UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS

EFECTO DE UN AMBIENTE DE MICROCOMPUTADOR SOBRE LOS PROCEDIMIENTOS DE AUDITORIA

TESIS

PRESENTADA A LA JUNTA DIRECTIVA DE LA

FACULTAD DE CIENCIAS ECONOMICAS

POR

WERNER GILBERTO MOLINA KLEE

PREVIO A CONFERIRSERLE EL TITULO DE

CONTADOR PUBLICO Y AUDITOR

EN EL GRADO ACADEMICO DE

LICENCIADO

GUATEMALA, OCTUBRE DE 1,996.-

MIEMBROS DE LA JUNTA DIRECTIVA

DE LA FACULTAD DE CIENCIAS ECONOMICAS

Decano	Lic. Donato Santiago Monzón Villatoro
Secretario	Licda. Dora Elizabeth Lemus Quevedo
Vocal 1o.	Lic. Jorge Eduardo Soto
Vocal 2o.	Lic. Josué Efraín Aguilar Torres
Vocal 3o.	Lic. Víctor Hugo Recinos Salas
Vocal 4o.	P.C. Cantón Lee Villela
Vocal 5o.	P.C. Jorge Alfredo Orozco Flores

TRIBUNAL QUE PRACTICO EL

EXAMEN GENERAL PRIVADO

Presidente	Lic. Pedro Rolando Brol Liuti
Secretario	Lic. César Villela Pérez
Examinador	Lic. Mario Danilo Espinoza Aquino
Examinador	Lic. José Adán de León
Examinador	Lic. Marco Antonio Ovando Cermeño

Cabrera y Asociados
ADORES PUBLICOS Y AUDITORES
CONSULTORES

Guatemala, Septiembre 30 de 1996

Licenciado
Donato Santiago Monzón Villatoro
Decano de la Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad Universitaria

Señor Decano:

Con base en el nombramiento que la decanatura me designará, para actuar como Asesor de Tesis en el trabajo del estudiante WERNER GILBERTO MOLINA KLEE, bajo el título "EFECTO DE UN AMBIENTE DE MICROCOMPUTADOR SOBRE LOS PROCEDIMIENTOS DE AUDITORIA", me permitó informarle que se procedió a brindar la asesoría necesaria para desarrollar dicho trabajo.

El trabajo ha sido investigado cuidadosamente para garantizar la calidad de su contenido, ya que trata de un tema de actualidad e influencia para el profesional de la Contaduría Pública, en el área del procesamiento electrónico de datos, satisface las exigencias académicas y constituye un valioso material como fuente de consulta a nivel técnico y profesional, en tal virtud, recomiendo que el trabajo sea aprobado para su discusión y defensa académica en el Examen General Público, del señor MOLINA KLEE.

Agradezco al señor Decano la confianza que brindó al suscrito para colaborar en esta forma con las actividades de la Facultad de Ciencias Económicas de la Universidad de San Carlos de Guatemala.
Atentamente,

"ID Y ENSEÑAD A TODOS"

Lic. Walter Augusto Cabrera Hernández
Colegiado No. 3,524

UIDAD DE SAN CARLOS
DE GUATEMALA

ACULTAD DE
IAS ECONOMICAS
Edificio "S-8"
Universitaria, zona 12
emala, Centroamérica

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS; GUATEMALA, TRES DE OCTUBRE DE MIL NOVECIENTOS NOVENTA Y SEIS.

Con base en el dictamen emitido por el Lic. Walter Augusto Cabrera Hernández, quien fuera designado Asesor y la opinión favorable del Director de la Escuela de Auditoria, se acepta el trabajo de Tesis denominado: "EFECTO DE UN AMBIENTE DE MICROCOMPUTADOR SOBRE LOS PROCEDIMIENTOS DE AUDITORIA", que para su graduación profesional presentó el estudiante WERNER GILBERTO MOLINA KLEE, autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Lic. DORA ELIZABETH LEMUS QUEVEDO
SECRETARIO

LIC. DONATO MONZON VILLATORO
DECANO

El Secretario

DIRECCION

DEDICO ESTA TESIS

A DIOS TODO PODEROSO	A EL SEA LA GLORIA Y LA HONRA INFINITA GRATITUD.
A MIS PADRES	Aura Amparo y Gilberto Emiliano Con gratitud a su esfuerzo.
A MIS HERMANOS	Carlos, Byron Stuardo, Lorena Ariel y Justo Otoniel.
A MI FAMILIA	Con especial cariño a Tía Tavi y mis sobrinos Carlos, Martina y Ana Lorena.
A MI CUÑADO Y CUÑADA	Juan Francisco y Sonia.
A MIS AMIGOS	Enrique Amurrio Comparini Licda. Angie Arévalo Alvizúrez Gloria Arlina Chong Segura Carlos Humberto Echeverría Licda. Claudia M. Guilló Antillón Licda. Norma Patricia Herrera De León Gloria Elena León Jó William Rolando Maldonado Juárez Juan Carlos Ordóñez Matias Vilma Regina Pernilla Méndez Con gran afecto por su apoyo y amistad.
A MI ASESOR	Lic. Walter A. Cabrera Hernández
A LOS LICENCIADOS	Lic. César Amézquita Marroquín Lic. Victor López Zaldaña Licda. Esperanza de Morales Lic. Orlando Recinos Lic. Roberto Salazar Casiano.

I N D I C E

Página

I N D I C E

I N D I C E

I N D I C E

INTRODUCCION

La presente investigación se ha desarrollado buscando obtener la atención sobre el efecto de los ambientes de los microcomputadores en los controles administrativos y financieros que se aplican en una entidad; así como tratar de evaluar el efecto que tienen estos ambientes en los procedimientos de auditoría aplicados como medios de control o instrumentos de evaluación para el control.

Como los controles de los microcomputadores y las medidas de seguridad utilizadas para los grandes sistemas de computo, varían en comparación de un sistema con otro, dada la complejidad de operaciones que pueden realizar cada uno de ellos, corresponde a la administración enfatizar en controles y medidas de control, para resguardar el patrimonio de la entidad.

En el presente trabajo se reconoce que el software de los microcomputadores puede no contener características de control y seguridad afectando el trabajo a desarrollar por los Contadores Públicos y Auditores tanto externos como internos, en la aplicación de sus procedimientos.

De lo anterior, se infiere la hipótesis sobre que "la confiabilidad de la información financiera producida en un ambiente de microcomputadores, dependerá de los controles prescritos por la administración y su adopción por parte de los usuarios, así como,

s procedimientos de control incluidos en los programas de licación para los microcomputadores en una auditoría". Que rvió como base para la realización de esta investigación, con se a un programa específico, que contiene todos los requisitos cnicos necesarios para la elaboración de una tesis académica en carrera de Contaduría Pública y Auditoría.

En el presente trabajo de investigación, se describe que son s microcomputadoros, los sistemas, configuraciones y racterísticas de los mismos.

La estructura del control interno y el ambiente de los crocomputadores, dando una definición y explicación sobre lo que n sistemas de seguridad física y lógica, seguridad del software, spaldo de hardware, respaldo de datos y segregación de funciones.

Los controles generales y de aplicación su definición, ntroles para los usuarios y para los procesamientos de datos.

Finalmente, se ha recopilado todo lo necesario para de terminar el efecto financiero de la realización de una auditoría un ambiente de microcomputadores y los riesgos correspondientes. omprendiendo esta investigación el estudio y evaluación para alizar la auditoría en ambiente de microcomputadores, riesgo de efectuar la auditoría, el resultado del estudio y evaluación.

Se finaliza el trabajo de tesis, exponiendo de una manera breve pero objetiva, las conclusiones y recomendaciones ha que llegó el investigador, basado en la hipótesis y la problemática propia del trabajo de investigación.

CAPITULO I

QUE SON LOS MICROCOMPUTADORES

El progreso técnico ha conducido al ser humano a sofisticar sus formas de producción y aprovechamiento del tiempo libre. Los desarrollos técnicos por su complejidad han comenzado a plantear dificultades paran su efectivo control. Así mismo, la cantidad de información relativa a personas, datos técnicos, estadísticas, documentos, han ido creciendo considerablemente.

Tanto el control de las máquinas como la clasificación, ordenamiento y el acceso directo a toda esta información ha exigido la invención de una máquina que sea capaz de reproducir algunos aspectos característicos de la capacidad mental humana, para auxiliar al hombre. Esta máquina es lo que conocemos con el nombre de computadora.

La palabra computadora designa a una serie de máquinas que responden a una función similar, la de ejecutar procesos repetitivos en forma rápida y exacta. Es decir, que desde las primeras computadoras hasta la actualidad se ha producido una evolución tan grande que resulta difícil reconocer su relación, existiendo actualmente un sin número de modelos y tamaños, desde los microcomputadores hasta los "mainframes", que son computadoras de procesos centralizados, principalmente dirigidas para grandes organizaciones.

1.1 SISTEMAS

Los microcomputadores, que también se les denomina como "computadoras personales" o "PCs", son términos que definen a una máquina de fácil manejo, económica, capaz de realizar y controlar a gran velocidad cálculos y procesos complicados, con fines generales.

Los componentes básicos de un microcomputador son un procesador, memoria, unidad de pantalla, unidad de almacenamiento de datos (disco duro), disqueteras, CDrom, cartuchera (tape backup) teclado, un ratón (mouse), un impresor, conexiones para un impresor y conexiones para comunicaciones (fax/modems).

Los microcomputadores en algunos casos, son usados para procesar distintas transacciones contables y producir informes para elaborar estados financieros.

Aunque fue necesario que llegaran los microcomputadores para que algunas entidades pudieran poner en servicio las redes de área local, el concepto de éstas no es nuevo. Representa un paso en el desarrollo y evolución de la tecnología de las computadoras. Los primeros que se construyeron en los años cincuenta eran conocidos como mainframes. Estos mainframes, eran grandes, muy caros y reservados a pocos y selectos usuarios, no estaban diseñados para dar respuestas directas (On-line) a las órdenes del usuario. Usaban un enfoque o método de procesamiento por lotes, en el cual

los usuarios llevaban las tarjetas perforadas que contenían datos y las órdenes de su programa. Los profesionales de las computadoras introducían estas tarjetas, generalmente al día siguiente enviaban a los usuarios los resultados impresos. Una sóla tarjeta mal codificada, significaba que el usuario tenía que presentar de nuevo todas sus tarjetas para ejecutar completo el proceso.

En ésta época había poca necesidad de compartir recursos, como impresoras y modems, porque había tan pocas computadoras que en las empresas medianas no podían darse el lujo de tener una. La solución a este problema del costo fue el concepto de tiempo compartido. Durante la década de los sesenta llegó a ser posible para una oficina el disponer de una terminal tonta, para conectar, vía línea telefónica, con un mainframe. Alquilando (o compartiendo) tiempo de este computador, el usuario podía disfrutar de los beneficios de las mecanización sin necesidad de hacer una enorme inversión de capital.

El principal problema que tenía el tiempo compartido era la lentitud con la que se enviaba la información por las líneas telefónicas. La producción de los microcomputadores a comienzos de la década de los setenta evitó este problema. Gracias a la drástica reducción de los precios, las empresas pudieron disponer de sus propias computadoras. Todo lo que un nuevo usuario necesitaba para ponerse a trabajar, era una terminal.

El concepto de distribución de los recursos informáticos por a la entidad, dotando a los distintos departamentos de sus pios microcomputadores, en lugar de usar una computadora central a todo el mundo, se denominó "procesamiento distribuido". Pero, cuando pudiera haber varios departamentos de una entidad que ieran sus propios microcomputadores, todavía existía el problema proporcionar la comunicación necesaria entre éstos. Así que las idades empezaron a tender cables entre los microcomputadores y scribir el software necesario para que las distintas unidades se unicaran.

A medida que los microcomputadores se fueron haciendo mas entes y menos caras, en el transcurso de la década de los enta, las entidades empezaron a reconsiderar el uso de las putadoras. Estas computadoras, mas grandes y con costos de enas de miles de dólares, no podían ejecutar los programas nerciales más modernos y sofisticados que estaban saliendo para s microcomputadores IBM PC y compatibles.

Hacia la mitad de los ochenta, en los Estados Unidos había les de empleados de oficinas que se llevaban sus computadoras rsonales al trabajo para usar el software de productividad rocrático que había ya disponible para los microcomputadores. s entidades comenzaron a experimentar graves problemas para ntener la integridad de sus datos, ya que los empleados empezaron intercambiarse discos flexibles y a llevar sus propias bases de tos. La respuesta a estos problemas fue crear el concepto de red.

1.2 CONFIGURACION

Un microcomputador puede ser utilizado en distintas configuraciones.

1.2.1 Un microcomputador de trabajo independiente operada por un solo usuario o varios usuarios en distintos momentos, teniendo acceso a uno o a varios programas;

1.2.2 Un microcomputador de trabajo que sea parte de una red de microcomputadores que están enlazados a través del uso de software especial y líneas de comunicación (Área local); y

1.2.3 Un microcomputador de trabajo conectada a un computador central, utilizándose como parte de dicho sistema (en línea).

1.3 AMBIENTE

Considerando que las características del hardware y software son diferentes, cuando un microcomputador está conectado a otros computadores, es considerado como una Red.

1.3.1 Red de estrella

Esta es una red de varios microcomputadores en diferentes lugares están interconectados a través de un

sistema de cómputo central para la transmisión de los datos, entre los distintos microcomputadores de la red.

1.3.2 Red de anillo

En una red de anillo, los microcomputadores no tienen que pasar los datos a través de un sistema de cómputo central, es decir, que un microcomputador se puede comunicar directamente con cualquier microcomputador. Las redes de anillo utilizan una estructura de difusión, es decir, que los mensajes circulan de un microcomputador a otro microcomputador en una sóla dirección, el microcomputador revisa los mensajes que vienen del microcomputador anterior con el objeto de reconocer su destino.

La configuración de esta red dependerá de tres criterios; distancia entre los microcomputadores, cantidad de tiempo tolerado para las trasmisiones, y cantidad de datos que deben de trasmitir entre los microcomputadores, tomando en cuenta todos estos factores se podrá sugerir la mejor solución.

1.3.3 Redes de área local

Una red de área local (LAN por sus siglas en inglés) en su sentido mas amplio. Es una red de comunicaciones usada por una sola organización, dentro de una distancia limitada, que permite a los usuarios compartir la información y los

recursos. El tratamiento o procesamiento distribuido, significa el enlace de los microcomputadores entre sí para compartir información y los periféricos. Las primeras redes de área local eran relativamente primitivas, y se enfrentaban a una seria escasez de software diseñado para mas de un usuario. En el mejor de los casos, aquellas primeras LAN usaban el bloqueo de archivos (file locking); en determinado momento, podía trabajar un sólo usuario con un sólo programa. Gradualmente, la industria de software se ha ido haciendo más sofisticada. Las actuales redes de área local pueden usar complejos programas de contabilidad y productividad por ejemplo, que permiten a varios usuarios trabajar simultáneamente con los mismos programas (bloqueo de registros, o récord locking).

Como puede verse, la expresión "red de área local" describe un método mediante el cual los microcomputadores pueden compartir información y recursos dentro de un área (local) limitada. Un LAN exige que las estaciones de trabajo (microcomputadores) individuales estén unidas físicamente por medio de cables y que haya algún software en la red, residente en un disco duro, que permita compartir datos y programas de aplicación.

Hace poco tiempo, las LAN se utilizaban principalmente para compartir equipos periféricos como impresoras, unidades de disco duro y plotters. Dado que el hardware representa el

costo principal en los microcomputadores, en la mayoría de oficinas estas primeras redes justificaban sobradamente su costo al asegurar que estos valiosos equipos no permanecieran ociosos. A la fecha, algunas redes (como las de Novell) aumentan aún mas las economías en las oficinas al permitir la creación de una estación de trabajo que no tenga disco flexible. Un chip especial de ROM (Read Only Memory) para autoarranque (autoboot), insertado en la tarjeta de comunicación, permite que el microcomputador, pase a formar parte de la red.

Es difícil generalizar acerca de las redes de rocomputadores, como consecuencia de la falta de compatibilidad ha afligido a la industria, a pesar de los esfuerzos del tituto de Ingenieros Eléctricos y Electrónicos (IEEE) por malizar las formas de transmisión de información en el entorno una red. La misma IBM, reconocida por muchos como la abanderada la industria, comercializa dos redes de área local tan erentes entre sí que una de ellas cumple las normas IEEE, ntras que la otra no.

CARACTERISTICAS

1.4.1 Características de los microcomputadores

- Proporcionan gran capacidad de manejo de información;

- El costo de adquisición es relativamente económico;

- Poseen operaciones de fácil manejo para el usuario;

- Existe una gran variedad de software de aplicación inmediata, por ejemplo sistemas de contabilidad, facturación, control de inventarios, chequeras, planillas, etc.

1.4.2 Características del cableado de las redes

Las redes necesitan un cableado que enlace a sus estaciones de trabajo individuales con el servidor de archivo y otros periféricos. Si sólo se dispusiera de un tipo de cableado, la elección sería sencilla, pero; existen varios tipos de cable, de los cuales examinaremos los mas importantes.

1.4.2.1 Cable de par trenzado (Twisted Pair)

El cable de par trenzado es, con gran diferencia, el mas barato de todos los tipos de medios de interconección para una red. Este tipo de cable consiste en dos conductores aislados trenzados entre sí, de modo que cada uno este expuesto a la misma cantidad de "ruido" de interferencia procedente del entorno que el otro. El ruido se incorpora a la señal que se este trasmitiendo.

Al trenzar los hilos, el ruido se reduce, pero no se elimina. El cable de pares trenzados se vende en una amplia gama de secciones y de pares. Los conductores tienen un número de calibre (American Wire Gauge, o AWG) basado en su diámetro. Un hilo de calibre 26, por ejemplo, tiene un diámetro de 0.01594 pulgadas. Para los usos en redes, los cables de calibres 22 y 24 son los dos tipos mas comunes. El cable de pares trenzados forma mazos por grupos que van desde 4 a 3000 pares trenzados, siendo muchas las redes que utilizan 25 pares. Las principales limitaciones del cableado con pares trenzados son su falta de velocidad y su limitado alcance. Puede manejar flujos de datos de aproximadamente 1 Megabit/segundo sobre distancias de algunos cientos de metros (100 metros de distancia entre cada terminal). Para una pequeña red de área local con un número limitado de usuarios, el par trenzado es la elección ideal, porque es al mismo tiempo barato y fácil de instalar.

1.4.2.2 Cable coaxial

El cable coaxial es casi tan fácil de instalar como el par trenzado, y es el medio de transmisión elegido por muchas de las principales redes de área local. El cable coaxial está formado por un conductor de cobre rodeado de un aislante. La camisa exterior, de cobre o aluminio, actúa como conductor y también

proporciona protección.

1.4.2.3 Redes en banda ancha

A diferencia de los anteriores; los sistemas de banda ancha pueden transportar al mismo tiempo distintas señales trasmitidas a diferentes frecuencias. Este es el método adoptado por las entidades de televisión por cable, utilizando cable coaxial de banda ancha, de 75 ohmios. Los abonados pueden elegir entre varias estaciones distintas, cada una de las cuales trasmite en su propia frecuencia asignada. Todos los sistemas de banda ancha pueden utilizar un sólo cable con amplificadores bidireccionales, o bien emplear el método de dos cables. En cualquiera de los dos casos, las señales de portadora se envían a un punto central conocido como el extremo de cabeza (head end), desde el cual se retransmiten a todos los puntos de la red.

1.4.2.4 Cable de fibra óptica

Uno de los avances mas significativos realizados en los medios de transmisión durante los últimos años ha sido el empleo de fibra óptica en las redes de área local. Este nuevo tipo de transmisión de datos tiene una serie de ventajas sobre los cables coaxiales y de pares trenzados. Además de unas

velocidades superiores a las de cualquiera de los otros medios, los cables de fibras ópticas son inmune a las interferencias electromagnéticas o de radiofrecuencia, y pueden trasmitir las señales sin pérdidas a lo largo de varios kilómetros.

Este método de transmisión es virtualmente inmune a cualquier recepción no autorizada. El cable está formado por vidrio puro estirado hasta formar fibras muy gruesas para constituir un núcleo, estas fibras van rodeadas por un recubrimiento (cladding), es decir, una capa de vidrio con un índice refractivo menor que el del que constituye el núcleo. En la red de fibra óptica, se emplea un láser o un diodo luminiscente (Light Emitting Diode, o LED) para enviar una señal a lo largo del núcleo del cable. Frecuentemente se utilizan repetidores ópticos a lo largo del circuito para amplificar la señal, de manera que llegue a su destino con toda su intensidad. En el extremo de recepción del cable, el mensaje se convierte de nuevo en una señal digital o analógica por medio de un fotodiodo. Por el cable puede ir una sola señal (monomodo) o pueden ir varias (multimodo). Puede ser de índice gradual, en la cual el índice de refracción disminuye lentamente desde el centro de la fibra hacia su porción exterior, o ser de salto de índice, en el cual el índice de refracción varía bruscamente. La fibra monomodo tiene un ancho de banda muy grande, pero el reducido

diámetro de su núcleo hace que los empalmes sean extremadamente difíciles. Por otra parte el monomodo exige el uso como fuente luminosa de un láser, mucho mas caro que un LED. Las fibras multimodo tienen un ancho de banda mucho menor, pero su empalme es mucho mas fácil.

1.4.3 Características de transmisión de las redes

Al igual que hay distintas formas de cablear una red de área local, también son varias las formas que una red puede adoptar. A estas formas diferentes es lo que se llama la "arquitectura de la red" o su "topología". Hay que tener presente que la forma de la LAN no limita la selección de los medios de transmisión. El cable de pares trenzados, el coaxial y las fibras ópticas se prestan a las distintas topologías.

1.4.3.1 La estrella

Uno de los primeros tipos de topologías de redes es el de estrella, que utiliza para la transmisión y la recepción de mensajes el mismo método del sistema telefónico. Del mismo modo que las llamadas telefónicas de un abonado (una estación de trabajo) a otro (otra estación de trabajo) son manejadas por una central de conmutación, en la topología de estrella de una LAN todos los mensajes han de pasar por una computadora central que

controla el flujo de datos. Con esta arquitectura es fácil añadir nuevas estaciones de trabajo. Para conectar una estación de trabajo a la LAN, todo lo que se necesita es un cable desde la computadora central a el microcomputador y su tarjeta de interfaz con la red.

El punto mas débil de la arquitectura en estrella es que toda la red de área local falla si le ocurre algo a la computadora central. Es precisamente el mismo punto débil que presentan los sistemas multiusuario dependientes de un procesador central.

1.4.3.2 En anillo

Otro de los tipos más importantes de arquitectura de red es el anillo. Una topología de anillo consta de varios nodos unidos entre sí formando un círculo. Los mensajes avanzan de un nodo a otro solamente en una dirección. (Algunas redes pueden enviar mensajes bidireccionalmente, pero en una sola dirección a la vez). La topología de anillo permite comprobar si un mensaje ha sido recibido. Cuando un nodo recibe un mensaje dirigido a él, copia el mensaje y a continuación se lo trasmite de nuevo al remitente. Una de las principales cuestiones de una topología de anillo es la necesidad de garantizar que todas las estaciones de trabajo tengan igual acceso a la red.

En una red en anillo con testigo (token ring), la estación transmisora trasmite a través de la red un paquete de datos conocido como testigo (token). Este contiene la dirección del remitente y la del microcomputador que ha de recibir el mensaje. Cuando la estación receptora ha copiado su mensaje, devuelve el testigo a la estación que lo había generado, la cual entonces puede enviar el testigo a la siguiente estación de trabajo del anillo.

La topología de anillo presenta muchas ventajas. Usando software de derivación o bypass, la red puede soportar el fallo de diversas estaciones de trabajo puenteándolas, mientras se mantiene la integridad de aquella. Es posible enlazar entre sí varias redes de anillo por medio de "puentes" que conmutan datos de un anillo a otro.

CAPITULO II

LA ESTRUCTURA DE CONTROL INTERNO Y EL AMBIENTE DE LOS MICROCOMPUTADORES

La mayor parte de los ambientes de los microcomputadores involucran una combinación de actividades manuales como computarizadas de procesamientos. En el caso más general los diferentes procedimientos de control se desarrollan para cada fase del procesamiento. Así como ocurre en un sistema totalmente manual, la administración es responsable de proporcionar el entorno de control y de establecer y mantener el sistema de control interno cuando se utiliza el PED.

El método de procesamiento de datos puede afectar significativamente la estructura organizacional y los procedimientos de control necesarios para satisfacer los objetivos del control interno. Generalmente, los microcomputadores tiene un impacto significativo sobre el control interno. Al determinar su efecto sobre el entorno del control, el Contador Público y Auditor considerará las diferencias entre las actividades manuales y de PED.

2.1 SEGURIDAD FISICA Y LOGICA

Por sus características físicas, los microcomputadores están expuestos a robos, daños físicos y lógicos, acceso no autorizado o uso indebido. Esto puede ocasionar perdida de la información

acenada en los microcomputadores; por ejemplo, información anciera para toma de decisiones.

Dentro los métodos existentes de seguridad física y lógica, se uentra la restricción de acceso a los microcomputadores, cuando estén en uso, guardar con llave dentro un gabinete especial o tector, instalar mecanismos de cierre para controlar el acceso de encendido y apagado, poseer tierra física y reguladores de taje para protegerlos no del daño que pudiera ocasionar las sonas sino contra las inclemencias del tiempo o cambio de tajes.

Existen controles para restringir el acceso físico no orizado al ambiente del microcomputador, terminales, archivos en cos o cintas magnéticas y documentación de sistemas y programas, así minimizar el riesgo del acceso físico no autorizado, que de resultar en:

- Revelación accidental o premeditada de información confidencial.

- Alteración accidental o premeditada de archivos de datos o programas.

- Destrucción accidental o premeditada de datos, programas o equipos.

- Robo de datos, programas o equipos.

- Uso no autorizado del computador.

Los controles de acceso podrán ser implantados a través de medios físicos o por verificaciones del software. Las restricciones físicas incluyen métodos electrónicos de vigilancia, cerraduras que utilizan tarjetas magnéticas, personal de vigilancia, cerraduras, etc. La determinación del mejor método a utilizar solo será posible después de efectuar una evaluación de la confidencialidad y valor de los datos, programas y equipos, y la relación costo/eficiencia de los diferentes métodos disponibles. Los controles mediante software se utilizan comúnmente para controlar el acceso a los archivos de datos y a la biblioteca de programas a través de terminales en línea.

2.1.1 Procedimientos de control

- Restricción del acceso a la sala del computador únicamente a las personas necesarias para la operación del mismo.

- Procedimientos especiales para visitantes, contratistas, técnicos de mantenimiento y personal de limpieza.

- Ubicación del computador como así también del

departamento de sistemas y programación, y del lugar donde se conservan los archivos de respaldo, en áreas bien seguras.

- Procedimientos y registros para controlar la entrega y devolución de medios físicos de acceso, tales como llaves, tarjetas magnéticas combinación de cerraduras, transmisores electrónicos y tarjetas de identificación.

- Notificación a la gerencia del departamento PED y al personal de vigilancia del retiro de cualquier funcionario de la empresa.

- Restricción del acceso a las terminales únicamente al personal autorizado.

- Control del acceso a los archivos de datos y programas, incluyendo:

  -- Registro del uso y del inventario de discos y cintas magnéticas.

  -- Registro de la salida y devolución al área de operación del computador de cintas magnéticas y disco.

Normalmente sólo las grandes instalaciones de computación podrán justificar el costo de contar con un bibliotecario permanente para discos y cintas, sin ninguna responsabilidad por la operación del computador. En las instalaciones menores, esta tarea formará parte de las responsabilidades de algún otro funcionario que no sea el operador; por ejemplo, el encargado del control de datos o el supervisor de procesamiento de datos.

- Obligatoriedad de los mismos controles de acceso para todos los turnos. Si éste no es el caso, se requiere una alternativa aceptable, tal como:

  - Entrega anticipada (preparación del trabajo) de los archivos de cintas y discos para el turno de la noche y durante los fines de semana, de acuerdo con la programación aprobada de los trabajos.

  - Permanencia de por lo menos un supervisor en el área de operaciones del computador en todos los turnos.

- Restricción del acceso a los sistemas, programas y documentación de operación. en algunas instalaciones, una copia debidamente protegida de esa documentación será conservada en microfilm o microficha, o formará parte de

una biblioteca de programas en disco, con acceso protegido mediante software.

- Restricción del acceso a los equipos de entrada de datos mediante el uso de medios físicos, tales como llaves, o electrónicos (control de contraseñas) incorporadas en los programas.

La mayoría de los microcomputadores están equipados con medios de entrada que permiten el acceso directo a los archivos de datos con fines de consulta o actualización. Se podrán utilizar diferentes niveles de contraseñas para restringir el acceso por motivos diversos. Deberá mantenerse un control estricto sobre las contraseñas, las que serán cambiadas a intervalos regulares y, en especial, cada vez que un operador sea reemplazado.

La protección física de un ambiente de microcomputadores es por lo general más difícil de controlar, debido al hecho de que el equipo está frecuentemente instalado dentro del propio departamento usuario y no en una sala separada. Sin embargo, se debe verificar que:

- El microcomputador está instalado lejos de las áreas de acceso de público.

- El local donde se encuentra instalado está debidamente

supervisado.

- El equipo no queda abandonado cuando está en funcionamiento.

2.1.2 Controles compensatorios e importancia de las debilidades

En aquellos casos en que no existan controles adecuados del acceso físico será necesario confiar en controles compensatorios tales como:

- Controles del usuario sobre la integridad y exactitud del procesamiento de datos.

- Elementos de respaldo para el equipo, archivo de datos, programas, documentación y personal, a fin de evitar la interrupción del procesamiento de datos.

- Control de la operación no autorizada del computador y registros del uso del computador.

Cuando las debilidades de los controles físicos sobre el acceso, en lo referente a integridad y exactitud del procesamiento, no están adecuadamente compensados, se debe considerar si es posible confiar en los resultados

del procesamiento. Podrá ser necesario aumentar el alcance de los procedimientos de auditoría. La falta de control sobre la divulgación no autorizada de datos y programas confidenciales es sumamente difícil de compensar, pero resulta poco probable que la misma tenga implicancia directa para la auditoría, a menos que los datos sean excepcionalmente valiosos.

2.1.3 Posibles pruebas de cumplimiento

- Observe el control físico sobre el acceso a la sala del computador, biblioteca de cintas, documentos de entrada, archivos de entrada y documentación de programas.

- Obtenga listas de todas las personas que tiene acceso a cada área dentro del área de computación. confirme si tales listas están autorizadas.

- Verifique si la documentación de sistemas y programas está disponible únicamente para los funcionarios autorizados.

- Realice una investigación del registro y autorización de las entregas y devolución de archivos en cinta y disco a la biblioteca.

- Obtenga listas de todas las terminales y considere la protección física de cada una. Verifique que las terminales cuando se encuentran inactivas estén bloqueadas o que no puedan ser utilizadas por parte de personas no autorizadas. Determine si únicamente el personal autorizado posee llaves o conoce las contraseñas.

- Discuta con los operadores y el personal de vigilancia los procedimientos de protección vigentes durante el turno de la noche y en los fines de semana, para determinar si son adecuados.

2.2 SEGURIDAD DE SOFTWARE

Es de vital importancia la seguridad de los programas y datos, cuando los microcomputadores son accesibles a muchos usuarios, existiendo el riesgo de que los programas y datos sean alterados sin autorización.

Debido a que el software de los microcomputadores puede no contener muchas medidas de control y seguridad, existen varios métodos de control, que pueden incluirse en los programas de aplicación para a asegurar que los datos sean leídos y procesados según la autorización correspondiente y evitar así la destrucción accidental de los datos; por ejemplo, limitar el nivel de acceso a la información y procesos, utilizar contraseñas para el ingreso de

sistemas.

2.2.1 Los controles sobre software

Los controles de software ayudan a garantizar la utilización de las versiones de software autorizadas. Básicamente, el software de sistemas es comprado a los fabricantes de computadores o a firmas especializadas quienes también se encargan de realizar su mantenimiento. El software de los microcomputadores incluye:

- Sistemas operativos, que coordinan el uso del equipo de computación, archivos, de datos y programas, y a menudo permiten la ejecución de más de un programa en forma concurrente.

- Programas utilitarios, que facilitan las tareas de operación del computador, tales como clasificación copia o "vuelcos" de memoria, o que ayudan a los programadores a efectuar modificaciones en los archivos de datos o programas. Estos últimos a menudo no dejan evidencia de auditoría y deben ser cuidadosamente controlados.

- Monitores de comunicación, que se encargan del manejo de las comunicaciones entre el computador y las terminales en líneas.

- Sistemas de manejo de bases de datos, que controlan la organización, acceso, integridad y exactitud de bases de datos.

- Traductores de lenguajes (compiladores), que se utilizan para convertir los programas de un lenguaje de computador a otro diferente, por lo general del lenguaje fuente (COBOL, RPG, etc.) al lenguaje objeto (lenguaje de máquina).

- Software correspondiente a la biblioteca de programas, que se utiliza para almacenar programas fuente y programas objeto, restringiendo el acceso a las bibliotecas de programas, controlando las modificaciones de programas, uso y alteraciones.

- Software para proteger el acceso a los archivos de datos, que se utiliza para identificación de los usuarios, autorización para el procesamiento de archivos de datos y control y registro de cualquier tentativa no autorizada de acceso a los archivos.

Una persona que esté en condiciones de modificar el software de sistemas podrá tener oportunidades de procesar transacciones no autorizadas y de modificar programas y archivos de datos. Sin embargo, el software de sistemas es complejo y por lo general está disponible

únicamente como programas objeto (es decir, en lenguaje de máquina). por consiguiente, sólo un técnico altamente capacitado tendrá conocimientos suficientes para realizar tales alteraciones.

Se debe estar enterado del tipo de software de sistemas que utiliza el cliente y de los medios de control disponibles que puedan tener significación para la auditoría. Además se averiguara cuáles fueron las modificaciones efectuadas por el cliente en el software que compró a terceros y estudiar el impacto de las mismas sobre los controles. También hay que determinar cuáles son los procedimientos que utiliza el cliente para minimizar la posibilidad de que los controles automatizados sean pasados por alto.

2.2.2 Procedimientos de control

- Separación de la función de software (grupo de apoyo técnico) del resto de las funciones PED, especialmente en materia de programas de aplicación. Será necesario crear un grupo separado de programadores que tendrá a su cargo la adquisición, modificación y mantenimiento del software de sistemas.

- Procedimientos para administración y control de la función de software.

- Autorización para la adición de programas utilitarios a la biblioteca de programas.

- Incorporación de elementos de protección y de acceso a los archivos, dentro del software de sistemas.

- Autorización, prueba y documentación de las modificaciones de software realizadas por personal del cliente. Los resultados de las pruebas deberán ser examinados por una persona que no sea la misma que originó la modificación.

- Control estricto de las rutinas utilitarias que permiten la alteración de programas, modificación de la asignación de terminales, del sistema operativo o de archivos de datos, sin dejar evidencia de auditoría. Este control deberá incluir:

  - Restricción de la disponibilidad de rutinas utilitarias al menor número posible de usuarios.

-- Registro de todos los usuarios mediante el software de sistemas.

-- Examen y aprobación por parte de la gerencia PED de los resultados de su utilización.

-- Control de contraseñas.

En general, el software de sistemas disponible para microcomputadores no es tan completo como el disponible para grandes sistemas. Existirá también un número menor de controles automatizados sobre la utilización del computador, uso de archivos de datos y programas medios de reenganche y controles internos de los rótulos de archivos. Si bien la mayoría de los fabricantes de microcomputadores suministra programas utilitarios que permiten a los usuarios efectuar la modificación en línea de programas, los mismos incluyen un menor número de controles automatizados.

2.2.3 Controles compensatorios e importancia de las debilidades

A pesar de los controles descritos en la sección anterior, una persona altamente capacitada, que conozca

todos los aspectos de una aplicación, incluyendo los controles por programa y del usuarios, podría llegar a alterar programas y archivos de datos sin dejar ninguna evidencia de tal alteración. Existen pocos procedimientos aislados de control específicamente capaces de prevenir o detectar estas modificaciones. Sin embargo, la existencia de fuertes controles tanto por programa como por parte del usuario sobre cada una de las aplicaciones, en combinación con una adecuada dirección y supervisión por parte del departamento PED, pueden reducir significativamente este riesgo.

2.2.4 Posibles pruebas de cumplimiento

- Determine, mediante el examen de los organigramas y la observación personal, si la función de programador de sistemas es independiente de las otras funciones PED.

- En los casos en que el cliente haya implantado nuevo software de sistemas, o alterado el existente, obtenga el registro de las modificaciones, seleccione algunas de ellas verifique:

  -- Si la modificación fue autorizada.

-- Las pruebas ejecutadas para garantizar que el software funciona correctamente.

-- La aprobación final de que la modificación fue correctamente ejecutada

-- Examine los datos de salida del sistema de control de trabajos ("job accounting system") y determine si el uso de rutinas utilitarias que permiten la modificación de programas, de la asignación de terminales, sistemas operativos o de archivos de datos sin dejar evidencia de auditoría, fue debidamente autorizado. Es necesario tener en cuenta, sin embargo, que la designación de esas rutinas utilitarias puede ser cambiada y, por consiguiente, resultar difícil de identificar.

-- Determine los medios utilizados por el cliente para prohibir que sean pasados por alto los controles de protección y de acceso a los archivos del software de sistemas y verifique la eficacia de tal prohibición.

RESPALDO DE HARDWARE

Al igual que software, los usuarios deben de tener la certeza

que sus proveedores de microcomputadores, tendrán a disposición rantías del equipo, así como la existencias de repuestos y cesorios, adecuados para los microcomputadores que posea la presa.

4 RESPALDO DE DATOS

En un ambiente de microcomputador, por norma los usuarios son sponsables de los procesos, incluyendo la identificación de los ogramas más importantes y de los archivos de datos que serán piados periódicamente y almacenados en un lugar alejado de los crocomputadores, es decir, en un lugar especial para el mismo.

Es de particular importancia establecer los mecanismos de spaldo que los usuarios deberán llevar a cabo sobre una base gular; como por ejemplo, hacer copias del software comprado, a avés de un tape backup (cinta de copia) o en disco flexibles.

5 SEGREGACION DE FUNCIONES

La segregación de tareas dentro del área del ambiente de crocomputadores, garantiza que los integrantes del personal PED desempeñan funciones incompatibles u que las funciones de una rsona sirven de control sobre las desempeñadas por otra.

También será necesario que exista separación de tareas entre personal PED y el personal del departamento usuario responsable

las transacciones enviadas para procesamiento, controles de s de entrada/salida, mantenimiento de registros contables ales y custodia de bienes.

La segregación de funciones es un elemento fundamental del rol interno. Muchos fraudes y robos de datos y programas se visto facilitados por otro miembro del departamento. Resulta cialmente importante que todo el personal sea obligado a tomar vacaciones anuales. Si durante su ausencia sus onsabilidades son transitoriamente absorbidas por otro ionario, ésto puede constituir en sí un valioso control sobre actividades del funcionario ausente.

2.5.1 Procedimientos de control

- Preparación de documentos fuente fuera del departamento PED.

- Acceso a los datos fuente enviados para procesamiento, únicamente por el personal de entrada y control de datos.

- Prohibición al personal PED de todo acceso a los registros contables preparados manualmente, excepto los documentos fuente.

- Designación de personas diferentes para las siguientes funciones:

  -- Gerente PED

  -- Análisis de sistemas, diseño y programación de aplicaciones.

  -- Mantenimiento de software de sistemas (apoyo técnico).

  -- Operación del computador.

  -- Control de datos.

  -- Bibliotecario de archivos.

- Prohibición a los operadores del computador de realizar modificaciones a los programas y datos. Igualmente, los operadores no deberá tener acceso a la documentación integral de sistemas y programas.

- Prohibición a los analistas de sistemas y a los programadores de operar el computador, aún durante la prueba de programas.

- Exclusión de los programadores del grupo de

personal con acceso a los programas de computador o a los archivos de datos utilizados para producción normal. En los casos en que el acceso a estos elementos se considere necesario por motivos técnicos, el mismo deberá ser adecuadamente supervisado.

- Control de las referencias sobre nuevos empleados.

- Aplicación de un sistema de rotación de tareas, especialmente para programadores y operadores de terminales del computador y en los casos de aplicaciones críticas.

- Medidas adecuadas para garantizar que el personal toma sus vacaciones anuales en forma normal y continuada.

En las empresas pequeñas, la implantación de la segregación de funciones descrita anteriormente no será, por lo general, factible. Los usuarios en general, considerarán que el costo del personal adicional necesario para alcanzar una mayor separación de tareas no es económicamente justificable. La segregación de funciones normalmente posible en este tipo de instalación incluirá las siguientes áreas:

- Gerente/supervisor de procesamiento de datos.

- Análisis de sistema/programación/mantenimiento de software de sistemas.

- Preparación de datos, a menudo fuera de la función de PED.

- Operación del computador/biblioteca de archivos/control de datos.

La necesidad de contar con procedimientos adecuados en materia de personal aumenta considerablemente en las instalaciones de microcomputadores debido a la concentración de toda la responsabilidad en un reducido número de personas. El retiro de un operador de computador clave o de un analista de sistemas/programador, agregado a la carencia de un reemplazante adecuadamente preparado, puede afectar seriamente la continuidad del procesamiento de datos del cliente. Este riesgo podrá ser compensado, hasta un cierto punto, mediante procedimientos de documentación.

La falta de segregación de funciones constituye posiblemente una de las debilidades de control interno más importantes dentro de una ambiente de microcomputadores.

2.5.2 Controles compensatorios e importancia de las debilidades

En los casos en que la separación de tareas se considere inadecuada, pueden existir controles compensatorios ya sea dentro del departamento PED o de los departamentos usuarios.

2.5.2.1 Departamento PED

- Examen por parte de la gerencia del listado del registro de uso del sistema, que podrá contener detalles de la utilización del computador, programas y archivos de datos. Esto podrá servir como compensación para debilidades de control causadas por la inexistencia de una separación adecuada de las funciones de operación del computador, manejo de la biblioteca de discos o cintas magnéticas y control de datos.

- Restricciones físicas y por programa con relación al uso de los dispositivos de entrada, abarcando funcionarios, tipos de transacción, archivos de datos y bibliotecas

de programas.

- Validación por computador en línea, controlada por programas, a fin de permitir que los datos puedan ser verificados por los usuarios en el momento de su entrada.

- Registros de la biblioteca de discos o cintas magnéticas llevados mediante software especializado o manualmente por un empleado encargado del control de datos.

- Programas conservados en forma permanente en archivos en disco(bibliotecas de programas).

- Controles incorporados en los programas (ejemplo, totales de entrada generados por el computador, archivos históricos de transacciones o balanceo de los archivos por el propio computador, utilizando registros de control).

- Suministro de software estándar por parte de las firmas especializadas únicamente en código objeto y no en código fuente, tornando así mas difícil cualquier alteración.

- Adecuada evidencia visible de auditoría producida por los programas de cada aplicación, ya sea en forma regular o a pedido del usuario.

2.5.2.2 Departamento usuario

- Conciliaciones de los datos de entrada/salida.

- Examen de los datos de salida detallados, incluyendo los informes de excepción.

- Firma manual de todos los documentos negociables emitidos por el computador.

- Pruebas manuales de los datos generados por el computador.

- Conciliación de los registros manuales de control con registros de control del computador.

En los casos en que no exista una separación adecuada de tareas podrá ser necesario aumentar el alcance de los procedimientos de auditoría.

2.5.3 Posibles pruebas de cumplimiento

- Examine el organigrama del cliente, concentrándose en el departamento PED y discuta con el personal del mismo sus responsabilidades individuales, a fin de confirmar si la separación de tareas es adecuada.

- Inspeccione la evidencia de que los supervisores analizan el usos del sistema de computación.

- Examine los archivos del personal para verificar si:

  -- Se obtuvieron referencias adecuadas.

  -- Cada funcionario tomó sus respectivas vacaciones durante el año anterior.

- En el caso de ex-operadores, bibliotecarios y programadores, determine si:

  -- Se les retiraron inmediatamente las tareas críticas o confidenciales después de la notificación de despido.

-- Se tomaron medidas adecuadas de protección, incluyendo el cambio de contraseñas, devolución de tarjetas de identificación, llaves, documentación y notificación al personal del departamento PED y al personal de vigilancia.

- Verifique si se realiza una rotación regular de tareas.

CAPITULO III

CONTROLES GENERALES Y DE APLICACION

3.1 DEFINICION

El control "comprende el plan de organización y todos los métodos coordinados y medidas adaptadas dentro de un negocio con el fin de salvaguardar sus activos, verificar la confiabilidad y corrección de los datos, promover la eficiencia operativa y fomentar la adhesión a las políticas administrativas prescritas".(1)

"Los auditores internos u otro grupo independiente dentro de la organización deben revisar y evaluar los sistemas propuestos cuando se encuentren en las etapas críticas de su desarrollo."(2)

De acuerdo con las autorizaciones generales o específicas de la gerencia, los usuarios y los analistas de sistemas, son los principales responsables de diseñar, implantar y probar un sistema en forma tal que sea eficiente, que deje un rastro para la auditoría e incluya procedimientos adecuados de control.

1) Kell Ziegler, Auditoria Moderna, Trans-editions, Inc. a division of John Wiley & Sons, Inc., página 122.

2) Ver SAS No. 9. "El efecto de la función de Auditoría Interna en el alcance del examen del Auditor Independiente". AICPA, 1976.

Los auditores internos u otro grupo independiente dentro de la ganización, por ejemplo un comité de sistemas, una comisión de abajo o un grupo de enlace entre el usuario y el PED son por lo neral responsables de informar a la gerencia si se están mpliendo los criterios establecidos. Como resulta poco práctico tablecer controles en sistemas que ya han sido desarrollados, es portante que los auditores internos u otro grupo independiente gan revisiones, después de implantar los controles necesarios.

Los auditores internos u otro grupo independiente deberán rificar los procedimientos de control por medio de materiales y cnicas tales como programas de auditoría por computador, servación de las operaciones, examen de los registros de control otros. En adición tales grupos deben hacer pruebas de los gistros de entrada y del proceso.

2 POR LOS USUARIOS

3.2.1 Datos de entrada

Existen controles del usuario sobre la preparación y aprobación de transacciones?

El objetivo de los controles, es garantizar que las transacciones fueron debidamente aprobadas por el usuario antes de ser procesadas.

La aprobación de los datos de entrada constituye la primera etapa del control del usuario sobre los datos a ser procesados por el computador. La aprobación o autorización de los datos de entrada, fuera de la función PED, constituye un aspecto importante de la separación de tareas entre el usuario y el personal PED.

En el caso de sistemas sofisticados, los programas del computador generalmente ejecutarán algunos procedimientos de autorización, tales como el control de los pedidos del cliente, para verificar el estado de su posición de crédito y la disponibilidad de existencias. En estos sistemas, por ejemplo, un pedido aceptado hará que el computador emita los documentos de expedición correspondientes, los que servirán de autorización para que las mercaderías puedan ser expedidas por el depósito.

3.2.1.1 Procedimientos de control

- Utilización de formularios de entrada estándar, numerados secuencialmente, controlados por el usuario.

- Autorización por la gerencia del departamento usuario de las transacciones de entrada significativas.

3.2.1.2 Controles compensatorios e importancia de la debilidades

Algunos errores de entrada podrán ser detectados automáticamente por los controles de validación efectuados por el propio computador. Sin embargo, no podemos esperar que estas verificaciones descubran todos los errores. Por ejemplo, una verificación de los precios puede revelar que el precio de un determinado ítem expedido por el depósito es incorrecto, pero no conseguiría identificar otra salida totalmente ficticia correspondiente a la misma partida, entrada al precio correcto.

3.2.1.3 Posibles pruebas de cumplimiento

- Procedimientos de prueba para mantener un control numérico sobre los documentos de entrada.

- Examen de un grupo de documentos de entrada ya procesados, para verificar si fueron debidamente aprobados por el departamento usuario.

- Rastreo de una muestra de documentos de

entrada hasta los controles por lotes.

3.2.2 Datos fijos

Existen controles del usuario sobre las modificaciones de los datos fijos que se realicen en los archivos maestros y tablas del sistema?

El objetivo de este control, es garantizar que todas las modificaciones de datos fueron debidamente aprobadas y procesadas en forma completa y exacta.

Normalmente el archivo maestro contienen datos acumulados de las transacciones y datos fijos. Los datos fijos representan información que relativamente muy pocas veces es alterada y que puede ser utilizada en cada ciclo de procesamiento. La misma incluye datos generales de referencia (ej., nombres y direcciones, códigos de referencia, categorías y códigos específicos), y valores contables (tasas de pago, intereses, depreciación o descuentos y costos unitarios de existencias). A menudo, en los casos en que los datos fijos son comunes a diferentes categorías de items (ej., empleados, clientes, proveedores, items de existencias o activo fijo), los mismos serán conservados en archivos de datos separados (o en tablas), o aun incorporados en la codificación del programa. En esos casos, los archivos maestros no siempre contendrán el total de datos fijos y sí "indicadores" que

señalaran a los programas del computador, la tabla de búsqueda o la rutina de programación correspondiente.

La modificación de los datos fijos puede incluir la inserción de registros, cambios en los registros existentes y eliminación de registros. En algunos sistemas, los registros obsoletos son borrados automáticamente por programas especiales. Ese tipo de registros puede incluir clientes o proveedores inactivos, items de existencia obsoletos o ex-empleados. Cada vez que los datos fijos son alterados, el cambio afectará todo el procesamiento subsiguiente hasta que dichos datos vuelvan a ser alterados. Por lo tanto la integridad y exactitud de los datos fijos debe ser cuidadosamente controlada. Este control debe ser impuesto principalmente por los usuarios.

Algunos sistemas permiten que cierto tipo de datos fijos, tales como precios de venta, descuentos o tasas de interés, sean salteados, en el caso de una transacción específica, mediante la entrada de datos adicionales simultáneamente con la entrada de la información. Este tipo de instrucción deberá ser controlada tan rigurosamente como cualquier otra alteración de los datos fijos.

3.2.2.1 Procedimientos de control

- Utilización de formularios diseñados

específicamente para entrar alteraciones, a fin de evitar errores de preparación.

- Uso de formularios de entrada previamente numerados, limitados únicamente al personal autorizado, que efectuará también el control de los mismos.

- Preparación o aprobación de los formularios de entrada de modificaciones únicamente por la gerencia del departamento usuario.

- Creación por parte del usuario, de totales de control por lotes correspondientes a las modificaciones y su posterior reconciliación con un listado de modificaciones. Este control por lo general sólo resultará adecuado si el volumen de las modificaciones es relativamente alto.

- Un listado de todas las modificaciones procesadas. Este listado deberá ser examinado por un gerente que no tenga relación directa con la preparación de las modificaciones. En alguna grandes empresas esta tarea estará a cargo de una función de control centralizado, en vez de corresponder al departamento usuario

que originó la modificación. El alcance de la verificación de las modificaciones, desde el listado hasta los documentos de origen debidamente autorizados, depende del volumen de modificaciones procesadas y de la importancia de los datos fijos que fueron alterados.

- Autorización individual para cada una de las instrucciones de saltear procesos o rutinas normales.

- Listado de computador de todas las instrucciones de saltear datos o rutinas a fin de que puedan ser examinadas por la gerencia.

3.2.2.2 Controles compensatorios e importancia de las debilidades

Resulta difícil compensar posibles debilidades en los controles del usuario sobre modificaciones de los datos fijos. Los procedimientos indicados a continuación, pueden no obstante reducir el riesgo representado por debilidades en los controles del usuario:

- Un control adecuado sobre la permanente

integridad y exactitud de los datos fijos.

- Control por programa de la validez y de la razonabilidad de las indicaciones. Estos controles pueden, por ejemplo, verificar si los códigos de cuentas son válidos, si el sueldo básico no excedió un cierto importe, o si no se han creado registros duplicados.

Aun cuando exista un grupo central de control de datos PED para ejecutar estos procedimientos, el usuario tendrá que examinar los datos de salida para verificar su razonabilidad, como parte de un control adicional para tener la seguridad de que no fueron procesadas modificaciones no autorizadas.

3.2.2.3 Posibles pruebas de cumplimiento

- Haga una prueba de los procedimientos de control numérico sobre los formularios de entrada.

- Seleccione listados de modificaciones al archivo maestro.

- Verifique la conciliación de los totales de control de los listados realizada por el usuario.

- Examine los documentos de origen que autorizaron las modificaciones.

- Verifique si los documentos de origen fueron correctamente aprobados.

- Seleccione listados de las modificaciones rechazadas.

- Determine si el informe contiene detalles suficientes como para permitir que el usuario corrija los errores.

- Verifique si los items fueron rechazados por motivos válidos.

- Verifique si los errores fueron corregidos y los items reingresados sin demoras al computador.

- Siga el rastro de los errores hasta los registros de corrección y hasta la evidencia de la ejecución de correctas modificaciones al archivo maestro.

- Verifique si los registros corregidos fueron debidamente autorizados.

- Seleccione algunos listados de instrucciones de saltear items.

- Examine los documentos de origen.

- Verifique si los documentos de origen fueron debidamente autorizados.

- Examine la evidencia existente referente a la inspección y aprobación del listado de computador por parte de la gerencia.

3.2.3 Sobre items rechazados y en suspenso

La existencia de controles del usuario sobre la permanente integridad y exactitud de los datos fijos correspondientes a archivos maestro y tablas. Garantizando la permanente integridad y exactitud de los datos que eventualmente podrán ser utilizados en cada ciclo de procesamiento.

Los controles sobre la modificación de los datos fijos por el usuario no detectarán necesariamente las alteraciones no autorizadas realizadas por:

- Otro usuario con acceso al archivo maestro.

- Una función de control de datos centralizada.

- El personal PED.

Por lo tanto, los procedimientos deberán de verificar la permanente integridad y exactitud de los datos fijos.

3.2.3.1 Procedimientos de control

- Conciliación de los totales de control del usuario con los totales acumulados por el computador referentes al número de registros existentes en el archivo y al contenido de campos significativos de datos fijos.

- Verificación de la permanente integridad y exactitud de los datos fijos en registros individuales. Para ello, será necesario obtener listados totales periódicos, realizar muestreos, cíclicos o consultas ad-hoc sobre registros específicos, a fin de verificarlos contra los registros del usuario.

3.2.3.2 Controles compensatorios e importancia de las debilidades

El ambiente de microcomputadores del cliente

podría incluir software que en cierta medida puede contribuir a evitar la realización de modificaciones no autorizadas a los datos fijos. Las debilidades que puedan existir en esta área pueden tener un enorme impacto en el grado de confianza que podremos depositar en los registros contables producidos mediante la utilización de los datos fijos.

3.2.3.3 Posibles pruebas de cumplimiento

- Examine y pruebe la conciliación realizada por el cliente de los totales de datos fijos, informados por el microcomputador, con los registros manuales.

- Verifique la existencia de listados indicando que los totales de datos fijos de cada registro maestro fueron acumulados y conciliados por el propio microcomputador con registros de control.

- Verifique si se han preparado listados periódicos de los datos fijos y si los mismos fueron controlados de acuerdo con los procedimientos del cliente; por ejemplo, mediante el uso de programas de consulta o de

muestreo.

- Ponga a prueba la exactitud de los datos fijos verificándolos con listados del cliente, o si estos no están disponibles, con listados especiales producidos para fines de auditoría.

3.2.4 Sobre los datos de salida

La existencia de controles del usuario sobre los datos de salida radica en detectar los errores e irregularidades en los datos de salida.

Los programas de aplicación incluyen generalmente, la función de imprimir totales de control durante las diferentes etapas del procesamiento, incluyendo cada uno de los informes finales de salida.

Estos totales deberán ser conciliados por los usuarios con sus propios totales de control, desarrollados manualmente, a fin de garantizar que los datos de entrada fueron correctamente procesados y que los datos acumulados del ciclo de procesamiento anterior fueron correctamente actualizados. Además, deberán incluirse controles de programa a programa en cada aplicación, a fin de que el propio sistema de computación pueda verificar si todos los datos de entrada y los datos

generados fueron procesados en forma completa, a través de todas las etapas.

Estos procedimientos de conciliación debe tener en cuenta los rechazados, items en suspenso y actualización de más de un archivo. Los usuarios responsables del examen y conciliación de los datos de salida no deberán tener ninguna otra responsabilidad que pueda resultar incompatible con el control de salida, como por ejemplo la conversión de datos.

En los casos en que la salida tome forma de instrumentos negociables o de autorización para la emisión de pagos, se deberán adoptar controles adicionales. En ocasiones se hace uso de computadores para generar cheques, certificados de intereses o de dividendos, pre-firmados.

Generalmente un buen control de entrada y salida van juntos. De ahí que la debilidad de uno de ellos neutraliza la eficacia del otro.

3.2.4.1 Procedimientos de control

- Conciliación de los movimientos del archivo maestro contra los totales preparados manualmente por los usuarios, a fin de garantizar que el total de datos acumulados,

incluyendo los items en suspenso del ciclo anterior más los datos de entrada del ciclo actual es igual al total que resultó al final del procesamiento del ciclo actual.

- Conciliación de los datos de salida generados por el computador y de los sub-totales de control con los totales de entrada, para garantizar que todos los datos entrados fueron procesados.

- Conciliación del total de items de entrada aceptados, conforme al resumen de los informes de validación y de cualquier dato generado informado por otros programas, contra el informe de actualización de archivos, a fin de asegurar que todas las transacciones aceptadas fueron procesadas.

- Conciliación del movimiento entre dos actualizaciones con las transacciones entradas o generadas, para garantizar que fueron procesados los archivos correctos, es decir, el total del final del ciclo anterior es igual al total inicial actual (control de ciclo a ciclo).

- Verificación de otros totales del computador, tales como:

  -- Totales de programa a programa, en los sistemas que utilizan varios programas en secuencia para realizar todo el procesamiento de los datos.

  -- Totales de salida relacionados entre sí, por ejemplo, análisis de antigüedad de cuentas por cobrar y el listado de las mismas, registro de facturas y el informe de actualización del mayor de ventas.

- Procedimientos para restringir la distribución de informes de salida confidenciales únicamente a las personas autorizadas.

- Uso de documentos negociables controlados numéricamente, los que estarán adecuadamente protegidos en todo momento.

- Examen por parte de la gerencia de los documentos de salida preparados en forma de instrumentos negociables. Los instrumentos que excedan un determinado valor deberán ser refrendados fuera del Departamento PED.

- Especificación del período de conservación de los documentos de origen, archivo de datos, microfilmación de documentos de salida del computador y listados del mismo. Tales períodos deberán estar de acuerdo con los objetivos de operación del cliente y al mismo tiempo,cumplir con las exigencias legales en vigor. Será necesario contar con archivos y referencias cruzadas adecuadas de los documentos fuente y de salida del computador.

- Procedimientos adecuados para determinar condiciones de excepción y para el manejo de los informes de excepción, incluyendo informes de datos no válidos o no apareados, que fueron aceptados para procesamiento. El usuario debe asegurar que el criterio utilizado para informar las excepciones es realista, útil y actualizado. Los informes de excepciones deberán tener fecha, contener comentarios sobre el tipo de medidas adoptadas y serán guardados en un archivo.

- Examen de los listados impresos por el computador por parte de la gerencia, para verificar si los mismos son razonables y detectar cualquier error de procesamiento.

3.2.4.2 Controles compensatorios e importancia de las debilidades

Esta es una de las áreas de control relativas al ambiente de microcomputador más importantes en cualquier sistema. Si los controles del usuario no son eficaces, se tendrá que determinar si algún otro grupo, tal como un grupo independiente de control de datos, ejerce ese control. Si ése no es el caso, se deberá considerar la posibilidad de aumentar el alcance de los procedimientos de auditoría.

3.2.4.3 Posibles pruebas de cumplimiento

- Examine y ponga a prueba las conciliaciones realizadas por el cliente que los totales de salida con los totales de entrada y los datos acumulados.

- Realice una prueba de los agregados a los totales de salida y concilie con los registros contables.

- Seleccione actualizaciones de archivos y verifique la evidencia de los procedimientos

utilizados por el usuario.

- Seguir el rastro de los totales de control de los datos generados a través de los controles de programa a programa hasta los informes de actualización de archivo.

- Conciliar los totales de los informes de actualizaciones de archivo con los informes anteriores, (Controles de ciclo a ciclo).

- Conciliar la actualización de archivos del microcomputador con los controles manuales.

- Confirmar que los totales pendientes de items en suspenso fueron correctamente incluídos en las conciliaciones antes mencionadas.

- Conciliar los totales de los saldos de los listados del computador, con los informes de actualización de archivos.

- Conciliar los totales de los análisis e informes del computador, por ejemplo, análisis de antigüedad de cuentas a cobrar, con los informes de actualización de archivos.

- Conciliar los totales de salida relacionados entre sí en los casos en que más de un archivo sea actualizado, por ejemplo, archivos de ítems pendientes, archivos maestros e históricos.

- Confirme si el usuario examinó los informes de salida para verificar su razonabilidad y si se tomaron medidas inmediatas para responder a las consultas que surgieron.

- Verifique si son eficaces los procedimientos para asegurar la distribución de informes confidenciales únicamente entre las personas autorizadas.

- Verifique el cumplimiento de las políticas del cliente en materia de conservación de documentos de salida.

3 POR EL PROCESAMIENTO DE DATOS

3.3.1 Controles sobre la digitación de datos

Este control trata de garantizar que los datos son digitados en forma íntegra y exacta para transcribirlos de los

documentos de entrada a un medio apto para el ambiente de microcomputador.

La digitación de los datos representa el proceso de transferencia de datos de los documentos de entrada preparados manualmente a un formato aceptado por el microcomputador.

3.3.1.1 Procedimientos de control

- Instrucciones escritas especificando las exigencias de la digitación de datos para cada tipo de transacción de entrada.

- Instrucciones escritas incluyendo una muestra de todos los documentos de origen utilizados.

- La exigencia de realizar la verificación de los campos de entrada importantes. La verificación se realiza mediante una nueva digitación de los datos a fin de controlar la exactitud de la primera transcripción. Si existen diferencias entre el producto de una operación y el de la otra, el registro es rechazado y deberá ser reingresado. Es posible que los empleados pasen por tanto los procedimientos de verificación. La mejor forma de limitar este riesgo es mediante una

adecuada supervisión.

- Sellado o anulación de los documentos de origen, a fin de evitar que sean procesados dos veces.

- Registro de los documentos de origen recibidos.

- Supervisión del trabajo de digitación de datos.

- Acceso restringido a los documentos de origen.

- Uso de dígitos de verificación. El dígito de verificación es un dígito adicional, agregado a los diversos campos (tales como códigos de cuenta, etc.). Como parte del programa de validación de datos el computador ejecutará un cálculo basado en los otros dígitos del código, que deberá dar como resultado el dígito de control o verificación. Si uno de los dígitos del código controlado fue entrado erróneamente, el computador no conseguirá obtener el mismo resultado para el dígito de control y el programa rechazará por lo tanto la mayoría de los códigos de cuenta que no

sean válidos.

3.3.1.2 Controles compensatorios e importancia de las debilidades

La digitación de datos es un procedimiento mecánico necesario en la mayoría de los ciclos de procesamiento de datos. Sin embargo, ésta no constituye con frecuencia el área de mayor preocupación para el auditor. Se puede decidir confiar, por ejemplo, en los controles generales del usuario y del procesamiento de datos sobre la integridad y exactitud del procesamiento de los mismos.

A la fecha, muchos clientes confían menos en los controles de digitación y más en los de validación de datos para garantizar la exactitud de la información entrada en el sistema.

Otro posible control compensatorio es el que requiere que el usuario verifique visualmente la información antes del procesamiento. Los datos son entrados y aparecen en la pantalla de una terminal o en un listado, pero no ser procesados hasta que el operador de la terminal confirme al computador que los mismos fueron ingresados correctamente.

3.3.1.3 Posibles pruebas de cumplimiento

- Examine las instrucciones escritas y determine si las mismas son adecuadas y están actualizadas.

- Observe los procedimientos para la anulación de los documentos de entrada; verifique si los mismos son anulados (por ejemplo, sellados) inmediatamente después de la digitación de los datos.

- Seleccione documentos, escogidos entre los ya procesados durante el período examinado, y verifique si fueron anulados y si existe evidencia de verificación de la digitación de datos.

3.3.2 Items en suspenso

Los controles del procesamiento de datos sobre los items en suspenso, garantizan que todos los datos en suspenso han sido correctamente identificados y se encuentran pendientes a la espera de solución.

3.3.2.1 Procedimientos de control

- Controles programados para garantizar el apareo de los registros en suspenso con los registros maestros, en ciclos de procesamiento posterior y eliminación del archivo de partidas en suspenso de todos los items apareados.

- Impresión de un listado de todos los movimientos, tanto de entrada como de salida, de los registros de items en suspenso, a fin de dejar una evidencia de auditoría perfectamente definida. Los movimientos realizados por medios manuales y aquellos generados por el computador deber ser llevados en forma separada, tanto en los archivos de datos como en los listados.

- Controles de actualización, a fin de garantizar que los totales de control iniciales y finales podrán ser conciliados.

- Informes de excepción emitidos en forma regular, señalando los items con valores altos o muy antiguos.

- Análisis regulares de antigüedad de todos los items pendientes.

- Utilización de programas de consulta para realizar un listado de todos los items en suspenso pendientes tanto en forma total como parcial, cada vez que sea solicitado.

3.3.2.2 Controles compensatorios e importancia de las debilidades

En teoría, un control compensatorio eficaz sería la inspección de todos los items en suspenso de los listados de computador después de cada actualización del archivo. Sin embargo, si ese control no fue debidamente incorporado en los programas de computador, se podrá no estar en condiciones de confiar en la integridad y exactitud de los listados en sí mismos y se necesita utilizar técnicas para seleccionar determinados items, a fin de efectuar la pruebas correspondientes.

Los controles del usuario sobre la entrada, modificación de datos fijos y salida, pueden a veces compensar la falta de controles adecuados incorporados en el programa referentes a los items en suspenso. Si los usuarios concilian los datos

de entrada y los totales de control de salida será muy difícil que cualquier transacción importante, erróneamente incluída en el archivo de items en suspenso, pueda pasar inadvertida. Se debe considerar la oportunidad de los controles compensatorios del usuario, a fin de poder tener la seguridad de que los items en suspenso fueron posteriormente incluídos en los registros del período contable correspondiente.

3.3.2.3 Posibles pruebas de cumplimiento

- Examine y ponga a prueba las conciliaciones del cliente de los movimientos de ingreso y egreso en los registros de items en suspenso.

- Verifique el cumplimiento por parte del cliente de los procedimientos relativos al examen y seguimiento de los items en suspenso, incluyendo aquellos de valor anormalmente alto o de mayor antigüedad.

- Obtenga el listado preparado por el cliente de todos los items en suspenso pendientes, seleccione algunos de ellos y efectúe el seguimiento de los mismos hasta el registro de las transacciones corregidas y su eliminación

del archivo de items en suspenso.

3.3.3 Controles por el procesamiento de datos sobre el procesamiento

Los controles de procesamiento para balancear los archivos de transacciones y maestros, asegura que toda la información que fue procesada contra los archivos de datos son correctos y detecta si los archivos no están balanceados.

Los controles de conciliación del archivo sirven para garantizar la exactitud de los resultados del procesamiento de datos. Los totales de control son establecidos por un programa y transferidos a un registro de control dentro del archivo de datos. Estos controles son luego verificados por los programas siguientes a fin de garantizar que toda la información correspondiente es correctamente procesada a través de todo el ciclo de procesamiento.

Los controles de conciliación normalmente incluirán verificaciones del rótulo de encabezamiento y del registro de control.

- **El rótulo de encabezamiento** es un registro al comienzo del archivo que contiene, generalmente, el nombre del programa que lo creó, el número de generación del

archivo, la fecha de su creación y la fecha de vencimiento (la fecha en que el archivo puede ser borrado o eliminado mediante la grabación de otro en su lugar).

- El registro de control generalmente contiene el número total de registros y el valor de los mismos y de los totales de control del archivo. Podrá también existir un registro de cierre, al final del archivo, que contendrá una señal de fin del mismo y el número de registros incluidos en el archivo.

Los controles de rótulo de encabezamiento y de registro de cierre son efectuados normalmente por el software del sistema.

Si bien estos procedimientos de control son realizados por el propio computador, es importante que el usuario o el grupo de control de datos también efectúe una verificación de los totales de control acumulados contra los totales calculados manualmente.

3.3.3.1 Procedimientos de control

- Los controles de balanceo, son incorporados en el programa para verificar que:

  -- El saldo de apertura del ciclo actual de

procesamiento es igual al saldo de cierre del ciclo anterior (controles de ciclo a ciclo o de programa a programa).

-- El saldo de apertura más el total de las transacciones procesadas es igual al saldo de cierre del ciclo actual (controles de actualización de archivos).

-- El saldo al final del primer programa o etapa de procesamiento dentro del ciclo actual es igual al saldo de apertura más las transacciones procesada en la primera etapa del procesamiento y así sucesivamente a través de cada etapa siguiente del sistema (controles de programa a programa).

- El total de los saldos individuales por registro, después de la actualización, es igual al saldo neto en el registro de control del archivo (controles de lectura y acumulación).

- Controles de rótulo de encabezamiento, mediante los cuales el programa que realiza la lectura del archivo verifica si se ha

utilizado el archivo correcto comparando el nombre del archivo, del programa y la fecha de su creación con los datos suministrados por el sector que preparó el trabajo dentro del departamento de procesamiento de datos.

- Registro de control o controles del registro de cierre, mediante el cual el programa que efectúa la lectura o procesamiento del archivo calcula en forma independiente, el número de registros contenidos en el archivo y su valor. Estos totales son comparados con los registros de control o de cierre, para garantizar que el archivo fue correctamente procesado en su totalidad.

- Indicación de los procedimientos a seguir para el caso en que los totales de control no puedan ser balanceados. Estos procedimientos pueden incluir:

  -- Interrupción inmediata del procesamiento.

  -- Informe al usuario sobre la discrepancias a fin de que pueda investigar las causas de esa situación mientras continúa el procesamiento.

3.3.3.2 Controles compensatorios e importancia de las debilidades

Si no existen registros de control de archivo, el número total de las transacciones y sus respectivos valores deberán ser comunicados al final de cada actualización, de modo que se pueda realizar la conciliación manual de los mismos. Si el cliente no cuenta con controles para balancear archivos podrá llegar a ser necesario que se aumente el alcance de los procedimientos de auditoría.

3.3.3.3 Posibles pruebas de cumplimiento

- Examinar los listados de salida a fin de obtener evidencia sobre la ejecución de los controles incorporados en el programa.

- En caso que existan errores de balanceo, determinar si fueron seguidos los procedimientos del cliente para balancear archivos.

CAPITULO IV

EL EFECTO FINANCIERO DE LA REALIZACION DE UNA AUDITORIA EN UN AMBIENTE DE MICROCOMPUTADORES Y LOS RIESGOS CORRESPONDIENTES

4.1 ESTUDIO Y EVALUACION PARA REALIZAR LA AUDITORIA EN AMBIENTE DE MICROCOPUTADORES

El estudio y evaluación orientado a la auditoría en un ambiente de microcomputadores, representa la posibilidad que el Contador Público y Auditor pueda formarse o presentar una opinión falsa o incorrecta acerca de la información financiera, la cual podría contener errores considerados importantes.

En tal sentido el Contador Público y Auditor debe de estudiar y evaluar las evidencias comprobatorias vinculadas con las afirmaciones contenidas en los estados financieros, con el objeto primordial de formarse una opinión acerca de la razonabilidad de los estados financieros. Para tal efecto, aplica procedimientos diseñados para obtener certeza razonable que los estados financieros han sido determinados adecuadamente en todos sus aspectos principales e importantes, no obstante, siempre ha de existir un riesgo indescartable de faltas de importancia que no sean descubiertas, debido principalmente a la naturaleza y extensión de las pruebas y limitaciones vinculadas con el sistema de control interno.

El Contador Público y Auditor puede disminuir en cierto grado riesgo, al implementar sus pruebas y procedimientos de itoría, siempre y cuando se tenga indicios o sospechas de la stencia de alguna falla o error importante.

El aspecto considerado por el Contador Público y Auditor en la neación, en cuanto al riesgo, es el tomar en cuenta todos los ectos y características propias de la entidad al realizar el n general de auditoría, vinculado directamente el alcance y ección que se espera obtener, incluyendo la estimación de eles de importancia para efectos de auditoría.

De acuerdo con lo anterior se puede indicar, que para el tador Público y Auditor siempre existirá un riesgo, y éste se culará con la posibilidad que una declaración incorrecta de ortancia de una o varias aseveraciones de los estados ancieros, represente un error o irregularidad, que ividualmente o en conjunto con otros errores o irregularidades, voquen de manera importante distorsiones en los estados ancieros tomados en conjunto, sin que el Contador Público y itor pueda detectar al realizar su auditoría.

RIESGOS DE NO EFECTUAR LA AUDITORIA

4.2.1 Definición

Etimológicamente la palabra riesgo significa

proximidad a un daño. Estar una cosa expuesta a perderse o sujeta a peligro.

El riesgo en contabilidad puede derivarse de error, omisión, incertidumbre o fraude.

Los riesgos en auditoría son los que corre el Contador Público y Auditor cuando el sistema de contabilidad genera errores que el control interno deja pasar y los procedimientos de auditoría no los detectan y por lo tanto se tiene estados financieros sustancialmente erróneos.

La auditoría de estados financieros debe estar orientada a proporcionar una seguridad razonable de que los mismos no hayan sido preparados falsamente. El Contador Público y Auditor no puede garantizar que los estados financieros sean absolutamente correctos, pero tiene la responsabilidad de llevar a cabo una investigación adecuada a fin de detectar errores importantes, por medio de la evaluación del control interno, para minimizar los riesgos de auditoría.

Para evitar tales riesgos, el Contador Público y Auditor planea el trabajo de la auditoría, debe de determinar si es necesario dedicar más atención o hacer una labor de auditoría más amplia en ciertas áreas o rubros de acuerdo con las debilidades o fortalezas del control interno.

4.2.2 Clasificación de los riesgos de auditoría

De conformidad con la Norma No. 14 de Auditoría, emitida por el Instituto Guatemalteco de Contadores Públicos y Auditores, el riesgo de una declaración incorrecta importante en las aseveraciones de los estados financieros consiste en:

- Riesgo inherente,
- Riesgo de control, y
- Riesgo de detección.

4.2.2.1 Riesgo inherente

"El riesgo inherente representa la susceptibilidad de una aseveración o una declaración incorrecta material, en el supuesto de que no exista procedimientos y políticas de estructura de control interno relacionados."(3)

La probabilidad de que el saldo de una cuenta o clase de transacción contenga un error que podría ser importante es mayor para algunos saldos o clases de cuentas que para otras; por ejemplo; los

3) Instituto Guatemalteco de Contadores Públicos y Auditores, Norma de Auditoría No.23, Página. 24

cálculos complejos, tienen mayor probabilidad de ser valuados incorrectamente que los cálculos sencillo, el efectivo es más susceptible a robo que los activos que conforman la propiedad, planta y equipo, las estimaciones contables ofrecen mayores riesgos que los registros basados en hechos reales.

4.2.2.2 Riesgos de control

"El riesgo de que una declaración incorrecta importante que pudiera ocurrir en una afirmación, no se evitara, ni se detectara oportunamente por medio de los procedimientos o políticas de la estructura de control interno de una entidad."(4)

Esta clase de riesgo va a estar determinado por el grado de efectividad que presentan los procedimientos de control establecidos por la estructura de control interno. El Contador Público y Auditor utiliza su criterio profesional para determinar el riesgo de control al estudiar y evaluar los procedimientos de control interno relacionados con el saldo de una cuenta o clase de

(4) Instituto Americano de Contadores Públicos (AICPA), Declaración de Normas de Auditoría No. 55 SAS 55, Evaluación de la Estructura de Control Interno, Abril de 1988 Página No. 78

transacción. Le sirve de base para establecer el riesgo de control las debilidades y fortalezas que presenta la estructura de control interno.

4.2.2.3 Riesgo de detección

"El riesgo de detección es aquel en que el auditor al planificar y aplicar sus procedimientos no detecte una declaración incorrecta importante en los estados financieros."(5)

El riesgo de detección está determinado por la efectividad de los procedimientos de auditoría y de su aplicación. El Contador Publico y Auditor podría en un momento determinado seleccionar un procedimiento de auditoría inadecuado, aplicar incorrectamente un procedimiento adecuado o bien malinterpretar los resultados de la auditoría. Este riesgo se reduce a través de una adecuada planeación y supervisión de la auditoría.

El riesgo inherente y el riesgo de control difieren del de detección, en que los primeros existen en forma independiente de la auditoría de

5 Instituto Guatemalteco de Contadores Públicos y Auditores, Ibid., Página. 49

los estados financieros, mientras que este último relaciona con los procedimientos del Contador Público y Auditor y puede ser modificado a su elección. El riesgo de detección debe mantener una relación inversa con el riesgo inherente y de control.

Entre menor sea el grado de riesgo inherente y de control que el Contador Público y Auditor cree que existe, mayor será el grado de riesgo de detección que pueda aceptar. Por lo contrario entre mayor es el riesgo inherente y de control que el Contador Público y Auditor cree que hay, menos es la posibilidad de que acepte el riesgo de detección.

Estos componentes de riesgo en auditoría pueden determinarse en términos cuantitativos tales como porcentajes, o en términos no cuantitativos que van por ejemplo, desde un mínimo hasta un máximo.

4.2.3 Evaluación del riesgo en auditoría

La evaluación del riesgo de control es un proceso que consiste en evaluar la efectividad de los procedimientos y políticas de la estructura del control interno de una

entidad, para evitar o detectar las declaraciones incorrectas importantes contenidas en los estados financieros. El riesgo de control se evalúa a nivel máximo cuando se determina la mayor probabilidad de una declaración incorrecta importante que pudiese ocurrir en una aseveración de los estados financieros, no se evitará, ni se detectará, oportunamente por medio de la estructura de control interno de una entidad. El Contador Público y Auditor evalúa a nivel máximo el riesgo de control cuando considera que los procedimientos y políticas no sean adecuadas o porque resultaría impráctico evaluar su efectividad.

Los procedimientos dirigidos a comprobar la efectividad del diseño y operación de un procedimiento o política de una estructura de control interno se denominan pruebas de controles. Cuando estas pruebas de controles se dirigen a comprobar la efectividad del diseño de un procedimiento o políticas de la estructura de control interno, se dirigen a establecer que éstos estén debidamente diseñados, para evitar o detectar las declaraciones incorrectas importantes en las aseveraciones de los estados financieros.

Las pruebas de control consisten en averiguaciones con el personal apropiado de la entidad, inspección de los documentos e informes, observación de la aplicación de los procedimientos o políticas y la ejecución de éstos por parte del mismo Contador Público y Auditor.

El nivel evaluado del riesgo de control, deberá ser documentado por el Contador Público y Auditor; la naturaleza y alcance de la documentación, se ven influenciados por el nivel evaluado de riesgo de control, la naturaleza de la estructura de control interno de la entidad y la naturaleza de la documentación de la entidad sobre su estructura de control interno.

El objetivo de las pruebas de los controles es el de proporcionar al Contador Público y Auditor la evidencia comprobatoria para usar la evaluación del riesgo de control.

Cuando el Contador Público y Auditor evalúa el riesgo de control por debajo del nivel máximo debe obtener la evidencia comprobatoria suficiente para apoyar el nivel evaluado. La evidencia comprobatoria suficiente para apoyar un nivel evaluado de riesgo de control específico es asunto de juicio profesional.

Por lo general la evidencia comprobatoria sobre la efectividad del diseño y operación de los procedimientos y políticas obtenidas directamente por el Contador Público y Auditor, por ejemplo a través de la observación, proporcionará mas seguridad que la obtenida indirectamente por entrevistas, indagación, o por suposición.

Cuando varios tipos de evidencia comprobatoria apoyan la

misma conclusión acerca del diseño y operación de un procedimiento política de la estructura de control interno, se aumenta el grado de seguridad. Por el contrario si varios tipos de evidencia comprobatoria conducen a diferentes conclusiones acerca del diseño y operación de un procedimiento o política de la estructura de control interno, se disminuye el grado de seguridad.

4.2.4 Análisis del riesgo general

El análisis del riesgo general constituye una revisión global sobre el tipo de negocios, basados en un conocimiento de industria en que opera la entidad, la organización de la misma, la naturaleza de su sistema contable y los problemas típicos del negocio.

El propósito de este análisis es el desarrollo de un plan para la auditoría. El análisis del riesgo general incluye:

- Identificación y evaluación de variables esenciales;

- Revisión preliminar;

- Revisión de la función de planteamiento financiero y de control; y

- Identificación de los ciclos del negocio y sus respectivos flujos de transacciones.

La planeación de la auditoría debe contemplar desde su inicio el conocimiento de las variables esenciales de una entidad; tales como: el prestigio de la entidad, de sus dirigentes y personal clave, los principios y políticas contables adoptadas por la entidad en relación con otras entidades que se dediquen a la misma actividad económica, los cambios ocurridos durante el año corriente en sistemas, personal y otros elementos de la entidad, las tendencias económicas en el tipo de negocios, etc.

La revisiones preliminares permiten al Contador Público y Auditor conocer con anticipación deficiencias y problemas que podrían afectar significativamente la situación financiera de una entidad y proponer las recomendaciones antes de que concluya el período de operaciones de la entidad.

La comprensión de la función de planteamiento financiero y de control permitirá al Contador Público y Auditor conocer la actividad económica que realiza la entidad, sus planes a corto y largo plazo, las técnicas específicas de control que utiliza la entidad, las políticas generales de la administración, la filosofía de la entidad.

El Contador Público y Auditor deberá identificar los

distintos ciclos de transacciones que operan en una entidad; por ejemplo, el ciclo de ventas, cuentas por cobrar e ingresos, compras, cuentas por pagar y egresos, inventarios-costos, nóminas, etc.

4.2.5 Análisis del riesgo específico

Dentro de la planeación de una auditoría se encuentra el análisis del riesgo específico, este incluye:

- La evaluación del nivel en que la estructura del control interno de la entidad alcance los objetivos de control;

- La medición de los riesgos cuando un objeto no es alcanzado o sólo es parcialmente alcanzado; y,

- Diseño de pruebas de cumplimiento y sustantivas balanceadas.

RESULTADO DEL ESTUDIO Y EVALUACION

El Contador Público y Auditor debe evaluar la efectividad de procedimientos y políticas de control que existen en la ructura de control interno de cada entidad y su relación con el cesamiento electrónico de datos.

El Contador Público y Auditor debe evaluar la estructura organizativa que presenta cada departamento de PED en las distintas entidades, para determinar el grado de separación de funciones que existe dentro del centro de PED y los usuarios. También debe evaluar la documentación con que cuenta el sistema en cada aplicación importante del PED. Debe determinar si la documentación es suficiente y apropiada a cada sistema.

Otro control que se debe evaluar dentro de los controles generales de los centros de PED, son las restricciones que deben existir en cuanto el acceso de las personas a los centros de PED. Debe evaluar el cumplimiento de rastro de control para tener la confianza de que personas ajenas al centro de PED no tengan acceso a los archivos de datos, programas o al equipo de PED.

El Contador Público y Auditor al evaluar los controles que se hayan implementado dentro de las aplicaciones del PED, para la entrada, procesamiento y salida de datos. Es muy importante que se establezca si los controles existentes en los sistemas, dan seguridad de que las transacciones se estén realizando de acuerdo con la autorización específica o general de la administración en la consecución de los objetivos de cada entidad.

Cuando se prestan implementaciones del nuevos sistemas o modificaciones a los ya existentes, el Contador Público y Auditor deberá evaluar si los procedimientos que se siguieron en la entidad en cuanto al diseño, prueba, aprobación e implementación del nuevo

istema son adecuados. Debe establecer el grado de participación e los departamentos usuarios en el desarrollo e implementación del uevo sistema.

EL Contador Público y Auditor deberá evaluar el riesgo de ontrol a un nivel máximo cuando existe una alta probabilidad de eficiencia de control en los centros de PED y que tenga incidencia ignificativa en los estados financieros de la entidad.

El nivel evaluado de control deberá ser documentado por el ontador Público y Auditor en los papeles de trabajo. También el ontador Público y Auditor podrá evaluar el riesgo de control por ebajo del máximo, en este caso deberá de identificar todas quellas fortalezas de control que existen en los departamentos de ED, y deberá llevar a cabo pruebas de cumplimiento para atisfacerse de tales controles.

CAPITULO V

CONCLUSIONES

1.- El presente trabajo llega a concluir de una manera objetiva, que no existe confiabilidad en la información producida en una ambiente de microcomputadores por si mismo, o por los controles prescritos por la administración, si no existe el profesional calificado para verificar el cumplimiento de los controles.

2.- Los procedimientos de auditoría, aplicados al control del ambiente de microcomputadores, funcionan eficientemente si forman parte de un trabajo profesional y respaldado por la administración de la entidad.

3.- La seguridad en los controles en un ambiente de microcomputadores es factor determinante en la aplicación de los controles tanto en el software como el hardware. Requiriendo la participación dinámica de profesionales de la Contaduría Pública y Auditoría con especialización en ambientes de PED.

4.- En todas las operaciones que se realizan en un ambiente de microcomputadores existe el riesgo inherente, el Contador Público y Auditor deberá ampliar el alcance de sus pruebas sustantivas para satisfacerse de la razonabilidad de las operaciones.

CAPITULO VI

RECOMENDACIONES

1.- Debido a la falta de confiabilidad en la información producida en un ambiente de microcomputadores, se recomienda que las medidas de control a establecer deben ser evaluadas, propuestas y examinadas en la práctica por un Contador Público y Auditor, de preferencia con especialidad en PED.

2.- El Contador Público y Auditor debe participar directamente en la elaboración de los procedimientos de auditoría, aplicables al control del ambiente de microcomputadores, conjuntamente con la administración para velar por el adecuado funcionamiento y eficiencia del mismo.

3.- Se recomienda al Contador Público y Auditor, que en un ambiente de microcomputadores realice una adecuada planificación e implementación de controles y medidas de seguridad en los procesamiento, para reducir a un nivel razonable, la posibilidad de que ocurran errores o irregularidades de importancia que distorsionen la información y no pueda ser detectada y consecuentemente corregida de acuerdo con el control del ambiente de microcomputadores implementados.

4.- Se recomienda a las entidades que utilicen ambientes de microcomputadores, implementar un eficiente sistema de seguridad, que proteja sus programas, archivos y equipos. De lo contrario, de suscitarse cualquier siniestro en PED y no contar con las condiciones para restablecer los datos incluidos en él, ocasiona el riesgo de poder continuar a corto plazo con las operaciones de la entidad.

5.- Es necesario modificar el pensum de estudios de la carrera de Contador Público y Auditor de la Universidad de San Carlos de Guatemala e implementar otros cursos de Auditoría de PED, que tengan como objetivo proporcionar al estudiante conocimientos sobre el control interno en los sistemas de PED, procedimientos y técnicas a aplicar en la auditoría de sistemas computarizados y la especialización del Contador Público y Auditor en otros campos.

CAPITULO VII

BIBLIOGRAFIA

01. AREAS DE RIESGO EN EL PROCESAMIENTO ELECTRONICO DE DATOS EN LOS BANCOS Y Y LA FUNCION DE LA AUDITORIA INTERNA.
Walter Augusto Cabrera Hernández,
Universidad de San Carlos de Guatemala,
Julio de 1991.

02. AUDITORIA MODERNA,
Walter O. Kell & Richard E. Ziegler,
Compañía Editorial Continental,
3ra. emisión,
Mayo de 1988.

03. COMO CREAR, ORGANIZAR Y DESARROLLAR LA UNIDAD DE AUDITORIA DE SISTEMAS EN UNA AUDITORIA INTERNA.
Victor Hugo Mazariegos Estrada,
Universidad de San Carlos de Guatemala,
Mayo de 1990.

04. DESARROLLO DE LA AUDITORIA TECNICAS DE COMPUTADOR.
Julio Igor Luna Urizar,
Universidad de San Carlos de Guatemala,
Noviembre de 1990.

05. DICCIONARIO ENCICLOPEDICO LAROUSSE,
Ramón García-Pelayo y Gross,
Tercera edición,
Ediciones Larousse,
México, 1988.

06. DICCIONARIO ENCICLOPEDICO SOPENA,
Editorial Ramón Sopena, S.A.
Barcelona, España, 1986.

07. DICCIONARIO PARA CONTADORES,
Kohler,
Editorial Hispano Americana, S.A.
México, 1982.

08. EL CONTROL INTERNO Y LOS SISTEMAS DE CONTABILIDAD A TRAVES DE COMPUTADORES ELECTRONICOS,
Armando Leonardo García,
Universidad de San Carlos de Guatemala,
Octubre de 1981.

09. GUIA DE CONTROL INTERNO Y CEADISC,
KPMG América Latina,
Diciembre de 1988.

10. GUIAS INTERNACIONALES DE AUDITORIA Y SERVICIOS RELACIONADO GUIA # 15,
AUDITORIA EN UN AMBIENTE DE PED,
Emitidas por el Comité de Prácticas Internacionales de Auditoría de la Federación Internacional de Contadores, IFAC, Febrero de 1984.

11. GUIAS INTERNACIONALES DE AUDITORIA Y SERVICIOS RELACIONADO GUIA # 16,
TECNICAS DE AUDITORIA CON AYUDA DEL COMPUTADOR,
Emitidas por el Comité de Prácticas Internacionales de Auditoría de la Federación Internacional de Contadores, IFAC, Octubre de 1984.

12. GUIAS INTERNACIONALES DE AUDITORIA Y SERVICIOS RELACIONADO GUIA # 20,
LOS EFECTOS DE UN AMBIENTE DE PED EN EL ESTUDIO Y EVALUACION DEL SISTEMA DE CONTABILIDAD Y LOS CONTROLES INTERNOS RELATIVOS,
Emitidas por el Comité de Prácticas Internacionales de Auditoría de la Federación Internacional de Contadores, IFAC, Junio de 1985.

13. GUIAS INTERNACIONALES DE AUDITORIA Y SERVICIOS RELACIONADO SUPLEMENTO #1 A LA GUIA 20,
AMBIENTE DE PED MICROCOMPUTADORAS INDEPENDIENTES,
Emitidas por el Comité de Prácticas Internacionales de Auditoría de la Federación Internacional de Contadores, IFAC, Octubre de 1987.

14. INSTITUTO AMERICANO DE CONTADORES PUBLICOS
DECLARACIONES DE NORMAS DE AUDITORIA SAS No. 9.
EL EFECTO DE LA FUNCION DE AUDITORIA INTERNA EN EL ALCANCE DEL EXAMEN DEL AUDITOR INDEPENDIENTE.
1976.

15. INSTITUTO AMERICANO DE CONTADORES PUBLICOS
DECLARACIONES DE NORMAS DE AUDITORIA SAS No. 55,
EVALUACION DE LA ESTRUCTURA DE CONTROL INTERNO INDEPENDIENTE.
1988.

16. LOS RIESGOS EN LA AUDITORIA
EN LA INFORMACION CONTABLE
PROCESADA POR P.E.D.,
Efraín de Jesús Velásquez Vásquez,
Universidad de San Carlos de Guatemala,
Julio de 1993.

17. NORMAS DE AUDITORIA NO. 23,
Instituto Guatemalteco de Contadores
Públicos y Auditores. I.G.C.P.A.

18. PRONUNCIAMIENTOS SOBRE CONTABILIDAD
FINANCIERA,
Instituto Guatemalteco de Contadores
Públicos y Auditores. I.G.C.P.A.

19. RIESGOS DE CONTROL EN UN SISTEMA DE
PROCESAMIENTO DE ELECTRONICO DE DATOS DE
EMPRESA DE SERVICIOS DE DISTRIBUCION DE AGUA.
Martin Arturo Lira Romer,
Universidad de San Carlos de Guatemala.
Julio de 1993.

20. SISTEMAS DE INFORMACION
PARA LA ADMINISTRACION
James A. Senn,
Grupo Editorial Iberoamérica,
3ra. edición, 1990.

A N E X O

GLOSARIO

Este glosario no tiene la intención de ser un diccionario completo de todos los términos de procesamiento electrónico de datos comúnmente utilizados. No obstante, explica algunos de los términos técnicos mas importantes empleados en esta tesis.

Actualización en tiempo real. Sistema en línea que permite al usuario actualizar los archivos maestros en forma directa, mediante el ingreso de una transacción por ver. Se dice que este tipo de sistemas es "actualizado por transacción".

Administrador de banco de datos (ABD). Un funcionario de cierta jerarquía que trabaja en forma independiente tanto del departamento de usuarios como de los programadores, responsables por el diseño y administración de la base de datos.

Analista de sistemas. Una persona cuya función es la de estudiar una actividad a fin de determinar exactamente qué será necesario conseguir, la razón de esa actividad, y la forma, el lugar y el momento más adecuado para conseguirlo. En particular, el analista es responsable por la especificación del diseño de sistemas, en lo referente a los datos de entrada, archivo, procesamiento, salidas y controles.

Aplicación. Actividad específica que hace uso de un computador.

Archivo. Un conjunto organizado de datos.

Archivo (registro diario) de transacciones. Un archivo de computador en el cual los datos acumulados "en línea" durante el día son almacenados como paso previo a la actualización del archivo.

Archivo histórico. Archivo que contiene registros de transacciones o registro actualizados del archivo maestro correspondientes a un período anterior. Ayuda a proporcionar evidencia de auditoría.

Archivo maestro. Un archivo con información acumulada, tal como el mayor de cuentas por cobrar. Podrá incluir también datos fijos.

Base de datos. Un conjunto de datos utilizados por diversas aplicaciones.

Biblioteca. Lugar donde se almacenan las cintas y discos magnéticos a ser utilizados en el procesamiento electrónico de datos. Se usa también para definir un conjunto de ciertos tipos de datos en disco; por ejemplo, biblioteca de programas.

Biblioteca de producción. Es la biblioteca de programas y de instrucciones de control de trabajo que se utiliza para el procesamiento normal.

bliotecas de programas. Conjunto de programas para computadoras unidos en un archivo y clasificados mediante el uso de catálogo. drá incluir las bibliotecas de producción y de prueba.

blioteca de prueba. Una biblioteca que contiene instrucciones de ogramas y de control de trabajo de todos los sistemas en sarrollo o que están siendo modificados.

oqueo. Procedimiento de control incorporados en algunos sistemas manejo de base de datos que automáticamente evitan o detectan tuaciones en las cuales dos usuarios intentan tener acceso ultáneamente al mismo ítem de la base de datos.

dena de programas. Una serie de programas relacionados entre sí, ilizados secuencialmente.

rátula de control. Un documento que acompaña un lote de nsacciones de entrada, cuyo propósito es el de registrar los tales de control.

tálogo. Un índice o tabla del contenido de ítems o archivos nacenados por el computador. Cada instalación de computación por general tiene varios catálogos diferentes. Por ejemplo, para ogramas o para lenguajes de control de trabajo.

clo. El procesamiento de todos los programas de un sistema de licación, durante un período determinado. Por ejemplo, un stema de cuentas por pagar puede tener un ciclo diario de lidación y un ciclo semanal de actualización y emisión de cheques utorizaciones de pagos.

mpilador (traductor de lenguaje). Software de sistemas que duce las instrucciones de programas de un lenguaje de mputación a otro, normalmente de lenguaje fuente a lenguaje jeto.

municación de datos. Es el proceso de transmisión de datos de un to a otro mediante el uso de circuitos telefónicos, teletipos u o tipos de equipos electrónicos.

ntraseña. Código alfabético o numérico que representa la ntificación confidencial del operador. Se ingresa a través de terminal y es controlado por el ambiente de microcomputadores liante la utilización de una tabla apropiada, a fin de garantizar únicamente el personal debidamente autorizado podrá ejecutar funciones que hayan sido restringidas.

ntrol de actualización de archivos. Un procedimiento de control asegura que el saldo de control de entrada del archivo más las nsacciones procesadas es igual al saldo de cierre.

ntrol de ciclo a ciclo. Procedimiento de control ejecutado a fin garantizar que se procesé el archivo correcto. Verifica que el al de control transportado del ciclo anterior de procesamiento igual al total a transportar al ciclo actual.

Control de lectura y acumulación. Procedimiento de control que verifica que la suma de los registros individuales en el archivo al final del ciclo de procesamiento es igual al saldo total del registro de control de archivo.

Control de programa a programa. Procedimiento de control utilizado en los casos en que se usan varios programas en secuencia para el procesamiento de datos. El mismo verifica que los totales de control al final de un programa sean correctamente transportados al siguiente.

Control de registros diarios. Procedimiento de control mediante el cual el sistema de computación registra información específica durante el procesamiento para su posterior impresión y examen; por ejemplo, transacciones ingresadas, accesos a la biblioteca de programas y al archivo maestro.

Control de Validación. Una técnica de control utilizada para detectar datos de entrada inexactos, incompletos o sin sentido. En esta tesis, consistencia y validación son utilizados como sinónimos. Algunas personas utilizan el termino "consistencia" únicamente para definir controles de formato o estructura, y "validación" para control de valores, por ejemplo, códigos de cuentas válidas o valores razonables.

Controles de aplicación. Procedimiento de control interno relacionados con una aplicación específica.

Control por el procesamiento de datos. Controles de aplicación vigente en los ambientes de microcomputadores.

Control por el usuario. Controles de aplicación impuestos por el departamento operativo que utiliza los datos.

Controles generales. Controles que se relacionan con la función global del procesamiento de datos y no con una aplicación en particular; por ejemplo, controles sobre modificaciones de software y procedimientos de respaldo.

Cuenta de registro. La cantidad total de registro individuales incluidas en un archivo de datos.

Datos fijos. Información, tal como nombre dirección, que permanece relativamente sin alteración y que podrá ser utilizada durante el ciclo de procesamiento.

Datos generados. datos que fueron creados automáticamente por el sistema de computación basándose en datos previamente ingresados.

Digitación. El proceso de transferencia de los datos de los documentos de entrada preparados en forma manual a un medio legible por la máquina.

Equipo ("hardware"). Las diversas unidades físicas que componen el computador o ambiente de microcomputador.

upo de apoyo técnico. Un grupo de personas dentro del ambiente microcomputadores, responsable por el mantenimiento del software sistemas y el equipo.

em. Un dato que no puede ser procesado inmediatamente, neralmente porque no consiguió pasar el control de validación. sistema lo acepta y luego lo mantiene en un archivo o sección parada hasta su resolución.

nú. Lista de las opciones disponibles, representada en la ntalla de un terminal que sirve de guía para el usuario.

crocomputador. Por lo general se refiere a un computador lativamente pequeño y de bajo costo.

quete de software. Programas de computadores ya listos, ministrados por los fabricantes de equipos o por firmas pecializadas en software.

ograma utilitario. Parte del software de sistemas utilizado en nciones tales como clasificación, copia, reestructuración de chivos de datos.

nto control. Un punto predeterminado en programas de gran tensión donde el contenido de la memoria del computador es piado en un archivo de apoyo, para posibilitar el reinició del ocesamiento en caso de desperfecto técnicos.

gistro. Conjunto de campos de información relacionados con un emento de actividad; por ejemplo, un registro de existencias drá consistir de campos separados para el código de producto, scripción, ubicación y cantidad disponible en stock.

tulo de encabezamiento. Registro al comienzo del archivo de mputador que por lo general contiene el nombre del archivo, mbre del programa que lo creó, el numero de generación del chivo, la fecha de su creación.

stema en línea. Un sistema que permite que el usuario tenga ceso directo al archivo de datos mediante el uso de una terminal fin de realizar consultas, actualizaciones o ambas cosas a la z.

stema operativo. Programa que administra la ejecución de los abajos por el computador y que generalmente también incluyen la ignación de los recursos del sistema y sirven de enlace entre los ogramas de cada aplicación, bibliotecas de programas y archivos datos.

ftware. Los programas utilizados en un computador. Incluye el ftware de sistemas y los programas de aplicaciones.

pología. Estructura o arquitectura del sistema.