por lo tanto, una idea a largo plazo que se pueden ver con claridad en cualquier instalación donde se tome la decisión de mejorar la seguridad de una aplicación.

Seguridad y Planeación a largo plazo.

La seguridad en computación rara vez se expresa como un objetivo primario de diseño. Así, muchas aplicaciones ya están diseñadas y puestas en práctica cuando se considera la seguridad por primera vez. Por lo tanto, la omisión de los aspectos de seguridad en esta etapa acarrea revisiones más costosas.

Es evidente que este enfoque es inaceptable debido al incremento en la complejidad, escala y nivel de inversión de las aplicaciones. En las aplicaciones en línea, de tiempo real y de bases de datos que las instituciones emplean actualmente, la incorporación de estándares mínimos de seguridad implica un esfuerzo material, si no es que un rediseño, para lograrlos. Es entonces, importante incorporar objetivos y estándares de seguridad como una parte integral de la actividad de planeación computacional a largo plazo. Los puntos claves son:

1. El impacto de la seguridad sobre la estrategia del equipo y los programas.

2. Las consideraciones de la seguridad de las terminales respecto a:

   - Los controles de la aplicación.

   - Los requisitos físicos y la ubicación.

   - La estrategia de las redes, la seguridad y el respaldo.

3. Los estándares de control de la aplicación, en especial los de inicio y de respaldo.

4. Los estándares de los datos y del diseño de archivos.

5. La función de la auditoría interna y externa y los requisitos durante las fases de diseño, aplicación y operación garantizan la calidad de la aplicación a corto plazo. Los elementos principales que se deben revisar son:

- Seguridad del equipo y los programas.

Los requisitos de seguridad para la aplicación varían de acuerdo con el tipo de aplicación y los niveles de seguridad exigidos por la institución o por la instalación de cómputo como un todo. En general, estos asuntos reciben atención durante la planeación a largo plazo. No obstante, pueden suceder que una aplicación altamente confidencial se esté llevando a cabo dentro de una instalación cuyos requisitos de seguridad sean bajos.

En las fases de iniciación del proyecto, los objetivos de seguridad deben estar definidos con claridad y deben incluír la consideración de los datos de transacciones, los datos registrados, en el archivo maestro y la seguridad del programa. Si se utilizan terminales, debe considerarse en forma detenida el asunto del acceso a ellas. La definición clara de estos aspectos permitirá la formulación de criterio y estrategias de diseño también claras.

- Controles de Aplicación.

Muy pocas instalaciones, si acaso, han evadido el dilema de omitir los controles clave de las aplicaciones. Los controles, como la seguridad, rara vez constituyen un objetivo primario por lo que generalmente se requiere de grandes revisiones para incorporarlos. Las necesidades de control se incluyen en dos categorías:

a) Los controles del usuario.

b) Los controles detallados de cada proceso, de los datos y los archivos, por parte de las operaciones.

Dentro de una instalación bien establecida es poco probable que surjan nuevos estándares de control. Los estándares mínimos ya pasaron por experiencias más agudas.

Además de los controles de rutina mencionadas hasta ahora, un asunto de gran importancia, que se incrementa en las aplicaciones grandes, es el de criterio de reinicio, el cual tiende a ser otra "relación débil". Aunque mucho de la programación de los sistemas operativos facilita el reinicio, éste siempre será difícil al menos que se haya previsto adecuadamente en el diseño de la aplicación. En consecuencia, el criterio de reinicio debe ser un objetivo del diseño explícito desde el principio del proyecto y se le debe prestar una consideración detallada en lo secesivo, a nivel de conjunto y dentro de los programas individuales.

- Supervisión y métodos de trabajo.

En general, es cierto que la seguridad es buena cuando existe una gerencia efectiva. Esto se puede aplicar a las situaciones donde existen estándares bien estructurados y definidos respecto al método de trabajo. Los métodos estructurados que incluyen verificaciones regulares también facilitan la supervisión. Aunque la más rigurosa supervisión no necesariamente detecta rutinas fraudulentas o no autorizadas en los sistemas y programas, con seguridad evita el abuso. Aún más asegura que los estándares de seguridad reciban la consideración debida como rutina en el proceso del diseño. Las principales consideraciones de seguridad como parte del proceso de diseño son:

1. Puntos de enlace claramente definidos; éstos refuerzan la división de responsabilidades y mejoran el proceso de control de calidad.

2. Programas de prueba y conversión; la puesta en marcha de nuevas aplicaciones es un período de riesgo y se requieren procedimientos bastante estructurados y controlados.

Ambas áreas son casi siempre débiles. La conveniencia y las presiones de tiempo por lo general perjudican la disciplina en los enlaces, mientras que muy pocas instalaciones cuentan con estándares estructurados y bien definidos para la planeación y ejecución de las pruebas para programas individuales o de

conjunto. Esto es particularmente cierto en los sistemas de línea, donde las terminales requieren nuevos y mejores estándares de pruebas. Todos estos aspectos se deben incluir de manera cuidadosa en los estándares de seguridad.

El advenimiento de un nuevo grupo de técnicas para el mejoramiento de la productividad del programador, como son el diseño y la programación estructurados y el concepto del equipo programador, benefician en forma considerable a la seguridad, la estructura formal de módulos de trabajo y la evaluación detallada de calidad a cargo de varios empleados, ofrecen un marco de trabajo riguroso para la seguridad y una base para la documentación evolutiva o documentación que se completa progresivamente. Por lo tanto, estas prácticas se deben estimular.

- Documentación.

Se necesitan precauciones de seguridad para las aplicaciones terminadas; las principales son:

1. El almacenamiento de la documentación para todas las aplicaciones en un lugar distante; se deben incorporar como rutina las modificaciones en un lugar distante; se deben incorporar como rutina las modificaciones por mantenimiento.

2. El acceso a la documentación se debe restringir al personal directamente relacionado con el proyecto y, en las instalaciones de alta seguridad, quizá sólo a módulos de esa aplicación.

El personal de procesamiento de datos que tiene más experiencia, reconoce que las copias de respaldo de archivos y programas sólo son de utilidad si cuentan con el respaldo de la documentación adecuada de los sistemas y la programación. Sin embargo, pocas instalaciones cuentan con procedimientos sensatos para su protección regular; aun en los lugares donde existen, el acceso es libre y cualquier empleado puede fácilmente sacar, estudiar o copiar la documentación de las aplicaciones.

Operaciones.

Así como la documentación de los sistemas y de los programas, la instalación puede estar expuesta a un riesgo considerable debido a la ausencia de:

1. Estándares adecuados para las actividades de operación, incluyendo, si corresponde, la preparación de datos.

2. Arreglos para el almacenamiento de la documentación duplicada.

En la mayoría de las instalaciones se acepta la necesidad de estándares de sistemas y programación. Esto no se aplica tan libremente en el caso de los estándares de operaciones, a pesar de que por lo general se acepta el mínimo de instrucciones de operación.

Los estándares de operación deben incluír:

- Buenas prácticas de mantenimiento.
- Evitar las malas prácticas de operación del equipo y la programación.
- Programación para el uso de las copias de seguridad de los programas, datos o archivos.
- Procedimientos de entrega para las aplicaciones nuevas.
- Etapas al establecer aplicaciones nuevas.

Estos requisitos también se aplican en la captura de datos cuando ésta forma parte de la función de operación. En general, los estándares son menos complejos, aunque la situación cambia debido a la existencia de la entrada de datos remota y en línea.

BIBLIOTECA DE RUTINAS ESTANDAR PARA USO EN DIVERSOS PROGRAMAS.

Control de biblioteca de archivos.

Se realizará un análisis de la biblioteca de archivos porque éstos, en su forma magnética, forman una parte importantísima de los registros contables de una empresa y resultan esenciales para la continuidad y eficacia de las operaciones mecanizadas. Los auditores verificarán que:

- Se han implantado estándares adecuados, instrucciones y manuales para la operación de la biblioteca y según las exigencias de cada sistema.
- Los procedimientos preven un almacenamiento seguro, una manipulación adecuada y el uso autorizado de los archivos y registros que se mantengan en la biblioteca.
- Los procedimientos se llevan a la práctica.
- Un mando de nivel adecuado autoriza la salida de los archivos.
- Se mantiene un registro completo y oportuno de los movimientos de los archivos y de las actividades de la biblioteca.
- El control sobre la biblioteca se puede ejercer independientemente.
- Se mantiene una seguridad adecuada de los archivos y existen medidas a largo plazo de proteccion, según indiquen los estándares.
- Los archivos se almacenan en lugares adecuados y en las condiciones óptimas para que no corran el riesgo de producir errores de lectura cuando se utilicen.

- El movimiento de los archivos de un centro a otro está protegido, para evitar que se corrompan los datos que contienen.

- Los cambios de turno del personal de operación del ordenador no afectan las medidas de seguridad. Cuando la biblioteca no está abierta, los trabajos de los operadores pueden reducir problemas, debiéndose tomar las medidas oportunas para resolver esta situación, incluso previniendo el empleo de archivos duplicados, por si los originales no pudieran leerse.

- El inventario de archivos es correcto y controlado.

- Comprobar que los registros de los archivos y la utilización de estos últimos se mantienen adecuadamente y de forma actualizada.

- Comprobar la autorización de salida de los archivos.

- Comprobar que se puede explicar el inventario de archivos magnéticos y verificar algunas partidas.

- Averiguar los cambios que se hayan hecho en el sistema de control de la utilización de archivos, que pueden ser formales o informales.

- Comprobar la rotación de archivos hacia el almacén de reserva y averiguar si las condiciones de almacenamiento son adecuadas y proporcionan la seguridad necesaria.

- Examinar la posibilidad de que los archivos se utilicen para fines no autorizados.

- Examinar la calidad de los archivos revisando los informes operativos; asegurarse de que se mantienen los estándares apropiados y que se hace limpieza cuando se considera necesario.

- Verificar el impacto que produce sobre el control de archivos el hecho de que la biblioteca no esté operativa cuando lo esté la sala del equipo de cómputo; examinar cuidadosamente el impacto que producen las disposiciones que se tomen para preveer la posibilidad de que no puedan leerse los archivos y tengan que regenerarse.

- Examinar los métodos de tratamiento y almacenaje de archivos.

- Inspeccionar el funcionamiento de la biblioteca de archivos y sus relaciones con la sección de operación.

- Evaluar el impacto de los cambios y los recubrimientos.

Biblioteca de documentación.

Al estudiar la biblioteca de documentación, el auditor deberá verificar que:

- Existe al menos un lugar definido como centro autorizado de documentación.

- Existen estándares que controlan el funcionamiento de tales bibliotecas de documentación.

- Se responsabiliza a las personas que produzcan especificaciones o modificaciones de software o de sistemas, para que depositen copias en la biblioteca.

- Se designa a alguien para que se encargue especificamente de la biblioteca y mantenga los registros, la seguridad de los documentos, actualice las copias y autorice la salida de la documentacion cuando se necesite.

- La seguridad y el control de la documentacion son adecuados.

- Las personas a las que se asigna la biblioteca son conscientes de su contenido, situación y existencia.

DESCRIPCION DE PUESTOS PARA CENTROS DE COMPUTO.

Los siguientes cuadros muestran ejemplos de los diferentes puestos en la organización; enunciando su objetivo del puesto asi como sus principales funciones.

Puesto y Objetivo	Funciones
Jefe de Departamento de Operación. Asegurar que el equipo de cómputo opere en óptimas condiciones.	Coordina a los operadores. Observa y controla el comportamiento del equipo de cómputo. Detecta fallas o paros anormales del Hardware o Software. Selecciona, capacita y actualiza al personal del departamento. Coordina y vigila los mantenimientos preventivos o correctivos. Garantiza la seguridad de la información asi como las normas de seguridad de la instalación.
Operador de equipo de cómputo. Vigila y agiliza el flujo de procesos. Reporta las fallas y administra los recursos eficientemente	Opera y controla el equipo de cómputo de acuerdo con las instrucciones Activa los procesos de usuarios. Prepara el equipo periférico para su funcionamiento. Asigna dispositivos periféricos a los procesos de operación. Verifica que el funcionamiento de los equipos se correcto, reportando las fallas si éstas existen. Supervisa la limpieza de equipos y lleva las bitácoras.

Existen otros puestos tales como jefe de operadores de equipo de cómputo, jefe de cintotecarios, jefe de capturistas, jefe del departamento de desarrollo de sistemas, programadores y programadores del sistema.

Puesto y Objetivo	Funciones
Captunsta. Grabar y verificar la información de documentos fuente a media magnética	Extrae del documento fuente la información a grabar en cinta o disco. Verifica y corrige la grabación de datos del documento fuente. Reporta las fallas que presente la terminal de captura. Elabora el informe de documentos grabados y verificados.
Cintotecario Identificar, registrar y almacenar cintas, discos cartuchos y otros medios magnéticos	Lleva el registro y control de las cintas y dispositivos magnéticos en la cintoteca así como su uso. Responsable de enviar copias de respaldo a lugares alternos reportando las cintas dañadas o con errores. Re-etiqueta las cintas y las ordena en los estantes asignados dentro de la cintoteca.

Otra área importante es el mantenimiento del sistema y el soporte técnico que implica otros puestos.

DESCRIPCION DE CINTOTECA.

Las características de su construcción, materiales a utilizar y aspectos técnicos de iluminación, condiciones ambientales y seguridad son:

- No deberá tener alfombra.
- Pisos de loseta vinílica que resista y permita la fácil limpieza de la Cintoteca.
- Los techos y muros se protegerán con pintura lavable (antipolvo).

- No deberá existir falso plafón.
- Altura libre entre suelo y techo apropiada.
- La iluminación será similar a la de un almacén. Con una acometida diferente a la del equipo de cómputo.

CAPTURA DE DATOS.

El hecho de introducir datos a una computadora consta de tres pasos:

a). Captura de datos.

b). Preparación de los datos.

c). Introducción de datos.

Captura de datos. Es el proceso de identificar y registrar eventos reales relevantes para las operaciones de una compañía. Preparación de datos. Es el proceso de convertir los datos capturados en forma leible para la máquina. Y La Introducción de datos es el proceso de leer los datos en la computadora.

Una vez que los datos están en forma leible para la máquina, los controles de hardware y software se aseguran que los datos son convertidos correctamente a código interno de la máquina. Por lo tanto, los controles de introducción de datos raramente le conciernen al auditor puesto que están basados en código máquina. Sin embargo, los controles de captura y preparación de datos son especialmente importantes por dos razones. La primera, la captura y la preparación de datos requieren cierta rutina, en ocasiones monótona, intervención humana y está propenso a error. Segundo, estos procesos son blancos perfectos para fraude.

La tabla siguiente presenta una variedad de maneras en los cuales los datos pueden ser capturados, preparados e introducidos en la computadora.

Metodo de Captura	Metodo y dispositivo para la preparacion de los datos	Metodo y dispositivo para la entrada de datos
Documentos	Tecleado	
	Cinta magnetica	Unidad de cinta magnetica
	Disco magnetico	Unidad de disco magnetico
	Cassette y diskette	
	Por producto	
	Cinta periodica	Reconocimiento de caracter
	Cinta magnetica	optico
	Cassette	Unidad de cinta magnetica
	Codificada	Reconocimiento de patrones
	Escrita a maquina	
	Pre-impresa	MICR, OCR y sensado de
	Escrita a mano	marca optica
	Fotografia	Lectora de microfilmaciones
	Tecleada	Terminales
Entrada Directa	Tecleada	Terminales
		Terminales de teclado
		Unidades de despliegue visual (VDU's) Proposito esp.
	Voz	Unidades de reconocimiento de voz
Hibrido	Mediciones Fisicas	Dispos. de control de procesos
	Codificada	Terminales Punto de Venta (POS)
		Cajeros Automaticos

Existen tres métodos para la captura de datos:

a) Basado en Documentos.

b) Entrada directa.

c) Método híbrido.

La captura de datos basada en documentos está compuesto por el registro de eventos en papel o en algún medio relacionado

como pueden ser hojas de lectura óptica o tarjetas. La captura de datos de entrada directa está compuesta del registro inmediato de un evento como una señal digital. El intervalo de tiempo entre la identificación de un evento y su registro es muy pequeño; la transcripción de un evento a un documento no es un paso intermedio. Los métodos híbridos son algunas combinaciones de captura de datos basada en documento y en entrada directa.

La Preparación de Datos ocurre de diferentes maneras y en una variedad de tiempos. En el caso usual esto toma lugar despues de la captura de datos. Los datos son capturados en un documento fuente, simplemente tecleada en una terminal en línea, y luego leida por un dispositivo de entrada, o transmitida a la computadora. En algunas ocasiones la preparación de datos ocurre antes de la captura de datos.

En la captura de datos esto puede ser posible introduciéndolos inmediatamente a la computadora, o algunos datos de preparación adicionales quizás necesarios. Si un método híbrido de captura de datos es usado, la preparación de datos ocurre antes y después de la captura de datos.

Los dispositivos de Datos de Entrada pueden estar fuera de línea o en línea de la computadora. Una lectora de tarjetas, lectora óptica, o terminal pueden permitir la entrada directa en la unidad central de procesamiento. De manera alterna, una lectora óptica puede escribir datos a una cinta magnética para procesos lentos, o una terminal quizá almacene datos temporalmente en un disco.

EVALUACION DE LOS METODOS DE CAPTURA

Históricamente, la captura de datos basada en documentos ha sido la mayor forma de captura de datos porque la preparación y captura de datos y los dispositivos necesarios para soportar la entrada directa y los métodos híbridos de captura de datos han sido altamente costosos. Recientemente, la tecnología que soporta la entrada directa y los métodos híbridos de la captura de datos han avanzado rápidamente y están siendo usados más en la actualidad.

Captura de Datos Basada en Documento.

Los métodos de captura basados en documento tienen dos grandes ventajas: a) Simplicidad, y b) Flexibilidad. Este tipo de captura requiere la preparación de documentos fuente que están pre-impresos, pre-marcados, pre-numerados, etc., y el entrenamiento de personal para preparar estos documentos. No se necesitan preparación de datos y dispositivos de entrada caros en los puntos de captura. La información puede ser recolectada fácilmente cerca de la fuente de información. Los capturistas requieren de bastante entrenamiento para las tareas de captura.

Los métodos de captura basados en documento tienen una gran desventaja: requieren más esfuerzo en la preparación y entrada de la información que en la entrada directa y los métodos híbridos. Frecuentemente, éste método representa gran intervención humana en la preparación y entrada de información, haciendo estos métodos mas costosos y propensos a error.

Captura de datos de entrada directa.

La captura de entrada directa reduce la intervención de recursos humanos en todo el proceso de captura, con lo cual se reducen los costos por mano de obra y la probabilidad de error del operador. Comparado con la captura basada en documento los costos de entrenamiento son más altos; sin embargo, la diferencia puede ser mínima. El equipo (hardware) y los programas (software) para soportar esta captura han sido diseñados para facilitar su uso.

La mayor desventaja de la captura de entrada directa es el costo de equipo y programas necesarios para soportar su uso. Si existe un gran número de puntos donde se captura, puede ser más costoso proveer facilidades de captura a todos estos puntos. Si los puntos de captura de datos estan físicamente dispersos, hardware y software de comunicaciones puede ser necesario.

Métodos Híbridos de Captura.

Este tipo de captura tiene algunas ventajas de los dos métodos anteriores. A través de la preimpresión, premarcación o

preperforación de la información constante en una hoja especial y la lectura directa de ésta información (usando una lectora óptica), la intervención de recursos humanos en el proceso de captura es reducida. Por lo tanto, los costos de mano de obra y el riesgo de errores que se pudieran presentar durante la entrada de información son reducidos. La información variante puede ser capturada directamente por terminal (tecleado).

La mayor desventaja de la captura híbrida son los costos para soportar el hardware y software necesarios. Sin embargo, la tecnología en técnicas de captura directa está avanzando rápidamente, y los ahorros en los costos de mano de obra pueden dejar atrás pronto los costos extras de hardware y software.

EVALUACION DE LOS METODOS DE PREPARACION DE DATOS

Una discusión de las ventajas y desventajas relativas a los diferentes métodos de preparación y entrada de datos sería muy extensa, puesto que estan muy relacionadas entre sí. A continuación se presenta una descripción aproximada.

Métodos de Perforación y Teclado (KEYPUNCH)

Los métodos de preparación de información basado en teclado son todavía los métodos dominantes. Sin embargo, hubo cambios de la utilizacion de tarjetas como medio de almacenamiento a lo que ahora conocemos como medio magnético como son las cintas y discos.

Cinta magnética. Los dispositivos teclado-a-cinta (key-to-tape) permiten que los datos fuente sean tecleados directamente a la cinta magnética la cual puede ser leida por una computadora. Existen ambos dispositivos; el independiente (stand-alone) y los agrupados (clustered). Un dispositivo independiente tiene su propia unidad de grabación de cinta, Un dispositivo clustered tiene varios teclados conectados a un multiplexor que lee alternamente de cada teclado. Los dispositivos agrupados son de precio más bajo que los stand-alone, pero antes de que puedan ser justificados requieren aplicaciones donde grandes cantidades del mismo tipo de datos estén siendo tecleados.

Puesto que los dispositivos teclado-a-cinta tienen buffer, ofrecen todas las ventajas más usuales: fácil y rápida corrección de posibles errores, salto automático de columnas, llenado de ceros o blancos, justificación a la izquierda o derecha en la entrada de datos en ciertos campos. Cuando un dispositivo envía los datos del buffer a la cinta, ejecuta un chequeo para asegurarse que el buffer fue escrito correctamente; por ejemplo, una prueba de paridad y una prueba de lectura despues de la escritura. La verificación de estos puntos simplemente requiere cambiar el dispositivo a modo de verificación. La correción de errores sucede escribiendo sobre los datos erróneos.

Hay pocas desventajas al utilizar los equipos teclado-a-cinta aunque están siendo supersedidos por los equipos teclado-a-disco. Algunos operadores se resisten todavía al cambio de tecnología y aunque existe un poco de incompatibilidad, ya está desapareciendo.

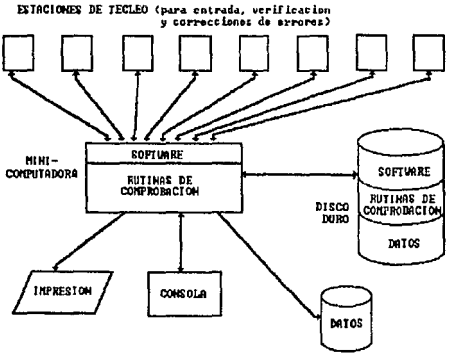


Figura 2.6

Disco magnético. Una extensión natural de los dispositivos teclado-a-cinta son los dispositivos teclado-a-disco. Sus características son: a) múltiples estaciones con teclado atadas a un solo procesador, b) capacidades de validación y edición ejecutadas por el procesador, c) un supervisor de la estación de control, y d) una unidad de cinta magnética para la salida de los datos.

Si las facilidades de comunicación son conectadas al sistema teclado-a-disco, el efecto es que el sistema constituye una terminal que puede ser colocada en alguna localidad remota. Los datos pueden ser capturados e introducidos cerca de la fuente de información, de manera que, periódicamente, se pueda identificar y corregir rápidamente los errores hechos.

La mayor desventaja del equipo teclado-a-disco esta relacionado a la consecuencia de las fallas del dispositivo. No solo una sino varias estaciones de teclado se vuelven inoperables. Los datos que ya han sido teclados pueden ser perdidos. Los sistemas teclado-a-disco también son costosos. Sin embargo, el costo va decreciendo; estos sistemas son ahora un fuerte competidor con los sistemas teclado-a-cinta.

Método de reconocimiento de patrones.

Los dispositivos de reconocimiento de patrones leen y evaluan los caracteres o marcas de un documento basándose en la presencia o ausencia de un flujo magnético o un patrón de luz formado. Estos dispositivos generalmente son más caros que los equipos con teclado. Sin embargo, eliminan una parte sustancial de la preparación de datos pudiendo leer los datos directamente del documento fuente. Estos pueden ser en línea (online) hacia la computadora o fuera de línea (offline) produciendo una cinta magnética para ser leída posteriormente.

- Reconocimiento de Caracteres de tinta magnética (MICR).

Este tipo de lectura surgió del uso extensivo por la industria bancaria para procesar los cheques. MICR requiere que los caracteres a ser codificados en un documento usen un tipo de

letra especial y una tinta magnética especial. La lectura toma lugar cuando el dispositivo sensa la presencia o ausencia de tinta magnética en una matríz de caracteres.

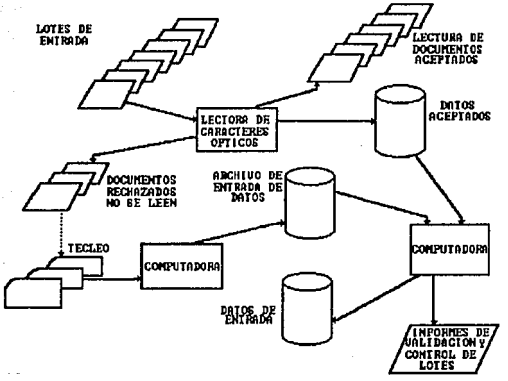


Figura 2.7

- Reconocimiento de caracter óptico (OCR).

La captura de datos usando un OCR puede ser preparada de diferentes maneras: Tecleada con máquina de escribir, impresa con offset, impresa por computadora, escrita a mano. Se pueden aceptar múltiples tipos de letras. Sin embargo, en general, el dispositivo OCR menos caro, es el que menos tipos de letras puede leer. Los caracteres escritos a mano deben seguir cierto estilo.

- Sensado de marcas ópticas.

Los dispositivos de sensado de marcas ópticas leen marcas en lugar de caracteres alfanuméricos. Como con un equipo OCR, las marcas pueden ser pre-impresas, tecleadas con máquina de escribir, escritas a mano, o producidas por computadora. La posición de las marcas en un documento o tarjeta indican su valor alfabético o numérico.

Terminales.

Existen dos tipos de terminales: teclado y VDU unidades de despliegue visual. Las terminales de teclado proveen únicamente una salida impresa. Los VDU's proveen una salida visual en una pantalla. Además, tienen algunas otras características y opciones; capacidades de desplegar páginas, puertos para impresoras, plumas de luz, etc.

La terminal de teclado fue el primer gran paso hacia el uso en línea de la computadora. Provee algunas ventajas. La primera, permite que los datos capturados esten inmediatamente disponibles para su procesamiento. Segundo, reduce el esfuerzo que envuelve la captura, la preparación y la entrada de datos. Como tercer ventaja es que se reduce la probabilidad de error.

Los VDU's tienen algunas características además de las que tienen las terminales de teclado. La ausencia de movimiento mecánico con un VDU resulta más rápido para teclear la información. El despliegue visual permite más ventajas al capturista.

Cuando, además de VDU's, tienen capacidades de validar información a través de un microprocesador o como minicomputadoras, se les denomina terminales inteligentes.

Terminales Puntos de Venta.

La productividad y la integridad de información en los supermercados o almacenes han sido considerablemente realzados por los dispositivos de entrada llamados puntos de venta. En el caso

de los supermercados la tecnología que permite estos avances es la fijada por las lectoras láser de revisión y pago capaces de leer códigos premarcados en un artículo de venta. En el caso de los almacenes es una lectora manual. Esta lectora lee tanto códigos ópticos como sellos magnéticamente codificados.

La naturaleza de operación de los supermercados y los almacenes es diferente. El vendedor en un supermercado pasa la mayor parte del tiempo en un punto de venta, mientras que el de una tienda menor se pasa el tiempo vendiendo en lugar de revisar y cobrar los artículos.

Comparado con las cajas registradoras, las mayores ventajas de usar los puntos de venta en los supermercados son:

1. Lectura óptica de un código premarcado, por ejemplo, el código universal del producto (UPC).

2. Crece la exactitud en el precio de los artículos puesto que una minicomputadora toma los precios de un archivo de precios basado en el código único del artículo.

3. Reduce el que se marque el precio sobre el artículo y sobre el cambio de los precios; el precio solo necesita ser marcado en la computadora y no en el artículo mismo.

Existen muchas otras ventajas al utilizar este medio de captura.

Los dispositivos de punto de venta presentan problemas cuando falla el hardware. Las terminales están conectadas, normalmente, a un controlador de la tienda que, por turno, está conectada a una computadora huesped (host computer). Si la falla ocurre la terminal generalmente puede actuar como un caja registradora independiente.

Además existen otros tipos de dispositivos de entrada como lectoras de microfilmaciones, unidades de reconocimiento de voz, dispositivos de control de procesos. Dispositivos de tonotoque, cajeros automáticos.

ELEMENTOS PARA LA ELABORACION DEL PRESUPUESTO DEL EQUIPO DE COMPUTO.

Definir las especificaciones mínimas para el equipo de cómputo que requiere el centro de cómputo conforme a las necesidades de recursos, que para los procesos, demandan las dependencias del Centro. Para tal efecto se puede dividir en cuatro partes: Hardware, Características de CPU, Equipo de comunicaciones, y Software.

Hardware.

Debe existir total compatibilidad en el equipo de cómputo que exista dentro del Centro de Cómputo.

Posibilidad de crecimiento del equipo en campo en al menos dos veces la capacidad existente, sin que exista degradación en el "performance" del mismo. El crecimiento del equipo deberá ser modular. Especificar que se requerirá para duplicar el poder de cómputo adicional (adicionar unidades de disco y cinta, controladores, unidad central de proceso, procesadores de comunicaciones, etc.), así como el costo correspondiente y el costo del mantenimiento mensual de cada dispositivo.

Interconexión con el equipo del centro de Cómputo.

Capacidad mínima del orden de MB en disco en línea en no menos de las unidades requeridas, con tiempo medio de acceso máximo del orden de ms.

Impresora(s) de un número mínimo de líneas por minuto de 132 columnas, con juego de caracteres de código ASCII, con las necesidades que se requieran.

Unidades de Cinta de determinado número de tracks, bpi, pulg/seg de velocidad, y KB/seg de transferencia.

Memoria suficiente para soportar concurrentemente determinados trabajos en proceso de lote cuyo tamaño promedio sea del orden de Kbytes cada uno, hasta n número de terminales (o combinación de micros y éstas) en modo interactivo y/o transac-

cional, con un promedio de n tareas simultáneas y un manejador de Base de Datos.

En el precio total de los equipos propuestos deberá especificarse el costo del mantenimiento mensual de cada dispositivo; así como, una tabla que indique los costos de diferentes opciones de mantenimiento mensual normal y sus posibles extensiones.

En caso de contratar mantenimientos limitado a un turno cinco días a la semana, indicar el costo adicional por hora-hombre de servicio.

Dado el tamaño del equipo se deberá contar con personal de Ingeniería de Servicio del proveedor en la instalación del cliente, durante el tiempo del mantenimiento contratado.

Indicar el stock mínimo de partes y refacciones que el proveedor tendría en la Sala de Cómputo del cliente.

El proveedor deberá especificar los requerimientos de la instalación física, eléctrica y del medio ambiente; así como, el consumo de potencia en KW, o KVA y la disipación de calor en BTU/HR. De cada uno de los equipos y periféricos propuestos.

Indicar el costo total de la instalación de los equipo propuestos y que conceptos incluye.

Especificar calendario de entrega de los equipos propuestos y tiempo de instalación.

Indicar los costos y condiciones en un contrato de renta con opción a comprar; así como si existe un límite de tiempo para el uso del equipo y el cargo adicional por exceder dicho tiempo.

Indicar las facilidades que proporcionaría el proveedor para la capacitación de personal del Centro en el mantenimiento al Hardware que sea contratado; así como, las facilidades para la adquisición de partes y refacciones que requiera el Centro.

Indicar las posibilidades de que el proveedor proporcione los manuales del hardware, para que en un futuro, personal del Centro pueda dar el mantenimiento al equipo contratado.

Indicar cual sería, para dos años, el costo de un stock mínimo de partes y refacciones que requerirá el equipo propuesto.

Los equipos propuestos deberán ser de un modelo que actualmente se está fabricando y el proveedor deberá garantizar, por escrito, su permanencia en el mercado; así como, que los equipos no serán descontinuados en un período de cuatro años a partir de la fecha de la propuesta presentada; en caso de que alguno de los modelos propuestos sea descontinuado por el fabricante, el proveedor debe comprometerse a sustituirlo por un modelo reciente, no descontinuado, de capacidad superior al modelo descontinuado, sin ningún tipo de cargo para el Centro de Cómputo, en un plazo no mayor a seis meses a partir de la fecha en que el fabricante anuncie que ha quedado descontinuado dicho modelo.

Características de CPU.

- Procesador.
- Bytes de Memoria
- Controlador de Discos.
- Controlador de Cintas.
- Tamaño mínimo de palabra de n bits.
- Juego de instrucciones científicas y comerciales.
- Instrucciones de punto flotante implementadas por Hardware.

Sistema Operativo.

El Sistema Operativo debe contemplar las siguientes características:

- Proceso en Batch.
- Proceso en Tiempo real.
- Procesos Interactivos.
- Compilador único para Batch y Procesos Interactivos.
- Compiladores reentrantes.
- Spooling.
- Contabilidad de Usuarios.
- Número máximo de terminales.
- Memoria Virtual.
- Tareas reentrantes.
- Comunicación entre programas.
- Mezcla de programas objeto.
- Manejo de prioridades.
- Debugging.
- Paginación.

- Segmentación.
- Multiprogramación.
- Posibilidad de Multiproceso.

Equipo de comunicaciones para soportar los enlaces.

Conexión local y remota hasta para n terminales (o combinación de micros y estas) síncronas/asíncronas dispersas; con posibilidad para conexión simultánea.

Enlace para comunicarse con el equipo de cómputo del centro, para transferencia de archivos y procesos.

Posibilidad de conexión a canal de alta velocidad para que desde las terminales se puedan accesar otros procesadores de la institución conectados a dicho canal.

Posibilidad de atender a usuarios vía líneas conmutadas.

Cantidad para soportar un mínimo de n líneas síncronas/asíncronas, para poder conectar hasta n terminales (o combinaciones de micros y éstas).

Software.

Indicar el Software que se incluye en el precio del equipo propuesto.

Indicar el Software que soporta el equipo propuesto; así como, los costos de venta o renta y mantenimiento mensual y que incluye.

P.e.

- Compilador COBOL ANSI'74.

- Compilador FORTRAN ANSI'85.
- Compilador FORTRAN IV.
- Compilador ALGOL.
- Compilador PASCAL.
- Compilador BASIC.
- Compilador C.
- Compilador o Intérprete LISP
- Compilador PL/1.
- Compilador APL.
- Procesador de Palabras.
- Editor de Pantalla.
- Sort.
- Merge.
- Hoja de Cálculo.
- Manejador de Base de Datos compatibles con el equipo.
- Ambiente de multiprogramación.
- Soporte de multiambiente.

- Interactivo.

- Poceso en lotes.

- Transacciones.

El software debe soportar código reentrante en programas producto y programas del usuario, también deberá permitir la definición de un archivo en disco de n MB y grabación de n archivos en disco de n MB y grabación de cintas con especificaciones ANSI.

Software de comunicaciones para soportar los requerimientos de Hardware.

Mismo Sistema Operativo en el Centro.

Compatibilidad de archivos generados por diferentes archivos.
Indicar las condiciones especiales para el uso del Software, en caso de instalarse en varios equipos.

Indicar la capacidad que en memoria principal y en disco requiere el software básico.

Indicar si existe la posibilidad de accesar desde los lenguajes de programación al Manejador de Base de Datos propuestos.

Indicar que lenguajes de IV Generación soporta el equipo propuesto, y para cada uno de estos lenguajes lo siguiente:

- Requerimientos de Hardware.

- Requerimientos de Software.

- Caracterfsticas.

- Un estudio de como se comporta el equipo propuesto, suponiendo que trabajen cinco usuarios concurrente-

mente con archivos de registros del orden de los miles de n bytes.

- Número de usuarios concurrentes que soporta y bajo que condiciones.

- Costos inherentes.

- Si es o no soportado por el proveedor del equipo de cómputo.

- Relación de cursos que se ofrecen y sus costos, incluyendo manuales para los asistentes.

Indicar si existe dentro del Software que soporte el equipo propuesto, un Diccionario de Datos para el ambiente de Desarrollo de aplicaciones; así como, la capacidad de Hardware requerida.

Indicar si dentro del Software que soporta el equipo propuesto existe un Manejador de terminales que permita el diseño de pantallas para captura de información y se puedan llamar éstas desde los lenguajes de programación que soporta el equipo; así como, el costo correspondiente.

CAPITULO 3

COMPONENTES DEL CENTRO DE COMPUTO.

SALA DE COMPUTO Y SU UBICACION.

Antes de realizar la obra civil de la Sala de Cómputo, se debe elegir la planta de ubicación de la misma atendiendo las condiciones mínimas siguientes:

1). Que el acceso para máquinas sea amplio.

2). Que no se crucen los conductos de agua horizontales con los verticales, excepto las del aire acondicionado que se especifiquen.

3). Que el suministro de energía eléctrica sea el adecuado. Comprobar si el centro de transformación de esta energía eléctrica es propio del edificio.

4). Que no existan interferencias electromagnéticas. Esto podría producir alteraciones y vibraciones en pantallas y máquinas, incluso acoplamientos.

5). Que el suelo real presente la suficiente resistencia.

6). Según las máquinas a instalar, será además aconsejable observar:

- Situación de pilares.
- Situación de puertas.
- Pasillos de seguridad.
- Previsión de espacios en futuras ampliaciones.

Una vez llevada a cabo la elección de la planta del edificio más indicada y ya destinada, por tanto, al equipo de cómputo, puede encontrarse ésta dividida en varias zonas:

- Sala de Cómputo (propiamente dicha).
- Sala de impresoras.
- Espacio para archivo o cintoteca.

Tanto el espacio destinado para las impresoras como el reservado para la cintoteca se pueden encontrar dentro o fuera de la misma sala de cómputo.

Como norma general, parece más lógico que ambas se encuentren en la sala, pues disfrutarían de las instalaciones propias de ésta y no habría que duplicar el gasto, siendo éste más reducido. En determinados casos, hay que situarlas en locales anexos por la falta de espacio.

Es importante tener en cuenta el suministro de energía eléctrica debido a que uno de los factores más esenciales para el buen funcionamiento de las computadoras es el suministro correcto de ésta. Dicha energía presenta unas exigencias tales, que es comparable con la mayoría de los casos con la que se obtendría en un laboratorio, debido a que la energía empleada para estos fines debe presentar ausencia de variaciones.

Ubicación.

La sala de Cómputo debe estar ubicada en un área que dé máxima seguridad de protección a la exposición de riesgos tales como incendios, inundación, terremoto, vibraciones, suciedad y húmedad excesivas.

Selección del local.

Deben analizarse los siguientes aspectos:

- Acceso de máquinas.
- Disponibilidad y requerimientos de la fuerza eléctrica adecuada.
- Espacio para el equipo de Aire Acondicionado.
- Ubicación del compresor.
- Sistema impulsor de aire.
- Intercambiador de calor.
- Altura del techo, área de paredes exteriores y área de ventanas de cristal.
- Capacidad de carga de piso (loza o piso firme).
- Normas de seguridad.
- Peligro de inundación.
- Protección contra incendios.

- Facilidad de comunicación interior y exterior con los restantes servicios.

Necesidades de espacio.

- Componentes específicos deseados.
- Relación largo-ancho del local.
- Situación de las columnas.
- Previsión para futuras ampliaciones.
- Espacio para archivar, en la sala del equipo de cómputo, cintas y discos del día.
- Espacio para estanterías, mesas, etc.
- Considerar la integración del área de trabajo del equipo de cómputo con otras áreas.

Acceso.

Es recomendable que al planificar una Sala de Cómputo se tomen en consideración la entrada y salida de máquinas (entrega inicial, entrega de ampliaciones, cambios de máquinas, mudanzas, etc.).

La zona de descarga de los equipos así como accesos y pasillos que conduzcan a la Sala de Cómputo, deben ser capaces de soportar la carga de los equipos a ser instalados. Ventanas, puertas y/o corredores a ser utilizados entre la zona de descarga y la sala deben estar dimensionados para acomodar equipo embalado, más el espacio para herramientas de transportación.

Las mismas consideraciones de espacio y peso deben ser usadas para ascensores, rampas y umbrales que pudieran ser usados como acceso a la Sala de Cómputo.

Dimensiones.

Las dimensiones mínimas de la sala están determinadas por la cantidad de componentes del sistema, el espacio mínimo requerido por cada unidad para su mantenimiento, área de operación, etc. El "layout" del sistema y las expansiones futuras deben también ser consideradas al planificar el tamaño de la sala. Paredes y paneles removibles pueden ser usados para facilitar ampliaciones futuras.

La sala estará dividida de acuerdo al número de áreas, que se requieran, separadas éstas por cancelería de aluminio y cristal.

En adición a la Sala de Cómputo se debe preveer espacio para lo siguiente:

a). Almacenamiento de cintas y/o discos magnéticos.

Estos elementos deben ser archivados en un área protegida, localizada cercan o adyacente a la Sala de Cómputo. Una bóveda a prueba de fuego puede ser usada para salvaguardar los archivos maestros.

El área de almacenamiento deberá tener las mismas condiciones de temperatura y humedad relativa de la Sala de Cómputo.

b). Suministros, formularios y papel para impresoras.

El área de impresoras deberá estar completamente cerrada, para evitar contaminación por polvo del papel al resto de la sala, además deberá contar con un pequeño mostrador para la salida de listados con ventanas de tipo "guillotina". Así mismo se requiere que el cancel cuente con persiana de vidrio en la parte superior que permitan controlar el flujo de aire en caso necesario.

c). Mesas de trabajo y muebles.

El Espacio para mesas de trabajo y/o escritorios en el área de computo debe ser previsto de acuerdo a las necesidades. También debe planearse espacio para cestos de papel, uno de los cuales debe colocarse cerca de la impresora.

d). Area y mobiliario para mantenimiento.

- Trafico. Se debe contemplar espacio para el tráfico normal desde la Sala de Cómputo hacia la cintoteca, y viceversa.

- Iluminación. La iluminación debe ser igual en toda el área del equipo y suficiente para la comodidad del persónal en la Sala de Cómputo.

- Acustica. Ciertos tratamientos acústicos de la Sala de Cómputo son deseables para absorber ruidos de máquinas.

- Restricciones. Comer, beber y fumar deben ser prohibidas en la Sala de Cómputo.

Piso falso.

- Debe permitir cambios en la ubicación de unidades.

- Debe cubrir los cables de comunicaciones entre la unidad central de procesos y de los dispositivos periféricos, cajas de conexiones y cables de alimentación eléctrica.

- Deberá proporcionar seguridad al personal.

- Debe permitir que el espacio entre los dos suelos actúe como una cámara plena de aire. Que facilite el reparto de las cargas.

3-6 Componentes del Centro de Cómputo.

- La altura recomendable derá de 30 cms. si el área de la sala de cómputo es de 100 m. cuadrados o menos, y de 40 cms. si es mayor de 100 m. cuadrados. La altura mínima podrá ser de 18 cms. si la sala es pequeña. Todo lo anterior es con el objeto de que el aire acondicionado puede fluir adecuadamente en la cámara plena.

- Puede ser de acero, aluminio o madera resistente al fuego.

- El mejor piso es el que esta soportado por pedestales o gatos mecánicos.

- Tener en cuenta la frecuencia con que se moverán los equipos.

- Cuando se utilice como cámara plena para el aire acondiconado tendrá que cubrirse el piso firme con pintura antipolvo.

Tratamiento de paredes.

El acabado de las paredes requiere una especial atención desde su primera fase, que sería el tendido del yeso, y una segunda, que es la pintura como posible terminación.

Primera fase: Tendido de Yeso.

La atención plástica que requiere éste yeso sería la unión con otros materiales, tales como la perlita.

Segunda fase: Pintura.

La pintura plástica sería la solución idónea junto con papeles vinílicos para este tipo de terminación. La pintura que sea utilice no será reflectante y, como siempre, no desprenderá polvo.

Tratamiento del techo.

Los techos falsos deberán ser lo suficientemente versátiles, de manera que cualquier inspección realizada no encuentre algún deterioro de sus acabados al ser manejado por manos poco cuidadosas de su integridad.

Además del polvo y la combustibilidad ,para su elección, hay que tener en cuenta la absorción acústica, muy importante para la transmisión de ruidos hacia las plantas contiguas.

Lo que fundamentalmente debe cumplir un techo falso en una Sala de Cómputo es:

1). Ausencia del polvo.

2). No combustible.

3). Absorción acústica.

INSTALACIONES DE AIRE ACONDICIONADO.

Climatización ambiental.

El Aire Acondicionado, juzgado como algo indiscutible por muchas razones hace apenas unos cuantos años, es un estándar obligatorio para la oficina de hoy en día.

El aire acondicionado debe de proporcionar un aire limpio, ventilación adecuada, control de la temperatura y una humedad relativa, además de eliminar corrientes por medio de los sistemas apropiados de aprovisionamiento y disposición. Dotar de aire acondicionado a un Centro de Cómputo sirve también, para eliminar el polvo y ruido exteriores, ya que las ventanas tienen que mantenerse cerradas todo el tiempo.

Capacidad del equipo de aire acondicionado.

Se tendrá en cuenta:

- Disipación térmica de las máquinas.
- Disipación térmica de las personas.
- Cargas latentes, aire de renovación.
- Pérdidas por puertas y ventanas.
- Transmisión de paredes, techos y suelos.
- Disipación de otros aparatos.
- Las cargas calorífica del equipo de cómputo y sus periféricos las proporcionará el proveedor, por lo común deben especificarse en BTU/hora o en Kcal/hora.
- El proveedor del equipo de cómputo, también proporcionará la cantidad de aire que requieren los ventiladores de los diferentes dispositivos de cómputo, por lo regular en pies cúbicos por hora o en metros cúbicos/hora.
- El calor disipado por los diferentes dispositivos de cómputo, obliga a necesitar aire frío todo el año.

Distribución del aire en la sala.

- Los componentes de las máquinas se refrigeran normalmente, mediante la circulación de aire por ventiladores.
- La entrada de aire se efectúa por debajo de las máquinas a través de rejillas.
- El aire caliente es expulsado por la parte superior de las máquinas.

3-9 Componentes del Centro de Cómputo.

- Debe considerarse con cuidado el sistema de distribución para eliminar áreas con excesiva velocidad de aire.

- El aire de renovación o ventilación vendrá en función del volúmen de la sala. Se proyectará para obtener de 1.5 a 2 renovaciones por hora y para crear una sobrepresión que evitará la entrada de polvo y suciedad por las puertas, procedentes de las zonas adyacentes.

- En las zonas contaminadas el aire de renovación se descontaminará previamente.

Distribución por techo.

Por medio de este sistema:

- Se impulsa el aire frío por el techo.

- Se retorna también por el techo a través de rejillas colocadas encima de las salidas de aire caliente.

- Se tratan menores volumenes de aire.

- Tiene poca flexibilidad para cambio de posición de unidades.

- Debe estudiarse para no crear corrientes de aire frío.

Distribución por piso falso.

De acuerdo con éste otro sistema.

- El espacio entre el suelo del edificio y el piso falso se utiliza como cámara plena de aire.

- Todo el aire se descarga en la sala a través de registros en el techo.

- El aire retorna a la unidad acondicionadora por rejillas en el techo.

- Se necesita una cierta cantidad de recalentamiento para controlar la humedad relativa del aire antes de que entre en la sala.

- El sistema debe tener controladores de la temperatura del aire en el piso falso.

- Hay que colocar cuidadosamente las rejillas y los retornos para no crear tiros de aire frío a caliente.

Riesgos que implica el aire acondicionado.

En todas las instalaciones existen grandes problemas con el aire acondicionado; el riesgo que éste implica es doble.

1. El aire acondicionado es indispensable en el lugar donde la computadora trabaje; las fluctuaciones o los desperfectos de consideración pueden ocasionar que la computadora tenga que ser apagada, de otra forma, ésta puede dañarse.

2. Las instalaciones de aire acondicionado son una fuente de incendios muy frecuentes y también son muy susceptibles al ataque físico, especialmente a través de los ductos.

Para poder afrontar estos riesgos se requiere lo siguiente:

- Se deben instalar equipos de aire acondicionado de respaldo donde se hayan establecido las aplicaciones de alto riesgo.

- Se deben instalar redes de protección en todo el sistema de ductos al interior y exterior.

- Se deben instalar extinguidores y detectores de incendios en los ductos.

- Se deben instalar monitores y alarmas de sonidos efectivas.

INSTALACIONES ELECTRICAS PARA LA SALA DE COMPUTO.

Cuadros y sistemas de emergencia.

Se instalará dentro de la Sala de Cómputo un cuadro eléctrico general, lo suficientemente amplio para posibles modificaciones. Deberá poseer distribución de fuerza a posibles máquinas, con acometida trifásica, además de neutro y tierra dotado de un contacto general; diferencial de alarma y pulsadores en serie de corte de corriente de emergencia que actúa sobre el contacto.

Iluminación.

Las última tecnología en la proyección y aprovechamiento de las fuentes de energía están consiguiendo unos rendimientos lumínicos sorprendentes, no sólo en la reflexión y control de todos los haces de luz, sino incluso en el reducido consumo y en el dominio del espectro luminoso para fines concretos, siendo muy importante utilizar los artefactos necesarios para cada función específica.

Equipo de alimentación ininterrumpida (U.P.S).

La razón básica para la instalación de un equipo de alimentación ininterrumpida (UPS) es obtener una alta fidelidad en el suministro de energía a la Sala de Cómputo.

La energía suministrada por las compañías distribuidoras de energía, presenta numerosas fallas al cabo del año.

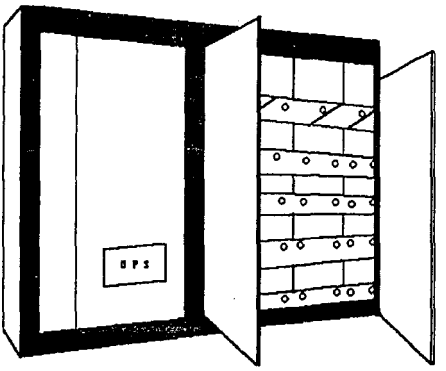


Figura 3.1 Unidad de Alimentación Ininterrumpida.

El grupo de continuidad o sistema de alimentación estática está formado por:

- Rectificador.
- Grupo de Baterías.
- Inversor.
- Bypass electrónico.
- Sistema de sincronismo.
- Controles e indicadores visuales y acústicos.

Responsabilidades del propietario.

Es responsabilidad del propietario del centro de cómputo el proveer e instalar lo siguiente:

a). El o los tableros de distribución eléctrica necesarios y su cableado a la red de suministro eléctrico.

b). Los cables de potencia con código de colores que vayan con blindaje aislado, desde la distribución hasta no más de un metro de cada unidad, terminando en un conector apropiado a la potencia de dicha unidad.

c). La distribución de cargas para equilibrar las fases. El consumo eléctrico por unidad es mostrado en la tabla.

d). Conectar cada unidad del sistema al conector correspondiente y en las máquinas que se suministran sin cable, proveerlo e instalarlo.

e). Los interruptores de emergencia y el cableado asociado.

Apagado de emergencia.

Sería conveniente proveer un medio de desconectar toda la potencia del sistema y apagar los ventiladores del sistema de aire acondicionado sin afectar la iluminación de la sala de Cómputo en caso de una emergencia.

INSTALACIONES DE SEGURIDAD CONTRA INCENDIO.

Seguridad física.

La seguridad es uno de los factores primordiales al planificar una instalación para equipo de cómputo.

Una vez en el interior del edificio y para la seguridad de las Salas de Cómputo, hay que considerar aspectos tales como la elección de la situación del equipo de cómputo, materiales utilizados,

equipo de protección contra incendios, aire acondicionado, sistemas eléctricos, así como el entrenamiento de personal.

En cuanto a la seguridad del suelo, paredes, techo, sería necesario que:

1). Las paredes sean de material anticombustible y construidas desde el piso falso hasta el techo falso.

2). En caso de que el lugar del equipo de cómputo tuviera una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio.

- Se procurará instalar ventanas irrompibles en la zona del equipo de cómputo, ya que mejorarán la seguridad del personal y del equipo de cómputo.

- Pueden también instalarse tomas de agua sobre las ventanas para protegerlas con una cortina de agua en caso de incendio.

3). El techo falso debe ser de un material incombustible o por lo menos resistente al fuego. Si se utilizan materiales entre el techo real y el falso, deben tomarse las debidas precauciones.

4). El piso falso debe ser de materiales incombustibles o resistentes al fuego. También es importante que el espacio creado entre el piso falso y el suelo real permanezca siempre limpio.

5). Las áreas de almacenamiento de información deben ser impermeables.

6). Se deberá instalar un sistema de drenaje en suelo real.

Seguridad lógica. Seguridad de la información.

Todo el conjunto de la información almacenada en la sala de cómputo, en forma de cintas magnéticas, discos, listados, fichas, etc. debe guardarse en armarios metálicos resistentes al fuego.

La duplicidad de archivos maestros debe encontrarse en una habitación separada de la sala, por motivos obvios de seguridad.

Seguridad del sistema eléctrico.

Se deberán instalar luces de emergencia alimentadas con baterías que iluminen el área de evacuación inmediatamente, en caso de una falla de energía eléctrica. En instalaciones que posean grupos de continuidad, parte de la iluminación deberá conectarse a dicho grupo.

El aire acondicionado deberá ser independiente para la Sala de Cómputo. Dicho sistema debe tener alarma en el área habitual de mantenimiento del edificio, para advertir al personal de servicio de una emergencia.

En cuanto a la seguridad y entrenamiento del personal, cualquier incidencia que ocurra en la sala de cómputo, se encuentre o no fuera de las horas de trabajo del personal, deberá activar la alarma correspondiente en un centro de control vigilado por personal destinado para este fin.

Protección contra incendios.

situación en el área del equipo de cómputo.

- El área del equipo de cómputo debe estar en un edificio o habitación que sea resistente al fuego.
- La sala del equipo de cómputo no debe situarse encima, debajo o adyacente a un área donde se procesen, fabriquen o almacenen materiales inflamables o explosivos.
- La sala de cómputo deberá contar con puertas de emergencia.
- Seguridad de la estructura de la sala de cómputo.

- Si el área de cómputo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles mejorará la seguridad del personal y del equipo contra los escombros y el agua.

- Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.

- Debe preveerse un sistema de drenaje en el piso firme.

Equipos contra incendio.

- Debe haber un sistema de detección de humos, por ionización, para aviso anticipado.

- El sistema deberá hacer sonar una alarma e indicar la situación del detector activado.

- El sistema de detección no deberá interrumpir la corriente de energía eléctrica al equipo de cómputo.

- Deben ubicarse en la sala de cómputo y del sistema de fuerza ininterrumpible, en lugares estratégicos, suficientes extinguidores portátiles de CO2 (recomendados para equipo eléctrico).

- Es adecuado el uso de gas HALON. Es un gas inodoro, no nocivo para la salud.

- Los detectores de ionización del aire se colocan tanto en el techo falso como abajo del piso falso, repartidos de una manera uniforme y todos ellos estarán conectados al tablero de control del equipo contra incendio, en este tablero se localiza un reloj que puede calibrarse de 0 a 60 segundos para provocar el disparo del gas halón a través de boquillas de aspersión estratégicamente distribuídos

en el techo de la sala del equipo de cómputo. También puede activarse manualmente a través de palancas. Los cilindros de gas Halón deben colocarse en la propia sala, o en un lugar inmediato a ella. Se precisan tuberías desde los cilindros hasta las boquillas.

- El gas Halón crea una atmósfera inerte y se dispara muy rápidamente.

Almacenamiento de información.

- Las cintas y discos magneticos se deberán alamacenar en una sola aparte, con acceso por la sala del equipo de cómputo, y deberá estar equipada con todos los equipos de seguridad posibles tanto de condiciones ambientales como de extinción de incendios, con garantía de 10 horas, ya que la información almacenada tiene más valor que el mismo equipo de cómputo.

- Estas cintas o discos magnéticos se deberán almacenar en armarios fabricados exprofeso.

SOFTWARE Y HARDWARE.

Software.

- Lenguajes.

- De Segunda generación (ensambladores).

- De Tercera generación (superlenguajes y Paquetes orientados a problemas específicos).

- De Cuarta generación (bases de datos).

- Tablas de rendimientos de los diferentes lenguajes.

- Simulación-Emulación.
- Librería de programas desglosada por operaciones.
- Número de programas.
- Lenguajes utilizados.
- Sistemas operativos.
- Programas de utilerías.
- Compiladores y ensambladores.
- Programas de control.
- Tamaño de memoria necesaria.
- Soportes de programación para tiempo real.
- Control de líneas de telecomunicación.
- Organización de las colas de datos.
- Organización de las colas de salidas.
- Organizacion de las colas de programas.
- Distribución dinámica de la memoria.
- Relación de las terminales soportados por el software.

Hardware.

Seguridad Funcional:

Tipo de Tecnología del equipo ofrecido:

- Dispositivos centrales.
- Dispositivos periféricos.
- Tipo de garantías.

Tiempo total de máquina:

- Por cada operación:
- Tiempo de proceso.
- Tiempo de preparación.
- Por el sistema total, teniendo en cuenta la multiprogramación y el multiproceso.
- Preparación de cintas magnéticas.
- Preparación de impresión.
- Preparación de memorias masivas.
- Facilidad de conmutación.
- Facilidad de operaciones de entrada.
- Facilidad de planificación de los trabajos.

3-20 Componentes del Centro de Cómputo.

Posibilidad de comprobación de:

- La antiguedad del primer equipo instalado.
- La fecha aproximada de lanzamiento de un nuevo equipo compatible.
- El número de equipos instalados.
- La estadística de fallas en los diferentes equipos y dispositivos periféricos.

Rendimientos y caracteristicas:

- Unidad de información.
- Tiempo de acceso.
- Número y tipo de canales.
- Tamaño de la memoria principal.

Número, sistema y velocidad de:

- Las impresoras.
- Las unidades de cinta magnetica.
- Rendimiento de los Equipos de lectura/escritura de datos.
- Seguridad funcional de la configuración propuesta.
- Duplicacidad de las unidades centrales.

Flexibilidad de procesamiento para:

- Problemas científicos.
- Problemas comerciales.
- Tiempo real.
- Multiproceso.
- Procesadores de comunicaciones.
- Mediante Hardware.
- Mediante Software.
- Asesoramiento comparado.

Información facilitada por otras empresas usuarias sobre:

- Las caracteristicas del equipo.
- Experiencia de estas conexiones.

Calidad del servicio prestado por la firma proveedora, en relación con:

- Apoyo al análisis y la programacion.
- Mantenimiento y servicio.
- Posibilidades de crecimiento.
- Modelos mínimo y máximo, con escalonamiento.

3-22 Componentes del Centro de Cómputo.

- Máxima configuración del modelo propuesto.
- Unidad central.
- Equipos periféricos.
- Precios.
- Tiempo necesario para el cambio.
- Compatibilidad.
- Con la estructura de personal de la empresa.
- Con los locales (sala del equipo de cómputo).
- Con las condiciones ambientales.
- Con el suministro de energía eléctrica.

CONTRATOS DE COMPRA-VENTA Y MANTENIMIENTO DE BIENES INFORMÁTICOS.

Ejemplo:

I. DECLARACIONES DE LA DEPENDENCIA O ENTIDAD.

I.1. Fundamento de Creación.
I.2. Capacidad Legal de su Representante.
I.3. Tipo de Adquisición.
I.4. Dictamen Técnico.
I.5. Domicilio Legal.

II. DECLARACIONES DEL PROVEEDOR.

II.1. Personalidad Jurídica.
II.2. Registro Padrón de Proveedores.
II.3. Domicilio Legal.
II.4. Capacidad Legal de sus Representantes.
II.5. Conocimiento de Especificaciones.
II.6. Relación Laboral.

III. DECLARACIONES CONJUNTAS.
III.1. Conformidad.

Claúsulas.

PRIMERA Objeto del Contrato.
SEGUNDA Relación de Anexos.
TERCERA Precio Convenido.
CUARTA Formas de pago.
QUINTA Impuestos.
SEXTA Patentes y Derechos de Autor.
SEPTIMA Propiedad de los Equipos.
OCTAVA Caso Fortuito o Fuerza Mayor.
NOVENA Entrega e Instalación de equipos.
DECIMA Transportación.
DECIMA PRIMERA Tiempo de Máquina para Compilación y Pruebas de Programas.
DECIMA SEGUNDA Información técnica.
DECIMA TERCERA Ayudas de Programación.
DECIMA CUARTA Partes y Refacciones.
DECIMA QUINTA Capacitación.
DECIMA SEXTA Asesoría Técnica.
DECIMA SEPTIMA Fianza.
DECIMA OCTAVA Seguros.
DECIMA NOVENA Garantías.
VIGESIMA Procedimientos para realizar las Pruebas de Aceptación del Equipo.
VIGESIMA PRIMERA Procedimiento para el Mantenimiento y Corrección de Fallas de los Equipos durante el perfodo de Garantía.
VIGESIMA SEGUNDA Mantenimiento a los Equipos.

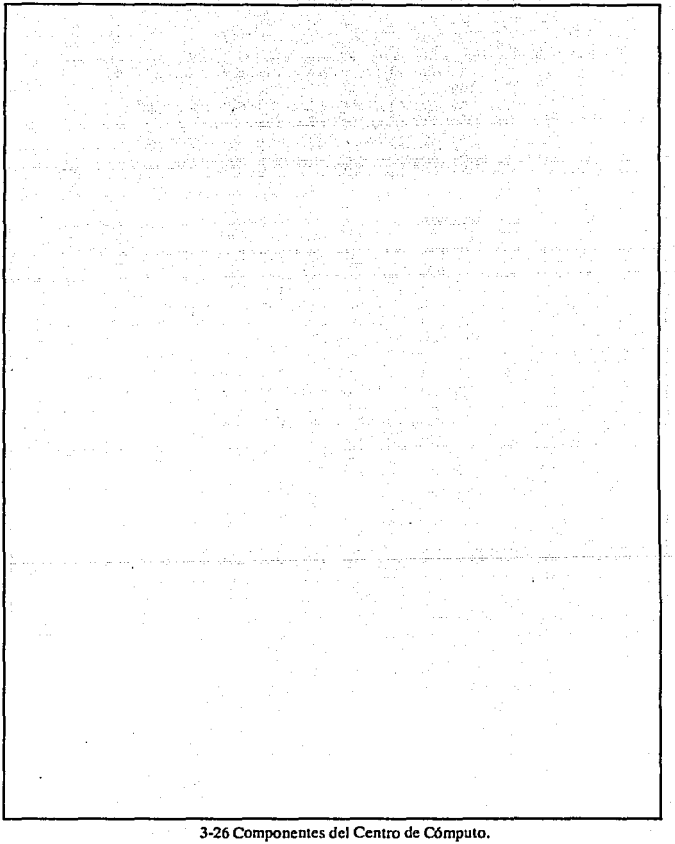
VIGESIMA TERCERA Procedimiento para la Corrección de Fallas.
VIGESIMA CUARTA Límite de Responsabilidades.
VIGESIMA QUINTA Rescisión.
VIGESIMA SEXTA Reconocimiento Contractual.
VIGESIMA SEPTIMA Sometimiento.
VIGESIMA OCTAVA Jurisdicción.

Anexos.

ANEXO "A" Relación de Equipos.
ANEXO "B" Ayuda de Programación.
ANEXO "C" Glosario de Términos.
ANEXO "D" Centros de Servicio del Proveedor.
ANEXO "E" Plan y Horario para el Mantenimiento.
ANEXO "F" Capacitación.

En caso de contrato de Mantenimiento, los siguientes puntos deben ser considerados en las claúsulas:

Mantenimiento Preventivo, Preventivos y Mixtos.
Crédito por Fallas.
Cambios de Ingeniería.
Sistema de Evaluación.
Fianza.
Refacciones.



3-26 Componentes del Centro de Cómputo.

CAPITULO 4

LOS SISTEMAS EXPERTOS.

¿QUE ES LA INTELIGENCIA ARTIFICIAL?

La Inteligencia Artificial (IA) se define como la ciencia que trata de la comprensión de la inteligencia y del diseño de máquinas inteligentes, es decir, el estudio y la simulación de las actividades intelectuales del hombre (manipulación, razonamiento, percepción, aprendizaje, creación, etc.), así como la capacidad otorgada a una computadora, de realizar actividades emulando el raciocinio del ser humano.

ANTECEDENTES DE LA INTELIGENCIA ARTIFICIAL.

La resolución de problemas es una de las constantes que han acompañado al hombre desde sus orígenes. Tanto los problemas que frenan las fronteras del saber (explicación de fenómenos y comportamientos, demostración de teoremas, etc.) como aquellos otros que impiden las realizaciones prácticas (ingenieria, planificación, etc.), o simplemente los creados por curiosidad o distracción (paradojas, acertijos, adivinanzas, juegos, etc.), han llenado el tiempo y consumido esfuerzos intelectuales del hombre.

En la década de los cincuenta apareció un interés especial por parte de los pedagógos y psicólogos, por encontrar los métodos

generales de resolución de problemas, con el fin de que estos métodos se pudieran enseñar a los estudiantes y con ello se mejorara su preparación. Se había ya observado en aquel entonces, que las personas aún conociendo toda la información necesaria para resolver correctamente un problema (definiciones, fórmulas, etc.) son muchas veces incapaces de conseguirlo, realizando con frecuencia razonamientos defectuosos.

Con la difusión de las primeras computadoras, en la segunda mitad de la década de los cincuenta, los estudios ya realizados en el campo de la resolución de problemas se intentaron trasladar a las computadoras. Surgen nuevos problemas como son la representación de los conocimientos en la memoria de la computadora, la representación de las relaciones entre los conocimientos, etc.

HISTORIA DE LA INTELIGENCIA ARTIFICIAL.

La IA, tal y como se conoce hoy en día, hace su aparición en la década de los cincuenta, cuando se comienzan a escribir programas de computadora de tipo simbólico para la resolución automática de problemas.

El desarrollo de la IA ha estado unido desde sus orígenes a los avances tecnológicos en el campo de las computadoras, y éstos están intimamente ligados a los desarrollos de la microelectrónica.

Para Forsyth (1986) la historia de la IA se divide en cuatro grandes décadas que son :

- 1950 Redes Neuronales.
- 1960 Búsqueda Heurística.
- 1970 Sistemas Expertos.
- 1980 Aprendizaje de las máquinas.

En 1943 S. Warren, Mc Culloch y Walter Pitts trabajaron con redes neuronales, que en pocas palabras consiste en el estudio de modelos que siguen la arquitectura del cerebro humano con el

fin de conseguir con ello la realización de las tareas propias del cerebro de una forma artificial, incluyendo, por supuesto, la inteligencia.

El término "Inteligencia Artificial" se cree que fue utilizado por primera vez en 1956 por John Mc Carthy, profesor auxiliar de matemáticas del Dartmouth College en Hanover, New Hampshire, Estados Unidos. El cual convocó a una conferencia considerada como el comienzo de la IA como disciplina independiente de la informática. Con ella pretendía reunir a los investigadores de dicho campo y establecer una fructífera comunicación entre ellos. Varios de los asistentes -Allen Newell, Herbert Simon, Marvin Minsky y John Mc Carthy- son reconocidos universalemnte como destacados pioneros de la IA.

En la década de los sesenta coincidiendo con la segunda época de la IA, Newell y Simon informaron de los trabajos que habían desarrollado en el Carriage Institute of Technology de Pittsburg, Kansas -actualmente Carnegie Mellon University-. Desarrollaron el famoso Logic Theorist, un programa para la demostración de teoremas- el primer programa de computadora que utilizó símbolos en sustitución de cantidades numéricas. Actualmente se le considera el primer programa efectivo de IA. Conjuntamente con J. C. Shaw de la Rand Corporation, Newell y Simon desarrolló el Information Processing Language (IPL II: Lenguaje para Proceso de Información), el primer lenguaje que permitió el proceso de conceptos por computadora, así mismo se considera el primer lenguaje de IA.

Pese a la gran euforia con que se vivió en los momentos iniciales (en 1967 Donald Michie de la Universidad de Edimburgo declaraba que en menos de veinte años existirían máquinas tan inteligentes como el hombre), y los grandes recursos que se emplearon, lo cierto es que no se obtuvo ningún éxito notable.

Uno de los problemas que surgieron en aquel entonces fue, la aparición de la explosión combinatoria en los cálculos exhaustivos que limitaba la profundidad en los mismos y el número de conocimientos que se podían procesar, es decir se calculaban todas las posibles soluciones para luego elegir la óptima. Aparecen entonces los primeros algoritmos de poda (Algoritmo alfa-beta de John Mc Carthy en 1961).

Marvin Minsky, que trabajó con Claude Shanon en Bell laboratories, estimuló el desarrollo de la Inteligencia sintética a través del Proyecto MAC del Instituto Tecnológico de Massachusetts (MIT), que posteriormente se llamó MIT AI Laboratory. John McCarthy, otro cofundador del AI Group, actualmente en Stanford University, es el inventor del Lenguaje LISP (proceso de listas), uno de los lenguajes más utilizados en IA. Cuando Mc Carthy creó el lenguaje LISP, en 1960 éste se consideró durante más de una década como un lenguaje inútil, base del PROLOG lo formuló J. Alan Robienson hasta 1965.

En la década de los setenta, coincidiendo con la tercera época de la IA los planteamientos en el campo de la resolución de problemas cambian. No conociéndose los mecanismos generales de resolución de la mente humana, se pensó en simular para campos muy concretos del conocimiento. Es decir se imita la forma externa o comportamiento aparente, que es precisamente el enfoque completamente opuesto a la línea de investigación de las redes neuronales.

El manejo eficaz de los conocimientos dio entonces sus primeros éxitos: los Sistemas Expertos. Este hecho llenó de nuevo de optimismo a la comunidad científica que entre otras cosas había visto como las subvenciones por parte de los gobiernos se recortaban y en muchos casos desaparecían ante la falta de logros palpables en el campo de IA.

En esta década empiezan a aparecer los primeros lenguajes adaptados a la IA. Tambien se empiezan a desarrollar las primeras computadoras simbólicas en Estados Unidos de Norteamérica, bajo el amparo del proyecto DARPA (1973).

En la década de los ochenta, existen dos grandes líneas de investigación y de desarrollo, que son:

- Divulgación o popularización de los Sistemas Expertos como una metodología que puede resolver de una forma adecuada múltiples problemas. Esta línea ha materializado sus investigaciones en el desarrollo de lenguajes, herramientas, entornos y sistemas vacios que funcionan en pequeñas computadoras (minicomputadoras y estaciones de trabajo).

- Generalización de los Sistemas Expertos que permitan ampliar el campo de conocimientos cuyos primeros logros han sido la comercialización de computadora o máquinas simbólicas y el desarrollo de las computadoras y lenguajes paralelos.

AREAS DE LA INTELIGENCIA ARTIFICIAL.

Dentro de la IA por su gran extensión podemos observar diferentes áreas a las cuales se han dedicado la mayor parte de los recursos de investigación en los países desarrollados como son:

- Sistemas de Lenguaje Natural : -percepción- cuyo principal objetivo es poderse comunicar con un ser humano o utilizando un lenguaje normal como lo es el inglés o español, sin necesidad de reglas estrictas de sintáxis o codificación.

- Estudia el uso del lenguaje natural (el que le es propio al hombre) como medio de comunicación con las máquinas (programas como las bases de datos, robots, etc.); es un problema complejo pues intervienen distintos procesos como son: la comprensión del lenguaje, la síntesis y el análisis de la voz, el resumen y la traducción.

- Sistemas de Reconocimiento Visual : - reconocimiento- cuyo principal objetivo es poder identificar objetos (y asociarlos con ideas o información) mediante dispositivos ópticos que simulan la vista del ser humano.

- Estudia la identificación , inspección, localización y verificación de objetos. Este campo está muy unido al de la robótica pues una de las necesidades básicas de los robots es el poder "ver".

- Sistemas de Reconocimiento de voz : cuyo principal objetivo es reconocer e interpretar correctamente el lenguaje hablado.

- Robótica: -manipulación- son computadoras que involucran la capacidad de un movimiento físico controlado, como por ejemplo los utilizados en plantas ensambladoras.

Estudia las máquinas capaces de realizar procesos mecánicos repetitivos y tareas manuales de las cuales es capaz el hombre.

- El aprendizaje Automático : - aprendizaje - estudia el aprendizaje de nuevos conocimientos de forma automática por los programas de ordenadores y por tanto de las máquinas.

- Tratamiento Inteligente de la Información : - razonamiento -estudia formas "inteligentes" para procesar y recuperar información almacenada en grandes bases de datos que de otra forma sería imposible, por el tiempo requerido en la búsqueda.

- Sistemas Expertos : son sistemas que utilizan el conocimiento humano para emular un proceso de análisis y toma de decisiones.

ANTECEDENTES DE LOS SISTEMAS EXPERTOS.

Los Sistemas Expertos también se conocen con el nombre de "SISTEMAS BASADOS EN CONOCIMIENTO" (knowledge Based Systems) y tuvieron sus orígenes en los años 60's.

Al igual que otros avances tecnológicos que requieren de un considerable trabajo previo de investigación, los Sistemas Expertos tuvieron su cuna en universidades norteamericanas, como Standford, Carnegie Mellon, y el Massachusetts Institute of Techonology (MIT).

La historia de los Sistemas Expertos puede dividirse en tres etapas:

- La primera época que llega hasta el año 1974, y que podríamos denominar "la prehistoria de los Sistemas Expertos". En la década de los 70's se desarrollaron Sistemas Expertos, básicamente para aplicaciones de Química, Medicina, Disciplinas Militares, Física, Ingeniería, Leyes y Ciencias Computacionales. Durante esta etapa se crearon las bases teóricas que van a posibilitar la concepción de los Sistemas Expertos; también se desarrollan los lenguajes de programación y las computadoras.

- La segunda época, comprende desde 1974 a 1984, es llamada por algunos autores "la década de los Sistema Expertos". En ella se construyen de una forma artesanal los Sistemas Expertos que han sido referencia obligada durante muchos años (MYCIN, PROSPECTOR, DENTRAL, etc.). En ésta década se ponen en marcha los grandes proyectos de investigación y desarrollo que de una u otra forma incluyen a los Sistemas Expertos.

- La tercera época comienza en 1984 y todavía seguimos en ella. Se caracteriza por la gran difusión de los lenguajes especializados, herramientas y sistemas vacios, gracias a su comercialización en pequeñas computadoras.

La tercera época terminara cuando se comercialicen las computadoras y los lenguajes paralelos.

Lenguajes creados especialmente para el desarrollo de Sistemas Expertos.

LENGUAJE	FORMALIZACION	COMERCIALIZACION
LISP	1958	
PROLOG	1972	1975
SMALLTALK	1972	1980
OPS	1978	1981

SISTEMAS EXPERTOS.

Definición de un sistema experto.

Sistema Experto o Sistema Basado en el conocimiento, es un Sistema que utilizando experiencia y razonamientos humanos, realiza funciones que un experto realizaría en un área determinada y ante situaciones específicas, asimismo es un conjunto de programas de computadora que son capaces, mediante la aplicación de conocimientos, de resolver problemas en un área determinada del conocimiento o saber y que ordinariamente requerirían de la inteligencia humana.

Una definición mas universal es la debida a Forsyth (1986) que dice, que "Un Sistema Experto es un programa de una computadora que reemplaza a un experto humano", que esta basada en la prueba de existencia de I. A. debida, a Alan Turing y que particulariza para los Sistemas Expertos: " Si la ejecución de un conjunto de programas de computadora puede convencernos de que su comportamiento es el que tendría un experto humano, entonces este conjunto de programas en un verdadero Sistema Experto.

Características de un sistema.

Un S. E. actual no se comporta como un experto humano pues no se conocen todavía los procesos elementales que se ponen en funcionamiento en el hombre cuando trata de resolver un problema y mucho menos cual es el fundamento de la inspiración.
La estructura básica de un Sistema Experto incluye los siguientes elementos:

- Capacidad de aprendizaje (Knowledge Adquisition).- Mediante este mecanismo es como el sistema adquiere toda la experiencia y conocimiento que los hacen "experto".

- Capacidad de Comunicación (User Interface).- Mediante este mecanismo el sistema se comunica con el usuario (no con el experto) para recibir preguntas e información y

proporcionar respuestas conclusiones y a su vez, preguntar al usuario mayor información sobre aspectos específicos.

- Capacidad de Razonamiento (Inference Engine).- Mediante este mecanismo el sistema puede razonar y obtener conclusiones sobre situaciones específicas planteadas por los usuarios.

- Conocimiento o Experiencia (Knowledge Base). Este elemento representa el conocimiento o experiencia específica sobre la materia.

Elementos de un sistema experto.

Un S.E. incluye tres elementos fundamentales: los datos están agrupados en lo que denominaremos Base de Hechos, los algoritmos no existen y en su lugar se utilizan sistemas de representación del conocimiento de tipo declarativo que forman la Base de Concimientos, el control es independiente y se denomina Motor de Inferencia, por último, la entrada y salida de datos es similar a los programas tradicionales.

Diferencias entre un Sistema Experto y un Experto Humano.

	SISTEMA EXPERTO	EXPERTO HUMANO
CONOCIMIENTO	ADQUIRIDO	ADQUIRIDO + INNATO
ADQUISICION DEL CONOCIMIENTO	TEORICO	TEORICO + PRACTICO
CAMPO	UNICO	MULTIPLES
EXPLICACION	SIEMPRE	A VECES
LIMITACION EN CAPACIDAD	SI	SI, NO EVALUABLE
REPRODUCIBLE	SI, IDENTICO	NO
VIDA	INFINITA	FINITA

Diferencias entre un sistema experto y un programa tradicional:

	SISTEMA EXPERTO	PROGRAMA TRADICIONAL
CONOCIMIENTO	EN PROGRAMA E INDEPEN-TE	EN PROGRAMA Y CIRCUITO
TIPO DE DATOS	SIMBOLICOS	NUMERICOS
RESOLUCION	HEURISTICA	COMBINATORIA
DEF. PROBLEMAS	DECLARATIVA	PROCEDIMENTAL
CONTROL	INDEPENDIENTE NO SECUENCIAL	DEPENDIENTE SECUENCIAL
CONOCIMIENTOS	IMPRECISOS	PRECISOS
MODIFICACIONES	FRECUENTES	RARAS
EXPLICACIONES	SI	NO
SOLUCION	SATISFACTORIA	OPTIMA
JUSTIFICACION	SI	NO
RESOLUCION	AREA LIMITADA	ESPECIFICO
COMUNICACION	INDEPENDIENTE	EN PROGRAMA

Así los elementos que forman un S.E. son:

- Representación del Conocimiento (Knowledge representation).
- Capacidad de Razonamiento (Inference Engine).
- Capacidad de Comunicación (User Interface).
- Capacidad de Aprendizaje (Knowledge Adquisition).

Representación del conocimiento.

Todo el conocimiento otorgado (o adquirido por) un Sistema Experto debe representarse en un computadora en forma física y en forma lógica.

Los dos componentes fundamentales de un Sistema Experto son la REPRESENTACION DEL CONOCIMIENTO y la CAPACIDAD DE RAZONAMIENTO. La Representación del conocimiento almacena información acerca del dominio del sujeto; sin embargo, la representación de conocimientos no es una colección pasiva de registros y de información, que se puedan encontrar en una Base de datos convencional.

Existen tres tipos básicos de representación lógica que son utilizados en la construcción de los Sistemas Expertos:

Reglas heurísticas (if-then rules).

Este tipo de representación es la más comúnmente utilizada por los Sistemas Expertos y consiste, como su nombre lo indica, en reglas lógicas que siguen el conocido esquema de IF-THEN. Sin embargo, las reglas de un Sistema Experto son mas flexibles y presentan mayores variantes que las empleadas en lenguajes de programación convencionales.

Esto se debe básicamente a que un Sistema Experto requiere de una capacidad de fundamentación, es decir, todas las reglas alimentadas a un sistema deben incluír el fundamento de dicha regla, misma que se utilizará para indicar al usuario el porque se llegará a la conclusión de un problema.

Esquemas (frames).

Los sistemas basados en esquemas(Frame-based Systems) representan el conocimiento mediante el uso de "Unidades" de información, en las cuales se indican las características y condiciones asociados con la información contenida.

Normalmente, estas unidades se agrupan en estructuras jerárquicas en donde se pueden interconectar mediante apun-

tadores, pueden "heredar" características de unidades de las cuales dependen y pueden tener asociadas reglas heurísticas o preguntas orientadas al usuario para obtener mayor información.

Redes semánticas (semantic networks).

Esta es una forma de representación de conocimiento muy similar a los Esquemas, la diferencia básica estriba es que en las redes no existen jerarquías y que las uniones entre las Unidades (Nodos) proporcionan una explicación de la relación lógica que existe entre ellos.

Existen otros tipos de representación que dependen de las características del conocimiento en que el sistema sea experto y el tipo de decisiones y/o razonamiento que se deba aplicar.

Capacidad de razonamiento (inference engine).

La capacidad de razonamiento de un Sistema Experto consiste en un programa (o un conjunto de programas) que permite manipular la base de conocimiento del propio sistema. Es importante hacer notar que son dos conceptos distintos e independientes.

Existen dos tipos básicos de razonamiento, los cuales funcionan primordialmente en sistemas basados en reglas Heurísticas.

- Orientado a Metas (Goal Driven o Barckward Chaining).

Este tipo de razonamiento parte de una meta especifica y prueba todas las reglas que componen dicha meta, hasta encontrar un valor verdadero (todas las condiciones de una regla se cumplen), obteniendo así una conclusión al problema planteado o determinar que no existe solución si en ningún caso se cumplen las condiciones.

- Orientado a Información (Data Driven o Forware Chaining).

Este tipo de razonamiento funciona en forma similar al anterior con la diferencia de que en éste caso se evaluan todas las reglas que en su conclusión (Then) tengan una posible respuesta a la Meta analizada, es decir, la búsqueda no termina al encontrar una regla con todas sus condiciones válidas. Por lo consiguiente, pueden existir dos o mas respuesta a la pregunta planteada. Esto dará al usuario mayor número de opciones de solución.

Capacidad de comunicación (user interface).

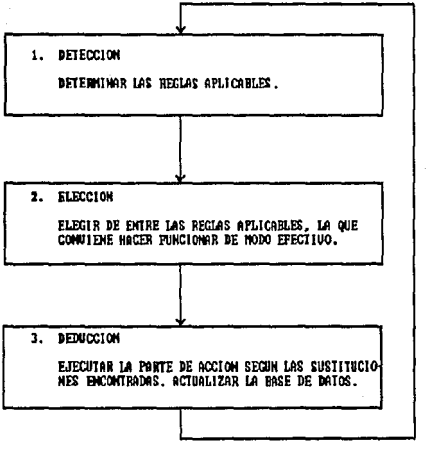
En la actualidad la mayoría de los Sistemas Expertos utilizan los medios de comunicación con el usuario, es decir, desplegados en videos o reportes impresos. Sin embargo, llegará el día en el que se empleen otras ramas de la inteligencia para que el sistema se comunique con los usuarios en una forma más "humana".

Capacidad de aprendizaje (knowdledge adquisition).

Los Sistemas Expertos no inteligentes deben ser alimentados mediante un proceso exclusivo de "entrada" de información, mediante el cual el experto que proporciona el conocimiento, coloca en el sistema todo su acervo.

En el caso de los sistemas inteligentes, después de una carga inicial de conocimiento, existe una capacidad de incrementar dicho conocimiento mediante "aprendizaje" que se deriva del empleo del Sistema Experto y la retroalimentación que el usuario proporcione mediante los resultados y conclusiones obtenidas. Parte de este aprendizaje se logra mediante el empleo de asociaciones, en las cuales el sistema infiere en forma autónoma conocimiento que no es proporcionado en forma directa por el experto que lo creó.

La ejecución se desarrolla siempre siguiendo una secuencia de ciclos elementales, como los que se representan a continuación:



CAPITULO 5

SISTEMA EXPERTO PARA AUDITAR CENTROS DE COMPUTO.

REQUERIMIENTOS.

Planteamiento de objetivos.

1. El sistema de auditoría a centros de cómputo debe cumplir con el esquema de un sistema experto.

2. La interfase del sistema con el usuario debe ser amigable.

3. El sistema debe presentar en opciones diferentes, la serie de cuestionarios sobre los controles, leer las respuestas correspondientes y almacenarlas si se requiere.

4. Podrá solicitarse al sistema la evaluación de las respuestas contestadas en línea o de archivos, recibiendo un reporte de riesgos y sugerencias para eliminar tales riesgos. En su caso, si no hay riesgo, proporcionar alguna conclusión positiva.

5. El sistema, por ser amigable, debe tener una opción de tutorial para conocer el manejo del mismo.

6. En el reporte de riesgos, sugerencias y conclusiones podrá ser mostrado en pantalla, grabado en algún archivo y/o transmitirse a una impresora.

7. El sistema debe trabajar de manera iterativa, es decir, terminará con la opción de "salida" o "fin" o de otra forma debe de continuar corriendo.

Análisis.

1. Para que el sistema de auditoría presente el esquema de un sistema experto, partimos del esquema planteado en el capitulo de Sistemas Expertos:

1.1 Debe contener un banco de conocimientos y una base de datos o hechos, que juntos, podrán interactuar con el usuario.

1.2 Una parte del sistema se encargará de hacer la interfase con el usuario, es decir, será capaz de presentar la serie de preguntas y recibir las respuestas proporcionadas por el elemento humano. Estas respuestas conformarán la base de hechos.

1.3 Otra parte del sistema se encargará de interpretar las respuestas de acuerdo a la base de conocimientos. También proporcionará un resultado a partir de la combinación del banco de conocimientos, la base de datos y los mecanismos de inferencia.

1.4 Ahora; de acuerdo con el esquema, debe tenerse al "experto" que alimentará el banco de conocimientos con todos los conocimientos sobre el tema. Al respecto; podrá sustituirse tal experto con la información más acertada posible que se pueda adquirir de los textos en cuanto a la parte de auditoría. La parte de computación ya está cubierta.

2. Para que el sistema sea amigable, se deberán presentar páneles de tipo menú. Al seleccionar una tecla de éstos páneles automáticamente pasará al siguiente nivel de menú, y asi hasta ejecutar las tareas básicas correspondientes.

3. Dentro de las opciones del menú del sistema, deberá existir alguna que permita tener acceso a todas las preguntas, de manera

que se puedan contestar en línea. En otras palabras, presentar las preguntas almacenadas, contestarlas y, posteriormente, almacenar toda ésta información en un medio magnético.

4. El banco de conocimientos junto con la interfase con el usuario, evaluarán las respuestas a los cuestionarios, de manera que se comparen con un conjunto de riesgos. Al final de ésta parte del proceso, se presenta un reporte sobre los posibles puntos en riesgo que tenga el centro de cómputo auditado.

5. Debe existir una opción de tutorial o descriptivo del sistema dentro del menú, que nos permita conocer el funcionamiento del sistema.

6. Podrá manejarse un reporte formateado a partir del resultado de una evaluación de respuestas a los cuestionarios, que además de almacenarse en medio magnético, se pueda tener la opción de imprimirse.

7. Lo más común es manejar un conjunto de pantallas con menú que puedan invocar a subsistemas correspondientes a la opción solicitada. Por lo cual, se puede establecer una opción de "SALIDA" o "FIN". Si el sistema presenta ésta opción, se tiene un sistema iterativo, es decir, que está en ejecución continua mientras no se seleccione la salida o fin de programa.

Definición de requerimientos.

1. El sistema auditor de centros de cómputo debe presentar todos y cada uno de los elementos que definen a un sistema experto.

Se requiere la base de datos más completa y mejor planeada posible. Para que los mecanismos de inferencia sigan los mismos estándares siempre y no se pierda en los archivos de la base de datos.

2. Dado que es más común el manejo por páneles o menues, éste sistema debe presentar páneles con el menú correspondiente en cada caso:

El menú principal debe considerar los puntos: Auditoría a controles, Evaluación de riesgos, Tutorial, Salida al sistema operativo sin perder la sesión del programa (SHELL) y Salida del programa.

A su vez, el menú de Auditoría a controles deberá manejar las diferentes opciones de acuerdo a los controles existentes como lo son: Gerenciales, Sistemas de Información (Divididos éstos en Diseño, Desarrollo y Mantenimiento, y Operación), Aplicaciones y Tecnología. Este submenú se justifica puesto que no siempre es necesaria toda la evaluación, quizas algunas instalaciones de cómputo no requieran evaluar alguno de los controles.

Obviamente se debe establecer la opción de regreso al menú anterior.

La opción de Evaluación de riesgos del menú principal, deberá presentar, a su vez, un nuevo menú que contendrá: Evaluación de auditoría, Generación de Reporte, Directorio de archivos, Lectura de archivos y el regreso al menú anterior.

Finalmente, las opciones de Tutorial en cada menú que se requiera leerá un archivo tipo texto y se presentará en pantalla, de manera ordenada, con el propósito de mostrar el manejo del menú correspondiente de una manera sencilla.

3. Como ya se mencionó, dentro de la opción de Auditoría a controles, se tiene otro submenú que establece los cinco tipos de controles a auditar, Gerenciales, Sistemas de Información (Dividida en 2), Aplicación y Tecnología además de la opción de regreso a menú principal. Al seleccionar una de éstas opciones el programá deberá leer el banco de conocimientos y tomar las preguntas necesarias para el punto en cuestión, y posteriormente desplegarlas esperando una respuesta en cada una.

3.1 Debe aceptar dos tipos de respuestas, Si o No, debido a que los controles en una instalación de cómputo, o se llevan al cabo o no. El hecho de solo aceptar éstas dos respuestas está apoyado sobre la base de que cualquier situación no puede realizarse a medias o a veces, ésto implica que no se hace.

3.2 Al momento de estar realizando el cuestionario, se podrá almacenar la serie de respuestas que hasta el momento se lleve requistrado a través de desplegar la pregunta con su respuesta previamente capturada, para poder ser modificada, si se desea.

3.3 Un pequeño tutorial podrá ser mostrado, si se desea, dentro de la captura de respuesta para el cuestionario. Así como poder escaparse de ésta opción en cualquier momento.

Las características de los puntos 3.2 y 3.3, se deberá satisfacer con las teclas de funciones y de escape.

4. La opción de Evaluación de riesgos permitirá ejecutar los mecanismos de inferencia para interpretar las respuestas que residen en la base de hechos en relación con el banco de conocimientos para determinar los riesgos que corren la instalación en cuestión. A su vez, se emitirá un reporte de riesgos, con opción a impresión, si el lenguaje lo permite.

5. Para poder tener la opción de tutorial, se tendrá que leer el archivo de texto correspondiente, y desplegarlo con algunas otras opciones, como lo son: Salir de la opción con la tecla ESC, pasar a la página siguiente o regresar.

6. El reporte del requerimiento 4, podrá ser almacenado en disco.

7. Todas las pantallas deberán poseer la opción de regreso al nivel de menú anterior o al que invocó a éste menú. Además, en el menú principal, se debe tener la opción de SALIDA o FIN.

8. En todas las opciones, o respuestas al sistema, se debe leer la tecla presionada, sin necesidad de usar la tecla de "ENTER".

DISEÑO.

Arquitectura.

El conjunto de información requerida es:

El banco de conocimientos, que comprende: La lista de preguntas a realizar, los procedimientos a seguir para determinar las respuestas a cada pregunta y los riesgos que pudieran existir dependiendo de las respuestas.

La base de datos o hechos, que comprende: La lista con la respuesta a cada pregunta y el resultado a la evaluación.

Aqui se debe dividir al sistema como un conjunto de subsistemas. Para esto, estableceremos las funciones necesarias para conformar el sistema. Se requieren las funciones para:

1. Presentar cada menu: Menu principal, menu1, menu2... etc.
2. Leer las opciones de cada menú.
3. Leer un archivo.
4. Escribir en un archivo.
5. Desplegar preguntas.
6. Leer respuestas.
7. Almacenar respuestas.
8. Ejecutar mecanismos de inferencia.
9. Generar reporte.
10. Manejar pantallas.

Cada menú hará interfase con el siguiente nivel de menú, de manera que al seleccionar una opción que requiera de otro submenú, éste se presentará inmediatamente, así como su regreso presentará al menú principal de manera instantánea.

Todas las funciones que presenten los diferentes menues, requieren de interactuar con el programa que leerá el teclado, esperando una opción.

En una de las opciones del menú de auditoría a controles, se leerá un archivo, además de hacer uso del programa que lee respuestas, así como, al final se grabarán en disco los resultados.

Finalmente, el programa que lee archivos, leerá el de las respuestas y hará interfase con el de mecanismos de inferencia para proporcionar un resultado que es la evaluación de riesgos. Que se presentarán al usuario vía el programa que genera reportes.

La siguiente figura muestra el diagrama de flujo de información entre algunos de los módulos que conformarán el sistema experto.

Es probable que se requieran otros módulos para formar las operaciones más básicas en el flujo de información, sin embargo, en la figura se muestran los más importantes del sistema.

El módulo LEE RESPUESTA deberá presentar las preguntas así como leer las respuestas, almacenarlas en alguna variable, para que a su vez, ésta se factible de almacenar en disco.

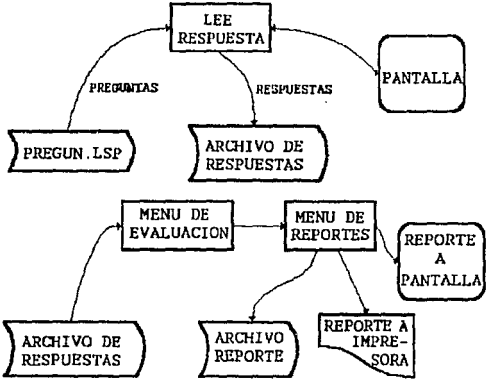
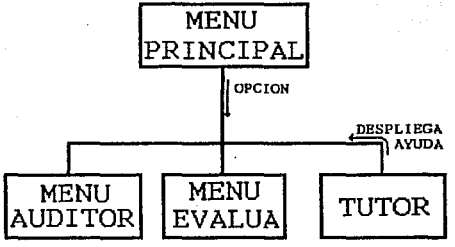


Diagrama de Estructura.

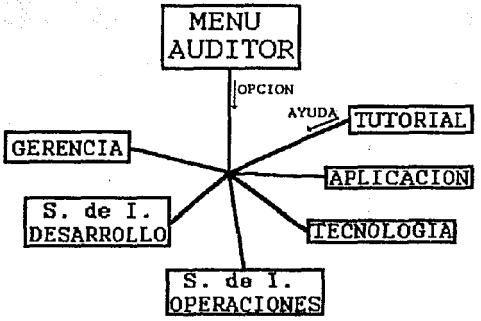
A continuación se presenta el dingrama de estructura del sistema que lo conforma la representación de las subrutinas y las relaciones entre ellas.



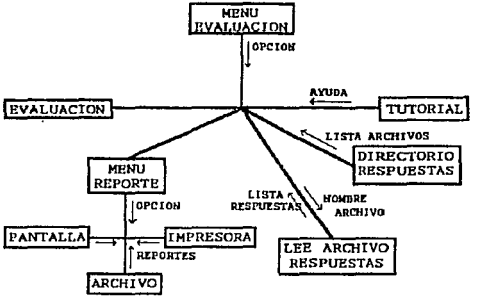
5 - 1 Diagrama de Estructura (fig. 1 de 4).

A través de opciones se podrá entrar a cualquiera de los tres puntos: Menú de auditoría, Menú de evaluación o el tutorial de éste menú.

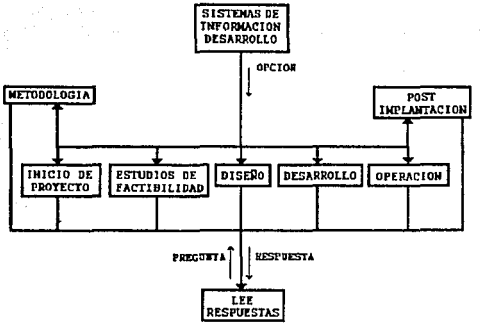
Las siguientes ilustraciones muestran de manera separada cada una de las opciones del primer menú, al igual que en el diagrama de flujo de información, podrán requerirse otros módulos que no están contemplados en el diagrama de estructura.



5 - 2 Diagrama de Estructura (fig 2 de 4).



5 - 3 Diagrama de Estructura (fig. 3 de 4).



5 - 4 Diagrama de Estructura (fig. 4 de 4).

DETALLE DE MODULOS.

A continuación se muestra el detalle de algunos de los módulos que forman parte del sistema experto así como los archivos que tales módulos emplean. Por ser una programación extensa, el detalle se limita a los módulos más importantes.

La estructura del archivo de preguntas PREGUN.LSP es la siguiente:

((Letra Número) (Texto) paso1 paso2)

Donde:

Letra: Es la que indica a que área de Sistemas de Información se va auditar, por ejemplo G es para la Metodología en el desarrollo de sistemas.

Número: Es el número de secuencia de las preguntas.

Texto: Es el texto propiamente de la pregunta.

Paso1: Es el siguiente paso dentro de la estructura de árbol si la respuesta a ésta pregunta fué SI.

Paso2: Es el siguiente paso dentro de la estructura de árbol si la respuesta a ésta pregunta fué NO.

Después de seleccionar el área de los sistemas de información que se quiere evaluar (Gerenciales, S.I. Desarrollo, S.I. Operaciones, Aplicaciones o Tecnología), se debe seleccionar otra subárea dentro de ésta.

La numeración de las preguntas va de la siguiente manera: A 1, A 2, A 3...,G 1, G 2, G 3, ..., Z 1, Z 2, ... Siendo de la A a la F para controles Gerenciales, de la G a la M para desarrollo de sistemas, de la N a la R para operación de sistemas, de la S a la V para aplicaciones y de la W a la Z para tecnología

Un menú con letras de la A a la F, de la G a la M, etc. se muestra en el tercer menú para la realización de las preguntas.

Los siguientes módulos leen las preguntas, las despliegan y leen las respuestas del usuario, note que es la codificación propia del sistema ya que después de diversos cambios, el pseudocódigo original cambió en relación a lo que en realidad se programó.

La mayor parte de las instrucciones son de manejo de pantallas y de menus. Otros módulos importantes son los que hacen la inferencia, solucionando los problemas mediante las reglas de producción y el encadenamiento hacia adelante. Para la solución de conflictos se utiliza los métodos de búsqueda en profundidad (depth-first-search) y búsqueda a lo ancho (breadth-first-search).

Depth-first-search es utilizada al momento de contestar cada pregunta, es decir, según el resultado de cada pregunta se hara la búsqueda de la pregunta que sigue o si ya se llego a la solución. Y Breadth-first-search se utiliza en la generación de reportes, ya que hace una comparación contra todas las reglas para obtener una solución y asi generar el reporte.

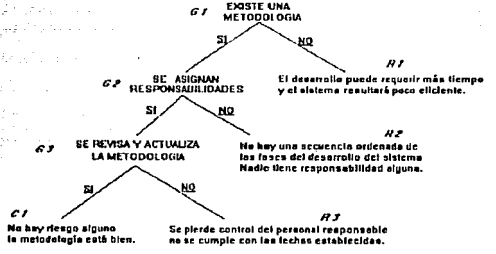
```
(DEFUN LEE_PREGUN () (SETQ LINE (READ)) (SETQ COMPAR (CAR LINE))
(COND
  ((EQUAL LINE 'NIL))
  ((EQUAL TIPO_CON (CAR COMPAR)) (SETQ LISTA (APPEND LISTA (LIST LINE)))
   (SETQ LIS_PARA (APPEND LIS_PARA (LIST COMPAR))) (LEE_PREGUN))
  ((CHAR> TIPO_CON (CAR COMPAR)) (LEE_PREGUN))
  ((CHAR< TIPO_CON (CAR COMPAR)) (SETQ LINE 'NIL) (RDS)) ))

(DEFUN HAZ_PREG (LIS_PRE) (CLEAR-SCREEN)
(COND
  ((NULL LIS_PRE) (FOREGROUND-COLOR 14)
   (PANT_AUX "                    ESC. Para continuar sin salvar a disco.")
   (SALIDA_2 "Desea revisar sus respuestas? (S/N)"))
  (T (SETQ CUESTION (CAR LIS_PRE)) (SETQ CHEC_RES (CAR CUESTION))
     (FOREGROUND-COLOR 14) (SETQ CHEC1_RES (LIST (CAR CHEC_RES)))
     (SETQ CHEC1_RES (APPEND CHEC1_RES (LIST ".")))
     (SETQ CHEC1_RES (APPEND CHEC1_RES (CDR CHEC_RES)))
     (SETQ CHEC1_RES (CAR (PACK CHEC1_RES))) (PRINC CHEC1_RES)
     (WRITE-STRING " ") (WRITE (SECOND CUESTION)) (FOREGROUND-COLOR 4)
     (LEE_RESP CUESTION) (FOREGROUND-COLOR 14))))

(DEFUN LEE_RESP (CUESTION OPCI READ-CHAR RDS WRS)
(LOOP
   (SETQ OPCI (CHAR-UPCASE (READ-CHAR)))
   ((EQUAL (ASCII OPCI) '255) (SETQ FLAG T) (LEE_RESP))
   ((AND FLAG (EQUAL OPCI ";")) (SETQ FLAG NIL) (RDS CAPITU)
    (SETQ C2 'NIL) (SETQ COMENT 'T) (FOREGROUND-COLOR 9)
    (SETQ C2 (CAAR LIS_PRE)) (MAKE-WINDOW 0 0 25 80) (SET-CURSOR 2 27)
    (WRITE-STRING "Procedimiento  a  seguir") (MAKE-WINDOW 5 9 13 62)
    (PANT_AUX "                              ESC. : TERMINA")
    (COMENTARIOS CHEC1_RES) (PANT_INFER) (FOREGROUND-COLOR 4)
    (HAZ_PREG LIS_PRE))
   ((AND (NOT (NULL LIS_RESP)) FLAG (EQUAL OPCI '<)) (SETQ FLAG NIL)
    (SALVA) (HAZ_PREG LIS_PRE))
   ((AND FLAG (EQUAL OPCI '=)) (SETQ FLAG NIL)(CLEAR-SCREEN)
    (DOS "DIR *.TXT") (ENTER) (PANT_INFER) (HAZ_PREG LIS_PRE))
   ((AND (AND FLAG (EQUAL OPCI '>)) (NOT (NULL LIS_RESP))) (PANT_AUX " F1 :
PROCEDIMIENTO    S : SI    N : NO    C : CONTINUAR    ESC. : SALIR")
    (WRITE-STRING "Respuestas   Actuales") (MAKE-WINDOW 5 9 13 62)
    (FOREGROUND-COLOR 14) (SALIDA_1_2) (PON_RESPUES LISTA LIS_RESP))
   ((EQUAL OPCI 'S) (SETQ OPCI 'SI)
    (ASIGNA_RES) (SETQ ACC_ION (THIRD CUESTION))
    (BUS_SIG_PRE (THIRD CUESTION)) (HAZ_PREG LIS_PRE))
   ((EQUAL OPCI 'N) (SETQ OPCI 'NO)
    (ASIGNA_RES) (SETQ ACC_ION (LAST CUESTION))
    (BUS_SIG_PRE (CAR (LAST CUESTION))) (HAZ_PREG LIS_PRE))
   ((AND (EQUAL (ASCII OPCI) '27) (NOT (NULL LIS_RESP))) (PANT_AUX " ")
    (ADVERTENCIA) (ADVERTENCIA) (ADVERTENCIA)
    (SALIDA "Desea salvar sus respuestas? (S/N)"))
   ((AND (EQUAL (ASCII OPCI) '27) (NULL LIS_RESP)))
   (WRITE-BYTE 7)))
```

CODIFICACION DE LOS MODULOS MAS IMPORTANTES

A continuación se muestra un ejemplo de los atributos de operación de los sistemas de inforación a manera de árbol:



G 1,2,3 son las preguntas, las soluciones a buscar son R1,2,3 o C1 donde la R significa Riesgo y C conclusión. Todas las áreas de evaluación tienen una estructura similar. SI y NO son la respuestas posibles a cada pregunta y dependiendo de éstas respuestas y el árbol de atributos se hace la búsqueda obteniendo, ya sea, un riesgo o una conclusión.

Lenguaje de programación.

El lenguaje que se utilizará es Lisp (List Processing) que se ha seleccionado entre otros por algunos factores técnicos:

La representación de datos es muy sencilla, no se tienen que declarar tipos de variables y solo hay tres maneras de representar datos: símbolos, números o listas.

Existe el manejo de las estructuras de control, aunque algo diferentes a las más comunes de otros lenguajes, pero fáciles de implantar.

El lenguaje LISP es fácil de aprender, sin embargo, requiere de mucha práctica.

La eficiencia en tiempo y espacio es bastante amplia comparada con la de otros lenguajes o compiladores como Pascal o C. Y por ser un intérprete, no requiere del proceso de ligado.

La desventaja sería que no es un lenguaje muy entendible, pero si se documenta bien no debe presentar problema alguno.

Comparando con otros lenguajes de su tipo, por ejemplo PROLOG en todas sus versiones, tenemos la ventaja de haber trabajado antes con LISP. Y con otros como C y PASCAL, son la declaración de variables y la complejidad en el manejo de algunas de ellas. Con Lisp no tenemos el problema, ya que reconoce símbolos y listas únicamente.

CASOS DE PRUEBA.

Para las pruebas del sistema, se ha solicitado a personal de empresas privadas que evalúen los resultados del sistema experto, comparando la realidad de las situaciones con los reportes emitidos por el propio sistema experto.

Los resultados de las pruebas se muestran a continuación

REPORTE DEL SISTEMA EXPERTO PARA AUDITAR CENTROS DE COMPUTO.

REALIZADO POR: Ing. Rocío F. Jaimes Cruz.
PUESTO: Titular. Información y Estadística.
EMPRESA: Banco Nacional de México.

Preguntas realizadas por el Sistema Experto Auditor a Centros de Cómputo con sus respectivas respuestas.

1. ¿Existe alguna metodología para el ciclo de vida del desarrollo de sistemas establecida por la organización? SI

2. ¿Se asignan responsables para las diferentes fases de la metodología del ciclo de vida del desarrollo de sistemas? SI

3. ¿Se revisa y actualiza periódicamente la metodología del ciclo de vida del desarrollo de sistemas? SI

4. ¿Participa el departamento usuario en la iniciación del proyecto? SI

5. ¿Se integran equipos de trabajo en el proyecto? SI

6. ¿Se cumple con los requisitos de información? NO

7. ¿Se realizan estudios de factibilidad para el proyecto? SI

8. ¿Se revisan los estudios de factibilidad económica? SI

9. ¿Se revisan los estudios de factibilidad tecnológica? SI

10. ¿Se tienen métodos para el control de costos? NO

11. ¿Se tienen documentados los requisitos de los usuarios? SI

12. ¿Están definidos los requisitos de los datos de entrada y salida? SI

13. ¿Se emplearán lenguajes de alto nivel? SI

14. ¿Se emplearán técnicas de programación estructurada? SI

15. ¿Se tiene el equipo de cómputo para desarrollar el sistema? SI

16. ¿Los programadores han revisado el diseño del sistema? SI

17. ¿El grado de conocimiento de los programadores es alto? SI

18. ¿Se emplearán estándares de prueba? SI

19. ¿Los usuarios revisan que los resultados son los esperados? SI

20. ¿Existe un procedimiento para controlar la operación del nuevo sistema? SI

21. ¿Este procedimiento contempla, además, el control del mantenimiento del nuevo sistema? SI

22. ¿El procedimiento contempla a uno o más responsables para la operación y el mantenimiento? NO

23. ¿Existe algún grupo de personas que controlan la calidad de los sistemas? SI

24. ¿Los reportes del grupo de control de calidad, sobre los resultados de los sistemas, son revisados por el personal del departamento de sistemas de información? SI

25. ¿Ya aceptado el reporte, por las personas de sistemas de información, es entregado a la gerencia? NO

Reportes entregados por el Sistema Experto después de la evaluación de las preguntas anteriores.

REPORTE DE RIESGOS.

Se han detectado los siguientes riesgos en su instalación:

La falta de información relativa a los requerimientos de los usuarios para el sistema que éstos necesitan y que es indispensable para iniciar el proyecto puede retrasar su diseño y desarrollo.

Si no se tiene un método para controlar los gastos acarreados por el desarrollo del sistema, siendo éste factible, el riesgo no es muy alto, sin embargo, se pueden perder recursos durante el desarrollo del mismo.

Si no hay responsables de operar y dar mantenimiento a los sistemas los riesgos son: tener un sistema parado o con fallas continuamente, los mantenimientos no serán aplicados a tiempo, no hay control o asignación de recursos de cómputo, no hay control de mantenimientos aplicados.

Si el personal de sistemas de información no está de acuerdo con los reportes de calidad, puede incurrirse en discrepancias entre gerencia y sistemas de información.

SUGERENCIAS.

Tome en cuenta las siguientes sugerencias:

Asegurese, antes de iniciar el proyecto, que toda la información que éste requiere ya se tenga; si no es asi, solicitarla a los usuarios que participan en el proyecto.

Aún cuando el proyecto es factible, defina un método que controle los costos que el desarrollo del sistema genera, la gerencia debe tener control de tal método.

Asigne responsables para ambas tareas, que dichas personas se encarguen de reportar el uso de recursos del sistema asi como los mantenimientos aplicados y las fechas en que fueron aplicados.

Asegurese que sistemas de inforación revisa y acepta los reportes del grupo de control de calidad, ésto reducirá discrepancias entre lo que reporta sistemas de información y la realidad que recibe la gerencia, también reduce posibles diferencias entre sistemas de información y control de calidad.

REPORTE DE CONCLUSIONES.

Se llegó a las siguientes conclusiones:

No existe riesgo alguno puesto que se tendrá una documentación adecuada desde el punto de vista usuario asi como de programación.

No existe riesgo alguno puesto que se tendrá una documentación adecuada desde punto de vista usuario asi como de programación.

No debe existir riesgo alguno en el aspecto de desarrollo del sistema, ya que se consideró el uso de los estándares de prueba y los usuarios revisan los resultados.

REPORTE DEL SISTEMA EXPERTO PARA AUDITAR CENTROS DE COMPUTO.

REALIZADO POR: Ing. Mónica Flores González.
PUESTO: Ingeniero de Sistemas.
EMPRESA: S E R T E L.

AUDITORIA A CONTROLES DE SISTEMAS DE INFORMACION.

DISEÑO, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Preguntas realizadas por el Sistema Experto Auditor a Centros de Cómputo con sus respectivas respuestas.

1. ¿Existe alguna metodología para el ciclo de vida del desarrollo de sistemas establecida por la organización? SI

2. ¿Se asignan responsables para las diferentes fases de la metodología del ciclo de vida del desarrollo de sistemas? SI

3. ¿Se revisa y actualiza periódicamente la metodología del ciclo de vida del desarrollo de sistemas? SI

4. ¿Participa el departamento usuario en la iniciación del proyecto? SI

5. ¿Se integran equipos de trabajo en el proyecto? SI

6. ¿Se cumple con los requisitos de información? SI

7. ¿La alta gerencia aprueba por escrito el proyecto? SI

8. ¿Se realizan estudios de factibilidad para el proyecto? SI

9. ¿Se revisan los estudios de factibilidad económica? SI

10. ¿Se revisan los estudios de factibilidad tecnológica? SI

11. ¿Se tienen métodos para el control de costos? SI

12. ¿Se tienen documentados los requisitos de los usuarios? SI

13. ¿Están definidos los requisitos de los datos entrada y salida? SI

14. ¿Se emplearán lenguajes de alto nivel? SI

15. ¿Se emplearán técnicas de programación estructurada? SI

16. ¿Se tienen el equipo de cómputo para desarrollar el sistema? SI

17. ¿Los programadores han revisado el diseño del sistema? SI

18. ¿El grado de conocimiento de los programadores es alto? SI

19. ¿Se emplearán estándares de prueba? SI

20. ¿Los usuarios revisan que los resultados son los esperados? SI

21. ¿Existe un procedimiento para controlar la operación del nuevo sistema? SI

22. ¿Este procedimiento contempla, además, el control del mantenimiento del nuevo sistema? SI

23. ¿El procedimiento contempla a uno o más responsables para la operación y el mantenimiento? SI

24. ¿Existen responsables para llevar al cabo el procedimiento de operación del sistema? SI

25. ¿Existe algún grupo de personas que controlan la calidad de los sistemas? SI

26. ¿Los reportes del grupo de control de calidad, sobre los resultados de los sistemas, son revisados por el personal del departamento de sistemas de información? SI

27. ¿Ya aceptado el reporte, por las personas de sistemas de información, es entregado a la gerencia? SI

28. ¿Son revisados los reportes por la gerencia, de tal forma que ésta quede satisfecha de la calidad de los sistemas? SI

Reporte entregado por el Sistema Experto después de la evaluación de las preguntas anteriores.

REPORTE DE CONCLUSIONES.

Se llegó a las siguientes conclusiones:

No existe riesgo alguno puesto que se tendrá una documentación adecuada desde punto de vista usuario asi como de programación.

La gerencia ha aprobado el proyecto y los requisitos de información están completos, no hay riesgo alguno, puede iniciarse el proyecto sin el menor problema.

Las condiciones para desarrollar el proyecto están bien: existen estudios de factibilidad y se podrán controlar los costos del mismo.

No existe riesgo alguno puesto que se tendrá una documentación adecuada desde punto de vista usuario asi como de programación.

No debe existir riesgo alguno en el aspecto de desarrollo del sistema, ya que se consideró el uso de los estándares de prueba y los usuarios revisan los resultados.

Todo está en orden en cuanto a procedimientos de operación y mantenimiento, puesto que tales procedimientos existen y comprenden responsables.

Lo que respecta a control de calidad de sistemas está operando muy bien, el grupo de control de calidad genera reportes que siendo aceptados por sistemas de información son entregados a la gerencia, la cual los revisa adecuadamente.

REPORTE DEL SISTEMA EXPERTO PARA AUDITAR CENTROS DE COMPUTO.

REALIZADO POR: Ing. Juan de Dios Vargas Cuadra.
PUESTO: Líder de Proyecto. Ingeniería de Sistemas. Tarjeta BANAMEX.
EMPRESA: Banco Nacional de México.

AUDITORIA A CONTROLES DE SISTEMAS DE INFORMACION.

DISEÑO, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Preguntas realizadas por el Sistema Experto Auditoría Centros de Cómputo con sus respectivas respuestas.

1. ¿Existe alguna metodología para el ciclo de vida del desarrollo de sistemas establecida por la organización? SI

2. ¿Se asignan responsables para las diferentes fases de la metodología del ciclo de vida del desarrollo de sistemas? SI

3. ¿Se revisa y actualiza periódicamente la metodología del ciclo de vida del desarrollo de sistemas? NO

4. ¿Participa el departamento usuario en la iniciación del proyecto? NO

5. ¿Está documentado el alcance del proyecto? SI

6. ¿Se cumple con los requisitos de información? SI

7. ¿La alta gerencia aprueba por escrito el proyecto? SI

8. ¿Se realizan estudios de factibilidad para el proyecto? SI

9. ¿Se revisan los estudios de factibilidad económica? SI

10. ¿Se revisan los estudios de factibilidad tecnológica? SI

11. ¿Se tienen métodos para el control de costos? NO

12. ¿Se tienen documentados los requisitos de los usuarios? NO

13. ¿Se tienen el equipo de cómputo para desarrollar el sistema? SI

14. ¿Los programadores han revisado el diseño del sistema? SI

15. ¿El grado de conocimiento de los programadores es alto? SI

16. ¿Se emplearán estándares de prueba? SI

17. ¿Los usuarios revisan que los resultados son los esperados? SI

18. ¿Existe un procedimiento para controlar la operación del nuevo sistema? NO

19. ¿Existe un procedimiento de mantenimiento para el sistema? NO

20. ¿Existe algún grupo de personas que controlan la calidad de los sistemas? SI

21. ¿Los reportes del grupo de control de calidad, sobre los resultados de los sistemas, son revisados por el personal del departamento de sistemas de información? NO

22. ¿Tales reportes son entregados a la gerencia? NO

Reportes entregados por el Sistema Experto después de la evaluación de las preguntas anteriores.

REPORTE DE RIESGOS.

Se han detectado los siguientes riesgos en su instalación:
Entre los riesgos más altos al no revisar y actualizar la metodología del cvds son: se pierde el control del personal responsable de las diferentes fases, no se cumplen con las fechas establecidas y no se emplean los recursos adecuados.

Si no se tiene un método para controlar los gastos acarreados por el desarrollo del sistema, siendo éste factible, el riesgo no es muy alto, sin embargo, se pueden perder recursos durante el desarrollo del mismo.

Si los usuarios no documentan todos sus requisitos del sistema éste puede ser mal diseñado y que no contemple completamente los requisitos del personal usuario.

Los siguientes riesgos son causados por la falta de procedimientos de operación y mantenimiento: la falla de un sistema no será atendida, la detección de los errores será muy laborioso, las correciones, si hubiera, se aplicarían
sin control.

La gerencia no recibe reportes de calidad del sistema por parte del grupo de control de calidad, por lo tanto el riesgo para la gerencia es de no saber si el sistema opera como ésta lo estableció, el sistema puede estar consumiendo muchos recursos, o puede estar entregando resultados inesperados.

SUGERENCIAS.

Tome en cuenta las siguientes sugerencias:

Determine una fecha fija para revisar y actualizar el documento de la metodología, que todos los participantes del proyecto asistan a tal revisión, que se agregue al documento las minutas de éstas juntas.

Aún cuando el proyecto es factible, defina un método que controle los costos que el desarrollo del sistema genera, la gerencia debe tener control de tal método.

Solicite a los usuarios, por escrito, la definición de todos sus requerimientos, éstos permitirá un diseño más claro.

Defina procedimientos de operación de cada sistema, así como los procedimientos para aplicar mantenimiento a cada uno de éstos.

Obligue al grupo de control de calidad y a la gerencia a entregar y solicitar, respectivamente, los reportes de calidad del sistema, además de que sean revisados por la gerencia.

REPORTE DE CONCLUSIONES.

Se llegó a las siguientes conclusiones:

La gerencia ha aprobado el proyecto, no hay riesgo en cuanto a la definición del sistema, aún cuando los usuarios no participen.

No debe existir riesgo alguno en el aspecto de desarrollo del sistema, ya que se consideró el uso de los estándares de prueba y los usuarios revisan los resultados.

REPORTE DEL SISTEMA EXPERTO PARA AUDITAR CENTROS DE COMPUTO.

REALIZADO POR: Act. Adriana Montiel Mendizabal
PUESTO: Ingeniero de Software.
EMPRESA: Banco Nacional de México.

AUDITORIA A CONTROLES DE SISTEMAS DE INFORMACION.

DISEÑO, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Preguntas realizadas por el Sistema Experto Auditor a Centros de Cómputo con sus respectivas respuestas.

1. ¿Existe alguna metodología para el ciclo de vida del desarrollo de sistemas establecida por la organización? NO

2. ¿Participa el departamento usuario en la iniciación del proyecto? NO

3. ¿Está documentado el alcance del proyecto? SI

4. ¿Se cumple con los requisitos de información? SI

5. ¿La alta gerencia aprueba por escrito el proyecto? SI

6. ¿Se realizan estudios de factibilidad para el proyecto? NO

7. ¿Se tienen planes de contingencia? SI

8. ¿Se tienen documentados los requisitos de los usuarios? NO

9. ¿Se tiene el equipo de cómputo para desarrollar el sistema? SI

10. ¿Los programadores han revisado el diseño del sistema? SI

11. ¿El grado de conocimiento de los programadores es alto? SI

12. ¿Se emplearán estándares de prueba? SI

13. ¿Los usuarios revisan que los resultados son los esperados? SI

14. ¿Existe un procedimiento para controlar la operación del nuevo sistema? SI

15. ¿Este procedimiento contempla, además, el control del mantenimiento del nuevo sistema? SI

16. ¿El procedimiento contempla a uno o más responsables para la operación y el mantenimiento? SI

17. ¿Existen responsables para llevar al cabo el procedimiento de operación del sistema? SI

18. ¿Existe algún grupo de personas que controlan la calidad de los sistemas? SI

19. ¿Los reportes del grupo de control de calidad, sobre los resultados de los sistemas, son revisados por el personal del departamento de sistemas de información? SI

20. ¿Ya aceptado el reporte, por las personas de sistemas de información, es entregado a la gerencia? SI

21. ¿Son revisados los reportes por la gerencia, de tal forma que ésta quede satisfecha de la calidad de los sistemas? SI

Reportes entregados por el Sistema Experto después de la evaluación de las preguntas anteriores.

REPORTE DE RIESGOS.

Se han detectado los siguientes riesgos en su instalación:

Al no tener una metodología, la gerencia corre el riesgo de que el sistema a desarrollar tarde más tiempo en concluirse, siendo éste deficiente y que la gerencia no tenga una relación de personas responsables de cada fase en el cvds.

Si los usuarios no documentan todos sus requisitos del sistema éste puede ser mal diseñado y que no contemple completamente los requisitos del personal
usuario.

SUGERENCIAS.

Tome en cuenta las siguientes sugerencias:

Defina una metodología de trabajo, por muy básico que ésta sea, es suficiente para empezar con el desarrollo.

Solicite a los usuarios, por escrito, la definición de todos sus requerimientos, éstos permitirá un diseño más claro.

REPORTE DE CONCLUSIONES.

Se llegó a las siguientes conclusiones:

la gerencia ha aprobado el proyecto, no hay riesgo en cuanto a la definición del sistema, aun cuando los usuarios no participen.

Las condiciones para desarrollar el proyecto están bien: existen estudios de factibilidad y se podrán controlar los costos del mismo.

No debe existir riesgo alguno en el aspecto de desarrollo del sistema, ya que se consideró el uso de los estándares de prueba y los usuarios revisan los resultados.

Todo está en orden en cuanto a procedimientos de operación y mantenimiento, puesto que tales procedimientos existen y comprenden responsables.

Lo que respecta a control de calidad de sistemas está operando muy bien, el grupo de control de calidad genera reportes que siendo aceptados por sistemas de información son entregados a la gerencia, la cual los revisa adecuadamente.

REPORTE DEL SISTEMA EXPERTO PARA AUDITAR CENTROS DE COMPUTO.

REALIZADO POR: Ing. Arturo González Jácome.
PUESTO: Ingeniero de Soporte a Software.
EMPRESA: I B M de México.

AUDITORIA A CONTROLES DE SISTEMAS DE INFORMACION.

DISEÑO, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Preguntas realizadas por el Sistema Experto Auditor a Centros de Cómputo con sus respectivas respuestas.

1. ¿Existe alguna metodología para el ciclo de vida del desarrollo de sistemas establecida por la organización? SI

2. ¿Se asignan responsables para las diferentes fases de la metodología del ciclo de vida del desarrollo de sistemas? NO

3. ¿Participa el departamento usuario en la iniciación del proyecto? SI

4. ¿Se integran equipos de trabajo en el proyecto? NO

5. ¿Se realizan estudios de factibilidad para el proyecto? NO

6. ¿Se tienen planes de contingencia? NO

7. ¿Se tienen documentados los requisitos de los usuarios? SI

8. ¿Están definidos los requisitos de los datos entrada y salida? SI

9. ¿Se emplearán lenguajes de alto nivel? SI

10. ¿Se emplearán técnicas de programación estructurada? SI

11. ¿Se tienen el equipo de cómputo para desarrollar el sistema? NO

12. ¿Se tienen planes de adquirir o rentar equipo? SI

13. ¿El grado de conocimiento de los programadores es alto? SI

14. ¿Existe un procedimiento para controlar la operación del nuevo sistema? NO

15. ¿Existe un procedimiento de mantenimiento para el sistema? NO

16. ¿Existe algún grupo de personas que controlan la calidad de los sistemas? NO

17. ¿El personal de sistemas de información entrega reportes a la gerencia acerca de la calidad de los sistemas? NO

Reportes entregados por el Sistema Experto después de la evaluación de las preguntas anteriores.

REPORTE DE RIESGOS.

Se han detectado los siguientes riesgos en su instalación:

El riesgo de no tener definidos a los responsables de cada fase del cvds es que no existe una secuencia ordenada en tales fases,

debido a que nadie tiene la responsabilidad de concluir correctamente cada una.

El riesgo por no tener equipos de trabajo al inicio del proyecto es de realizar doble trabajo, olvidar algunas partes del sistema que pueden afectar la conclusión del mismo, confusión entre los programadores o usuarios al no tener un control de actividades dentro del proyecto.

Si no se tiene un plan de contingencia, el riesgo es muy alto si se intenta seguir con el proyecto, si algo no previsto ocurre, no habrá manera de afrontarlo.

Los siguientes riesgos son causados por la falta de procedimientos de operación y mantenimiento: la falla de un sistema no será atendida, la detección de los errores será muy laborioso, las correciones, si hubiera, se aplicarían sin control.

La gerencia no recibe reportes de calidad del sistema por parte del departamento de sistemas de información, por lo tanto el riesgo para la gerencia es de no saber si el sistema opera como ésta lo estableció, el sistema puede estar consumiendo muchos recursos, o puede entregar resultados inesperados.

SUGERENCIAS.

Tome en cuenta las siguientes sugerencias:

Si bien se tiene la metodología a seguir, es importante que usted establezca en ésta, los nombres de las personas que tiene responsabilidad de terminar cada fase del cvds, además de cubrir los objetivos de cada una de las fases.

Defina equipos de trabajo para el inicio del proyecto, separando

actividades y definiendo éstas por escrito, ésto mejorará la productividad.

Desarrolle un plan de contingencia, asi se podría seguir con el proyecto, aun cuando éste no tenga estudios de factibilidad, que de cualquier forma se recomienda hacer éstos estudios.

Defina procedimientos de operación de cada sistema, así como los
procedimientos para aplicar mantenimiento a cada uno de éstos.

Defina un grupo de control de calidad de sistemas u obligue al departamento de sistemas de información para que, ya sea uno, otro o ambos, entreguen reportes sobre el correcto o incorrecto funcionamiento del sistema.

REPORTE DE CONCLUSIONES.

Se llegó a las siguientes conclusiones:

No existe riesgo alguno puesto que se tendrá una documentación adecuada desde punto de vista usuario así como de programación.

Los programadores pueden empezar por programar en papel las rutinas del sistema para que, cuando se tenga equipo de cómputo, éstos puedan empezar a capturar dichas rutinas.

CONCLUSIONES.

La auditoría informática es un área de reciente creación y necesaria para toda empresa y organización que posea bienes informáticos o bien, que se encuentre involucrada con sistemas de información.

En México, recientemente, se han introducido textos de origen extranjero que tratan de la auditoría informática, además algunas universidades comienzan a introducir materias relacionadas con éste tema.

Por ello, nos permitimos sugerir a las autoridades de ésta Facultad que consideren la idea de crear materias relacionadas con la Auditoría Informática para la carrera de Ingeniería en Computación, ya que las empresas están introduciendo nuevos departamentos para la ejecución de tales tareas.

Nos hemos dado cuenta, con nuestra poca experiencia en el campo, que muchos de los lineamientos de control que se deberían de llevar al cabo en el desarrollo de sistemas, no se cumplen en su totalidad.

Un elemento de suma importancia en nuestro sistema experto, es el nivel de exactitud en cuanto a riesgos, sugerencias y conclusiones, podemos afirmar que éste sistema es tan bueno como cercano es el juicio emitido por un experto sobre un problema o situación real.

Consideramos que la realización de nuestro sistema, no sólo fue factible, sino una necesidad, dada la escasez de profesionales en auditoría informática. Además creemos que éste sistema no

reemplazará a un auditor, por el contrario, simplemente va a aligerar sus funciones.

La mayor parte de los sistemas expertos que han sido desarrollados para tesis, o simplemente para las materias de Inteligencia Artificial o Sistemas Expertos, han sido realizados utilizando cualquier lenguaje de alto nivel, desde ensamblador hasta Pascal o C, o mejor aún en PROLOG. Sin embargo, pocos han empleado el lenguaje LISP (List Processing). Dado que nosotros trabajamos con LISP en la materia de Inteligencia Artificial nuestra decisión fue emplear este lenguaje.

Los requerimientos especificaban un Sistema Experto amigable, lo que consideramos que si se cumplió. Estamos seguros que la información que el sistema proporciona es rápida y de gran utilidad para quien lo utilice, además, se emplea la validación de datos de entrada así como de salida. El sistema proporciona ayuda en cualquier punto donde se encuentre el usuario.

Se trató de evitar toda ambigüedad o redundancia de información, es decir, se procuró que las preguntas fueran claras y precisas, y que los riesgos, sugerencias y/o conclusiones también lo fueran.

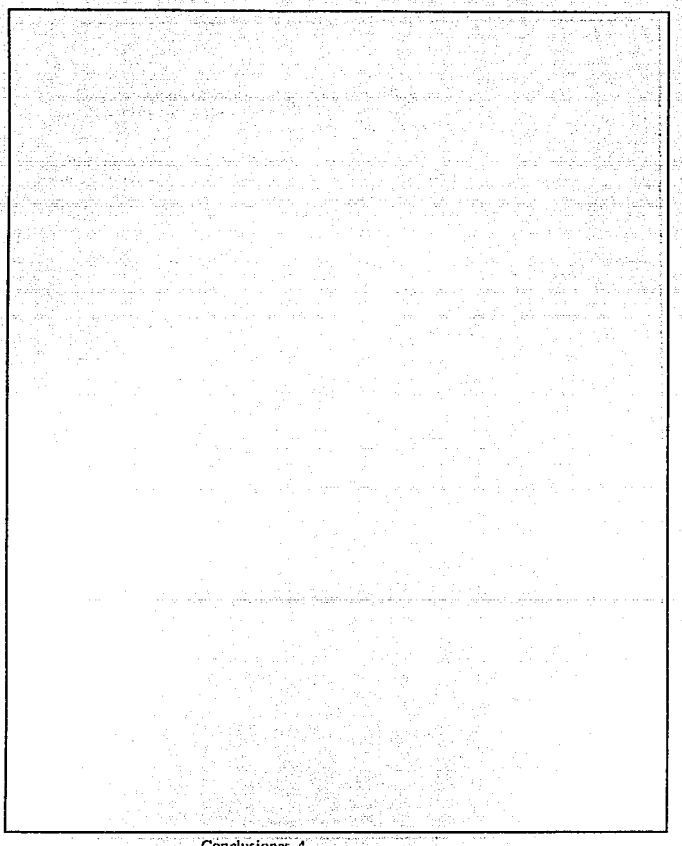
Así mismo, el sistema comprende una serie de archivos de datos, programas y archivos para instalar, lo que lo hace fácil de instalar. El hardware mínimo que requiere el sistema es: Una PC/XT con 640 KBytes, Drive de 3.5", monitor a color (para la presentación) e impresora (para reportes impresos). El Software mínimo es, MULISP-86, DOS 3.3 y recientes.

El costo de nuestro Software comprende un estudio de los costos de desarrollo (nos referimos a la persona dedicada a la formación desde un nivel básico hasta mantenimiento del sistema), explotación (equipo utilizado, medios de comunicación, licencias de software y cursos de formación) y mantenimiento (actualización de las Bases de Conocimiento así como del sistema propio).

Estamos seguros que el tema de auditoría informática es demasiado amplio, como para querer cubrirlo con unas cuantas

preguntas. Por lo tanto invitamos a nuestros compañeros universitarios y futuros profesionistas a que se profundice en el mismo. El campo de trabajo así lo demanda.

Por nuestra parte, el desarrollo de este trabajo nos ha permitido destacar en el desempeño de nuestros puestos en las diferentes compañías para las cuales trabajamos.



Conclusiones. 4

BIBLIOGRAFIA.

ADMINISTRACION DE CENTROS DE COMPUTO.
Ricardo Hernández Jiménez.
Trillas, 1990.

ARTIFICIAL INTELLIGENCE.
Elaine Rich.
Mc Graw Hill, 1988.

ARTIFICIAL INTELLIGENCE AN APPLICATION-ORIENTED-APPROACH.
Daniel Schutzer.
Van Nostrand Reinhold Company, 1987.

ARTIFICIAL INTELLIGENCE & EXPERT SYSTEMS SOURCEBOOK.
V. Daniel Hunt.
Chapmon and Hall, 1986.

AUDITORIA EN CENTROS DE COMPUTO.
David H. Li.
Trillas, 1990.

AUDITORIA INFORMATICA.
A. J. Thomas, I. J. Douglas.
PARANINFO, 1988.

DESARROLLO Y ADMINISTRACION DE PROGRAMAS DE COMPUTADORA (SOFTWARE).
Víctor Gerez, Mauricio Mier, Rolando Nieva y Guillermo Rodríguez.
CECSA, 1985.

EDP AUDITING CONCEPTUAL FOUNDATIONS AND PRACTICE.
Ron Weber
Mc. Graw Hill, 1985.

EXPERT SYSTEMS A NEW AUDIT ERA.
The EDP auditors Foundation, Inc.
1989, Vol I.

INSTALACIONES DE SALAS INFORMATICAS.
Carlos A. Soriano Calvo, Fernando Navarro García.
PARANINFO, 1989.

MULISP-86 REFERENCE MANUAL.

SEGURIDAD EN CENTROS DE COMPUTO.
Leonard H. Fine.
Trillas, 1990.

SISTEMAS EXPERTOS UNA METODOLOGIA DE PROGRAMACION.
J. P. Sánchez y Beltrán.
Macrobit, mayo 1990.

VENTURA PUBLISHER REFERENCE GUIDE.
Xerox Ventura Publisher's