UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

MATERIAL DIDÁCTICO DE AUDITORÍA EN INFORMÁTICA

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TÍTULO DE :

LICENCIADO EN CONTADURÍA

P R E S E N T A :

JORGE HIDALGO ROSETE

ASESOR DE TESIS: LIC. Y C.P. JOSÉ A. ECHENIQUE GARCÍA

MÉXICO, D. F. **2003**

Facultad de Contaduría y Administración

AGRADECIMIENTOS

A Dios : por haberme permitido realizar como hijo, estudiante y padre y haber estado conmigo en los momentos más dichosos y difíciles de mi vida.

A mis padres Jorge y Celia : porque con su apoyo y esfuerzos pude lograr esta meta y tener la convicción de hacerlo.

A mis abuelos Fortunato y Clarita : porque ellos fincaron el camino sobre el cual hemos sido educados tres generaciones de mi familia.

A mis hermanos Marisela, Ana Lilia, Norma, Fortunato y Leticia : porque a lo largo de nuestra vida siempre nos hemos apoyado incondicionalmente en los momentos más difíciles.

A mis hijos Javier y Haydeé : porque con menos me han dado mucho más.

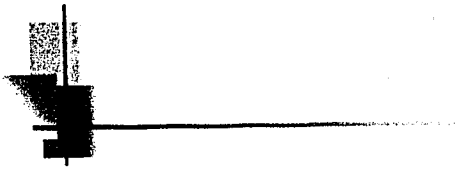
A mi esposa Sara : por su apoyo en esta importante etapa de mi preparación.

Al Profesor, Lic. y C.P. José A. Echenique García : por haber colaborado en la realización de este trabajo y porque su persona y calidad moral representan una síntesis de todos los buenos maestros que han dedicado su vida al servicio de la docencia.

***Gracias a Dios** por darme todo lo bueno que poseo y que después de 30 años pude al fin terminar.*

INDICE

C



INTRODUCCION

INTRODUCCION

El nuevo factor de la producción es la información, la cual sustituye hoy a los antiguos factores de producción para creación de la riqueza y también a recursos claves como son tierra, capital y trabajo.

El trabajo manual es sustituido por el intelectual y el poder en la sociedad, basado históricamente en la violencia (militar), la riqueza (económico) y el conocimiento, cada vez depende más de este último, por lo que el poder en la actualidad se encarna en la capacidad de almacenar, gestionar, distribuir y crear información.

El conocimiento y la información se convierten en el recurso estratégico y generador de cambios en la sociedad, de la misma manera que el capital y el trabajo lo fueron de la sociedad industrial. El día de hoy, el ámbito empresarial valora altamente la Sociedad de la Información, las Tecnologías de la Información y de la Comunicación como herramientas posibilitadoras del conocimiento, por lo que ya no se discute sobre la factibilidad y oportunidad de incorporarlas, sino sobre la forma de hacerlo lo más racional y eficazmente posible para la generación de procesos rentables y como parte de la estrategia de oportunidad de la empresa.

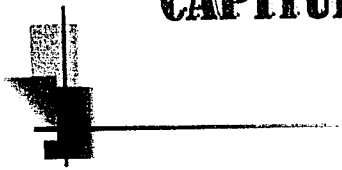
La Sociedad de la Información o denominada también del Conocimiento, alcanzará su plenitud cuando un porcentaje significativo de sus integrantes o miembros tenga acceso a cualquier tipo de información, en cualquier formato (voz, texto, gráficos, imágenes fijas y video), en cualquier momento y desde cualquier lugar. Adicionalmente a lo anterior, el escenario que deben enfrentar actualmente las empresas para ser eficientes, rentables y competitivas en el mercado moderno es el siguiente:

- *Internacionalización de las empresas.*
- *Globalización de los mercados.*
- *Aparición de nuevos competidores.*
- *Desarrollo de nuevas formas organizativas.*
- *Disminución de los ciclos de vida de productos y procesos.*
- *Implantación de nuevos modelos de negocios.*
- *Mayor complejidad de los problemas empresariales.*
- *Necesidad de reducir tiempos de desarrollo de nuevos productos.*
- *Mayor frecuencia en que se producen los cambios en el entorno empresarial.*
- *Creciente sofisticación de la demanda de productos generados.*
- *Mejoras en la atención del cliente enfocándose al servicio en lugar de al producto.*
- *Transformaciones políticas y económicas a escala mundial.*

La destreza de una organización para poder integrarse y enfrentar los cambios y requerimientos situacionales de las nuevas economías, depende fundamentalmente de sus Directivos, que no sólo precisan de ser magníficos gestores sino auténticos líderes que tienen la función de llevar a cabo esta tarea. Lo anterior no puede llevarse a cabo si no cuentan con información soportada por sistemas ágiles, oportunos, eficientes, seguros, confiables y costeables sobre los cuales deberán basarse sus decisiones.

De la explicación de los dos últimos párrafos, surge la necesidad de trasladar y ampliar la tradicional auditoría administrativa y financiera, a su nuevo ámbito de aplicación, la auditoría en informática, para determinar si la información o los medios a través de los cuales se almacena, procesa, transmite y desarrolla son susceptibles de sufrir alteraciones, pérdida o sustracción en agravio de los usuarios de la misma, así como de determinar si la construcción de los sistemas de información cumplen con los elementos básicos de eficiencia, eficacia y control interno.

CAPITULO I



FUNDAMENTOS DE AUDITORIA EN INFORMATICA

CAPÍTULO I. DIFERENCIAS ENTRE LAS AUDITORIAS

Inciso 1.

La teoría de la auditoría puede aplicarse al examen y evaluación de numerosos objetos. Para lo relacionado con esta exposición, solamente vamos a tener en cuenta los objetos auditables más comunes asociados con las organizaciones económicas.

En la práctica profesional, la auditoría se comporta, básicamente, como un estándar metodológico en donde el tipo de auditoría depende del objeto auditable. Esto significa que cuando se habla de auditoría financiera, lo que se hace es aplicar la metodología de la auditoría al examen y evaluación de los estados financieros de una determinada entidad. Lo mismo sucede cuando se hace, por ejemplo, auditoría tributaria, se aplica la metodología de la auditoría al examen del área de impuestos, con el objeto de establecer si se están interpretando y aplicando, en forma adecuada las normas tributarias. De esta manera surgen los diferentes tipos de auditoría, dependiendo de los distintos objetos auditables a los cuales se les aplique la metodología que tiene la auditoría para desarrollar el proceso de examen y evaluación correspondientes:

Auditoría fiscal. *Se encarga de verificar el correcto y oportuno pago de los diferentes impuestos y obligaciones fiscales de los contribuyentes desde el punto de vista fisco; Secretaría de Hacienda y Crédito Público, direcciones o tesorerías de hacienda estatales y tesorerías municipales. En este rubro recae también los organismos que imponen gravámenes a los contribuyentes como el I.M.S.S. e Instituto del Fondo Nacional para la Vivienda de los Trabajadores, etc.*

Auditoría interna. *Se refiere a dos puntos básicos principalmente:*

- *A).- Revisión total o parcial de estados financieros con objeto de expresar una opinión para efectos internos sobre los rubros o cuentas revisados.*
- *B).- Verificar, evaluar y proponer controles contables, financieros y de operación básicos.*

Auditoría operacional. *Su objetivo es la promoción de eficiencia de operación, comprendiendo el examen de la eficiencia obtenido en la asignación y utilización de los recursos financieros, humanos y materiales, mediante el análisis de la estructura organizacional, los sistemas de operación y los sistemas de información.*

Auditoría integral. *Se encarga de la revisión de los aspectos contable-financieros, operacionales y administrativos de la entidad sujeta a revisión en una misma asignación de auditoría*

Auditoría gubernamental. *Se refiere a la revisión de los aspectos financieros, operacionales, administrativos, de resultados de programas y de cumplimiento de disposiciones legales que enmarcan la actividad de las entidades públicas.*

Auditoría externa. *Esta auditoría es la practicada por contadores públicos independientes a la dependencia o entidad con objeto de emitir una opinión sobre la situación que guarda el área auditada.*

Auditoría de legalidad. *Este tipo de auditoría tiene como finalidad revisar si la dependencia o entidad, en el desarrollo de sus actividades, ha observado el cumplimiento de disposiciones legales que le sean aplicables (leyes, reglamentos, decretos, circulares, etc.).*

Auditoría financiera. *Esta modalidad de auditoría, tiene como objeto de estudio el sistema contable y los correspondientes estados financieros, con miras a emitir opinión independiente sobre la razonabilidad financiera mostrada en los estados financieros del ente auditado.*

Auditoría administrativa. *Este tipo de auditoría, tiene como objeto de estudio el proceso administrativo y las operaciones de las organizaciones, con miras a emitir opinión sobre la habilidad de la gerencia para manejar el proceso administrativo y el grado de economicidad, eficiencia y efectividad de las operaciones del ente auditado.*

Auditoría informática. *La auditoría informática tiene como objetivo de estudio las áreas de sistemas computarizados, sus sistemas de información automatizados, así como la tecnología de información utilizada, la plantilla del personal informático y nivel de conocimientos para desempeñar sus funciones y tiene como objetivo emitir una opinión independiente sobre la validez técnica del sistema de control interno informático, además del grado de confiabilidad de la información generada por el sistema auditado.*

Existen 4 acepciones de auditoría informática en la actualidad:

- *Auditoría Informática como soporte a la auditoría tradicional o financiera, etc.*
- *Auditoría Informática con el concepto anterior, pero añadiendo la función de auditoría para la gestión del entorno informático.*
- *Auditoría informática como función independiente, enfocada hacia la obtención de la situación actual de un entorno de información e informático en aspectos de seguridad y riesgo, eficiencia y veracidad e integridad.*
- *Las acepciones anteriores desde un punto de vista interno y externo.*
- *Auditoría como función de control dentro de un departamento de sistemas.*

Un profesional especializado en auditoría, debe también estarlo en los respectivos objetos auditables, esto quiere decir que, para hacer por ejemplo auditoría de impuestos, es ***necesario saber auditoría e impuestos,*** *ambos con amplia solvencia profesional, teniendo en cuenta que no se podrá evaluar una realidad que no se conoce y mucho menos emitir una opinión sobre aspectos técnicos de la misma.*

CAPÍTULO I. ANTECEDENTES DE LA AUDITORIA EN INFORMATICA

Inciso 2.

La introducción de las máquinas de proceso de datos en las empresas se produjo en los años 50, principalmente dedicadas a sustituir a los empleados en las tareas repetitivas para el cálculo de nóminas y facturas de clientes.

Dada su utilización como ''supercalculadoras'', con un volumen considerable de datos de entrada, y un volumen similar de datos de salida en función de los anteriores, el auditor se limitaba a verificar la corrección de los datos de salida frente a los datos de entrada, ignorando la lógica y funcionamiento interno de las máquinas de proceso de datos. Este tipo de auditoría se suele denominar "auditoría alrededor del computador", prácticamente era una auditoría convencional con un elemento "exótico" que producía información de distinta manera que los empleados de la empresa.

Esta situación se prolongó hasta mediados de la década de los 60, cuando las organizaciones de auditoría propugnaron un cambio en el enfoque, en base a los resultados de baja calidad obtenidos en las auditorías de las áreas que procesaban datos a través de computadores.

Este cambio consistía fundamentalmente en la adaptación de los criterios para la evaluación del ***control interno*** *en los sistemas organizativos, financieros y contables procesados en el centro de proceso de datos y concretamente en la sala del ordenador. Esta etapa se suele denominar "auditoría del computador".*

Con la introducción de nuevas tecnologías, como las comunicaciones entre computadores en tiempo real, pronto se detectaron las limitaciones del enfoque ya que se producían pérdidas progresivas de las pistas de auditoría y el auditor era incapaz de controlar determinadas actividades.

Así, a finales de los años 70, se llega a una tercera etapa: la ''auditoría a través del computador'', en este enfoque se estudia también el tratamiento lógico de la información a través de los programas y las aplicaciones que la procesan.

Posteriormente, a principios de los años 80, se empieza a aplicar técnicas de tratamiento de la información por medio de computadores como apoyo a la labor los auditores. El auditor de sistemas de información empieza también a contemplar el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia. Surge de modo la denominada ''auditoría con el computador''.

En la misma década se empieza a aplicar los principios básicos de la auditoría operativa a la auditoría de los sistemas de información, dando lugar a la "auditoría operativa de proceso de datos", que se centra principalmente en la eficiencia del tratamiento automático de los datos.

CAPÍTULO I. CONCEPTO DE AUDITORIA EN INFORMATICA

Inciso 3.

Se puede decir que auditoría en informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medios del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada torna de decisiones.

Es un proceso formal ejecutado por especialista de las áreas de auditoría e informática orientado a revisar e informar de lo siguiente:

- *Verificar y asegurar que las políticas y procedimientos establecidos para el uso adecuado de la tecnología informática en la organización, se lleven a cabo de una manera oportuna, racional y eficiente.*
- *Evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa.*
- *Asegurar que todos los recursos de informática operen en un ambiente de seguridad y control eficientes, para garantizar que la información que se procesa en el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.*
- *Evaluar que los recursos humanos, materiales, financieros, tecnológicos, etc. relacionados con la función informática, operan bajo un nivel altamente satisfactorio de confiabilidad, productividad y rentabilidad para la empresa.*

Los factores que pueden influir en una organización o empresa para llevar un adecuado control de sus recursos automatizados a través de la aplicación de la auditoría en informática son:

- *Necesidad de controlar el uso evolucionado de las computadoras.*
- *Controlar el uso de la computadora, que cada día se vuelve más importante y costosa.*
- *Los altos costos que producen los errores en una organización.*
- *Abuso en las computadoras.*
- *Posibilidad de pérdida de capacidades de procesamiento de datos.*
- *Posibilidad de decisiones incorrectas.*
- *Valor del hardware, software y personal.*
- *Necesidad de mantener la privacidad individual.*

- *Necesidad de mantener la privacidad de la organización.*

- *Posibilidad de pérdida de información o de mal uso de la misma.*

- *Toma de decisiones incorrectas.*

En el proceso de la información se deben detectar sus errores u omisiones y evitar su destrucción por causas naturales (temblores, inundaciones, etc.) o cualquier contingencia que pudiera suscitarse, por lo que la auditoría en informática contribuye a establecer los indicadores y sugerencias preventivos para estar preparados ante dichas contingencias.

La auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- *Objetivos de protección de activos e integridad de datos.*

- *Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.*

CAPÍTULO I. IMPORTANCIA DE LA AUDITORIA EN INFORMATICA

Inciso 4.

La información es un recurso necesario para la organización y para la continuidad de las operaciones, ya que provee de una imagen a su ambiente actual, su pasado y su futuro. Si la imagen de la organización es apropiada, ésta crecerá adaptándose a los cambios de su entorno.

En cuanto a la información, los siguientes conceptos han impactado y cambiado la perspectiva de los directivos de los más grandes organismos durante la década de los 90's e influenciado a ser tomados muy en cuenta en los lineamientos y objetivos definidos:

La información debe considerarse como uno de los principales recursos de la organización y por ello manejarse con la misma importancia que los financieros y humanos. La información y las herramientas de obtención, tratamiento y difusión deberán reflejarse en el balance de los activos empresariales. La información es patrimonio de la organización en su conjunto, no de las personas o de los departamentos encargados de su obtención o utilización. La gestión de la información requiere de una planificación a escala global de la empresa y no departamental.

Debe ser considerada igual de relevante la información que se presenta de manera formal que la de manera informal, la cuestión es determinar cuál es necesaria para realizar correctamente las actividades fundamentales de la organización.

Las tecnologías de información (TI) no deben ser consideradas siempre como instrumentos de reducción de costos ya que en la mayoría de los casos es muy costosa y mal empleada resulta más cara.

El principal objetivo del desarrollo de los sistemas de información debe ser el de satisfacer en todo momento las necesidades de la comunidad de usuarios.

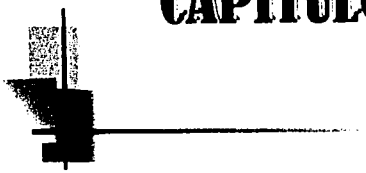
Actualmente se designa más esfuerzo y recursos a las tecnologías de información (TI) que al desarrollo y uso de los sistemas de información, situación que debe ser equilibrada.

La información se genera en la base de todas las actividades realizadas en la administración empresarial, y casi las tres cuartas partes del tiempo total de trabajo de los directivos, están dedicadas al procesamiento de dicha información; por ello resulta conveniente, diseñar sistemas para producirla, procesarla, gestionarla y hacerla llegar en el momento a los usuarios respectivos asegurando que sea confiable y exacta para tomar decisiones.

La toma de decisiones incorrectas con información errónea, proporcionada por los sistemas, trae como consecuencia efectos significativos, que afectan directamente a la organización.

Las conclusiones que se desprenden de los conceptos vertidos en este capítulo, nos dicen que el entorno informático, llámese áreas, productos y servicios generados en la entidad son de capital importancia para la organización además de invertirse un gran presupuesto para su desarrollo y mantenimiento, por lo que se debe cuidar que se cumplan adecuadamente los objetivos de efectividad, oportunidad y confianza en la información que genera, siendo estos los elementos que evalúa la auditoría informática para lograr la operatividad y toma de decisiones eficiente en la organización.

CAPITULO II



PRELIMINARES

CAPÍTULO II. VARIACION DEL OBJETO

Inciso 1.

Para dar inicio a este capítulo comenzaremos diciendo que las Técnicas de Auditoría son los métodos prácticos de investigación y prueba que el contador público utiliza para lograr la información y comprobación necesaria para poder emitir su opinión profesional — estas técnicas emanan del Boletín 5010 de Normas y Procedimientos de Auditoría elaborado por la Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos.

La utilización de la medios electrónicos informáticos o Tecnología de Información (TI), para dar apoyo a la ejecución de las Técnicas de Auditoría se denomina CAATs. Esta modalidad de llevar a cabo la auditoría permite ampliar la cobertura del examen, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente. Existen paquetes de computadora (software) que permiten elaborar auditorías a sistemas financieros y contables que se encuentran en medios informáticos.

En un excelente trabajo acometido por The Canadian Institute of Chartered Accountants, una institución de reconocido prestigio internacional se plantea la cuestión de cuáles son actualmente los "libros" o soporte de los documentos financieros objeto de la labor del auditor en un entorno informatizado y concluye que dichos libros están materializados en los archivos electrónicos, es decir los archivos creados y mantenidos en forma electrónica por las aplicaciones contables.

El objeto es distinto, está en un soporte diferente. El auditor financiero ve alterado el objeto de su actividad en el sentido de que se ha introducido la Tecnología de Información (TI), ahora está en soporte magnético y este cambio trae consecuencias de gran calado en cuanto a procedimientos de auditoría financiera.

Ha de cambiar sus procedimientos en función de las nuevas circunstancias y por tanto de la expansión de su alcance. La auditoría financiera sigue siendo auditoría y financiera con la diferencia de que en su objeto, el mismo de siempre, es decir en la información financiera, se ha introducido la Tecnología de Información (TI).

Se presenta la alternativa al auditor de utilizar los listados procedentes de los referidos archivos magnéticos como fuente de información o acceder directamente a los archivos electrónicos y proceder a su análisis de forma también electrónica. La situación se hace más dramática por el hecho cada vez más extendido de que el soporte documental de los apuntes electrónicos no exista en absoluto. El rastro de auditoría tradicional ha desaparecido.

Afortunadamente la propia (TI) que incide en los procedimientos que el auditor ha de aplicar, proporciona paralelamente medios de ejecutarlos de forma eficiente y directa. Las CAATS ponen a disposición del auditor una amplia variedad de herramientas que no sólo viabilizan los nuevos procedimientos sino que mejoran sensiblemente su aplicación y amplían la gama disponible.

Por tanto deducimos claramente que la introducción de la tecnología de información (TI), en los sistemas de información afecta a los auditores de una forma dual:

cambia el soporte del objeto de su actividad

- *posibilita la utilización de medios informatizados (CAATS) para la realización de sus procedimientos.*

De todo ello se desprende la nueva situación del auditor financiero: ha de aplicar procedimientos que utilizan técnicas asistidas por computador a un objeto consistente en un sistema de información basado en las nuevas Tecnologías de Información (TI).

CAPÍTULO II. CONCEPTO Y OBJETIVOS DEL CONTROL INTERNO

Inciso 2.

Concepto:

El Boletín E-02 del Instituto Mexicano de Contadores Públicos, señala respecto al control interno:

> *el estudio y evaluación del control interno se efectúa con el objeto de cumplir con la norma de ejecución del trabajo que requiere que: "El auditor debe efectuar un estudio y evaluación adecuado del control interno existente, que le sirva de base para determinar el grado de confianza que va a depositar en él y le permita determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría".*

El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración.

El conocimiento y evaluación del control interno deben permitir al auditor establecer una relación específica entre la calidad del control interno de la entidad y el alcance, oportunidad y naturaleza de las pruebas de auditoría. Por otra parte, el auditor deberá comunicar las debilidades o desviaciones al control interno del cliente que son definidas en este boletín como "situaciones a informar".

Definición y elementos de la estructura del control interno:

La estructura de control interno de una entidad consiste en las políticas y procedimientos establecidos para proporcionar una seguridad razonable de poder lograr los objetivos específicos de la entidad. Dicha estructura consiste de los siguientes elementos:

1. *El ambiente de control.*
2. *El sistema contable.*
3. *Los procedimientos de control.*

Control interno informático:

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la organización y/o la Dirección de Informática, así como los requerimientos legales

La misión del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable, sean correcta, válidas y seguras.

Objetivos básicos del control interno.

De lo anterior se desprende que los cuatro objetivos básicos del control interno son:

- *La protección de los activos de la empresa.*
- *La obtención de información financiera veraz, confiable y oportuna.*
- *La promoción de la eficiencia en la operación del negocio.*
- *Lograr que en la ejecución de las operaciones, se cumplan las políticas establecidas por los administradores de la empresa.*
- *Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.*

Se ha establecido que los dos primeros objetivos abarcan el aspecto de ***controles internos contables*** *y los tres últimos se refieren a* ***controles internos administrativos.***

Objetivos generales del control interno.

El control interno contable comprende el plan de organización y los procedimientos y registros que se refieren a la protección de los activos y a la confiabilidad de los registros financieros, por lo tanto, está diseñado en función de los objetivos de la organización para ofrecer seguridad razonable de que las operaciones se realizan de acuerdo con las normas y políticas señaladas por la administración.

Cuando hablamos de los objetivos de los controles contables internos podemos identificar dos niveles:

a).- Objetivos generales de control interno aplicables a todos los sistemas.

b).- Objetivos de control interno aplicables a ciclos de transacciones.

Los objetivos generales de control aplicables a todos los sistemas se desarrollan a partir de los objetivos básicos enumerados anteriormente y son más específicos, para facilitar su aplicación. Los objetivos de control de ciclos de transacciones se desarrollan a partir de los objetivos generales de control de sistemas, para que se apliquen a las diferentes clases de transacciones agrupadas en un ciclo.

Tipos de Control Interno Informático:

- ***Controles preventivos****: para tratar de evitar un hecho, como un software de seguridad que impida los accesos no autorizados al sistema.*
- ***Controles detectivos****: cuando fallan los preventivos para tratar de conocer cuanto antes el evento, el responsable y desde dónde está accesando, así como el registro de la actividad diaria para detectar errores u omisiones, etc.*
- ***Controles correctivos****: facilitan la vuelta a la normalidad cuando se ha producido incidencias; por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad.*

Técnicas de Auditoría Asistidas por Computadora:

Los procedimientos de auditoría con informática varían de acuerdo con la filosofía y técnica de cada organización y departamento de auditoría en particular. Sin embargo, existen ciertas técnicas y/o procedimientos que son compatibles en la mayoría de los ambientes de informática. Estas técnicas caen en dos categorías: métodos manuales y métodos asistidos por computadora.

Utilización de las técnicas de auditoría asistidas por computadora:

En general, el auditor debe utilizar la computadora en la ejecución de la audit¿ría, ya que esta herramienta permitirá ampliar la cobertura del examen, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente. Existen paquetes de computadora (software) que permiten elaborar auditorías a sistemas financieros y contables que se encuentran en medios informáticos. Además, el empleo de la computadora por el auditor le permite familiarizarse con la operación de] equipo en el centro de cómputo de la institución. Una computadora puede ser empleada por el auditor en:

- *Transmisión de información de la contabilidad de la organización a la computadora del auditor, para ser trabajada por éste, o bien acceso al sistema en red para que el auditor elabore las pruebas.*
- *Verificación de cifras totales y cálculos para comprobar la exactitud de los reportes de salida producidos por el departamento de informática, de la información enviada por medios de comunicación y de la información almacenada.*
- *Pruebas de los registros de los archivos para verificar la consistencia lógica, la validación de condiciones y la razonabilidad de los montos de las operaciones.*
- *Clasificación de datos y análisis de la ejecución de procedimientos.*
- *Selección e impresión de datos mediante técnicas de muestreo y confirmaciones.*
- *Llevar a cabo en forma independiente una simulación del proceso de transacciones para verificar la conexión y consistencia de los programas de computadora.*

Con fines de auditoría, el auditor interno puede emplear la computadora para:

- *Utilización de paquetes para auditoría; por ejemplo, paquetes provenientes del fabricante de equipos, firmas de contadores públicos o compañías de software.*
- *Supervisar la elaboración de programas que permitan el desarrollo de la auditoría interna.*

- *Utilización de programas de auditoría desarrollados por proveedores de equipo, que básicamente verifican la eficiencia en el empleo del computador o miden la eficiencia de los programas, su operación o ambas cosas.*

Todos los programas o paquetes empleados en la auditoría deben permanecer bajo estricto control del departamento de auditoría. Por esto, toda la documentación, material de pruebas, listados fuente, programas fuente y objeto, además de los cambios que se les hagan, serán responsabilidad del auditor.

En aquellas instalaciones que cuentan con bibliotecas de programas catalogados, los programas de auditoría pueden ser guardados utilizando contraseñas de protección, situación que sería aceptable en tanto se tenga el control de las instrucciones necesarias para la recuperación y ejecución de los programas desde la biblioteca donde están almacenados. Los programas desarrollados con objeto de hacer auditoría deben estar cuidadosamente documentados para definir sus propósitos y objetivos y asegurar una ejecución continua.

Cuando los programas de auditoría estén siendo procesados, los auditores internos deberán asegurarse de la integridad del procesamiento mediante controles adecuados como:

- *Mantener el control básico sobre los programas que se encuentren catalogados en el sistema y llevar a cabo protecciones apropiadas.*
- *Observar directamente el procesamiento de la aplicación de auditoría.*
- *Desarrollar programas independientes de control que monitoreen el procesamiento del programa de auditoría.*
- *Mantener el control sobre las especificaciones de los programas, documentación y comandos de control.*
- Controlar la integridad de los archivos que se están procesando y las salidas generadas.

La Informática como Herramienta de las Auditorías Operativa y Financiera:

No Resulta difícil justificar que las posibilidades del auditor utilizando medios electrónicos se amplía enormemente con respecto a trabajos manuales sobre listados en papel, el incremento en velocidad, eficiencia y seguridad es evidente.

Por todo ello el auditor puede valerse sustancialmente de las diversas herramientas informáticas que tiene a su disposición y que podríamos mencionar algunos de esos programas:

- ***Tratamiento de textos** -- utilizado generalmente en la práctica como una máquina de escribir superautomatizada para circulares, memorandums y reproducción de N número de copias de trabajos de oficina. Con una mayor especialización permite automatizar operaciones, generar documentos, relacionar documentos, etc.*
- ***Hoja de cálculo** – utilizada para efectuar cálculos, automatizar resultados de diferentes documentos numéricos y en algunos casos obtención de promedios, etc., así como generar actualizaciones automáticas, importar ficheros de otras aplicaciones y producir gráficos disponiendo de una amplia gama de fórmulas financieras y económicas, etc.*

- ***Generador de papeles de trabajo*** *-- fundados esencialmente en el tratamiento de textos de donde se obtienen plantillas, formatos, etc.; permite edición y actualización. Clasifica los documentos, por áreas, sectores, personal involucrado, etc.*

- ***Flowcharting*** *-- produce diagramas representativos de funciones realizadas o a realizar, flujo de documentos, etc.*

- ***Utilerías*** *-- existe una amplia gama que cubre desde comunicaciones, visualizadores de archivos, búsquedas o incluso rectificadores de archivos.*

- ***Administradores*** *-- efectúan el seguimiento administrativo de las auditorías, horas empleadas, áreas, control presupuestario, etc.*

- ***Auditores*** *-- permiten detectar accesos a los archivos de los sistemas, hora, terminal, tipo de acceso (consultas, modificaciones, etc.), usuario, etc.*

Programas de Revisión Analítica:

Normalmente se utiliza la hoja de cálculo para obtener, de los datos que habitualmente se le introducen (Balance, Cuentas de Pérdidas y Ganancias, etc.), promedios, proporciones o funciones que brindan una nueva visión comparativa de su contenido permitiendo observar las condiciones financieras en que se encuentra determinada organización.

Sistemas Expertos:

Las aplicaciones más avanzadas en cualquier campo son las conocidas como sistemas expertos, relativos a la también llamada inteligencia artificial. Se trata de usar el computador para que proporcione resultados o conclusiones producto del procesamiento de unos datos específicos en base a unos conocimientos preexistentes en el mismo.

Este sistema, además de en la auditoría informática, ya se ha utilizado en diversos campos, por ejemplo en la medicina para dar diagnósticos o tratamientos en base a los datos del paciente que se introducen en la aplicación.

En el campo de la auditoría operacional o administrativa, su utilización más evidente es en el análisis y evaluación del control interno. No ha sido hasta el momento una aplicación que se haya prodigado, posiblemente por la dificultad de completar una base de conocimientos adecuada que sólo los expertos pueden proporcionar. Se dice, como es costumbre, que las grandes empresas ya han desarrollado sistemas expertos que aplican en mayor o menor medida. Sin embargo, que se sepa, no se ha dado mucha publicidad al respecto.

Los fundamentos de un sistema experto, aplicando la misma filosofía establecida por las Normas Técnicas, consiste en crear unos cuestionarios cuya respuesta se "sí" o "no" para evitar respuestas diversas y confusas, divididos por áreas de actividad y que se parta de la base de que una totalidad de respuestas positivas implica un sistema excelente. Menos de un determinado número de respuestas, implicaría un control débil o muy débil.

Destacan entre sus ventajas, siempre bajo la supervisión del auditor; la objetividad del sistema, la utilización de fórmulas estadísticas, la cuantificación y especificación de pruebas de cumplimiento y sustantivas adecuadas, la actualización de la base de conocimiento con los nuevos sistemas analizados y el soporte legal que implica en caso de litigio.

Programas de Test Check:

Esta práctica, cada vez en menor uso, consiste en introducir en la aplicación que el auditado utilice, un conjunto de valores cuyo resultado se conoce. Estos valores se comparan con los que eventualmente proporcione la aplicación.

Programas Integradores:

Son aquellas aplicaciones que interrelacionan todas las demás para crear un entorno único que utiliza la totalidad de la información obtenida a través de las diferentes herramientas creando un sistema de auditoría.

Varias de las aplicaciones mencionadas proporcionan medios de programación o sin ser tan ambiciosos se manejan paramétricamente o lo que es lo mismo, a través de comandos brindando la posibilidad de realizar operaciones complejas de forma directa y cómoda.

Como ejemplo, el software ACL (Audit Computer Languaje) se ha diseñado para automatizar las pruebas de auditoría, el cual capta información de los archivos magnéticos de un computador, permitiendo revisar e interrogar los datos con la ayuda del mismo u otro computador; este software provee al auditor de una poderosa herramienta para acrecentar su eficiencia, ayudándole a reducir tiempos en la obtención de reportes , análisis, definición de criterios, estadísticas y más.

CAPÍTULO II. BENEFICIOS Y LIMITACIONES DE LA AUDITORIA EN INFORMATICA

Inciso 4.

La proliferación de la tecnología de información (TI) ha incrementado la demanda de control de los sistemas de información así como el control sobre la privacidad de la información y sobre los cambios de los sistemas. Además, hay una preocupación relevante sobre la caída de los sistemas que es la continuidad del servicio y sobre la seguridad de la continuidad del procesamiento de la información, en caso de que los sistemas se caigan. Otra área de preocupación es la proliferación de subsistemas incompatibles y el ineficiente uso de los recursos de sistemas.

El mayor estímulo para el desarrollo de la auditoría en informática dentro de la organización normalmente está dado por el abuso en el uso de las computadoras. El abuso en computadoras es cualquier incidente asociado con la tecnología en computación, en el cual la víctima sufra o pueda sufrir una pérdida y un daño hechos intencionalmente, por desconocimiento o para obtener una ganancia. El problema más serio está en los errores u omisiones que causan pérdidas a la organización.

El abuso tiene una importante influencia en el desarrollo de la auditoría en informática, ya que en la mayoría de las ocasiones el propio personal de la organización es el principal factor que puede provocar las pérdidas dentro de ésta, como por ejemplo la utilización del equipo en trabajos distintos a los de la organización, la obtención de información para fines personales (Internet) los juegos o pasatiempos y los robos hormiga.

Otros factores para llevar a cabo la auditoría informática es prever que el software se corrompa o destruya ya que pudiera ser posible que la organización no pueda continuar con sus operaciones si no se recupera rápidamente. Si la información es robada, se puede proporcionar información confidencial a la competencia.

Algunos de los principales problemas a observar en la auditoría en informática es el inadecuado sistema de control interno, la deficiente salvaguarda de los activos e integridad de los datos y la baja eficiencia de los sistemas automatizados.

El tipo y características del control interno dependerán de una serie de factores como por ejemplo, si se trata de un medio ambiente de microcomputadoras o macrocomputadoras, si están conectadas en serie o trabajan en forma individual, si se tiene internet o extranet, lo cual hace que la división de responsabilidades y la delegación de autoridad dificulten más el proceso de control interno.

Como se vé, la evaluación que se debe desarrollar para la realización de la auditoría en informática debe ser hecha por personas con un alto grado de conocimientos en informática y con mucha experiencia en el área a auditar.

CAPITULO III

METODOLOGIA GENERAL PARA LA AUDITORIA EN INFORMATICA

CAPÍTULO III. AUDITORIA ADMVA PARA EL AREA DE INFORMATICA

Inciso 1.

ANTECEDENTES DE LA AUDITORÍA ADMINISTRATIVA.

En 1962 se edita el libro "The Management Audit" (La Auditoría Administrativa) del ingeniero William P. Leonard, en los Estados Unidos, y es a partir de este hecho que los estudiosos e investigadores de esta rama de especialización de la auditoría consideran como el nacimiento formal y estructurado de la auditoría administrativa.

Leonard manifiesta en su libro que las estructuras administrativas siempre habrán de estar alerta permanente para recibir los cambios que se dan en los negocios, la economía, las políticas y disposiciones gubernamentales, y en la sociedad en general, para adecuar la administración a ellos. Impacto que se captará por medio de un ordenado y riguroso proceso de evaluación, que incluye la medición de la calidad de las decisiones, denominado auditoría administrativa.

La obra de Leonard abarca un repaso de los elementos básicos de la administración (planeación, organización, coordinación, dirección y control); evaluación de los métodos y eficiencia administrativa y ejecutiva, conceptos fundamentales de la auditoría administrativa; preparación, iniciación, recopilación, análisis e interpretación de información; y preparación, presentación y seguimiento del informe de auditoría administrativa.

ESTRUCTURA ORGANICA DEL AREA.

Evaluación:

Para lograr la evaluación de la estructura orgánica se deberá solicitar el manual de organización de la dirección de informática, el cual deberá comprender, como mínimo:

- *Organigrama con jerarquías.*
- *Funciones.*
- *Objetivos y políticas.*
- *Análisis, descripción y evaluación de puestos.*
- *Manual de procedimientos.*
- *Manual de normas.*
- *Instructivos de trabajo o guías de actividad*

También se deben solicitar:

- *Objetivos de la dirección.*
- *Políticas y normas de la dirección.*
- *Planeación.*

El director de informática y aquellas personas que tengan un cargo directivo deben llenar los cuestionarios sobre estructura orgánica, funciones, objetivos y políticas.

Básicamente, el departamento de informática puede estar dentro de alguno de estos tipos de dependencia:

A) Depende de alguna dirección o gerencia, la cual, normalmente, es la dirección de finanzas. Esto se debe a que inicialmente informática, o departamento de procesamiento electrónico de datos, nombre con que se le conocía, procesaba principalmente sistemas de tipo contable, financiero o administrativo; por ejemplo, la contabilidad, la nómina, ventas o facturación.

El que Informática dependa del usuario principal, normalmente se presenta en estructuras pequeñas o bien que inician en el área de informática.

La ventaja que tiene es que no se crea una estructura adicional para el área de informática y permite que el usuario principal tenga un mayor control sobre sus sistemas.

La desventaja principal es que los otros usuarios son considerados como secundarios y normalmente no se les da la importancia y prioridad requerida. Otra desventaja es que, como la información es poder, a veces hace que un área tenga un mayor poder. También, en ocasiones, sucede que el gerente o director del área usuaria del cual depende informática tiene muy poco conocimiento de informática; ello ocasiona que el jefe de informática cree una isla dentro de la gerencia y que acuerde directamente con otras gerencias usuarias, lo que da lugar a problemas con las líneas de autoridad. Este tipo de organización se usaba cuando comenzó el área de informática y en la actualidad sólo es recomendable para instalaciones muy pequeñas.

B) La segunda posibilidad es que la dirección de informática dependa de la gerencia general; esto puede ser en línea o bien en forma de asesoría.

La ventaja de alguna de estas organizaciones es que el director de informática podrá tener un nivel adecuado dentro de la organización, lo cual le permitirá lograr una mejor comunicación con los departamentos usuarios y por lo tanto, proporcionarles un mejor servicio y asignar las prioridades de acuerdo con los lineamientos dados por la gerencia general.

La desventaja es que aumentan los niveles de la organización, lo que elevará el costo de la utilización de los sistemas de cómputo.

C) La tercera posibilidad es para estructuras muy grandes, en las que hay bases de datos, redes o bien equipos en diferentes lugares.

En esta estructura se considera la administración corporativa. La dirección de informática depende de la gerencia general y existen departamentos de informática dentro de las demás gerencias, las cuales reciben todas las normas, políticas, procedimientos y estándares de la dirección de informática, aunque funcionalmente dependan de la gerencia a la cual están adscritas. La dirección de informática es la responsable de las políticas, normatividad y controles.

Las funciones, organización y políticas de los departamentos deben estar perfectamente definidas para evitar la duplicidad de mando y el que en dos lugares diferentes se estén desarrollando los mismos sistemas, o bien que sólo en un lugar se programe y no se permita usar los equipos para programar en otro lugar que no sea la dirección de informática. Esto se puede dar en instalaciones que tengan equipo

en varias ciudades o lugares y para evitarlo se deben tener bien definidas las políticas y funciones de todas las áreas.

La ventaja principal de esta organización consiste en que se puede tener centralizada la información (base de datos) y descentralizados los equipos; pero se debe tener una adecuada coordinación entre la dirección de informática y los departamentos de informática de las áreas usuarias para evitar duplicar esfuerzos o la duplicidad de mando.

En la actualidad, con la proliferación de computadoras personales y la creación de las redes tanto internas como externas, así como de bases de datos que son utilizadas por diferentes usuarios a diversas profundidades, este tipo de organización se puede considerar como la más recomendable. Lo que hay que tener muy claro es que en este tipo de organización el departamento de informática es el responsable de las normas y políticas de adquisición de equipo y de utilización del mismo.

Dentro de esta misma forma de organización se debe evaluar la posibilidad de tener una estructura por proyectos, lo cual permitirá que los diseñadores de los sistemas estén más cerca de las áreas usuarias. Esto se puede lograr mediante la creación de una fuerza de trabajo independiente, con todos los recursos, pero con la obligación de cumplir con los objetivos y metas señalados para un sistema dentro de los diferentes planes.

La respuesta a si un tipo de organización corporativa es la más conveniente y en qué grado está en función de la decisión sobre tener una organización centralizada o descentralizada.

La descentralización del procesamiento de la información ocurre en la actualidad como algo natural, debido al incremento de las minicomputadoras y a los sistemas en redes. Sin embargo, si se desea controlar el desarrollo, implementación y adquisición de equipos y de software, se deben tener políticas de descentralización muy bien definidas, para evitar la proliferación de equipo y de software que impida la adecuada comunicación y la adquisición de equipo no compatible y que dificulte la integridad de los datos, lo cual hace necesario que el personal sea entrenado en diferentes equipos, sistemas y plataformas.

D) La cuarta forma de organización es la creación de una compañía independiente que dé servicio de informática a la organización o bien de outsourcing.

Estructura orgánica:

Uno de los elementos más críticos es el relativo al personal y a su organización. Un personal calificado, motivado, entrenado y con la adecuada remuneración, repercute directamente en el buen desempeño del área de informática.

Funciones:

Las funciones en informática pueden diferir de un organismo a otro, aunque se designen con el mismo nombre; por ejemplo, la función del programador en una organización puede ser diferente en otra.

Objetivos:

Uno de los posibles problemas o descontentos que puede tener el personal, es el desconocimiento de los objetivos de la organización, lo cual puede deberse a una falta de definición de éstos, lo que provoca que no se pueda tener una planeación adecuada.

ANÁLISIS DE ORGANIZACIONES.

Entre las diferentes formas de la estructura organizacional de la dirección de informática no existe una evaluación concreta y aceptada de las funciones de ésta. Las funciones que en una organización son consideradas como de programador pueden ser de analista o de analista programador y en algunas se han dividido ciertas funciones con diferentes niveles, por ejemplo, programador I, programador II, etc.

Esto ha dado por resultado que, al no existir una definición clara de los niveles, funciones y conocimientos, las personas se designen con el título que ellos consideran pertinente; por ejemplo, ingeniero en sistemas (sin haber obtenido el grado), analista de sistemas o bien que en algunos países existan escuelas que confieran grados académicos que no son reconocidos oficialmente. Al analizar las organizaciones debemos tener muy en cuenta si están definidas las funciones y la forma de evaluar a las personas que ingresan a los diferentes niveles de la organización.

Si no existe un organigrama, el auditor debe elaborar uno que muestre el actual plan de organización, ya que esto facilita el estudio y proporciona una imagen general de la organización.

Criterios para analizar organigramas:

- *Agrupar funcione similares y relacionarlas entre sí.*
- *Agrupar funciones que sean compatibles.*
- *Localizar la actividad cerca de la función a la que sirva.*
- *Localizar la actividad cerca o dentro de la función mejor preparada para realizarla.*
- *No asignar la misma función a dos personas o entidades diferentes.*
- *Separar las funciones de control y aquellas que serán objeto del mismo.*
- *Ningún puesto debe tener dos o más líneas de dependencia jerárquica.*
- *El tramo de control no debe ser exagerado, ni muy numerosos los niveles jerárquicos.*

Cuando se estudia la estructura orgánica es importante hacer algunas anotaciones sobre las tareas asignadas a cada puesto y responder las siguientes preguntas:

- *¿Existen líneas de autoridad justificadas?*
- *¿Hay una extralimitación de funciones?*

- *¿Hay demasiada supervisión de funcionarios?*
- *¿Es excesiva la supervisión en general?*
- *¿Hay agrupamientos ilógicos en las unidades?*
- *¿Hay uniformidad en las asignaciones?*

EVALUACIÓN DE LOS RECURSOS HUMANOS.

El desarrollo del personal implica:

- *Establecer promociones y oportunidades de desarrollo.*
- *Educación y capacitación. Estas actividades mantienen la moral y las habilidades de los empleados en un nivel adecuado para cumplir con los objetivos y metas encomendadas y les permitirá tener mayor motivación y mejores remuneraciones. En el área de informática es muy importante la capacitación para tener actualizado a nuestro personal en una disciplina en la que puede quedarse rezagado muy rápidamente, aunque, por otro lado, debido: a la presión de tiempo con la que se trabaja, en muchas ocasiones no se le al personal la oportunidad para capacitarse.*

Se deberá obtener información sobre la situación del personal del área, para lo cual se puede utilizar la tabla de recursos humanos y la tabla de proyección de recursos humanos. A continuación un ejemplo de cuestionario para obtener información sobre los siguientes aspectos:

- *Desempeño y comportamiento.*
- *Condiciones de ambiente de trabajo.*
- *Organización en el trabajo.*
- *Desarrollo y motivación.*
- *Capacitación y supervisión.*

SITUACIÓN PRESUPUESTAL Y FINANCIERA.

Se obtendrá información presupuestal y financiera del departamento, así como del número de equipos y características para hacer un análisis de su situación desde un punto de vista económico. Entre esta información se encuentra:

- *Costos del departamento, desglosado por áreas y controles.*
- *Presupuesto del departamento, desglosado por áreas.*
- *Características de los equipos, número de ellos y contratos.*
- *Costos y presupuestos asignados a la adquisición y mantenimiento de éstos.*

CAPÍTULO III. INVESTIGACION PRELIMINAR

Inciso 2.

El primer paso en el desarrollo de la auditoria, es la revisión preliminar del área de informática. El objetivo de la revisión preliminar es el de obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoria. La revisión preliminar significa la recolección de evidencias por medio de entrevistas con el personal de la instalación, la observación de las actividades en la instalación y la revisión de la documentación preliminar.

La revisión preliminar elaborada por un auditor interno difiere de la realizada por el auditor externo en tres aspectos; en primer lugar, el auditor interno normalmente requiere de menos revisiones y trabajos, especialmente en la parte gerencial y de organización, ya que él es parte de la organización y está familiarizado con la misma. En segundo, el auditor externo se enfoca más en las causas de las pérdidas y en los controles necesarios para justificar sus decisiones. En tercero, si el auditor interno supone serias debilidades en los controles internos, en lugar de proceder directamente con las pruebas sustantivas, deberá continuar con la fase de revisión detallada para señalar recomendaciones para mejorar los controles internos.

Es necesario iniciar el trabajo de obtención de datos con un contacto preliminar que permita una primera idea global. El objeto de este primer contacto es percibir rápidamente las estructuras fundamentales y diferencias principales entre el organismo a auditar y otras organizaciones que se hayan investigado, además de obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoria. Al terminar la revisión preliminar, el auditor puede proceder en uno de los tres caminos siguientes:

- *Diseño de la auditoria. Puede haber problemas debido a la falta de competencia técnica para realizar la auditoria.*

- *Realizar una revisión detallada de los controles internos de los sistemas con la esperanza de que se deposite la confianza en los controles de los sistemas y de que una serie de pruebas sustantivas puedan reducir las consecuencias.*

- *Decidir el no confiar en los controles internos del sistema. Existen dos razones posibles para esta decisión. Primero, puede ser más eficiente desde el punto de vista de costo / beneficio el realizar pruebas sustantivas directamente. Segundo, los controles del área de informática pueden duplicar los controles existentes en el área del usuario. El auditor puede decidir que se obtendrá un mayor costo / beneficio al dar una mayor confianza a los controles de compensación y revisar y probar mejor estos controles.*

La investigación preliminar debe incorporar fases de evaluación del control gerencial y del control de las aplicaciones. Durante la revisión de los controles gerenciales el auditor debe entender a la organización, las políticas y prácticas gerenciales usadas en cada uno de los niveles, dentro de la jerarquía de la instalación en que se encuentran las computadoras. Durante la revisión de los controles de las aplicaciones, el auditor debe entender los controles ejercidos sobre el mayor tipo de transacciones que fluyen a través de los sistemas de aplicaciones más significativos dentro de la instalación de computadoras.

Se debe recopilar información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitudes de documentos; la finalidad es definir el objetivo y alcance del estudio, así como el programa detallado de la investigación.

Se deberá observar el estado general del departamento o área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

En el caso de la auditoría en informática debemos comenzar la investigación preliminar con una visita al organismo, al área de informática y a los equipos de cómputo y solicitar una serie de documentos. La investigación preliminar se debe hacer solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

- *Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud documentos para poder definir el objetivo y alcances del departamento.*
- *La eficiencia en el departamento de informática sólo se puede lograr si sus objetivos están integrados con los de la institución y si permanentemente se adapta a los posibles cambios de éstos.*

Para poder analizar y dimensionar la estructura a auditar se debe solicitar:

A nivel organización total:

- *Objetivos a corto y largo plazos.*
- *Manual de la organización.*
- *Antecedentes o historia del organismo.*
- *Políticas generales.*

A nivel del área de informática:

- *Objetivos a corto y largo plazo.*
- *Manual de organización del área que incluya puestos, funciones, niveles jerárquicos y tramos de mando.*
- *Manual de políticas, reglamentos internos y lineamientos generales.*
- *Número de personas y puestos en el área.*
- *Procedimientos administrativos del área.*
- *Presupuestos y costos del área.*

En el momento de hacer la planeación de la auditoría o bien en su realización, debemos evaluar que pueden presentarse las siguientes situaciones:

A).- Se solicita la información y se ve que:

- *No se tiene y se necesita.*
- *No se tiene y no se necesita.*

B).- Se tiene la información pero:

- *No se usa.*
- *Es incompleta.*
- *No está actualizada.*
- *No es la adecuada.*
- *Se usa, está actualizada, es la adecuada y está completa.*

Esta adaptación únicamente puede ser posible si los altos ejecutivos y los usuarios de los sistemas toman parte activa en las decisiones referentes a la dirección y utilización de los sistemas de información y si el responsable de dicho sistema constantemente consulta y pide asesoría y cooperación a los ejecutivos y usuarios.

CAPÍTULO III. PLANEACION DE LA AUDITORIA EN INFORMATICA

Inciso 3.

Para hacer una adecuada planeación de la auditoría en informática hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. Con ello podremos determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios.

Dentro de la auditoría en general, la planeación es uno de los pasos más importantes, ya que una inadecuada planeación provocará una serie de problemas que pueden impedir que se cumpla con la auditoría o bien hacer que no se efectúe con el profesionalismo que debe tener cualquier auditor.

El trabajo de auditoría deberá incluir la planeación de la auditoría, el examen y la valuación de la información, la comunicación de los resultados y el seguimiento.

La planeación deberá ser documentada e incluirá:

- *El establecimiento de los objetivos y el alcance del trabajo.*
- *La obtención de información de apoyo sobre las actividades que se auditarán.*
- *La determinación de los recursos necesarios para realizar la auditoría.*
- *El establecimiento de la comunicación necesaria con todos los que estarán involucrados en la auditoría.*
- *La realización, en la forma más apropiada, de una inspección física para familiarizarse con las actividades y controles a auditar, así como identificación de las áreas en las que se deberá hacer énfasis al realizar la auditoría y promover comentarios y la promoción de los auditados.*
- *La preparación por escrito del programa de auditoría.*
- *La determinación de cómo, cuándo y a quién se le comunicarán los resultados de la auditoría.*
- *La obtención de la aprobación del plan de trabajo de la auditoría.*

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de varios objetivos:

1. *Evaluación administrativa del área de procesos electrónicos.*
2. *Evaluación de los sistemas y procedimientos.*
3. *Evaluación de los equipos de cómputo.*

4. *Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (Software, hardware, redes, bases de datos, comunicaciones).*

5. *Seguridad y confidencialidad de la información.*

6. *Aspectos legales de los sistemas y de la información.*

Para lograr una adecuada planeación, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas y con base en esto planear el programa de trabajo, el cual deberá incluir tiempos, costos, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la auditoría.

El proceso de planeación comprende el establecer:

- *Metas.*
- *Programas de trabajo de auditoría.*
- *Planes de contratación de personal y presupuesto financiero. Informes de actividades.*

Las metas se deberán establecer de tal manera que se pueda lograr su cumplimiento, sobre la base de los planes específicos de operación y de los presupuestos, los que hasta donde sea posible, deberán ser cuantificables. Deberán acompañarse de los criterios para medirlas y de fechas límite para su logro.

Los programas de trabajo de auditoría deberán incluir: las actividades que se van a auditar, cuándo serán auditadas, el tiempo estimado requerido, tomando en consideración el alcance del trabajo de auditoría planeado y la naturaleza y extensión del trabajo de auditoría realizado por otros. Los programas de trabajo deberán ser lo suficientemente flexibles para cubrir demandas imprevistas.

CAPÍTULO III. AREAS A AUDITAR EN INFORMATICA

Inciso 4.

Para efectos de facilitar el desarrollo del proceso de auditoría operacional, al área informática se deben precisar con claridad las áreas auditables.

Análisis y evaluación de la organización:

Entre las diferentes formas de estructura organizacional de la dirección de Informática no existe una evaluación concreta y aceptada de las funciones de ésta. Esto ha dado por resultado que, al no existir una definición clara de los niveles, funciones y conocimientos, las personas se designen con el título que ellos consideren pertinente; por ejemplo, ingeniero de sistemas (sin haber obtenido el título), analista de sistemas, o bien que en algunos países existan escuelas que confieran grados académicos que no son reconocidos oficialmente. Al analizar las organizaciones debemos tener muy en cuenta si están definidas las funciones y la forma de evaluar a las personas que ingresan a la organización.

Si no existe un organigrama, el auditor debe elaborar uno que muestre el actual plan de organización, ya que esto facilita el estudio y proporciona una imagen general de la organización.

El criterio para analizar organigramas es el siguiente:

- *Agrupar funciones similares y relacionadas entre sí.*
- *Agrupar funciones que sean compatibles.*
- *Localizar la actividad cerca de la función a la que sirva.*
- *Localizar la actividad cerca o dentro de la función mejor preparada para realizarla.*
- *No asignar la misma función a dos personas o entidades diferentes.*
- *Separar las funciones de control y aquellas que serán objeto del mismo.*
- *Ningún puesto debe tener dos o más líneas de dependencia jerárquica.*
- *El tramo de control no debe ser exagerado, ni muy numerosos los niveles jerárquicos.*

Las empresas comienzan con soluciones informáticas, acordes con sus necesidades mas significativas y disponibilidad presupuestal. Después van evolucionando al ritmo del crecimiento de la entidad en cumplimiento de su objeto social, por ésta razón, no puede esperarse encontrar un modelo estándar de organización informática en todas las empresas.

Para desarrollar el proceso de auditoría informática, se parte de un modelo mínimo deseable de organización de un área informática integrada por las siguientes unidades funcionales :

- *Desarrollo de. Sistemas.*
- *Métodos y Procedimientos.*
- *Servicios de Procesamiento Electrónico de Datos.*
- *Investigación Informática.*

Para realizar la auditoría a cualquier área auditable de sistemas computarizados, se aplicarán todos los pasos que conforman la metodología de la auditoría general.

Por lo que respecta a los informes, puede presentarse uno por cada área auditada o integrarlos para presentar solamente uno por toda el área informática.

Evaluación de los Recursos Humanos:

El desarrollo del personal implica:

- *Establecer promociones y oportunidades de desarrollo.*
- *Educación y capacitación. Estas actividades mantienen la moral y las habilidades de los empleados en un nivel adecuado para cumplir con los objetivos y metas encomendadas y les permitirá tener mayor motivación y mejores remuneraciones. En el área de informática es muy importante la capacitación para tener actualizado a nuestro personal en una disciplina en la que puede quedarse rezagado muy rápidamente, aunque, por otro lado, debido a la presión del tiempo con la que se trabaja, en muchas ocasiones no se le da al personal la oportunidad para capacitarse.*

Se deberá obtener información sobre la situación del personal del área, para lo cual se puede utilizar la tabla de recursos humanos y la tabla de proyección de recursos humanos. A continuación un ejemplo de cuestionario para obtener información sobre los siguientes aspectos:

- *Desempeño y comportamiento.*
- *Condiciones de ambiente de trabajo.*
- *Organización en el trabajo.*
- *Desarrollo y motivación.*
- *Capacitación y supervisión.*

Auditoría al área de Desarrollo de Sistemas:

Con el objeto de facilitar la auditoría al área de desarrollo de sistemas, se dividen las aplicaciones de desarrollo en dos grandes grupos:

Aplicaciones de alto riesgo: son aplicaciones integrales que se interrelacionan con otros sistemas automatizados y/o pueden dar servicio en tiempo real a usuarios externos y/o proporcionan información al área de Contabilidad para generar sus reportes diarios de operación y/o estados de resultados.

Aplicaciones de bajo riesgo: son aplicaciones locales que generan información a áreas específicas de usuarios y la disponibilidad de su información no afecta, hasta cierto límite, a la operación de la organización pudiendo diferirse la generación de sus resultados por un cierto tiempo.

En el caso de las aplicaciones de alto riesgo, se aconseja la participación activa del auditor interno en cada una de las fases del ciclo de desarrollo de sistemas, evaluando detenida y oportunamente cada uno de los puntos claves de control, para asegurar que al final del desarrollo del proyecto se obtenga un sistema atendido, desde su origen, en todos los detalles de sus especificaciones técnicas, funcionales y de control.

Por lo que respecta a las aplicaciones de bajo riesgo, se considera suficiente auditar solamente el proceso de desarrollo de sistemas debido a que los datos no son de alto riesgo y además, porque resulta sumamente costoso dedicar personal de auditoría para atender el desarrollo de todas las aplicaciones en sus diferentes fases.

Conocimiento del área de Desarrollo de Sistemas:

A partir del organigrama específico de las unidades de desarrollo de sistemas y de los manuales de funciones y procedimientos, el auditor analizará la forma como está organizada el área, la actividad funcional, los estándares de trabajo, la capacidad del personal y cómo se ejerce la dirección, la supervisión y la operación, en términos generales, a manera de estudio preliminar.

Objetivos de la Auditoría en el departamento de Desarrollo de Sistemas:

1. *Verificar la existencia. de objetivos definidos, de acuerdo con las reales capacidades del área de desarrollo de sistemas y las necesidades de los usuarios.*

2. *Analizar la estructura organizacional del área a la luz de las soluciones de la administración moderna sobre la materia.*

3. *Examinar los manuales de funciones y de procedimientos del personal del área para establecer su efectividad y si están debidamente actualizados y documentados.*

4. *Evaluar el personal, del área, en la perspectiva de verificar la competencia para el desempeño de los respectivos cargos.*

5. *Examinar el sistema de información del área con el objeto de confirmar su efectividad.*

6. *Verificar si el personal trabaja con base en una metodología estándar válida para el desarrollo de sistemas.*

7. *Evaluar el trabajo del personal de desarrollo de sistemas con base en los parámetros de medición fundamentales de la auditoría operacional: economía, eficiencia y efectividad.*

8. *Verificar si las aplicaciones son convertidas al computador solamente si van a producir mayores beneficios que cualquier otra alternativa.*

9. *Evaluar el control de calidad que se practica a todas las actividades del Desarrollo de sistemas.*

Para llevar a cabo el proceso de desarrollo de sistemas se deben contemplar los siguientes pasos para establecer antecedentes y documentación de cada uno los sistemas:

***Existencia de una Metodología para el desarrollo de sistemas**: las organizaciones informáticas deben establecer una metodología, suficientemente documentada para facilitar el control del desarrollo de sistemas, además es necesario establecer un mecanismo que garantice la actualización permanente de esa metodología.*

Estudio Preliminar: *participación del departamento usuario para quien se va a desarrollar el sistema, con el objeto de asegurar el diseño que cumpla todas sus necesidades; integrar un equipo de trabajo coherente con la actividad de desarrollo y asignarle las responsabilidades y funciones correspondientes.*

Estudio de Factibilidad: *se tienen que observar varias alternativas de solución; preparar un estudio de factibilidad tecnológica y aplicativa del proyecto; preparar un estudio de factibilidad económica del proyecto, se debe aceptar la continuidad del proyecto después de la presentación de los dos estudios anteriores; se deberá elaborar el plan de actividades del proyecto a nivel general (plan maestro).*

Diseño Detallado del Sistema: *se definen los documentos fuente, las entradas, las salidas, los archivos, las especificaciones de procesamiento, los controles del sistema, interrelaciones con los demás sistemas, usuarios secundarios, etc., se definen también los objetivos y todas las especificaciones técnicas, funcionales y de control.*

Desarrollo y Pruebas: *desarrollo de programas, datos de prueba, desarrollo de la documentación a usuarios y del sistema, etc., pruebas individuales de programas. Posteriormente se efectúan las pruebas de módulos del sistema, pruebas integrales de sistema e interconexión con otros sistemas, así como pruebas en paralelo para cotejar que los resultados del sistema desarrollado sean iguales o mejores que el antiguo sistema; antes de llevar a cabo la implantación del sistema, todos los usuarios de éste deberán estar de acuerdo con los resultados del desarrollo y operación. Los auditores del proyecto deberá verificar el control interno y seguridad del mismo.*

Implantación y Post- implantación del sistema: *observar el sistema con volúmenes de información y operación reales y llevar a cabo las adecuaciones pertinentes para su óptima operación.*

Auditoría al área de Métodos y Procedimientos Automatizados:

Para facilitar la integración de los usuarios a los servicios de procesamiento electrónico de datos, se deberá organizar una unidad funcional que se encargue de asesorar a todas las unidades usuarias en la determinación del tipo y nivel de tecnología informática necesaria para satisfacer sus requerimientos de sistematización

La asesoría se orienta, básicamente, en dos direcciones:

1.- Métodos y procedimientos.

2.- Aspectos técnicos.

En lo que respecta a los métodos y procedimientos, la asesoría se concretará en la optimización de los procedimientos de trabajo, manuales yautomatizados.

En cuanto a los aspectos técnicos, la asesoría tiene que ver con la puesta en marcha de los componentes de Hardware y de Software necesarios para atender los procesos de sistematización por computador.

Objetivos de la Auditoría en el área de Métodos y Procedimientos Automatizados:

Verificar que el área de Informática cuente con la documentación correspondiente de los todos los procedimientos automatizados que se producen en el área informática como por ejemplo, la utilización de

los equipos de cómputo (mainframes,, midis, minis y microcomputadores que son utilizados por personal del área de Informática y usuarios), documentación de usuarios para la descripción y utilización de reportes generados por el área de Producción, estándares de documentación para el área de Informática, etc.

Determinar si la función de asesoría técnica a los usuarios:

1. *Analiza junto con el usuario los requerimientos de información solicitados.*
2. *Evalúa la capacidad de los equipos para procesar satisfactoriamente los datos de las aplicaciones en funcionamiento.*
3. *Examina los proyectos de inversión informáticos requeridos por las áreas usuarias y participa activamente en la determinación del alcance de los beneficios, con el objeto de facilitar la autorización correspondiente.*
4. *Participa en la planeación de los requerimientos de Hardware y de Software para que estén disponibles, en las fechas previstas.*
5. *Establece, en conjunto con el usuario el plan estratégico para la iniciación y desarrollo de los proyectos.*
6. *Evalúa la funcionalidad de los métodos, sistemas y procedimientos que operan en las áreas usuarias.*
7. *Participa en la instalación de los elementos de hardware y de software verificando su correcta funcionalidad.*

Auditoría operacional al área de Procesamiento Electrónico de Datos:

El área de procesamiento electrónico de datos como responsable de mantener en forma eficiente y permanente la disponibilidad de los recursos informáticos al servicio de los usuarios, es relativamente compleja en la óptica de la auditoría operacional.

Conocimiento del área de Procesamiento Electrónico de Datos:

El área de servicios de procesamiento electrónico de datos comprende, normalmente los siguientes elementos de tipo organizacional:

- *Unidad de operación del computador: responsable de la operación del computador y de vigilar el mantenimiento permanente de los equipos y componentes asociados para asegurar el cumplimiento de los horarios establecidos por la administración.*
- *Unidad de instalaciones y seguridad: responsable de coordinar la instalación y los cambios de equipo, líneas de comunicación y terminales, garantizando que cumplan con las especificaciones técnicas y de seguridad para evitar fallas que afecten con alguna regularidad los procesos.*
- *Unidad de operación de sistemas: responsable de cubrir los calendarios de los sistemas en producción o en funcionamiento de acuerdo con la planeación establecida.*

- *Unidad de Soporte Técnico: responsable de la instalación, puesta en marcha, mantenimiento y disponibilidad continua del software necesario y de los paquetes de apoyo para el desarrollo de sistemas, con el objeto de asegurar una eficiente funcionalidad del computador.*

Objetivos de la Auditoría operacional en el área de Procesamiento Electrónico de Datos:

La auditoría al área de procesamiento electrónico de datos tiene los siguientes objetivos:

1. *Comprobar que la unidad de procesamiento electrónico de datos, trabaja con base en una adecuada planeación estableciendo objetivos, políticas, programas, procedimientos y presupuestos, coherentes con la planeación general de la organización en el corto, mediano y largo plazo.*

2. *Evaluar la composición organizacional de la unidad de procesamiento electrónico de datos con el objeto de cerciorarse de la validez técnica del modelo de organización, la asignación de responsabilidades, la definición de funciones y los procedimientos en sus diferentes expresiones.*

3. *Comprobar la existencia de manuales suficientemente claros, actualizados, comunicados oportunamente al personal y que se estén utilizando conforme han sido aprobados por la dirección*

4. *Verificar la competencia del personal de la unidad de procesamiento de datos.*

5. *Establecer si la unidad de procesamiento electrónico de datos está trabajando con base en los conceptos de: economicidad, eficiencia y efectividad.*

6. *Verificar que se mantenga la disponibilidad permanente de los recursos de hardware y de software, en condiciones óptimas para atender los requerimientos de los usuarios. Esto implica que exista un mantenimiento sistemático de los recursos de cómputo para asegurar un servicio congruente con los horarios establecidos.*

7. *Verificar la existencia y confiabilidad de las siguientes funciones en todas las dependencias operativas de la unidad de procesamiento electrónico de datos:*

   - *Dirección.*
   - *Supervisión.*
   - *Operación.*
   - *Control de calidad.*

Auditoría al área de Investigación Informática:

Las empresas que han sistematizado sus procesos y que en consecuencia, han destinado sumas considerables de dinero para financiar los recursos informáticos, normalmente disponen de una oficina de investigaciones informáticas dedicada a mantener a la organización actualizada sobre el particular.

Conocimiento del área de Investigación Informática:

La unidad de investigación informática es la responsable de mantener a la entidad, en un ambiente tecnológico actualizado, de manera que satisfaga los requerimientos de información de la organización en el corto, mediano y largo plazo.

Objetivos de la Auditoría en el área de Investigación Informática:.

Determinar si la unidad de investigación informática:

1. *Trabaja con base en objetivos y políticas perfectamente definidos.*
2. *Ha estructurado una modalidad organizativa, acorde con las necesidades operativas y los conocimientos modernos, en administración de negocios.*
3. *Tiene manuales de funciones y procedimientos coherentes con la composición organizacional.*
4. *Dispone de un sistema de información confiable y oportuno.*
5. *Posee un recurso humano competente.*
6. *Ha diseñado un sistema de seguridad efectivo.*
7. *Ejecuta su proceso operativo con los parámetros de: economicidad, eficiencia y efectividad.*

Auditoría al área de Sistemas en Producción:

En auditoría informática, el área mas dispendiosa es la constituida por los sistemas en producción, especialmente cuando los procesos están en línea y en tiempo real.

Se puede hablar de un estándar metodológico para auditar los sistemas en producción, que es lo que vamos a exponer a continuación, sin embargo, debe tenerse en cuenta que la naturaleza de cada aplicación exige su propio sistema de control interno y de auditoría. En consecuencia, el auditor debe tener presente esta circunstancia para definir y abordar el auditaje de los sistemas en producción ya que no es igual auditar una empresa de producción, una empresa de servicios o una empresa comercial cuyos procesos pueden estar dándose en ambientes de computación, tipo batch o en línea, a través de modalidades de baja, mediana o alta complejidad.

Conocimiento del área de Sistemas en Producción:

A partir de un estudio preliminar del área de sistemas en producción, el auditor definirá el orden de prioridades a seguir en el proceso de auditoría.

Para conocer cada uno de los sistemas en funcionamiento, es necesario examinar la correspondiente documentación expresada por lo menos en los siguientes manuales:

- *Del sistema.*
- *Del programa.*
- *De conversión.*
- *De operación.*
- *De biblioteca.*
- *Del usuario.*
- *De control.*

Objetivos de la Auditoría en el área de Sistemas en Producción:

La auditoría de los sistemas en producción, normalmente se guía por los siguientes objetivos:

1. *Evaluar el grado de organización y de asignación de responsabilidades en la preparación de los datos, en el origen.*
2. *Comprobar que todos los datos enviados a proceso sean debidamente autorizados.*
3. *Verificar que todos los datos autorizados sean debidamente validados.*
4. *Verificar que todos los datos autorizados y validados sean debidamente procesados.*
5. *Cerciorarse de que todos los datos se procesen con exactitud.*
6. *Verificar que estén establecidos mecanismos de control interno para que sólo personal autorizado del área de producción, tenga acceso a manipular la información confidencial que se genera por medio de reportes y de ser necesario se establezcan controles muy estrictos para la información que se almacena en medios magnéticos del área.*
7. *Evaluar que la productividad del área en el proceso de la información, corresponda o vaya en relación directa a la tecnología de información con que cuenta la organización y también a los recursos humanos (en capacidad y número) asignados a esta área.*
8. *Verificar que no se desperdicien y/o desaprovechen los recursos materiales asignados para esta función por dispendio, robo o mal uso de ellos.*
9. *Verificar la existencia de suficientes pistas de auditoría.*
10. *Comprobar que estén completos y sea efectiva la documentación del área de sistemas en producción.*

Auditoría al área de Base de Datos:

La avanzada tecnología de las bases de datos y los riesgos asociados han obligado a la gerencia, al personal de sistemas informáticos, a los usuarios y a los auditores a preocuparse por los sistemas de control interno informático especializados, sobre esta materia.

Conocimiento del área de Base de Datos:

Los principales componentes de un sistema de base de datos son normalmente los siguientes :

- ***Administrador de la base de datos:*** *el administrador de la base de datos es la persona responsable del mantenimiento y control de la base de datos. En consecuencia, debe responder por el diccionario de la base de datos, los métodos de acceso a la base de datos, las estructuras de datos y en general todo lo relacionado con la funcionalidad y control del sistema.*

- ***Software de la base de datos o sistema manejador de la base de datos:*** *está integrado por los programas que se utilizan para accesar los datos, actualizar las bases de datos y servir de interfase, en relación con otros programas, tales como los sistemas operacionales y los programas aplicativos, necesarios para el funcionamiento total del sistema de procesamiento de datos.*

- ***Diccionario de datos:*** *es una lista ordenada de las definiciones de todos los datos. Este recurso es fundamental para el administrador de la base de datos.*

- ***Bitácora de registros históricos de la base de datos:*** *es un instrumento que resulta de gran utilidad para rastrear las entradas y las salidas de la base de datos, incluyendo los reportes que muestran los cambios que se hayan hecho a la base de datos, al diccionario y al Software del sistema, entre otros.*

- ***Estándares operativos de la base de datos:*** *constituyen la documentación de la estructura de la base de datos, de sus características operativas, del diccionario de la base de datos y de cualquier otro tipo de documentación relacionado con la funcionalidad e integridad de la base de datos.*

- ***Software de seguridad de la base de datos:*** *este tipo de software, está formado por todos los programas orientados especialmente a la protección física de la base y de los datos del sistema. Este recurso de software comprende los programas de naturaleza protectiva, diseñados especialmente para asegurar la integridad de las bases de datos, en el contexto de seguridad total del sistema.*

Seguridad Lógica:

Uno de los puntos más importantes a considerar para poder definir la seguridad de un sistema es el grado de actuación que puede tener un usuario dentro de un sistema, ya sea que la información se encuentre en un archivo normal o en una base de datos o bien que se posea una minicomputadora o un sistema de red (interna o externa). Para esto podemos definir los siguientes tipos de usuarios:

Propietario: *Es, como su nombre lo indica, el dueño de la información, el responsable de ésta, y puede realizar cualquier función (consultar, modificar, actualizar, dar autorización de entrada a otro usuario). Es responsable de la seguridad lógica, en cuanto puede realizar cualquier acción y puede autorizar a otros usuarios de acuerdo con el nivel que desee darles.*

Administrador: *Sólo puede actualizar o modificar el software con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.*

Usuario principal: *Está autorizado por el propietario para hacer modificaciones, cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.*

Usuario de consulta: *Sólo puede leer la información pero no puede modificarla.*

Usuario de explotación: *Puede leer la información y utilizarla para explotación de la misma, principalmente para hacer reportes de diferente índole los cuales, por ejemplo, pueden ser contables o estadísticos.*

Usuario de auditoría: *Puede utilizar la información y rastrearla dentro del sistema para fines de auditoría.*

Los usuarios pueden ser múltiples, y pueden ser el resultado de la combinación de los antes señalados. Se recomienda que exista sólo un usuario propietario y que el administrador sea una persona designada por la gerencia de informática.

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

La integridad *es responsabilidad de los individuos autorizados para modificar datos o programas (usuario administrador) o de los usuarios a los que se otorgan accesos a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo (usuario responsable y principal).*

La confidencialidad *es responsabilidad de los individuos autorizados para consultar (usuario de consulta) o para bajar archivos importantes para microcomputadoras (usuario de explotación).*

La disponibilidad *es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de base de datos, al monitoreo de teleproceso o al software de telecomunicaciones (usuario administrador).*

El control implantado para minimizar estos riesgos debe considerar los siguientes factores:

1. *El valor de los datos siendo procesados.*

2. *La probabilidad de que ocurra un acceso no autorizado.*

3. *Las consecuencias para la organización si ocurre un acceso no autorizado.*

4. *El riesgo y repercusiones en caso de que un usuario no autorizado utilice la información.*

La seguridad lógica abarca los siguientes puntos:

- *Rutas de acceso.*
- *Claves de acceso.*
- *Software de control de acceso.*
- *Encriptamiento.*

Objetivos de la Auditoría al área de Base de Datos:

1. *Evaluar la forma de cómo se está aplicando el concepto de proceso administrativo al área de base de datos, en términos de sus funciones básicas de planeación, organización, integración, dirección y control.*

2. *Verificar si en el diseño y desarrollo de la base de datos, se consideraron los siguientes elementos desde la perspectiva del control;*

   - *Acceso a la base de datos.*
   - *Control de la información.*
   - *Fraudes de naturaleza informática.*
   - *Grado de privacidad.*
   - *Contingencias naturales o de otro tipo.*
   - *Planes de respaldo y recuperación.*
   - *Manejo de errores.*
   - *Pistas de auditoría..*

3. *Comprobar la efectividad de los procedimientos de control establecidos para proteger la base de datos.*

4. *Verificar la competencia del personal que labora al servicio de la base de datos.*

5. *Evaluar la efectividad del sistema de seguridad física y lógica de la base de datos.*

Auditoría al área de Procesamiento Distribuído:

La comunicación de datos, las bases de datos y los sistemas de procesamiento distribuido son temas estrechamente relacionados para efectos funcionales y de control, de manera que los tres ambientes pueden considerarse como una sola área auditable por su alto grado de afinidad o probablemente haya que dividirlos, como se ha hecho para efectos de esta exposición, con el objeto de facilitar el análisis y la manera de controlarlos y auditarlos.

Los sistemas de procesamiento distribuido son modalidades de sistemas descentralizados, sustentados en NODOS de similar poder de comunicación y de procesamiento de datos constituyendo REDES, desde modelos sencillos hasta altamente sofisticados como expresión de la moderna tecnología informática.

Conocimiento del área de Procesamiento Distribuido:

Un sistema de procesamiento distribuido se caracteriza porque:

- *Los computadores del sistema se encuentran ubicados en lugares distantes*

- *Cada computador ejecuta la mayor parte del procesamiento de datos en el lugar de su ubicación.*

- *Los computadores del sistema son vinculados a un computador central a través de una red de comunicaciones.*

- *Los datos, el procesamiento, la comunicación y la administración de los recursos del sistema, están totalmente distribuidos.*

La filosofía de un sistema de procesamiento distribuido se apoya en los siguientes objetivos:

- *Llevar el computador y la información a las áreas usuarias en vez del ejercicio contrario.*
- *Tener acceso y capacidad de comunicación con los grandes centros de computación y las bases de datos.*
- *Tener intercambio con los usuarios por medio de terminales económicas.*

Objetivos de la Auditoría en el área de procesamiento distribuido:

1. *Verificar si existen por escrito objetivos y políticas perfectamente definidos y coherentes con los objetivos generales de la organización. en relación con los sistemas de procesamiento de datos.*
2. *Analizar el modelo de organización que está operando, en el área de procesamiento de datos distribuido.*
3. *Comprobar la existencia de manuales técnicamente preparados, aceptados y puestos en práctica por el personal.*
4. *Evaluar la competencia del personal de acuerdo con su responsabilidad y funciones.*
5. *Evaluar los procedimientos de control interno operantes en el área de procesamiento de datos distribuido.*
6. *Comprobar la existencia efectiva de un sistema d seguridad para el área de procesamiento de datos distribuido.*
7. *Verificar si la administración está trabajando con base en los conceptos de economicidad, eficiencia y efectividad.*

Auditoría a los Programas Producto o Programas Propietario (software proporcionado por proveedores externos):

El área que maneja los programas producto (soporte técnico) fue abarcada en el capitulo de auditoría a los sistemas en funcionamiento, sin embargo, debido a su especial importancia que constituye para la auditoría le dedicamos un espacio independiente para precisar mejor sus componentes y los estándares de control correspondientes.

Conocimiento del área de Software del Sistema:

El área de software del sistema (soporte técnico), para efectos de auditoría, comprende entre otros, los siguientes conceptos:

- *Software operacional.*

- *Software de comunicación de datos.*
- *Software de inteligencia distribuida*
- *Software del sistema administrativo de las bases de datos*

***SOFTWARE OPERACIONAL**: está constituido por todos los programas que manejan el sistema computarizado, tales como:*

- *Los programas supervisores del sistema.*
- *Los programas de carga e inicio del sistema.*
- *Los programas utilitarios.*

***SOFTWARE DE COMUNICACION DE DATOS**: está integrado por todos los programas que gobiernan el tramo de comunicación de datos del sistema, este software permite :*

- *El acceso al sistema de telecomunicaciones.*
- *La operatividad de los monitores de telecomunicación, encargados de supervisar la función total de comunicación de datos.*
- *La funcionalidad de los procesadores frontales de comunicación y de los concentradores remotos.*

***SOFTWARE DE INTELIGENCIA DISTRIBUIDA**: este tipo de Software operativo, está constituido por paquetes ubicados en los extremos de los encadenamientos de comunicación de datos y se encarga de la operatividad del sistema de procesamiento distribuido.*

***SOFTWARE DEL SISTEMA ADMINISTRADOR DE LAS BASES DE DATOS**: esta modalidad de Software, permite manejar o administrar la base de datos y reside normalmente en la computadora central o una localidad remota cuando se trata del caso de bases de datos distribuidos.*

En la etapa de conocimiento del área, el auditor debe abordar los manuales del software del sistema y familiarizarse, en lo posible con su funcionamiento. Cuando se estime necesario, el auditor podrá asesorarse de personal altamente técnico sobre la materia para desarrollar su trabajo.

Objetivos de la Auditoría al software de Programas Producto o Programas Propietario.

En el caso del software de programas producto, el auditor deberá hacer hincapié en la estudio y cautela que deberá hacer y tener el área de informática con respecto a la dependencia hacia el proveedor del producto, y el riesgo al que se expone y expone a la organización a la que proporciona servicio en caso de que el proveedor no esté establecido sólidamente y su producto avalado por una firma de reconocido prestigio internacional o nacional.

- *Establecer la existencia de objetivos y políticas definidos en relación con el área de soporte técnico.*
- *Evaluar los criterios de administración del área de soporte técnico.*
- *Verificar que el personal trabaja con base en los manuales del área.*
- *Comprobar la competencia del personal responsable del manejo del software de los programas producto.*
- *Evaluar el nivel de segregación funcional, definido para administrar el área de soporte técnico.*

- *Verificar la efectividad del sistema de control vigente, para el área de soporte técnico.*
- *Comprobar que los recursos de soporte técnico se administran con base en los conceptos de: economía, eficiencia y efectividad.*
- *Evaluar el respaldo que se tiene del proveedor de los programas producto para dar apoyo al personal de soporte técnico.*
- *Comprobar la capacitación técnica que debe dar el proveedor al personal de soporte técnico para conocer el software.*
- *Verificar la seguridad, integridad y confidencialidad que deben tener los programas producto para el desarrollo de sus funciones.*
- *Evaluar si el proveedor está sólidamente establecido o se corre el riego de algún día prescindir de su respaldo y probablemente de la continuidad del programa producto que vendió.*
- *Si la adquisición de los programas producto corresponden a los objetivos para los cuales se invirtió este importe.*

Auditoría a un ambiente de Microcomputadores:

Los microcomputadores se han convertido en un elemento de evidente utilidad para agilizar el procesamiento de datos, con un alto grado de velocidad, exactitud y confiabilidad pero a su vez han abierto la puerta a un potencial considerable de nuevos riesgos para las organizaciones. Por consiguiente, es necesario definir un área auditable para este concepto y analizar sus elementos desde la óptica de la auditoria operacional.

Conocimiento del ambiente de Microcomputadores:

El conocimiento del área de micros, para efectos de auditoría puede abordarse de la siguiente manera:

- *Realice una visita a las instalaciones de PED, para observar en forma general su nivel de organización.*
- *Solicite y analice el inventario de los recursos de hardware y software y la hojas de responsabilidad y resguardo de equipo asignado a usuarios.*
- *Solicite los contratos de adquisición de máquinas y programas.*
- *Examine la documentación de todos los recursos microinformáticos.*
- *Solicite la lista de los usuarios, permanentes y ocasionales.*
- *Examine la nómina y los respectivos contratos de vinculación.*

- *Examine los últimos reportes de uso de las máquinas: para examinar la utilización racional de los equipos, detectar accesos no autorizados o posibles intentos de violación a aplicaciones no permitidas a los usuarios.*

- *Examine las pólizas de seguro y los contratos de mantenimiento.*

- *Analice el informe de la última auditoría.*

- *Cerciórese de las adquisiciones de recursos informáticos, correspondientes al período auditado.*

- *Evalúe que el equipo asignado y software al que tiene permiso de acceso, realmente sea el que se requiere para las funciones que desempeña este usuario y que realmente dichos accesorios sean necesarios para desempeñar su trabajo.*

- *Cerciórese de que haya una estandarización de equipos y software contratados por la organización, en la asignación de éstos para los usuarios.*

- *Verifique que los usuarios de los sistemas y equipos de cómputo, hayan sido capacitados en la medida de sus funciones para la utilización de ésos.*

- *Examine que los equipos asignados a usuarios, no tengan software diferente a los permitidos y contratados por la organización para su uso.*

Objetivos de la Auditoría del ambiente de Microcomputadores.

1. *Comprobar la existencia de objetivos y políticas perfectamente definidos, en todo lo relacionado con microcomputadores.*

2. *Evaluar el modelo de estructura organizacional vigente para el área de microcomputadores.*

3. *Analizar el grado de segregación funcional, que opera en el área de microcomputadores, con el objeto de verificar la existencia de líneas de autoridad y de responsabilidad suficientemente confiables.*

4. *Verificar si el personal que trabaja en el área de microcomputadores, lo hace de acuerdo con manuales de funciones y procedimientos técnicamente preparados.*

5. *Verificar si la gerencia administra el área de micros con base en los conceptos de economicidad, eficiencia y efectividad para asegurar el ejercicio de una gestión de éxito sobre el particular.*

6. *Comprobar la efectividad del sistema de control interno vigente para el área de micros.*

CAPÍTULO III. DOCUMENTACIÓN DE LA ORGANIZACIÓN Y DE INFORMÁTICA

Inciso 5.

Sub - inciso 5.1.

Se recopila la información para tener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento. La eficiencia en el departamento de informática sólo se puede lograr si sus objetivos están integrados con los de la institución y si permanentemente se adapta a los posibles cambios de éstos.

Para poder analizar y dimensionar la estructura a auditar se debe solicitar:

A nivel organización total:

- *Objetivos a corto y largo plazos.*
- *Manual de organización.*
- *Antecedentes o historia del organismo.*
- *Políticas generales.*

A nivel del área de informática:

- *Objetivos a corto y largo plazos.*
- *Manual de organización del área, que incluya puestos, funciones, niveles jerárquicos y tramos de mando.*
- *Manual de políticas , reglamentos internos y lineamientos generales.*
- *Número de personas y puestos en el área.*
- *Procedimientos administrativos del área.*
- *Presupuestos y costos del área.*

Del área de Recursos materiales y técnicos:

- *Solicitar documentos sobre los equipos, así como el número de ellos, su localización y sus características (de los equipos instalados, por instalar y programados).*
- *Estudios de viabilidad.*
- *Fechas de instalación de los equipos y planes de instalación.*
- *Contratos vigentes de compra, renta y servicio de mantenimiento.*
- *Contratos de seguros.*
- *Convenios que se tienen con otras instalaciones.*

- *Configuración de los equipos y capacidades actuales y máximas.*
- *Configuración de equipos de comunicación (redes internas v externas) y localización de los equipos.*
- *Planes de expansión.*
- *Ubicación general de los equipos.*
- *Políticas de operación.*
- *Políticas de uso de los equipos.*
- *Políticas de seguridad física y prevención contra contingencias internas y externas.*

Del área de Sistemas:

- *Descripción general de los sistemas instalados y de los que estén por instalarse, que contengan volúmenes de información.*
- *Manual de formas.*
- *Manual de procedimientos de los sistemas.*
- *Descripción genérica.*
- *Diagramas de entrada, archivos, salida.*
- *Fecha de instalación de los sistemas.*
- *Proyecto de instalación de nuevos sistemas.*
- *Bases de datos, propietarios de la información y usuarios de la misma.*
- *Procedimientos y políticas en casos de desastre.*
- *Sistemas propios, rentados y adquiridos.*

Por último, se deberá revisar el grado de cumplimiento de los documentos administrativos:

- *Organización.*
- *Normas y políticas.*
- *Planes de trabajo.*
- *Controles.*
- *Estándares.*
- *Procedimientos.*

Del software de manejo de librerías:

Las funciones del software restringen el acceso a librerías críticas; los procedimientos que gobiernan el uso de esas funciones deberán ser revisados, evaluados y probados. El auditor deberá revisar, evaluar y probar lo siguiente:

- *Documentación de librerías.*
- *Programas fuente y ejecutables.*
- *Jobs en ejecución y lineamientos de control.*
- *Parámetros de corridas.*
- *Uso de software para restringir el acceso a librerías.*
- *Restricción del acceso a librerías de producción.*
- *Restricción de funciones que pueden ser usadas para modificar el estado de un programa (pruebas a producción).*
- *Acceso a librerías en prueba.*
- *Convenciones para dar nombre a librerías que son usadas para facilitar la seguridad.*
- *Métodos para clasificar y restringir el acceso a librerías por tipo (fuentes, objeto, carga y control de jobs).*
- *Si el software ejecuta funciones de identificación de usuario y procedimientos de autentificación.*
- *Procedimientos inusuales de librerías.*
- *Capacidades de la bitácora de auditoría.*
- *Los números de versión del software.*

Los reportes escritos pueden ser usados para organizar las actividades de las librerías de logs de acceso al software manejador de librerías o bitácoras de auditoría.

En caso de que se tenga la información se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa, de ser así, se considerará dentro de las conclusiones de la evaluación, ya que como se dijo, la auditoría no sólo debe considerar errores sino también señalar los aciertos.

La organización debe estar estructurada de tal forma que permita lograr eficiente y eficazmente los objetivos y que esto se logre a través de una adecuada toma de decisiones.

CAPÍTULO III. DESARROLLO Y MANUAL DE ESTÁNDARES

Inciso 5.

Sub - inciso 5.2.

Manual de Estándares de Funcionamiento y Procedimientos:

Los estándares en la actividad informática, tratan de establecer lineamientos para asignar una identificación y/o un orden a los recursos tangibles e intangibles del área, así como para las actividades programáticas del software como nombres de programas, rutinas y nombres de campos en la programación; trata también de establecer una metodología para desarrollo de software (diseño y programación), para las aplicaciones de la organización, nombres de archivos de datos y sus campos, reportes, etc.; identificación de claves de equipo de telecomunicaciones, para reconocer a través de la red de cómputo a mainframes y minicomputadores: para la documentación y manuales del área; para identificación de usuarios que ingresan a correos electrónicos particulares de la organización o públicos; en realidad los estándares definen y marcan un orden para el desarrollo de las actividades del área de informática.

Además, deben existir estándares de funcionamiento y procedimientos que gobiernen la actividad del departamento de Informática por un lado y sus relaciones con los departamentos usuarios por otro. Estos estándares son el vehículo ideal para transmitir al personal de Informática la filosofía, mentalidad y actitud hacia los controles necesarios con la finalidad de crear y mantener un entorno controlado para la vida de los sistemas de información de la empresa.

De particular importancia son estos aspectos relacionados con la adquisición de equipos o material para el departamento, con el diseño y el desarrollo / modificación de sistemas de información y con la producción o explotación. Además, dichos estándares y procedimientos deberán estar documentados, organizados, actualizados y ser comunicados adecuadamente a todos los departamentos afectados. La Dirección de Informática debe promover la adopción de estándares y procedimientos y dar ejemplo de su uso.

Por otro lado, deben existir documentadas descripciones de los puestos de trabajo dentro de Informática, como parte del manual de estándares, delimitando claramente la autoridad y responsabilidad en cada caso. Las descripciones deberían incluir los conocimientos técnicos y/o experiencia necesarios para cada puesto de trabajo.

El auditor deberá evaluar la existencia de estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo, adecuados y actualizados.

Entre las acciones a realizar, se pueden citar:

- *Evaluación del proceso por el que los estándares, procedimientos y puestos de trabajo son desarrollados, aprobados, distribuidos y actualizados.*
- *Revisión de los estándares y procedimientos existentes para evaluar si transmiten y promueven una filosofía adecuada de control. Evaluación de su adecuación, grado de actualización y nivel de cobertura de las actividades informáticas y de las relaciones con los departamentos usuarios.*
- *Revisión de las descripciones de los puestos de trabajo para evaluar si reflejan las actividades realizadas, en la práctica.*

El auditor de las funciones de informática, deberá asentar en su informe las inconsistencias al respecto y dejar consigna relevante en el caso de no tener estándares, ya que se puede caer en errores fatales por la carencia de éstos.

CAPÍTULO III. ORGANIGRAMA Y DESCRIPCION DE PUESTOS DE INFORMATICA

Inciso 5.

Sub - inciso 5.3.

Una vez elaborada la planeación de la auditoría, la cual servirá como plan maestro de los tiempos, costos y prioridades y como medio de control de la auditoría, se debe empezar la recolección de la información para con ello proceder a efectuar la revisión sistematizada del área, a través de los siguientes elementos:

A) Revisión de la estructura orgánica:

- *Jerarquías (definición de la autoridad lineal, funcional y de asesoría).*
- *Estructura orgánica.*
- *Funciones.*
- *Objetivos.*

B) Se deberá revisar la situación de los recursos humanos.

C) Entrevistas con el personal de procesos electrónicos:

- *Jefatura.*
- *Análisis.*
- *Programadores.*
- *Operadores.*
- *Personal de bases de datos.*
- *Personal de comunicación y redes.*
- *Personal de mantenimiento.*
- *Personal administrativo.*
- *Responsable de comunicaciones.*
- *Responsable de Internet e Intranet y si lo hubiere, de Extranet.*
- *Responsable de redes locales o nacionales.*
- *Responsable de sala de usuarios.*
- *Responsable de capacitación para el área de informática.*

D) Se deberá conocer la situación en cuanto a:

- *Presupuesto.*
- *Recursos financieros.*
- *Recursos materiales.*
- *Mobiliario y equipo.*
- *Costos.*

E) Se hará un levantamiento del censo de recursos humanos y análisis de situación en cuanto a:

- *Número de personas y distribución por áreas.*
- *Denominación de puestos y personal de confianza y de base (sindicalizado y no sindicalizado).*
- *Salario y conformación del mismo (prestaciones y adiciones).*
- *Movimientos salariales.*
- *Capacitación (actual y programa de capacitación).*
- *Conocimientos.*
- *Escolaridad.*
- *Experiencia profesional.*
- *Antigüedad (en la organización, en el puesto y en puestos similares fuera de la organización).*
- *Historial de trabajo.*
- *Índice de rotación del personal.*
- *Programa de capacitación (vigente y capacitación otorgada en el último año).*

F) Por último, se deberá revisar el grado de cumplimiento de los documentos administrativos:

- *Organización.*
- *Normas y políticas.*
- *Planes de trabajo.*
- *Controles.*
- *Estándares.*
- *Procedimientos.*

La información nos servirá para determinar:

1. *Si las responsabilidades en la organización están definidas adecuadamente.*
2. *Si la estructura organizacional está adecuada a las necesidades.*
3. *Si el control organizacional es el adecuado.*
4. *Si se tienen los objetivos y políticas adecuadas, si se encuentran vigentes y si están bien definidas.*
5. *Si existe la documentación de las actividades, funciones y responsabilidades.*
6. *Si los puestos se encuentran definidos y señaladas sus responsabilidades.*
7. *Si el análisis y descripción de puestos está de acuerdo con el personal que los ocupa.*
8. *Si se cumplen los lineamientos organizacionales.*
9. *Si el nivel de salarios está de acuerdo con el mercado de trabajo.*
10. *Si se tiene un programa de capacitación adecuado y si se cumple con él.*

11. Si los planes de trabajo concuerdan con los objetivos de la empresa.

12. Si se cuenta con los recursos humanos necesarios que garanticen la continuidad de la operación o si se cuenta con los "indispensables".

13. Si se evalúan los planes y se determinan las desviaciones.

14. Si se cumple con los procedimientos y controles administrativos.

La organización debe estar estructurada de tal forma que permita lograr eficiente y eficazmente los objetivos y que esto se logre a través de una adecuada toma de decisiones.

Una forma de evaluar el cómo la gerencia de informática se está desempeñando, es mediante la evaluación de las funciones que la alta gerencia debe realizar.

***Planeación:** determinar los objetivos del área y la forma en que se van a lograr esos objetivos.*

***Organización:** proveer de las facilidades, estructura, división del trabajo, responsabilidades, actividades de grupo y personal necesario para realizar las metas.*

***Recursos humanos:** seleccionando, capacitando y entrenando al personal requerido para realizar las metas.*

***Control:** comparando lo real contra lo planeado, como base para realizar los ajustes necesarios.*

Evaluación de puestos de los recursos humanos:

El desarrollo del personal implica:

- *Establecer promociones y oportunidades de desarrollo.*
- *Educación y capacitación. Estas actividades mantienen la moral y las habilidades de los empleados en un nivel adecuado para cumplir con los objetivos y metas encomendadas y les permitirá tener mayor motivación y mejores remuneraciones. En el área de informática es muy importarte la capacitación para tener actualizado a nuestro personal en una disciplina en la que puede quedarse rezagado muy rápidamente, aunque, por otro lado, debido a la presión de tiempo con la que se trabaja, en muchas ocasiones no se le da al personal la oportunidad para capacitarse.*

Se deberá obtener información sobre la situación del personal del área, para lo cual se puede utilizar la tabla de recursos humanos y la tabla de proyección de recursos humanos y obtener información sobre los siguientes aspectos:

- *Desempeño y comportamiento.*
- *Condiciones de ambiente de trabajo.*
- *Organización en el trabajo.*
- *Desarrollo y motivación.*
- *Capacitación y supervisión.*

CAPITULO IV

AUDITORIA DE SISTEMAS

CAPÍTULO IV. DOCUMENTACION Y ESTANDARES

Inciso I.

Los sistemas y su documentación deben estar acordes con las características y necesidades de una organización específica; no se deberá tener la misma documentación para un sistema que se va a usar en computadoras personales, el cual debe ser documentado en forma más sencilla (el usuario no necesariamente debe saber de computación) que un sistema en red.

También deben existir diferentes niveles de documentación (documentación para usuarios, para responsables de la información técnica, etc.).

Se debe evaluar la obtención de datos sobre la operación, el flujo, el nivel, la jerarquía de la información que se tendrá a través del sistema, así como sus límites e interfases con otros sistemas. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la - ejecución deseada corresponde al actual

La auditoria en informática debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas (pantallas, las cuales deben tener una estructura "amigable") y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, las bases de datos, su uso y su relación con otros archivos y sistemas, frecuencia de acceso, conservación, seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuente a usarse.

Dentro del estudio de los sistemas en uso se deberá solicitar:

- *Manual del usuario.*
- *Descripción de flujo de información.*
- *Descripción y distribución de información (uso y distribución de reportes).*
- *Manual de formas.*
- *Manual de reportes.*
- *Lista de archivos y especificación.*
- *Definición de bases de datos.*
- *Definición de redes.*

Con la información obtenida podremos dar respuesta a las siguientes preguntas:

¿Se está ejecutando en forma correcta y eficiente el proceso de información?.

¿Puede ser simplificado para mejorar su aprovechamiento?.

¿Se debe tener una mayor interacción con otros sistemas?.

¿Se tiene un adecuado control y seguridad sobre el sistema?.

¿Está la etapa de análisis sustentada con la documentación suficiente y adecuada?.

¿Se debe usar otro tipo de técnicas o de dispositivos (redes, bases de datos)?.

¿Los informes de salida son confiables y adecuados?.

¿Las pantallas y el sistema son amigables?.

Políticas de Respaldos:

Los respaldos de la información deben realizarse mensual, semanal o diario y se deben observar los siguientes puntos:

- *Contar con políticas formales por escrito para efectuar los respaldos mensuales, semanales y diarios de la información.*
- *Los medios magnéticos de respaldo no deben estar almacenados en un mismo lugar, aunque se tengan los medios magnéticos de operación en el site, por lo que si hubiera una contingencia grave (incendio, inundación) no se tendría el riesgo de perder parte o la totalidad de la información, ya que se cuenta en otro lugar con los respaldos.*
- *Debe tenerse acceso restringido al área en donde se tienen almacenados los medios magnéticos, tanto de operación como de respaldo.*
- *Se deben tener identificadas los elementos magnéticos por fecha, concepto y consecutivo y es conveniente elaborar y actualizar una relación sobre dichos elementos magnéticos, el contenido de los datos de registro y los responsables de efectuarlos.*
- *Se debe contar con una política que indique los procedimientos a seguir en cuanto al almacenamiento de los elementos magnéticos en un lugar diferente al de la ubicación del site, en donde se pueda tener acceso las 24 horas del día y donde se designen responsables de mantener actualizada la información vital de la organización.*

El hecho de no contar con estas políticas de respaldo que contemplen los puntos anteriores puede provocar que no se sigan los procedimientos adecuados para realizar los respaldos, que haya riesgo de pérdida de información en caso de alguna contingencia y no tener una disponibilidad inmediata de la información de respaldo para conseguir continuidad en los procedimientos de la organización.

Controles en operación, mantenimiento y cambios correctivos:

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora. Los instructivos de operación proporcionan al operador información sobre los procedimientos que debe seguir en situaciones normales y anormales del procesamiento y si la documentación es incompleta o inadecuada lo obliga a

improvisar o suspender los procesos mientras investiga lo conducente, generando probablemente errores, reprocesos, desperdicio, de tiempo de máquina; se incrementan, pues, los costos del procesamiento de datos.

Debemos de considerar la operación de los sistemas en línea, los cuales deben de estar residentes en todo momento, con su correspondiente sistema de comunicación, mientras que en cuanto a los sistemas en lote (batch) se debe planear y programar su operación. Para lograr esto existen instalaciones que tienen equipos de computación y comunicación dedicados exclusivamente a los sistemas en línea y otros equipos dedicados únicamente a procesos en lote (batch).

El auditor de informática deberá verificar en la implementación de los sistemas, el comportamiento de los mismos, para dejar constancia que sus características están de acuerdo a la especificación de la documentación de requerimientos, evaluando el sistema mismo, su seguridad, confidencialidad y satisfacción de los usuarios. Las pruebas del sistema tratan de garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes, archivos, anotando las fallas que pudieran ocurrir y realizando los ajustes necesarios. Los niveles de prueba pueden ser agrupados en módulos, programas y sistema total.

Con respecto al mantenimiento de los sistemas, ¿qué sucede con respecto al mantenimiento correctivo o modificación de un sistema cuando este no ha sido bien desarrollado (analizado, diseñado, programado y probado) pero es instalado?. La respuesta es sencilla; necesitará cambios frecuentes por omisiones o nuevos requerimientos.

En el caso de sistemas, muchas organizaciones están gastando cerca del 80 % de sus recursos de cómputo en mantenimiento.

El mantenimiento excesivo es consecuencia de falta de planeación y control de desarrollo de sistemas.

Por su parte, el control debe tener como soporte el establecimiento, de normas de desarrollo que han de ser verificadas continuamente en todas las etapas del desarrollo de un sistema. Estas normas no pueden estar aisladas, primero, del contexto particular de la dirección de informática (ambiente) y segundo, de los lineamientos generales de la organización, para lo cual es necesario contar con personal en desarrollo que posea suficiente experiencia en el establecimiento de normas de desarrollo de sistemas. Estas mismas características deben existir en el personal de auditoría de sistemas.

Es poco probable que un proyecto llegue a un final feliz cuando se ha iniciado sin éxito.

Difícilmente estaremos controlando realmente el flujo de la información de un sistema que desde su inicio ha sido mal analizado, mal diseñado, mal programado e incluso mal documentado.

El excesivo mantenimiento de los sistemas generalmente es ocasionado por un mal desarrollo. Esto se inicia desde que el usuario establece sus requerimientos (en ocasiones sin saber qué desea) hasta la instalación del sistema, sin que se haya establecido un plan de prueba de éste para medir su grado de confiabilidad en la operación que se efectuará.

Control de estándares:

Deben existir estándares de funcionamiento y procedimientos que gobiernen la actividad del Departamento de Informática por un lado y sus relaciones con los departamentos usuarios por otro. Estos estándares son el vehículo ideal para transmitir al personal de Informática la filosofía, mentalidad y actitud hacia los

controles necesarios con la finalidad de crear y mantener un entorno controlado para la vida de los sistemas de información de la empresa.

De particular importancia son estos aspectos relacionados con la adquisición de equipos o material para el departamento, con el diseño y el desarrollo / modificación de sistemas de información y con la producción o explotación.

Además, dichos estándares y procedimientos deberán estar documentados, organizados, actualizados y ser comunicados adecuadamente a todos los departamentos afectados. La Dirección de Informática debe promover la adopción de estándares y procedimientos y dar ejemplo de su uso.

En la actualidad, la mayoría de las empresas tienen su departamento de elaboración y control de estándares para dar soporte a las actividades de la organización.

Integridad de los datos y manejo de cifras de control:

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al :

- *Suprimir u omitir datos.*
- *Adicionar datos.*
- *Alterar datos.*
- *Duplicar procesos.*

Esto es de suma importancia en el caso de sistemas en línea, en los que los usuarios responsables de la captura y modificación de la información. Por ello, se debe tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles.

El primer nivel es en el que se pueden hacer únicamente consultas; el segundo nivel es aquel en el que se puede hacer captura, modificaciones y consultas y el tercer nivel es aquel en el que se puede hacer todo lo anterior y además se pueden realizar bajas. Todo lo anterior debe estar acompañado de un diseño de prioridades otorgadas a los usuarios.

Anteriormente la responsabilidad de captura era del área de informática; en la actualidad es principalmente responsabilidad del usuario, pero esto no elimina la posibilidad de errores y consecuentemente la necesidad de auditar sus controles. Ahora existen diversas formas de captura de la información, por ejemplo, scanners, pero debe existir una persona que sea responsable del control de esta información y asegurarse de que es confiable y oportuna.

Lo primero que debemos evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de ésta.

Controles en el Desarrollo de Sistemas:

Los datos son uno de los recursos más valiosos de las organizaciones y aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidad, que los demás inventarios de la organización, por lo cual se debe tener presente:

- *La responsabilidad de los datos es compartida conjuntamente por alguna función determinada de la organización y la dirección de informática.*
- *Un problema que se debe considerar es el que se origina por la duplicidad de los datos, el cual consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.*
- *Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.*
- *Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.*

En todo centro de informática se debe contar con una serie de políticas que permitan la mejor operación de los sistemas. Estas políticas son evaluadas durante el transcurso de la auditoria, por lo que sólo son mencionadas en esta sección, pero se encuentran estudiadas en detalle en diferentes capítulos.

Controles en Base de Datos:

Cuando varios usuarios utilizan una base de datos, pueden existir problemas si no fue diseñada para usuarios múltiples. Uno de estos problemas surge cuando no existe un control sobre la actualización inmediata. Esto significa que dos o más usuarios pueden estar elaborando cambios al mismo archivo en el mismo momento y no existe control sobre la actualización inmediata de los archivos.

Este tipo de problemas existe principalmente en las bases de datos de computadoras personales, ya que los grandes sistemas de cómputo tienen control sobre las actualizaciones inmediatas.

También pueden existir problemas en el uso de recursos excesivos de cómputo, lo cual se agrava si no se tiene un mantenimiento constante sobre las bases de datos.

***Problemas de seguridad**. Las bases de datos deben tener suficiente control para que se asegure que sólo personal autorizado pueda acceder datos y se debe definir el tipo de usuario que pueda adicionar, dar de baja, actualizar o acceder datos dependiendo de su llave de entrada, así como el usuario propietario de la base de datos.*

Cada vez se accede más a las bases de datos a través de redes, con lo que el riesgo de violación de la confidencialidad e integridad se acentúa. También las bases de datos distribuidas pueden presentar riesgos de seguridad.

Se establecen cinco objetivos de control a la hora de revisar la distribución de los datos:

- *El sistema de proceso distribuido debe tener una función de administración de datos centralizada que establezca estándares generales para la distribución de datos a través de las aplicaciones.*
- *Deben establecerse funciones de administración de datos y de base de datos, muy fuertes para que se pueda controlar convenientemente la distribución de datos.*
- *Deben existir pistas de auditoría para todas las actividades realizadas por las aplicaciones contra sus propias bases de datos y con otras compartidas.*
- *Deben existir controles de software para prevenir interferencias de actualización sobre las bases de datos en sistemas distribuidos.*
- *Deben realizarse las consideraciones adecuadas de costos y beneficios en el diseño de entornos distribuidos.*

CAPÍTULO IV. CONFIDENCIALIDAD DE LOS SISTEMAS

Inciso 2.

Encriptar es el arte de proteger la información transformándola con un determinado algoritmo dentro de un formato para que no pueda ser leída normalmente, en otras palabras, es la transformación de los datos a una forma en que no sea posible leerla por cualquier persona a menos que cuente con la llave de descripción: su propósito es asegurar la privacidad y mantener la información alejada de personal no autorizado, aun de aquellos que la puedan ver en forma encriptada.

También es una forma de confidencialidad de la información y de los sistemas, sólo aquellos usuarios que posean la clave de acceso podrán "desencriptar" un texto para que pueda ser leído. Las tecnologías modernas de encriptamiento, hacen casi imposible que una persona no autorizada utilice la información.

Debido a que Internet y otras formas de comunicación electrónica se ha convertido en algo normal y rutinario, la seguridad se ha convertido en un factor muy importante. El encriptamiento se usa para proteger mensajes de correo electrónico (E-mail), firmas electrónicas, llaves de acceso, información de tipo financiero e información confidencial. Existen en el mercado diferentes paquetes y formas para encriptar la información.

Los sistemas de encriptamiento pueden ser clasificados en sistemas de llave simétrica, los cuales usan una llave común para el que envía información y para el que la recibe y sistemas de llave pública, el cual utiliza dos llaves, una que es pública, conocida por todos y otra que solamente conoce el receptor.

Criptoanálisis es el arte de desencriptar comunicaciones sin conocer las llaves apropiadas. Existen muchas técnicas para lograrlo y entre las más comunes están:

- *Ataque a textos encriptados; esta es una situación en la cual el atacante no conoce nada acerca del contenido del mensaje y debe trabajar únicamente en el contenido del mensaje. En la práctica es muy posible adivinar el contenido de algún texto, ya que normalmente tienen encabezados fijos.*

- *Ataque conociendo el texto original; el atacante conoce o puede adivinar el contenido del texto debido a algunas partes del texto encriptado. El objetivo es desencriptar el resto del texto usando esta información, esto también puede ser hecho al determinar la llave usada para encriptar.*

- *Ataque hecho por medio de escoger un texto encriptado; el atacante tiene el objetivo de determinar la llave con la cual se encriptó el texto.*

- *Atacar en la parte central; este tipo de ataque es relevante para la comunicación criptografiada y para los protocolos clave de intercambio. La idea es que cuando dos personas están intercambiando llaves de seguridad para lograr la comunicación, el atacante se pone en medio de la línea de comunicación y el atacante realiza un intercambio separado de llaves, posteriormente, el atacante, con las llaves de acceso, puede realizar cualquier función. Una forma de prever este tipo de ataques, es encriptar la llave de acceso al momento de enviar; así, una vez enviada, el emisor y receptor verifican la firma digital para realizar las operaciones necesarias.*

- *Ataque en el tiempo; este es un nuevo tipo de ataque y está basado en la medición repetitiva de los tiempos exactos de ejecución.*

Aunque existen diversas formas para atacar la información encriptada, es conveniente que el programador conozca las formas de encriptamiento, sus ventajas y desventajas, así como su costo, para determinar la mejor para cada uno de los sistemas y que el auditor verifique la forma de encriptarniento y su seguridad de acuerdo con los requerimientos de seguridad de cada sistema.

CAPÍTULO IV. SEGURIDAD EN LOS SISTEMAS

Inciso 3.

SEGURIDAD.

Las nuevas tecnologías de información y telecomunicaciones así como el entorno más complejo en el que ellas se desarrollan, ha provocado la aparición de vulnerabilidades en los recursos utilizados, que deben minimizarse con medidas de seguridad oportunas.

Algunos aspectos que han contribuido a la vulnerabilidad de los recursos utilizados en los sistemas de información son ;

- *la creciente utilización de los sistemas distribuidos,*
- *la mayor complejidad de los procesos,*
- *el número de usuarios y su ubicación dispersa,*
- *la proliferación de intercambio de archivos por correo electrónico,*
- *la utilización de la red de redes (Internet) para el comercio electrónico.*

Podemos decir que la seguridad en los sistemas de información la conforman un conjunto de técnicas, medidas y procedimientos encaminados a garantizar la disponibilidad, la integridad, la confidencialidad y la autenticación de la información y los recursos informáticos de la organización. Además de ésas características, los sistemas de información deben cumplir en mayor o menor grado con los siguientes requisitos;

- ***Responsabilidad*** *--- que los sistemas de seguridad implantados, puedan identificar las acciones que los usuarios realizan.*

- ***Auditabilidad*** *--- todos los sistemas de seguridad deben proporcionar estadísticas acerca de entradas al sistema, uso e identificación de recursos, las acciones realizadas por cada usuario, etc.*

- ***Servicios de aceptación*** *--- impiden que un usuario pueda negar haber recibido un documento electrónico. Estos servicios pretenden cubrir las funciones de una firma manuscrita, pero de una manera más segura.*

- ***Reclamación de origen*** *--- permite probar quién es el generador de un determinado documento.*

- ***Reclamación de propiedad*** *--- permite probar que un determinado documento electrónico es propiedad de un usuario en particular, se usa en transacciones mercantiles, donde la posesión de un documento concede determinados derechos a su poseedor.*

- ***Certificación de fechas*** *--- se utiliza en las comunicaciones electrónicas este servicio y sirve para determinar a qué hora y en qué fecha se ha generado o entregado un documento.*

Por último, las normas de seguridad informática deben ser;

- *no excesivamente detallistas,*
- *aprobadas por la Dirección o la más alta autoridad.*

- *publicadas, implementadas y del conocimiento de todas las áreas de la entidad,*
- *identificadas, mantenidas, actualizadas, clasificadas, etc.,*
- *controladas por personal técnico capacitado y único responsable de la integridad y confidencialidad de dicha información (debe existir control interno muy especial para esta desarrollar esta función).*

El equipo auditor examinará la documentación en materia de seguridad existente en la organización y comprobará que han sido definidos, al menos, procedimientos de clasificación de la información, control de acceso, identificación y autenticación de soportes, gestión de incidencias y controles de auditoría. Con posterioridad, pasará a comprobar si las medidas de seguridad definidas se encuentran realmente operativas.

Tras verificar que las funciones, obligaciones y responsabilidades, en materia de seguridad de cada puesto de trabajo están claramente definidas y documentadas, comprobará que se han adoptado las medidas necesarias para que todo el personal conozca tanto aquellas que afecten al desempeño de su actividad como las responsabilidades en que pudiera incurrir en caso de incumplirlas.

Examinando la relación actualizada de usuarios del sistema y de derechos de acceso establecidos, comprobará que cada usuario está autorizado para acceder únicamente a aquellos datos y recursos informáticos que precisa para el desarrollo de sus funciones.

El equipo auditor deberá comprobar si se han establecido procedimientos de identificación y autenticación para el acceso al sistema. Cuando el mecanismo de autenticación se base en contraseñas, determinará si el procedimiento de creación, almacenamiento, distribución y modificación de las mismas garantiza su confidencialidad. También determinará si los usuarios desconectan sus puestos de trabajo al finalizar la jornada y si existe algún mecanismo que produzca la desconexión automática de un usuario tras un período de inactividad determinado, o bien, que precise introducir una contraseña para poder reanudar el trabajo.

En ningún caso, olvidará verificar el cumplimiento de los procedimientos establecidos para solicitar nuevos accesos o modificaciones sobre los derechos definidos para un usuario y que, exclusivamente, el personal autorizado se ocupará de conceder, alterar o anular los derechos de acceso sobre los datos y recursos informáticos.

Seguridad Lógica:

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una computadora, así como de controlar el mal uso de la información. Estos controles reducen el riesgo de caer en situaciones adversas.

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencial de la organización para perder información o bien para que ésta sea utilizada en forma inadecuada; asimismo, esto hace que se vea disminuida su defensa ante competidores, el crimen organizado, personal desleal y violaciones accidentales.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema y restringe el acceso a datos, a los programas de uso general, de uso específico, de las redes y terminales.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

- *Cambio de los datos antes o cuando se le da entrada a la computadora.*
- *Copia de programas y/o información.*
- *Código oculto en un programa.*
- *Entrada de virus.*

La seguridad lógica puede evitar una afectación de pérdida de registros y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

El tipo de seguridad puede comenzar desde la simple llave de acceso (contraseña o password) hasta los sistemas más complicados, pero se debe evaluar que cuanto más complicados sean los dispositivos de seguridad más costosos resultan, por lo tanto, se debe mantener una adecuada relación de seguridad - costo en los sistemas de información.

Uno de los puntos más importantes a considerar para poder definir la seguridad de un sistema es el grado de actuación que puede tener un usuario dentro de un sistema, ya sea que la información se encuentre en un archivo normal o en una base dé datos o bien que se posea una minicomputadora o un sistema en red (interna o externa). Para esto podemos definir los siguientes tipos de usuarios:

- ***Propietario.*** *Es, como su nombre lo indica, el dueño de la información, el responsable de ésta y puede realizar cualquier función (consultar, modificar, actualizar, dar autorización de entrada a otro usuario). Es responsable de la seguridad lógica, en cuanto puede realizar cualquier acción y puede autorizar a otros usuarios de acuerdo con el nivel que desee darles.*
- ***Adininistrador.*** *Sólo puede actualizar o modificar el software con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.*
- ***Usuario principal.*** *Está autorizado por el propietario para hacer modificaciones cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.*
- ***Usuario de consulta.*** *Sólo puede leer la información pero no puede modificarla.*
- ***Usuario de explotación.*** *Puede leer la información y utilizarla para explotación de la misma, principalmente para hacer reportes de diferente índole, los cuales por ejemplo, pueden ser contables o estadísticos.*
- ***Usuario de auditoría.*** *Puede utilizar la información y rastrearla dentro del sistema para fines de auditoría.*

Los usuarios pueden ser múltiples y pueden ser el resultado de la combinación de los antes señalados. Se recomienda que exista sólo un ***usuario propietario*** *y que el administrador sea una persona designada por la gerencia de informática.*

CAPÍTULO IV. ANALISIS COSTO / BENEFICIO

Inciso 4.

Análisis Costo/Beneficio pronosticado contra Costo/Beneficio obtenido:

El desarrollo e implantación de sistemas de información en la organización es una inversión y como tal es susceptible de valoración a lo largo del tiempo. Como en cualquier proyecto que una organización lleve a cabo, habrá costos y beneficios económicos. Debe haber un análisis comparativo para comprobar si los beneficios justifican los costos, si no, el proyecto tiene pocas posibilidades de llevarse a cabo.

Normalmente a la hora de realizar un análisis costo beneficio de un sistema de información se acude a técnicas convencionales de valoración de inversiones, por ejemplo, tasa interna de retorno o TIR, valor actualizado neto o VAN, período de amortización (payback), etc. Normalmente resulta complicado, debido a la dificultad de estimar a priori beneficios. Los costos suelen ser más cuantificables en un principio. Los costos han de estimarse al principio del proyecto, en la fase de viabilidad y revisarse en las fases siguientes.

Utilizar una metodología de análisis de costos facilita la labor.

Entre los costos a considerar en un proyecto de desarrollo e implantación de un sistema de información en la organización, merecen la pena ser destacados:

1. Costos económicos :

*Hay un número de diferentes tipos de **costos asociados a un proyecto**, como por ejemplo;*

- *Análisis de sistemas y diseño: se debe considerar el costo total del proyecto, por supuesto, los costos relativos al estudio de viabilidad no estarán incluidos en este cálculo.*
- *Compra del hardware: hay que barajar alternativas como leasing o renting.*
- *Costos del software: a menudo son los más duros de estimar. El software puede escribirse y desarrollarse de forma exclusiva para la empresa o comprado en la forma de paquete de aplicaciones.*
- *Costos de formación: el personal necesita formarse para utilizar el sistema.*
- *Costos de instalación: puede ser un costo significativo si se tienen que construir nuevas instalaciones, tender cables, adaptaciones, adecuaciones, etc.*
- *Costos de conversión y cambio: tienen que ver con el almacenamiento de los datos del viejo sistema al nuevo de una forma segura. Hay también costos asociados con el cambio resultante del viejo al nuevo sistema.*
- *Costos de oportunidad: si el propósito de la automatización es reemplazar a la gente con máquinas, habrá que pagar dinero doblemente (liquidaciones o reubicaciones, etc.).*

2. Costos operativos:

- *Mantenimiento de hardware y software.*
- *Costos de electricidad, papel, etc.*
- *Costos asociados con el personal para operar el nuevo sistema, por ejemplo un centro de informática, empleados para la introducción de datos, etc.*

Los beneficios, *como ya hemos apuntado son más difíciles de cuantificar. Algunos pueden ser estimados con un alto nivel de certidumbre, otros pueden ser muy inciertos. Muchos beneficios son difíciles de medir.*

Ejemplos de beneficios son:

- *Ahorros en los costos de trabajo: pueden ser predecibles permitiendo incertidumbres en las estimaciones futuras de salarios.*
- *Beneficios debidos a un procesamiento más rápido.*
- *Mayor seguridad y confiabilidad en los procesos e información .*
- *Ahorro de tiempo en el proceso de la información.*
- *Una mejor toma de decisiones.*
- *Mejor servicio al cliente.*
- *Reducción de errores.*

Realizar un análisis ***costo/beneficio*** *del desarrollo e implantación de un determinado sistema de información en la empresa va a suponer, en definitiva, evaluar si ha habido una optimización del negocio por el uso del sistema de información en concreto.*

Normalmente si esto ha ocurrido puede haber sido debido a dos elementos fundamentalmente; una óptima gestión de costos y en este sentido, se podrán haber reducido los costos operativos del negocio o reducido los propios costos de mantenimiento del sistema de información en cuestión.

Un segundo elemento de optimización del negocio puede venir del valor producido, tanto por un aumento de valor de los productos o procesos actuales, así como la posibilidad de haber añadido valor por innovación, esto es, utilizando nuevas formas de llevar a cabo los procesos.

Contemplado friamente y desde el punto de vista "rentabilidad de un recurso", los sistemas de información a desarrollar o adquirir, no siempre expondrán las ventajas y beneficios intangibles que se obtendrán de su aprovechamiento, operación y explotación, debido a que los estudios tradicionales de ***costo/beneficio*** *se elaboran con elementos medibles para su determinación.*

La organización debe tener en consideración ***el valor de dejar de hacer o no llevar a cabo*** *en lo que respecta a un proyecto de sistemas de información, ya que si un desarrollo no es conveniente porque el estudio de* ***costo/beneficio*** *resulto negativo, qué tanto perderá la organización por no contar con aquel y dejar de tener oportunidad en la obtención de información, no contar con los elementos necesarios y exactos para una mejor toma de decisiones, no obtener mejoras en el servicio al cliente, carecer de un procesamiento más rápido y completo de la información, oportunidad para responder a los cambios internos y externos de la organización, reducción de tiempo extraordinario y costos del personal encargado de generar y procesar la información cotidiana y especial.*

Los elementos enunciados en el párrafo anterior, tienen un alto grado de incertidumbre como para ser determinados cuantitativa y cualitativamente y poder formar parte del análisis del estudio de ***costo/beneficio****, por lo que los Directivos Estratégicos y Directivos Tácticos de la organización, deberán valorar cada uno de los beneficios intangibles y decidir si es factible llevar a cabo el proyecto de desarrollo e implantación o soportar el efecto de no hacerlo.*

CAPÍTULO IV. ENCUESTAS A USUARIOS

Inciso 5.

Entrevistas y cuestionarios a usuarios:

Las entrevistas se deberán llevar a cabo para comparar los datos proporcionados y la situación de la Dirección de Informática, desde el punto de vista USUARIOS: su objetivo es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora y los sistemas en operación.

Las entrevistas se deberán de hacer, en caso de ser posible a todos los usuarios o bien en forma aleatoria a algunos de ellos, tanto a los más importantes como a los de menor importancia en cuanto al uso del equipo. La entrevista no siempre tiene la efectividad que se desea ya que los entrevistados pueden ser presionados por los analistas de sistemas o piensan que si se hacen algunos cambios a los sistemas, éstos pueden afectar su trabajo. El gerente debe hacer del conocimiento de los entrevistados el propósito del estudio.

Una guía para la entrevista puede ser la siguiente:

- *Prepárese para la entrevista estudiando los puestos de las personas que van a ser entrevistadas y sus funciones dentro de la organización.*
- *Preséntese y dé un panorama del motivo de la entrevista.*
- *Comience con preguntas generales sobre las funciones, la organización y los métodos de trabajo.*
- *Haga preguntas específicas sobre los procedimientos que puedan dar como resultado señalamiento de mejoría.*
- *Siga los temas tratados en la entrevista.*
- *Limite el tomar nota a lo más relevante, para evitar distracciones.*
- *Al final de la entrevista, ofrezca un resumen de la información obtenida y pregunte cómo se le podrá dar seguimiento.*

*El **diseño de un cuestionario** debe tener una adecuada preparación, elaboración, preevaluación y evaluación. Algunas guías generales son:*

1. *Identificar el grupo que va a ser evaluado.*
2. *Escribir una introducción clara, para que el investigado conozca los objetivos del estudio y el uso que se le dará a la información.*
3. *Determine qué datos deben ser recopilados.*
4. *Elabore las preguntas con toda precisión (no haga preguntas en negativo de tal forma que la persona que las responda lo pueda hacer con toda claridad.*
5. *Estructure las preguntas en forma lógica y secuencial de tal forma que el tiempo de respuesta y escritura sea breve (aunque se deben dejar abiertas las observaciones).*
6. *Elimine todas aquellas preguntas que no tengan un objetivo claro o que sean improcedentes.*

7. *Limite el número de preguntas para evitar que sea demasiado el tiempo de contestación y que se pierda el interés de la persona.*

8. *Implemente un cuestionario piloto, para evaluar que todas las preguntas sean claras y que las respuestas sean las esperadas.*

9. *Diseñe e implemente un plan de recolección de datos.*

10. *Determine el método de análisis que será usado.*

11. *Distribuya los cuestionarios y deles seguimiento para obtener las respuestas deseadas; asimismo, analice los resultados.*

Procure que su cuestionario responda a las siguientes preguntas:

- *¿ Qué áreas pueden ser mejoradas?.*
- *¿Qué información necesita que actualmente no tiene o que es difícil de obtener?*
- *¿Qué cuellos de botella ocurren durante el día? ¿Cómo se pueden eliminar?*
- *¿Cómo se puede cambiar el procedimiento para eliminarlos?*
- *¿Existe un procedimiento que sea redundante o repetitivo?*
- *¿Cómo se podría eliminar esta repetición?*

Desde el punto de vista del usuario los sistemas deben:

1. *Cumplir con los requerimientos totales del usuario.*
2. *Cubrir todos los controles necesarios.*
3. *Ser fácilmente modificables.*
4. *Ser confiables y seguros.*
5. *Poderlos usar a tiempo, y con el menor tiempo y esfuerzo posible.*
6. *Ser amigables.*

Para que un sistema cumpla con los requerimientos del usuario se necesita una comunicación completa entre éste y el responsable del desarrollo del sistema. En ella deben definir claramente los elementos con que cuenta el usuario, las necesidades del proceso de información y los requerimientos de información de salida, almacenada o impresa.

En esta misma etapa debió haberse definido la calidad de la información que será procesada por la computadora, estableciéndose los riesgos de la misma de minimizarlos. Para ello se debieron definir los controles adecuados, estableciéndose además los niveles de acceso a la información, es decir, quién tiene privilegio de consultar, modificar o incluso borrar información.

Esta etapa habrá de ser cuidadosamente verificada por el auditor interno especialista en sistemas y por el auditor en informática, para comprobar que se logró una adecuada comprensión de los requerimientos del usuario y un control satisfactorio de información.

Para verificar si los servicios que se proporcionan a los usuarios son los requeridos y que se están proporcionando en forma adecuada, cuando menos será preciso considerar la siguiente información:

- *Descripción de los servicios prestados.*
- *Criterios que utilizan los usuarios para evaluar el nivel de servicio prestado.*
- *Reporte periódico del uso y concepto del usuario sobre el servicio.*
- *Registro de los requerimientos planteados por el usuario.*
- *Tiempo de uso.*

CAPITULO V

AUDITORIA DEL EQUIPO DE COMPUTO

CAPÍTULO V. DOCUMENTACION Y CONTROLES

Inciso 1.

Control de Respaldos para Medios de Almacenamiento Masivo.

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes, cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia en la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además, se deben tener perfectamente identificados físicamente los archivos para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de proceso.

Los respaldos de la información deben realizarse mensual, semanal o diario y se deben observar los siguientes puntos:

- *Contar con políticas formales por escrito para efectuar los respaldos de la información.*
- *Todos los medios magnéticos de respaldo no deben estar almacenados en un mismo lugar, aunque se tengan los medios magnéticos de operación en el site, por lo que si hubiera una contingencia grave (incendio, inundación), no se tendría el riesgo de perder parte o la totalidad de la información ya que se cuenta en otro lugar con los respaldos.*
- *Debe tenerse acceso restringido al área en donde se tienen almacenados los medios magnéticos, tanto de operación como de respaldo.*
- *Se deben tener identificados los medios magnéticos por fecha, concepto y consecutivo, y es conveniente elaborar y actualizar una relación sobre el contenido de los datos, de los registros y responsables de efectuarlos.*
- *Se debe contar con una política que indique los procedimientos a seguir en cuanto al almacenamiento de los medios magnéticos de respaldo en un lugar diferente de la ubicación del site, en donde se pueda tener acceso las 24 horas del día y donde se designen responsables de mantener actualizada la información vital de la organización.*

El hecho de no contar con estas políticas de respaldo que contemplen los puntos anteriores puede provocar que no se sigan los procedimientos adecuados para realizar los respaldos, que haya riesgo de pérdida de información en caso de alguna contingencia y no tener una disponibilidad inmediata de la información de respaldo para recuperar la información y conseguir una continuidad en la organización.

Se debe elaborar por escrito una serie de políticas y procedimientos para la elaboración de los respaldos, contemplando los pasos a seguir, la información que debe de ser respaldada, según el período correspondiente (mensual, semanal o anual), así como al personal asignado para cada caso.

También se debe especificar la forma de etiquetación, nomenclatura, pruebas, rotación de cintas, los nombres de los responsables de efectuar los respaldos y los medios magnéticos que serán designados para ser resguardados fuera de las instalaciones. También se debe tener una relación por escrito de la ubicación y el contenido de los medios magnéticos, que debe ser entregada al responsable de la seguridad del site, así como al gerente del área de informática.

Dentro de las políticas de respaldo, se debe contar con un punto que indique los procedimientos a seguir en cuanto al almacenamiento de los medios magnéticos de respaldo en un lugar diferente al de la ubicación del site, donde se pueda tener acceso las 24 horas del día y donde se designen responsabilidades de mantener actualizada la información vital de la organización.

Software del manejo de librerías. *Las funciones del software restringen el acceso a librerías críticas; los procedimientos que gobiernan el uso de esas funciones deberán ser revisados, evaluados y probados. El auditor deberá revisar, evaluar y probar lo siguiente:*

- *Documentación de librerías.*
- *Programas fuentes y ejecutables.*
- *Jobs en ejecución y lineamientos de control.*
- *Parámetros de corrida.*
- *Uso de software para restringir el acceso a librerías.*
- *Restricción del acceso a librerías de producción.*
- *Restricciones de funciones que pueden ser usadas para modificar el estado de un programa (pruebas a producción).*
- *Acceso a librerías en prueba.*
- *Convenciones para dar nombre a librerías que son usadas para facilitar la seguridad.*
- *Métodos para clasificar y restringir el acceso a librerías por tipo (fuentes, objeto, carga y control de jobs).*
- *Si el software ejecuta funciones de identificación de usuario y procedimientos de autentificación.*
- *Procedimientos inusuales de las librerías.*
- *Capacidades de la bitácora de auditoría.*
- *Los números de versión del software.*

Los reportes escritos pueden ser usados para organizar las actividades de las librerías de logs de acceso al software manejador de librerías o bitácoras de auditoría.

De adquisiciones de equipo y de centralización y descentralización.

El equipo que se adquiere para una organización debe cumplir con el esquema de adquisición de ésta. En lo posible, se deben tener equipos estándares dentro de la organización, a menos que por requerimientos específicos se necesite un equipo con características distintas. Esto no implica que los equipos tengan que ser del mismo proveedor, aunque sí deben tener la misma filosofía. Las compras por impulso u oportunistas pueden provocar que se tengan diferentes equipos, modelos, estructuras y filosofías. Esto puede provocar problemas de falta de compatibilidad, expansión y de confianza.

Si no se tienen políticas y estándares de compra de equipos de cómputo, cada departamento o empleado puede decidir el adquirir diferentes equipos, los cuales pueden no ser compatibles, o bien el conocimiento y entrenamiento requerirá de mayor tiempo y costo. La conexión de un tipo de termina] o computadora personal a una computadora principal (mainframe) puede requerir de equipo o de software adicional. Los sistemas elaborados para un tipo de computadora pueden no servir en otro tipo de máquina. El mantenimiento es otro factor que puede incrementarse en caso de no tener compatibilidad de equipos.

Tener diferentes plataformas de programación, sistemas operativos, bases de datos equipos de comunicación y lenguajes propietarios, provoca que se incrementen los costos, que se haga más problemático el mantenimiento, que se requiera personal con diferente preparación técnica, y que se necesiten diferentes programas de capacitación.

La posibilidad de que se pueda expandir un equipo es otro de los factores a evaluar. Al crecer una organización, es muy probable que se requiera que los equipos también crezcan y sean más rápidos. Esto es de mayor importancia dependiendo del tamaño de las computadoras, ya que es un factor fundamental en los grandes equipos y de relativamente poca importancia en las computadoras personales, debido a que no es tan alto su costo de reemplazo.

En muchas ocasiones se cambia o se compra una computadora por el factor publicitario, sin que se tenga la evaluación real de los equipos, o bien se adquieren equipos (principalmente computadoras personales) que son ensamblados con partes de diferentes proveedores a costos muy bajos. Se deberá evaluar la ventaja de adquirir lo último en tecnología, contra el costo que esto representa, así como el tener equipos muy baratos pero con baja confianza en el proveedor.

En la actualidad cada día las computadoras son más poderosas y menos costosas y las organizaciones también cada día dependen mas de las computadoras, así es que existe la tendencia de comprar cada día computadoras más poderosas, sin considerar que en el futuro existirán computadoras más poderosas a menor precio. La decisión de adquirir o cambiar una computadora deberá estar basada en un estudio muy detallado que demuestre el incremento de beneficios en relación con su costo y en la relación costo/beneficio de los equipos actuales.

Renta, renta con opción a compra o compra:

Las computadoras y el software pueden rentarse, rentarse con opción a comprarse y en el caso del software, producirse. Cada una tiene sus ventajas y desventajas y es función del auditor el evaluar en cada instalación en específico por qué se escogió una opción y si las ventajas que se obtienen son superiores a sus desventajas.

El auditor deberá evaluar:

- *¿Existe un comité de compra de equipo?*
- *¿Quién participa en el comité?*
- *¿Existen políticas de adquisición de equipos?*
- *¿Cómo se determina el proveedor del equipo?*
- *¿Cómo se evalúan las propuestas de instalación, mantenimiento y entrenamiento?*
- *¿Cómo se evalúa el costo de operación y el medio ambiente requerido para cada equipo?*
- *¿Se evalúan las opciones de compra, renta y renta con opción a compra?*

Los factores a considerar dentro de estas opciones son los siguientes:

Ventajas.

- ***Renta:***

  1. *Compromiso a corto plazo.*
  2. *Menor riesgo de obsolescencia.*
  3. *No requiere de inversión inicial.*

- ***Renta con opción a compra:***

  1. *Menor riesgo de obsolescencia.*
  2. *No requiere de inversión inicial.*
  3. *Se puede ejercer la opción de compra.*
  4. *Los pagos normalmente incluyen servicios.*
  5. *Menor costo que renta.*

- ***Compra:***

  1. *Se puede tener valor de recuperación.*
  2. *Normalmente es menor su costo que el de compra a largo plazo.*

Desventajas.

- ***Renta:***

  1. *Más caro que compra o renta con opción a compra.*
  2. *El equipo puede ser usado.*
  3. *Algunos vendedores de equipo no lo rentan.*

- ***Renta con opción a compra:***

  1. *Es más caro que compra.*
  2. *No tiene valor de recuperación para el comprador.*

- ***Compra:***

  1. *Requiere de inversión inicial o de préstamo.*
  2. *Amarra al comprador a su decisión.*
  3. *El comprador debe conseguir u obtener servicio de mantenimiento.*

Centralización vs. Descentralización.

El tener equipos en forma centralizada o descentralizada puede tener y desventajas, dependiendo del tipo de organización. El auditor deberá evaluar a la organización y la justificación que se tiene para que en una determinada organización se tengan equipos en forma centralizada o descentralizada. En este punto se evalúan las grandes computadoras e instalaciones, eliminando las computadoras personales, ya que éstas deberán estar descentralizadas para cada usuario.

Centralización.

- ***Ventajas:***

1. *Economía de escala.*
2. *Acceso a grandes capacidades.*
3. *Operaciones y administración más profesionales.*
4. *Accesos múltiples a datos comunes.*
5. *Seguridad, control y protección de los datos.*
6. *Un mejor reclutamiento y entrenamiento del personal especializado.*
7. *Una mejor planeación de la carrera profesional del personal de informática.*
8. *Control de los gastos de informática.*
9. *Estandarización de equipos y de software.*

- ***Desventajas:***

1. *Falta de control de los usuarios sobre el desarrollo y operación de los sistemas.*
2. *La responsabilidad del desarrollo de los proyectos está limitada a un selecto personal.*
3. *Posible frustración dentro de la organización por desconocimiento de los cambios en los servicios de informática.*

Descentralización.

- ***Ventajas:***

1. *Autonomía local y control por parte de los usuarios.*
2. *Mayor responsabilidad ante las necesidades de los usuarios.*
3. *Reducción de los costos de telecomunicación.*
4. *Acceso inmediato a las bases de datos descentralizadas.*
5. *Los analistas de sistemas locales tienen mayor atención a las necesidades de los usuarios.*
6. *Oportunidad de crear una carrera profesional dentro de las áreas funcionales de los usuarios.*
7. *Consistente con la descentralización establecida dentro de una estructura corporativa.*

- ***Desventajas:***

1. *Pérdida de control gerencial central.*
2. *Posibilidad de incompatibilidad de datos, equipos y software.*
3. *Posibles errores para seguir los estándares de sistemas dentro de las prácticas de desarrollo.*
4. *Duplicación de personal y de esfuerzo.*

Control de Operación.

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora. Los instructivos de operación proporcionan al operador información sobre los procedimientos que debe seguir en situaciones normales y anormales del procesamiento y si la documentación es incompleta o inadecuada, lo obliga a improvisar o suspender los procesos mientras investiga lo conducente, generando probablemente errores, reprocesos, desperdicio de tiempo de máquina; se incrementan, pues, los costos del procesamiento de datos.

Debemos de considerar la operación de los sistemas en línea, los cuales deben de estar residentes en todo momento con su correspondiente sistema de comunicación, mientras que en cuanto a los sistemas en lote (batch) se debe planear y programar su operación. Para lograr esto existen instalaciones que tienen equipos de computación y comunicación dedicados exclusivamente a los sistemas en línea y otros equipos dedicados únicamente a procesos en lote o batch.

Se debe verificar que el instructivo de operación contenga la siguiente información:

- *Diagramas.*
- *Mensajes y su explicación.*
- *Parámetros y sus explicación.*
- *Fórmulas de verificación.*
- *Observaciones e instrucciones en caso de error.*
- *Calendario de procesos y entrega de resultados.*

Instructivos de operación:

1. *Diagrama de flujo por cada programa.*
2. *Diagrama particular de entrada-salida.*
3. *Mensaje y su explicación.*
4. *Parámetros y su explicación.*
5. *Diseño de impresión de resultados.*
6. *Cifras de control.*
7. *Fórmulas de verificación.*
8. *Observaciones.*
9. *Instrucciones en caso de error.*
10. *Calendario de procesos y resultados.*

CAPÍTULO V. SEGURIDAD DE LOS EQUIPOS

Inciso 2.

Durante mucho tiempo se consideró que los procedimientos de auditoría y seguridad eran responsabilidad de la persona que elabora los sistemas, sin considerar que son responsabilidad del área de informática en cuanto a la elaboración de los sistemas, del usuario en cuanto a la utilización que se le dé a la información y a la forma de accesarla y del departamento de auditoría interna en cuanto a la supervisión y diseño de los controles necesarios.

La seguridad del área de informática tiene como objetivos:

- *Proteger la integridad, exactitud y confidencialidad de la información.*
- *Proteger los activos ante desastres provocados por la mano el hombre y de actos hostiles.*
- *Proteger a la organización contra situaciones externas como desastres naturales y sabotajes.*
- *En caso de desastre, contar con los planes y políticas de contingencias para lograr una pronta recuperación.*
- *Contar con los seguros necesarios que cubran las pérdidas económicas en caso de desastre.*

En la actualidad, principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente en paquetes que son copiados sin autorización (''piratas") y borra o altera toda la información que se tiene en medios magnéticos .

Los virus son pequeñas subrutinas escondidas en los programas que se activa cuando se cumple alguna condición, por ejemplo, haber obtenido una copia en forma ilegal y puede ejecutarse en una fecha o situación predeterminada. El virus normalmente es puesto por los diseñadores de algún tipo de programa (software) para "castigar" a quienes lo roban o copian sin autorización o bien por alguna actitud de venganza en contra de la organización. (En la actualidad existen varios productos para detectar los virus) existen varios tipos de virus pero casi todos actúan corno "caballos de Troya'', es decir, se encuentran dentro de un programa y actúan con determinada indicación, como ejemplo clásico tenemos los desfalcos por computadora (desde un punto de vista técnico).

El uso inadecuado de la computadora comienza desde la utilización del tiempo de máquina para usos ajenos al de la organización , la copia de programas para su comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

En forma paralela a los fraudes, se han desarrollado y perfeccionado los sistemas de seguridad tanto física como lógica; la gran desventaja del aumento de la seguridad lógica, es que se requiere consumir un número mayor de recursos de cómputo para lograr tener una idónea seguridad.

Seguridad lógica y confidencialidad:

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una computadora, así como de controlar el mal uso de la información. Estos controles reducen el riesgo de caer en situaciones adversas.

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencia de la organización para perder información o bien para ésta sea utilizada en forma inadecuada; asimismo, esto hace que se vea disminuida su defensa ante competidores, el crimen organizado, personal desleal y violaciones accidentales.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema y restringe el acceso a datos, a los programas de uso general, de uso específico, de las redes y terminales.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

- *Cambio de los datos antes o cuando se le da entrada a la computadora.*
- *Copias de programas y/o información.*
- *Código oculto en un programa.*
- *Entrada de virus.*

La seguridad lógica puede evitar una afectación de pérdida de registros y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

El tipo de seguridad puede comenzar desde la simple llave de acceso (contraseña o password) hasta los sistemas más complicados, pero se debe evaluar que cuanto más complicados sean los dispositivos de seguridad más costosos resultan. Por lo tanto, se debe mantener una adecuada relación de seguridad /costo en los sistemas de información.

Un método eficaz para proteger sistemas de computo es el software de control de acceso. Dicho de manera simple, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden al usuario una contraseña antes de permitirles entrar a información confidencial. Sin embargo, éstos pueden ser eludidos por delincuentes sofisticados. El sistema integral de seguridad, debe comprender:

- *Elementos administrativos.*
- *Definición de una política de seguridad.*
- *Organización y definición de responsabilidades.*

Confidencialidad, integridad y disponibilidad:

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

- ***La confidencialidad*** *es responsabilidad de los individuos autorizados para consultar (usuario de consulta) o para bajar archivos importantes para microcomputadoras (usuario de explotación).*

- ***La integridad*** *es responsabilidad de los individuos autorizados para modificar datos o programas (usuario administrador) o de los usuarios a los que se otorgan accesos a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo (usuario responsable y principal).*

- ***La disponibilidad*** *es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de base de datos, al monitoreo de teleproceso o al software de telecomunicaciones (usuario administrador).*

Control y rutas de acceso:

El acceso a la computadora no significa tener una entrada sin restricciones. Limitar el acceso sólo a los niveles apropiados puede proporcionar una mayor seguridad.

El objetivo de la seguridad de los sistemas de información es controlar las operaciones y su ambiente mediante el monitoreo del acceso a la información y a los programas, para poder darle un seguimiento y determinar la causa probables de desviaciones. Por ello es conveniente al utilizar algún tipo de software dentro de un sistema, contar con una ruta de acceso.

Como se ha señalado, un usuario puede pasar por uno o múltiples niveles de seguridad antes de obtener el acceso a los programas y datos. Los tipos de restricciones de acceso son:

- *Sólo lectura.*
- *Sólo consulta.*
- *Lectura y consulta.*
- *Lectura y escritura, para crear, actualizar, borrar, ejecutar o copiar.*

El esquema identifica a los usuarios del sistema, los tipos de dispositivos por los cuales se accesa al sistema, el software usado para el acceso al sistema los recursos que pueden ser accesados y los sistemas donde residen estos recursos. Los sistemas pueden ser en línea, fuera de línea, en batch, y rutas de telecomunicación.

El esquema de las rutas de acceso sirve para identificar todos los puntos de control que pueden ser usados para proteger los datos en el sistema. El auditor debe conocer las rutas de acceso para la evaluación de los puntos de control apropiados.

Claves de acceso:

Un área importante en la seguridad lógica es el control de las claves de acceso de los usuarios. Existen diferentes métodos de identificación para el usuario.

- *Un password o código.*

- *Una credencial con banda magnética.*

- *Algo específico del usuario (características propias).*

La identificación es definida como el proceso de distinción de un usuario de otros. La identificación de entrada proporcionará un reconocimiento individual; cada usuario debe tener una identificación de entrada única que debe ser reconocida por el sistema.

- ***Password**, código o llaves de acceso. La identificación de los individuos usualmente conocida y está asociada con un password o clave de acceso. Las claves de acceso pueden ser usadas para controlar el acceso a la computadora, a sus recursos, así como definir nivel de acceso o funciones específicas.*

- ***Credencial con banda magnética**, esta credencial es como la bancaria, pero se recomienda que tenga fotografía y firma. La ventaja más importante de la credencial es prevenir la entrada de impostores al sistema. Una credencial ordinaria es fácil de falsificar, por lo que se debe elaborar de una manera especia, que no permita que sea reproducida.*

- ***Validación por características**. Es un método con tecnología biométrica. Consiste en la verificación de la identidad de la persona, basándose en características propias. Algunos de los dispositivos biométricos son:*

  1. *Las huellas dactilares.*
  2. *La retina.*
  3. *La geometría de la mano.*
  4. *La firma.*
  5. *La voz.*

- ***Firma electrónica o firma digital.** La firma digital tiene la misma función que la firma escrita en cualquier documento. La firma digital es un fragmento de información confidencial y propia de cada usuario que asegura a la persona que envía o autoriza un documento. El receptor o terceras personas pueden verificar que el documento y la firma, corresponden a la persona que lo firma y que el documento no ha sido alterado.*

  Para generar una firma digital, se usan algunos algoritmos públicos. La firma digital es un conjunto de datos que son creados usando una llave secreta, aunque existe una llave pública que es usada para verificar que la firma fue realmente generada usando la llave privada correspondiente. El algoritmo usado para generar la firma electrónica es de tal naturaleza, que si no se usa la llave secreta no es posible usar la firma electrónica.

  La firma digital es un bloque de caracteres que acompaña a un documento (o archivo) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación), de tal forma que el autor queda vinculado al documento de la firma.

  Existe una serie de firmas digitales que identifican y certifican desde el usuario inicial hasta el último usuario. En el caso de envío de documentos, pueden certificar la organización que envía el documento, su departamento y la persona que lo manda o autoriza.

Un sistema seguro de firmas digitales debe comprender dos partes: un método para firmar el documento que sea de tal manera confiable que no pueda ser usado por otras personas, y otro que verifique que la firma fue realmente generada por el que la firma representa, de tal forma que posteriormente no pueda ser cuestionada.

El resultado de un conjunto de datos encriptados es la firma digital. Normalmente, junto con la información, la llave pública que es usada para firmar. Para verificar la información, el receptor primero determina si la llave pertenece a la persona a la cual debe pertenecer, y después de desencriptarla verifica si la información corresponde al mensaje; entonces la firma es aceptada como válida.

Software de control de acceso:

Controla el acceso a la información, grabando e investigando los eventos realizados y el acceso a los recursos, por medio de la identificación del usuario. El software de control de acceso tiene las siguientes funciones:

- *Definición de usuarios.*
- *Definición de las funciones del usuario después de acceder el sistema.*
- *Establecimiento de auditoría a través del uso del sistema.*

El software de seguridad protege los recursos mediante la identificación de los usuarios autorizados con las llaves de acceso, que son archivadas y guardadas por este software.

Esto se hace a través de la creación de archivos o tablas de seguridad, estos paquetes frecuentemente incluyen facilidades para encriptar dichas tablas o archivos.

La bitácora de auditoría, es un programa complementario a otro software como el de las bases de datos o individual que generalmente es proporcionado por el proveedor.

Cada bitácora debe incluir la identificación del usuario: si el acceso es exitoso, deben consignarse todos los elementos accesados, día, hora, terminal y el dato específico de lo que fue modificado durante el acceso; si el acceso no fue exitoso registrará la mayor información posible sobre día, hora, terminal y claves de acceso con las cuales intentaron entrar al sistema.

CAPÍTULO V. MANTENIMIENTO DE LOS EQUIPOS

Inciso 3.

Existen básicamente tres tipos de contrato de mantenimiento. El contrato de ***mantenimiento total****, que* ***incluye el mantenimiento correctivo y preventivo****, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no las incluye. El contrato que incluye refacciones es como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente el más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización de los equipos (este tipo de mantenimiento normalmente se emplea en equipos grandes).*

El segundo tipo de mantenimiento es "por llamada", en el cual se llama al proveedor en caso de descompostura y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerla (casi todos los proveedores incluyen en la cotización de compostura el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como "en banco" y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo y éste hace una cotización de acuerdo con el tiempo necesario para su compostura más las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento debemos primero analizar cuál de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalle que las cláusulas estén perfectamente definidas, que no exista subjetividad y que haya penalización en caso de incumplimiento, para evitar contratos que sean parciales hacia el proveedor.

Para poder exigir el cumplimiento del contrato se debe tener un estricto control sobre las fallas, la frecuencia y el tiempo de reparación.

Evaluación del mantenimiento:

Cuando se evalúa la capacidad de los equipos, no se debe olvidar que la capacidad bruta disponible se deberá disminuir por las actividades de mantenimiento preventivo, fallas internas y externas no previstas y mantenimiento e instalación de nuevos sistemas.

El enfoque de esta sección se orienta a evaluar, mediante los controles que se tengan en la dirección, la utilización del sistema de cómputo. Un control adecuado permitirá sustentar sólidamente cualquier solicitud de expansión de la configuración presente. Se debe tener control de las fallas y del mantenimiento no sólo del equipo central, sino del total de los equipos, incluyendo computadores personales, impresoras, equipo de comunicaciones y periféricos.

Paralelamente al mantenimiento de los equipos, se deberá llevar estadísticas de los siguientes puntos para ver y analizar la productividad de los recursos humanos y programáticos.

- *Programadores que utilizan el equipo o el tiempo para aplicaciones ajenas a la organización.*
- *Personal que utiliza la computadora para trabajos personales, trabajos no autorizados o juegos.*

- *Tiempo real de utilización en trabajos de la organización.*

- *Programas que, por estar mal elaborados (generalmente cuando se usan grandes archivos), degradan la máquina.*

Los siguientes son puntos que deberán ser tomados en cuenta para determinar el rendimiento y productividad de los elementos de la tecnología de información que se esté utilizando y ***el tiempo empleado por los proveedores del servicio de mantenimiento para resolver los problemas:***

- *Degradación del equipo por fallas en equipos periféricos. La computadora puede considerarse como un proceso en línea el cual, al fallar alguna de las unidades principales (memoria, unidad central), no permite la utilización del resto del equipo, pero existen unidades secundarias (cintas, impresoras, terminales, discos) que al fallar provocan que se vea reducida la posibilidad de utilización del equipo.*

  Si tenemos una impresora y se descompone, un alto porcentaje de utilización del equipo se ve disminuida, aunque el proveedor considere que sólo una unidad secundaria fue dañada. Lo mismo sucede si se tienen dos unidades de disco y se descompone una (en caso de tener sólo una unidad de discos, la falla es total), la utilización del equipo se reduce al 50 %.

  Para controlar este tipo de degradación se puede tener un reporte que contenga :

  1. *Dispositivo que integra la configuración del equipo (por ejemplo: cinta, disco, impresora).*

  2. *Número de dispositivo: si tenemos por ejemplo dos cintas, se anota 1 y 2, dependiendo de cuál fue la que falló.*

  3. *Tipo de falla: se anotará una buena descripción del tipo de falla, para lo cual se puede elaborar un catálogo.*

  4. *Porcentaje de degradación. Este dato deberá ser anotado por los responsables de la dirección de informática basándose en la experiencia y en las implicaciones que tenga en el sistema total (por ejemplo, si se tienen dos unidades de disco la degradación es del 50 % , si se descomponen las dos es del 100 % y si se tiene sólo una, también es del 100 % ; en el caso de la impresora si se tiene sólo una puede ser del 66.6 % , etc.).*

  5. *Número de horas que duró la falla, desde el momento de la descompostura hasta el momento en que la entregue reparada el proveedor.*

  6. *Obtener estadísticas o reportes concentrados que indiquen lo siguiente:*

     - *tiempos totales de falla en los equipos*
     - *tiempos totales de mal uso de los equipos*
     - *tiempo de atención del mantenimiento del equipo (lapso de tiempo transcurrido entre el momento en que se reportó la falla al proveedor del mantenimiento y el momento en que se reanudó el servicio en ese determinado equipo).*

CAPÍTULO V. ORDEN Y PLAN DE CONTINGENCIA PARA EL CENTRO DE COMPUTO

Inciso 4.

Una dirección de informática bien administrada debe tener y observa reglas relativas a la ubicación, orden y cuidado de la sala de máquinas. Los dispositivos del sistema de cómputo y los archivos magnéticos pueden ser dañados si se manejan en forma inadecuada, lo que puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Por ello, se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro de la sala de máquinas.

Ubicación y Construcción del centro de Cómputo:

En la actualidad se considera extremadamente peligroso tener el centro de cómputo en áreas con alto tráfico de personas o bien en un lugar cercano a la calle o tener invitados a conocer el centro, ya que el excesivo flujo de personal interfiere con la eficiencia en el trabajo y disminuye la seguridad.

Referente a los materiales de construcción del centro de cómputo, no deben ser altamente inflamables, que no despidan humo tóxico y que las paredes queden perfectamente selladas para evitar la entrada de polvo el cual debe ser evitado.

Otro punto importante es la orientación del centro de cómputo, el cual no debe estar expuesto al sol ni en lugares calurosos o tener grandes ventanales que propicien la entrada del sol, debido a que alterarían la temperatura ambiente a la que deben trabajar los equipos de cómputo y en un momento dado dañarían los medios magnéticos en los que se almacena la información de la organización.

Ductos de aire acondicionado:

Los ductos del aire acondicionado deben estar siempre limpios ya que son una de las principales causas de polvo.

Las instalaciones del aire acondicionado son una fuente de incendio muy frecuente, son susceptibles de ataques físicos, especialmente a través de los ductos, y ataques de forma nociva como pueden ser insectos, ratas, polvo, bacterias, humedad, etc. Se deben instalar redes de protección en todo el sistema de ductos, en exteriores como en interiores y contar con detectores de humo que indiquen la presencia de fuego.

Instalación eléctrica y suministro de energía:

El auditor debe auxiliarse de un especialista para evaluar la instalación eléctrica y el suministro de energía.

Se debe revisar el contar con los planos de la instalación eléctrica, debidamente actualizados. También es común en las oficinas, que al no tener identificados los contactos para las computadoras, éstos sean utilizados para equipos que pueden producir picos, ya que utilizan grandes cargas de corriente, como fotocopiadoras o aires acondicionados.

Se debe tener protección contra roedores o fauna nociva en los cables del sistema eléctrico o comunicaciones, ya que es común que los roedores se coman el plástico de los cables. Si se determina usar veneno o fumigante que éste no provoque problemas al personal que ahí labora.

Los incendios a causa de la electricidad son siempre un riesgo, para reducirlo, los cables deben ser puestos en paneles y canales resistentes al fuego. Los cables deben estar fuera del paso del personal y no deben estar dispersos por toda la oficina, así mismo deben estar identificados por tipo de polaridad y color.

Seguridad contra desastres provocados por agua:

Los centros de cómputo no deben colocarse en sótanos o en áreas de planta baja, sino de preferencia en las partes altas de una estructura de varios pisos aunque hay que cuidar que en zonas sísmicas no queden en lugares donde el peso ocasionado por equipos o papel pueda provocar problemas.

Se debe evaluar la mejor opción, dependiendo de la seguridad de acceso al centro de cómputo, cuando en la zona existen problemas de inundaciones o son sísmicas. En caso de ser zona de inundaciones o con problemas de drenaje la mejor opción es colocar el centro de cómputo en áreas donde el riesgo de inundación no sea evidente.

Algunas causas de esto pueden ser la ruptura de cañerías o el bloqueo del drenaje, por lo tanto, la ubicación de las cañerías en un centro de cómputo es una decisión importante, así como considerar el nivel del manto freático.

Debe considerarse el riesgo que representa el drenaje cuando el centro de cómputo se localiza en un sótano.

Deben instalarse, si es el caso, detectores de agua o inundación, así como bombas de emergencia para resolver inundaciones inesperadas.

Otro de los cuidados que se deben tener para evitar daños por agua es poseer aspersores contra incendio especiales que no sean de agua.

Detección de humo y fuego:

Los detectores de fuego y humo se deben colocar tomando en cuenta la cercanía o no con los aparatos de aire acondicionado, ya que éstos pueden difundir el calor o el humo y no permitir que se active el detector.

El que se elija deberá ser capaz de detectar los distintos tipos de gases que desprenden los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y en consecuencia los incendios ocasionados por un cortocircuito tal vez no sean detectados.

Los detectores de humo y calor se deben instalar en el centro de cómputo en las áreas de oficina, incluyendo el depósito de papelería y el perímetro físico de las instalaciones. Es necesario colocar detectores de humo y de calor bajo el piso y en los conductos de aire acondicionado.

Las alarmas contra incendios deben estar conectadas con la alarma central del lugar o bien directamente con el departamento de bomberos.

La organización se debe cerciorar que los controles de seguridad contra incendios, satisfagan los estándares mínimos del departamento de bomberos.

Temperatura y humedad:

Los cambios de temperatura durante la operación del computador deben ser disminuidos. La variación cíclica de temperatura sobre el rango completo de operación no debe realizarse en menos de ocho horas.

La disipación térmica, el movimiento de aire, así como los mínimos y máximos de temperatura y humedad permitidos deben ser especificados por el proveedor del equipo, aunque la temperatura ideal recomendada es de 22 grados centígrados. Generalmente la humedad debe ser agregada, ya que al enfriar el aire se remueve la mayoría del vapor de agua por condensación.

Se recomienda que se instalen instrumentos registradores de temperatura y humedad. Dichos instrumentos son necesarios para proveer un continuo registro de las condiciones ambientales en el área del equipo.

Plan de contingencia y procedimientos de respaldo para casos de desastre:

Los accidentes pueden surgir por un mal manejo de la administración, por negligencia o por ataques deliberados hechos por ladrones, por fraudes, sabotajes o bien por situaciones propias de la organización (huelgas). El trabajar con posibilidad de que ocurra un desastre es algo común, aunque se debe evitar en lo posible y planear de antemano las medidas en caso de que esto ocurra.

La organización debe tener todos los controles, las funciones y los dispositivos para evitar un desastre, pero en caso de que ocurra, debe contar con un plan de contingencia que permita restaurar el equipo en el menor tiempo posible y con las mínimas consecuencias. En cada dirección de informática se debe establecer y aprobar un plan de emergencia, el cual debe contener tanto el procedimiento como la información necesarios para reanudar la operación del sistema de cómputo en caso de desastre.

Algunas compañías se resisten a tener un plan para casos de desastre o emergencia, pues consideran que es imposible que ocurra un accidente. En los sistemas en línea o en tiempo real, el plan difícilmente puede ser usado en otro equipo, por lo que la única alternativa es tener una alta seguridad en los equipos o bien computadoras en forma de tándem, sin embargo, es necesario que el plan de contingencia con el que se cuenta, permita restaurar el servicio en el menor tiempo posible, con la menor afectación a la organización.

El plan de contingencia debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia se tenga la seguridad de que funcionará.

La prueba del plan de contingencia o emergencia debe hacerse sobre la base de que un desastre es posible y que se han de utilizar respaldos (posiblemente en otras instituciones). Habrá que cambiar la configuración y posiblemente se tengan que usar algunos métodos manuales, no sólo simulando un ambiente ficticio cercano a la realidad, sino considerando que la emergencia puede existir.

El plan de contingencias y el plan de seguridad tienen como finalidad proveer a la organización de requerimientos para su recuperación ante desastres.

Los desastres pueden clasificarse de la siguiente manera:

- *Destrucción completa del centro de cómputo.*
- *Destrucción parcial del centro de cómputo.*

- *Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire acondicionado, etc.).*
- *Destrucción parcial o total de los equipos descentralizados.*
- *Pérdida total o parcial de información, manuales o documentación.*
- *Pérdida de personal clave.*
- *Huelga o problemas laborales.*

La metodología tiene como finalidad conducir de la manera más efectiva, un plan de recuperación ante una contingencia sufrida por la organización. El plan de contingencia es definido como: la identificación y protección de los procesos críticos de la organización y los recursos requeridos para mantener un aceptable nivel de operación y ejecución, protegiendo estos recursos y .preparando procedimientos para asegurar la sobrevivencia de la organización en caso de desastre.

En la elaboración del plan de contingencias deben de intervenir los niveles ejecutivos de la organización y el personal usuario y técnico de los procesos. Para la preparación del plan, se seleccionará el personal que realice las actividades clave de éste. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración, de la dirección de informática (por ejemplo, los jefes de operación, de análisis y programación, y de auditoría interna), cada uno de ellos debe tener tareas específicas, como la operación del equipo de respaldo, la interfase administrativa y la de logística, por ejemplo, el proporcionar los archivos necesarios para el funcionamiento adecuado. Cada miembro del grupo debe tener asignada una tarea y contar con una persona de respaldo, se deberá elaborar un directorio de emergencia con teléfonos particulares que contenga además los nombres y direcciones de las personas que intervienen en el plan, éste deberá estar almacenado en un lugar seguro y accesible.

Entre los objetivos del plan de contingencia se encuentran:

- *Minimizar el impacto del desastre en la organización.*
- *Establecer tareas para evaluar los procesos indispensables de la organización.*
- *Evaluar los procesos de la organización, con el apoyo y autorización respectivos a través de una buena metodología.*
- *Determinar el costo del plan de recuperación, incluyendo la capacitación y la organización para restablecer los procesos críticos de la organización cuando ocurra una interrupción de las operaciones.*

La metodología del plan de contingencias determina los procesos críticos de la organización para restablecer sus operaciones, y debe tomar en cuenta ser eficaz y eficiente, los aspectos legales, el impacto de servicio al cliente y los riesgos para que sobreviva la organización.

Seguros:

Los seguros de los equipos en algunas ocasiones se dejan en segundo término, aunque son de gran importancia. Se tiene poco conocimiento de los riesgos que entraña la computación, ya que en ocasiones el riesgo no es claro para las compañías de seguros, debido a lo nuevo de la herramienta, a la poca experiencia existente sobre desastres y al rápido avance de la tecnología.

Como ejemplo de lo anterior tenemos las pólizas de seguros contra desastres, ya que algunos conceptos son cubiertos por el proveedor del servicio de mantenimiento, lo cual hace que se duplique el seguro, o bien que sobrevengan desastres que no son normales en cualquier otro tipo de ambiente.

Se deben verificar las fechas de vencimiento de las pólizas, pues puede suceder que se tenga la póliza adecuada pero vencida, y que se encuentre actualizada con los nuevos equipos.

El seguro debe cubrir todo el equipo y su instalación, por lo que es probable que una sola póliza no pueda cubrir todo el equipo con las diferentes características (existe equipo que puede ser transportado, como computadoras personales, y otras que no se pueden mover, como unidades de disco duro), por lo que tal vez convenga tener dos o más pólizas por separado, cada una con las especificaciones necesarias.

Se debe tomar en cuenta que existen riesgos que son difíciles de evaluar y de asegurar, como la negligencia. El seguro debe cubrir tanto daños causados por factores externos (terremotos, inundación, etc.) como internos (daños ocasionados por negligencia de los operadores, daños debidos al aire acondicionado, etc.).

También se debe asegurar contra la pérdida de los programas (software), de la información, de los equipos y el costo de recuperación de lo anterior. En el caso de los programas se tendrá en cuenta en el momento de asegurarlos, el costo de crearlos nuevamente y su valor comercial. En el caso del personal, se pueden tener fianzas contra robo, negligencia, daños causados por el personal, sabotaje, acciones deshonestas, etc.

Es importante que la dirección de informática esté preparada para evitar en lo posible el daño físico al personal, oficinas, equipo de cómputo, así como al sistema de operación. Además, deberá tener cuidado de que existan normas y prácticas eficaces.

Condiciones generales del seguro de equipo electrónico:

En la póliza de seguro se certifica que, a reserva de que el asegurado haya pagado a los aseguradores la prima mencionada en la parte descriptiva, y con sujeción a los demás términos, exclusiones, disposiciones y condiciones contenidas o endosadas, los aseguradores indemnizarán en la forma y hasta los límites estipulados en la póliza.

Una vez que la instalación inicial y la puesta en marcha de los bienes asegurados haya finalizado satisfactoriamente, este seguro se aplica, ya sea que los bienes estén operando o en reposo, o hayan sido desmontados con el propósito de ser limpiados o reparados, o mientras sean trasladados dentro de los predios estipulados, o mientras se estén ejecutando las operaciones mencionadas, o durante el remontaje subsiguiente.

La compañía aseguradora en ningún caso será responsable por: pérdidas, daños materiales, perjuicios o gastos causados directa o indirectamente por falta de funcionamiento o por fallas, errores o deficiencias de cualquier dispositivo, aparato, mecanismo, equipo, instalación o sistema, sea o no propiedad del asegurado o que esté bajo control o simple posesión, como consecuencia de la incapacidad de sus componentes físicos o lógicos.

Para efectos de esta cláusula, se entiende por componentes lógicos los sistemas operativos, programas, bases de datos, líneas de código, aplicaciones y demás elementos de computación electrónica, también denominados software, y por componentes físicos, los dispositivos electrónicos o electromecánicos tales como procesadores, microprocesadores, tarjetas de circuitos impresos, discos, unidades lectoras, impresoras, reproductoras, conmutadores, equipos de control y demás elementos conocidos bajo la denominación genérica de hardware.

Los aseguradores no serán responsables por pérdidas o daños, de los cuales no hayan recibido notificación dentro de un determinado número de días después de su ocurrencia.

Una vez notificado a los aseguradores, podrá el asegurado llevar a cabo las reparaciones o reemplazos de pérdidas de menor cuantía, debiendo en todos los demás casos, dar a un representante de los aseguradores oportunidad de inspeccionar la pérdida antes de que se efectúen las reparaciones o alteraciones. Si el representante de los aseguradores no llevara a cabo la inspección dentro de un lapso considerado como razonable bajo estas circunstancias, el asegurado estará autorizado a realizar las reparaciones o reemplazos respectivos.

Es requisito indispensable del seguro que la suma asegurada se igual al valor de reposición del bien asegurado por otro bien nuevo de la misma clase y capacidad, incluyendo fletes, impuestos y derechos aduaneros, si los hubiese, y gastos de montaje.

Si la suma asegurada es inferior al monto que debió asegurarse, los aseguradores indemnizarán solamente aquella proporción que la suma asegurada guarde con el monto que debió asegurarse. Cada uno de los bienes estará sujeto a estas condiciones separadamente.

CAPÍTULO V. PRODUCTIVIDAD

Inciso 5.

Esta parte se relaciona con la dirección de las operaciones de la computadora en términos de la eficiencia y satisfacción del usuario. Esta sección debe ser comparada con la opinión del usuario.

La función clave del personal de cargas de máquina está relacionada con el logro eficiente y efectivo de varios aspectos:

- *Satisfacer las necesidades de tiempo de clientes y usuarios.*
- *La dirección de informática, conjuntamente con los usuarios, deberán determinar el nivel de importancia de proceso de cada aplicación para asignar las prioridades de cómputo en el C.P.D. y ser compatible con la utilización de equipo.*
- *Ser compatible con los programas de recepción y transcripción de datos.*
- *Mantener la utilización de los equipos en línea.*
- *Mantener la utilización de los equipos de teleproceso en niveles óptimos de operación.*
- *Entregar a tiempo y correctamente los productos de los procesos en lotes (batch).*

La experiencia muestra que los mejores resultados se logran en organizaciones que utilizan sistemas formales de programación de actividades, los cuales balancean los factores y miden resultados.

Se deberán evaluar los procedimientos de programación de cargas de máquina para determinar si se ha considerado atenuar los picos de los procesos generados por cierres mensuales o bien los picos de los sistemas en línea y poder balancear las cargas de trabajo de lotes (batch) y línea, dando prioridad a los procesos en línea o contar con equipos que permitan en forma independiente cumplir con las necesidades de procesos en línea, con su comunicación y procesos en lote.

Se deberá contar con un plan de crecimiento a corto y mediano plazo en cuanto a requerimientos de cómputo de nuevas aplicaciones, actividad en línea, actividad en lote, actividades de respaldo, etc. para que no se vea afectada la productividad actual y se conserve el nivel de servicio: también se deberá considerar la antigüedad de los actuales equipos de cómputo en relación a los planes de crecimiento para analizar la posibilidad de establecer su incremento en la configuración de sus recursos o cambio.

En lo posible, se deberá contar con software y hardware de monitoreo de eficiencia de operación, para analizar el rendimiento y comportamiento de aplicaciones y tecnología de información en el computador y mejorar/optimizar el servicio de cómputo.

Se deberá procurar que la distribución física del equipo sea funcional, que la programación de las de máquina satisfaga en forma eficaz al usuario, asimismo se tendrá cuidado con los controles que se tengan para la utilización de equipo y que el mantenimiento de los equipos satisfaga las necesidades.

CAPITULO VI

PRESENTACION DE LA AUDITORIA

CAPÍTULO VI. ANALISIS EVALUACION Y PRESENTACION DE LA AUDITORIA

Inciso 1.

Técnicas para la interpretación de la información:

Para interpretar la información se puede utilizar desde técnicas muy sencillas hasta técnicas complejas de auditoria.

1. Análisis crítico de los hechos:

Una de las primeras técnicas es el análisis crítico de los hechos. Esta técnica sirve para discriminar y evaluar la información; es una herramienta muy valiosa para la evaluación y se basa en la aplicación de las siguientes preguntas:

Pregunta	***Finalidad que determina***
Qué	*El propósito*
Dónde	*El lugar.*
Cuándo	*El orden y el momento, sucesión.*
Quién	*La persona*
Cómo	*Los medios*
Cuánto	*La cantidad*

*La pregunta más importante es **qué**, pues la respuesta permitirá saber si puede ser:*

- *Eliminada.*
- *Modificada o cambiada.*
- *Simplificada.*

*Las respuestas que se obtengan deben ser sometidas a una nueva pregunta; **"por qué"**, la cual planteará un nuevo examen que habrá de justificar la información obtenida. Cada interrogante se debe descomponer de la siguiente manera:*

A. Propósito:

- *Qué se hace.*
- *Por qué se hace.*
- *Qué otra cosa podría hacerse.*
- *Qué debería hacerse.*

B. Lugar:

- *Dónde se hace.*
- *Por qué se hace ahí.*
- *En qué otro lugar podría hacerse.*
- *Dónde debería hacerse.*

C. Sucesión:

- *Cuándo se hace.*
- *Por qué se hace entonces.*
- *Cuándo podría hacerse.*
- *Cuándo deberá hacerse.*

D. Persona:

- *Quién lo hace.*
- *Por qué lo hace esa persona.*
- *Qué otra persona podría hacerlo.*
- *Quién debería hacerlo.*

E. Medios:

- *Cómo se hace.*
- *Por qué se hace de ese modo.*
- *De qué otro modo podría hacerse.*
- *Cómo debería hacerse.*

F. Cantidad:

- *Cuánto se hace.*
- *Por qué se hace esa cantidad (volumen).*
- *Cuánto podría hacerse*
- *Cuánto debería hacerse.*

2. Evaluación de los sistemas:

Se debe evaluar el desarrollo que ha tenido el sistema mediante el análisis de los pasos que comprendió el desarrollo del sistema y comparar lo que se planeó contra lo que realmente se está obteniendo.

Análisis:

Se debe evaluar la información obtenida en los sistemas para poder:

- *Determinar el objeto y compararlo con lo obtenido.*
- *Buscar la interrelación con otros sistemas.*
- *Evaluar la secuencia y flujo de interacciones*
- *Evaluar la satisfacción del usuario*

Entre las etapas de análisis están:

1. *Análisis conceptual:*

   - *Evaluar el sistema funcional.*
   - *Evaluar la modularidad del sistema.*
   - *Evaluar la segmentación del sistema.*
   - *Evaluar la fragmentación del sistema.*
   - *Evaluar la madurez del sistema.*
   - *Evaluar los objetivos particulares del sistema.*
   - *Evaluar el flujo actual de información.*
   - *Definir el contenido de los reportes y compararlo con el objetivo.*

2. *Evaluar el modelo de reportes:*

   - *Evaluar los controles de operación.*
   - *Cuantificar el volumen de información.*
   - *Evaluar la presentación y ajustes.*

Se debe conocer en términos generales, el nivel del sistema funcional para obtener los elementos suficientes que permitan evaluar el nivel de interacción, su grado de estructuración y la madurez del sistema con el fin de determinar si se justifica su automatización.

Evaluación de los sistemas de información:

Esta función tiene una gran importancia en el ciclo de evaluación de las aplicaciones de sistemas de información por computadora. Busca comprobar que la aplicación cumpla las especificaciones requeridas por el usuario, que se haya desarrollado dentro de lo presupuestado y que efectivamente cumpla con los objetivos y beneficios esperados.

Un cambio a un sistema existente, como la creación de uno nuevo, introduce necesariamente cambios en la forma de obtener la información y un costo adicional. Ambos deberán ser evaluados antes y después del desarrollo.

Se debe evaluar el cambio (si lo hay) de la forma en que las operaciones son ejecutadas, comprobar si mejora la exactitud de la información generada, si la obtención de los reportes efectivamente reduce el tiempo de entrega, si es más completa, en qué tanto afecta las actividades del personal usuario, si aumenta o disminuye el personal de la organización y los cambios de las interacciones entre los miembros de la organización. De ese modo se sabrá si aumenta o disminuye el esfuerzo por generar la información para la toma de decisiones, con el objeto de estar en condiciones de determinar la productividad y calidad sistema.

Evaluación en la ejecución:

Se refiere al uso de cuestionarios para recabar datos acerca de la actuación de la aplicación en la computadora, con objeto de conocer qué tan bien o qué tan mal está siendo usada y si opera eficientemente.

Los cuestionarios son medios para recopilar datos acerca del uso de los recursos de la computadora y pueden ser cuestionarios, manuales, encuestas de opiniones, evaluación de documentación, obtención de información electrónica integrada al equipo (hardware) y de programas ejecutándose (software), obteniéndose en ambas las estadísticas acerca de su uso.

Los dispositivos de hardware son dispositivos electrónicos que pueden ser conectados a varios puntos del equipo, como lo son en la unidad de control, los canales de comunicación, etc., que durante la ejecución de una aplicación registran cantidad, frecuencia y dirección de los componentes del equipo. Los datos son almacenados normalmente sobre cinta magnética o disco, para que puedan ser analizados después; por ejemplo, algunos de éstos contabilizan la frecuencia de uso de la unidad central de proceso en relación con la espera para operaciones de entrada-salida. Analizando estos datos quizá se detecte la necesidad de agregar procesadores de entrada-salida con objeto de acortar la espera del procesador central, eliminando los cuellos de botella que por esta causa se generan.

Las estadísticas de software son juegos de instrucciones ejecutables conectadas al sistema operativo con el fin de colectar datos acerca de la operación del sistema y acerca de los programas de aplicación. Este tipo de monitor requiere memoria y proceso adicional, lo que disminuye la rapidez del procesador. Los datos también son almacenados en cinta magnética o cualquier otro dispositivo de almacenamiento secundario con el fin de analizarlos después. Este monitor ayuda a detectar qué recursos adicionales se necesitan o qué recursos existentes deben ser ejecutados para lograr más eficiencia.

Basándose en esta información, el auditor contará con los datos necesarios para hacer las evaluaciones tendientes a mejorar el servicio e incrementar la eficiencia y la planeación de necesidades..

Evaluación en el impacto:

Es la evaluación que se hace sobre la manera en que afecta a la gente que interviene en la aplicación (usuarios) con el objeto de determinar cómo la implantación y el uso del sistema de información afecta a la

organización distinguiendo qué factores son directamente atribuibles al sistema. Las principales áreas que deben interesar son las que intervienen en la toma de decisiones y en las actividades de operación.

Esta evaluación se hace con el fin de detectar a la gente involucrada; las actividades que son necesarias realizar, la calidad de la información, y el costo de operación resultante.

Algunas expectativas deben ser elaboradas y jerarquizadas antes de empezar a diseñar el sistema con el fin de que, cuando se instale, se compruebe si los resultados satisfacen plenamente lo planeado. Estos datos también son importantes para guiar futuros proyectos.

Asimismo se debe evaluar el efecto que tiene sobre el ambiente del sistema (personas, leyes, etc.). Para ello contamos con varias técnicas que nos ayudan en este propósito, las cuales son: bitácora de eventos, registro de actitudes, contribución, peso y análisis de sistemas.

Evaluación económica:

La evaluación económica es la actividad que se encarga de obtener el costo de una aplicación y cuantificar los beneficios esperados, con el objeto de justificar su desarrollo, o comprobar que la aplicación se desarrolló según lo presupuestado. Ello ha de ser considerado por el auditor para evaluar el impacto económico del sistema dentro de la organización en relación con los beneficios obtenidos por éste.

En el impacto se mide cómo una aplicación de sistemas de información, ha contribuido o mejorado la eficiencia en el área donde se usa. Asimismo la evaluación después de su implementación, es crítica para conocer cómo el sistema opera y dónde pueden necesitarse cambios.

La evaluación económica es importante puesto que el capital de la organización no es gratuito, debiéndose cuantificar los beneficios y los costos del sistema en términos monetarios para estar en condiciones de justificar o no su desarrollo e implantación.

Cuando la aplicación ha sido realizada, se busca obtener el costo real contra el beneficio real para comprobar o determinar el porqué de la diferencia con lo presupuestado y/o la calidad de la aplicación.

Estas técnicas nos ayudan a obtener los elementos necesarios para evaluar por medio de un análisis de costo/ beneficio de la aplicación. Nos permite además evaluar si fue desarrollado en las condiciones económicas esperadas, por lo que este análisis deberá efectuarse antes y después del desarrollo de la aplicación. La justificación la encontramos en el hecho de que cualquier tipo de organización busca alcanzar sus objetivos con recursos económicos limitados.

Evaluación subjetiva:

Partiendo de la premisa de que los usuarios son los principales afectados directamente por el sistema, sus puntos de vista y necesidades deberán ser considerados para la evaluación.

Los que procesan los datos, el personal de sistemas y el personal de alta dirección deberán también participar en la determinación de los beneficios económicos de la actividad particular desarrollada.

La justificación de evaluación subjetiva se centra en que la opinión del grupo usuario proporciona un punto de vista más completo de la aplicación, ayudando a obtener aquellos factores que hubiéramos pasado por alto.

Un procedimiento de la evaluación subjetiva es el uso de cuestionarios que se aplicarán a un grupo de administradores, usuarios y personal de sistemas para contestar una secuencia de preguntas que a la larga dejan una contribución en pesos. Incluyen especificaciones detalladas de la intención del proyecto y simples respuestas; no hay referencia a costos, sólo se estiman los beneficios del proyecto.

Estas preguntas serán proporcionadas a los miembros del grupo, en varios tiempos o etapas y todos reciben retroalimentación de las respuestas de otros miembros, entre cada ronda de preguntas. La gente entonces puede cambiar sus evaluaciones y aclarar su retroalimentación; se puede saber quién formuló las evaluaciones y su nivel. El proyecto es evaluado en términos de cuánto pagaría por la información sin hacer referencia a términos vagos para su valoración.

Otro método es por medio del desarrollo de una metodología que mida el valor de la información generada por la aplicación y la ganancia de su uso; esto implicaría un valor estimado por el usuario de los posibles beneficios.

Usando la estimación subjetiva es posible obtener diversas opiniones dentro del informe mientras se obliga a los miembros del grupo a examinar sus propios razonamientos acerca de la aplicación a través de la retroalimentación de otras opiniones. Este método se centra en la pregunta: "¿cuánto pagaría por esta información?" y no en "¿cuál es el valor de la información?", la cual descansa sobre la mala definición y dificultad para comprender el concepto del valor de la información.

Para poder obtener la contestación a estas preguntas, el auditor deberá encarar la tarea de determinar cuánto dinero le cuesta a la organización asignar el proyecto específico y poder compararlo con otros proyectos (costo de oportunidad).

Controles:

Un punto muy importante a considerar dentro de la auditoría son los controles los cuales se dividen en generales, operativos (dependiendo del sistema) y técnicos (equipos y sistemas).

Los controles generales normalmente se aplican a todo el procesamiento de la información y son independientes de las aplicaciones, estos controles incluyen:

- *Planeación.*
- *Organización.*
- *Políticas y procedimientos.*
- *Estándares.*
- *Admón. de recursos.*
- *Seguridad.*
- *Confidencialidad.*

Los controles operativos comprenden cada uno de los sistemas en forma individual y constan de :

- *Control de flujo de la información.*
- *Control de proyectos.*
- *Organización del proyecto.*
- *Reporte de avance.*
- *Revisiones del diseño del sistema.*
- *Técnicas:*

    1. *De usuario:*
    2. *De control.*

- *Control de cambios a programa:*

    1. *Requisición de cambio.*
    2. *Razón del cambio.*
    3. *Naturaleza del cambio.*
    4. *Persona que lo solicita.*
    5. *Persona que revisa y autoriza.*
    6. *Frecuencia de cambios.*

7. *Persona asignada al mantenimiento.*
8. *Bitácora de cambios.*

- *Mantenimiento y documentación.*
- *Producción.*
- *Controles de documentación.*
- *Documentación:*

1. *Del sistema.*
2. *Del programa.*

- *Mantenimiento y acceso a la documentación.*
- *Control de sistemas y programas.*
- *Sistemas en lote (batch):*

1. *De entrada.*
2. *Autorización de entrada.*
3. *Armado de lotes.*
4. *Verificación de lotes.*

- *Control de programas*
- *Reporte de control:*

1. *Balanceo de lotes.*
2. *Reporte de errores.*
3. *Reporte de excepción.*
4. *Reporte de transacciones.*
5. *Reporte de cambios en el archivo maestro.*

- *Validación de entradas:*

1. *Verificación de secuencia.*
2. *Campos omitidos.*
3. *Totales de control.*
4. *Transacciones válidas.*
5. *Caracteres válidos.*
6. *Campos válidos.*
7. *Códigos válidos.*
8. *Pruebas de razonabilidad.*
9. *Dígito verificador.*
10. *Etiquetado de archivos.*

- *Controles de programas misceláneos:*

1. *Control de programa a programa.*
2. *Verificación de etiquetas de archivo.*
3. *Intervención del operador.*
4. *Punto de verificación y reinicio.*
5. *Control de salida.*
6. *Formato de salida.*
7. *Control de formas de salida.*
8. *Corrección de errores.*
9. *Controles corrida a corrida.*
10. *Sistemas en línea.*

- *Controles de entrada:*

    1. *Acceso a terminales.*
    2. *Acceso a programas, archivos, datos y a la computadora.*
    3. *Comunicaciones.*
    4. *Información confidencial.*

- *Controles de programas:*

    1. *Reportes de control.*
    2. *Validación de entrada.*

- *Corrección de errores.*
- *Puntos de verificación y reinicio.*
- *Controles de salida:*

    1. *Formatos de reporte.*
    2. *Formas de control de salida.*
    3. *Información confidencial.*

Los controles técnicos que se deben evaluar son:

- *Controles de operación y uso de la computadora.*
- *Supervisor.*
- *Capturistas.*
- *Bibliotecario.*
- *Operadores.*
- *Controles de entrada y salida.*
- *Recepción de información.*
- *Detección y corrección de errores.*
- *Distribución de la información.*
- *Calendarización.*
- *Reporte de fallas y mantenimiento preventivo.*
- *Controles sobre archivos.*
- *Recuperación de desastres.*
- *Controles de usuarios.*
- *De origen de datos.*
- *Origen de documentación fuente.*
- *Autorización de documentación fuente.*
- *Recolección y preparación de entrada y documentación fuente.*
- *Manejo de errores de documentación fuente:*

    1. *Tipos de errores que pueden aparecer.*
    2. *Pasos a seguir para su corrección.*

Los métodos a utilizar para recuperar documentos fuente corregidos son:

- *Retención de documentos fuente.*
- *Controles de entrada de datos.*
- *Conversión de datos y captura.*
- *Validación de datos.*
- *Manejo de errores en datos y captura.*
- *Controles de salida de datos.*
- *Balanceo y conciliación de salidas.*
- *Distribución de salidas.*
- *Procedimientos documentados que describen los métodos de distribución.*

- *Calendarización, revisión y distribución de salida por parte de los usuarios.*
- *Bitácoras de reportes.*
- *Manejo y retención de registros de salida y documentos contables.*
- *Formatos de salida:*

    1. *Frecuencia.*
    2. *Número de copias.*

Controles técnicos:

- *Programática.*
- *Aplicaciones.*
- *Sistemas.*

Recursos de los programas por aplicación:

- *Calendario de programas.*
- *Errores y recuperación.*

Registro contable:

- *Equipos.*
- *Unidad control de procesos.*
- *Memoria secundaria.*
- *Dispositivos periféricos.*

Controles lógicos del sistema:

- *Sistemas operativos.*
- *Sistemas de utilería.*
- *Sistemas de bibliotecas.*
- *Sistemas de mantenimiento de archivo.*
- *Sistemas de seguridad:*

    1. *Control de acceso al sistema.*
    2. *Control de cambios al sistema:*

- *Redundancia en la información.*
- *Inconsistencia de datos.*
- *Seguridad.*

Controles de seguridad, respaldo y confidencialidad.

Sobre las bases de los objetivos de la auditoría en informática se deben presentar, de acuerdo con la información obtenida, los controles existentes, las conclusiones, opiniones y alternativas de solución debidamente fundamentadas en cuanto a:

- *Evaluación de los sistemas.*
- *Evaluación de los equipos.*

3. Presentación de la Auditoría:

La presentación de las conclusiones de la auditoría podrá hacerse en la siguiente forma:

1.- Una breve descripción de la situación actual en la cual se reflejen los puntos más importantes. Esta presentación es para los niveles más altos de la organización.

2.- Una descripción detallada que comprende:

- *Los problemas detectados.*
- *Posibles causas, problemas y fallas que originaron la situación presentada.*
- *Repercusiones que pueden tener los problemas detectados.*
- *Alternativas de solución.*
- *Comentarios y observaciones de la dirección de informática y de los usuarios sobre soluciones propuestas.*

Si se opta por alguna alternativa de solución, cuáles son sus repercusiones, ventajas y desventajas y tiempo estimado para efectuar el cambio.

1.- Se debe hacer hincapié en cómo se corregirá el problema o se mejorará una determinada situación, se obtendrán los beneficios, en cuánto tiempo y cuáles son los puntos débiles.

2.- Se debe romper la resistencia a la lectura que tienen algunos ejecutivos por medio de conclusiones concretas que sean sencillas (se procurará que se entiendan los términos técnicos y si es posible, usar técnicas audiovisuales).

CAPÍTULO VI. DICTAMEN DE LA AUDITORIA EN INFORMATICA

Inciso 2.

DISEÑO DE PAPELES DE TRABAJO:

El diseño de los papeles de trabajo depende de las pruebas que se han definido para levantar evidencia suficiente y competente.

El formato de cada papel de trabajo deberá estar de acuerdo con el objetivo y evidentemente, el tipo de información que se vaya a obtener del área auditada.

Cuando el papel de trabajo recoge información detallada a nivel del origen. se denomina cédula analítica o de comprobación y cuando el papel de trabajo se utiliza para resumir la información que se encuentra en las cédulas analíticas, toma el nombre de cédula sumaria.

Normalmente. todo papel de trabajo tiene los siguientes componentes:

1.- Identificación.
Nombre de la empresa.
Nombre del papel de trabajo.
Fecha o período auditado.

2. Cuerpo del papel de trabajo; en el cuerpo del papel de trabajo se registra la información que se ha obtenido, en el orden y grado de detalle deseado. Cuando el papel de trabajo contenga información que permita cubrir totalmente un punto de control, se debe redactar una conclusión relacionada con la efectividad del sistema de control o en su defecto, puntualizando los hallazgos detectados.

3. Responsabilidad; en la parte final del papel de trabajo se define la responsabilidad de quienes participaron en su elaboración, a nivel de: preparación, revisión, aprobación.

En el evento de encontrar deficiencias de control interno o hallazgos como se denominan en auditoría operacional, entonces los papeles de trabajo deberán facilitar la presentación de los atributos correspondientes, en la forma siguiente: condición, criterio, efecto, causa.

Además debe redactarse: la conclusión y la recomendación.

El área de informática debe tener una carpeta de papeles de trabajo. para efectos de auditoría, que comprenda por lo menos los siguientes archivos:

1.- Archivo permanente.

2.- Archivo corriente.

En el archivo permanente van los papeles de trabajo que sirven para varias auditorías y al archivo transitorio o corriente se llevan los papeles de trabajo útiles únicamente para la auditoría del período auditado.

Otros componentes de los papeles de trabajo son el índice y las marcas. El ***índice*** *sirve para organizar los papeles de trabajo y poderlos ubicar y hacer cruces entre ellos con facilidad y las* ***marcas*** *se utilizan para expresar conceptos repetitivos.*

OBTENCION DE EVIDENCIAS.

En la fase del proceso de auditoría denominada " obtención de evidencias" se ejecutan las pruebas de auditoría, diligenciando los papeles de trabajo, debidamente diseñados, con base en el nivel de detalle de la información que se haya previsto obtener para determinar el grado de validez del sistema de control interno que opera en el área de informática.

ANALISIS DE EVIDENCIAS.

El auditor, organiza los papeles de trabajo diligenciados y analiza los resultados de las pruebas para detectar las deficiencias de control interno y su correspondiente materialidad o grado de riesgo que puedan representar en el área de informática.

RECOMENDACIONES DE CONTROL INTERNO.

Detectadas las deficiencias de control interno, por cada una de las fases del ciclo del área de informática, se deben presentar en un formato que permita ubicar el problema de control y formular la recomendación correspondiente en:

1. *Area de control.*
2. *Puntos de control.*
3. *Deficiencias de control.*
4. *Causas.*
5. *Efectos.*
6. *Recomendaciones.*
7. *Análisis de costo/beneficio.*

INFORME DE AUDITORIA.

El informe de auditoría al área de informática debe hacerse con base en el siguiente formato:

1. *Alcance de la auditoría: en el alcance de la auditoría, se define el objeto auditable.. En este caso, el área de informática, integrada básicamente, por las funciones propias de su especialidad.*

2. *Declaración de normas aplicadas: el auditor debe expresar que su trabajo fue ejecutado con base en las normas de auditoría generalmente aceptadas, denominadas normas personales, normas para la ejecución del trabajo y normas para la preparación de informes. El auditor debe manifestar, si así lo hizo, que su trabajo fue realizado, de acuerdo con las normas internacionales de auditoría y que, en consecuencia, se ejecutaron las pruebas que se consideraron necesarias en las distintas circunstancias.*

3. *Opinión del auditor: en la opinión, el auditor expresará si el sistema de control interno del área de informática es confiable, si se está poniendo en práctica una metodología adecuada y si los productos y servicios producidos aseguran óptimos niveles de economicidad, eficiencia, efectividad y servicio.*

Como puede apreciarse, la opinión del auditor está ampliamente dirigida hacia el concepto de auditoría operacional, lo cual implica, obviamente un enfoque de tipo gerencial.

Elaboración del Informe Final.

Una vez ejecutada la auditoría informática se procederá a la materialización de ésta por escrito, de forma documental en un informe final, que será el exponente principal de la calidad del trabajo realizado.

El informe final debe estructurarse claramente en cinco partes:

1. *Preparación*
2. *Planificación*
3. *Situación actual*
4. *Diagnóstico*
5. *Recomendaciones.*

Estas cinco fases metodológicas pueden agruparse en dos grandes etapas, la primera de preparación y planificación de la auditoría informática y la segunda, la propia realización de la auditoría informática.

El auditor debe avalar su juicio siempre por escrito en el principal documento de la auditoría informática, que es el informe final. Como producto de la auditoría informática existirán otros documentos como informes parciales, borradores y papeles de trabajo, necesarios para conjugar la visión analítica utilizada en la ejecución de la auditoría informática con la visión sintética a expresar en el informe final.

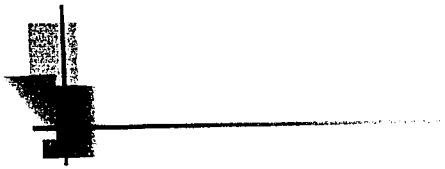
Como regla general, el informe sólo debe incluir hechos importantes y consolidados, es decir, verificados objetivamente y documentalmente probados y soportados.

La estructura del informe final de la auditoría informática recogerá los siguientes puntos:

- *Presentación: se detalla el equipo de trabajo, fechas de comienzo y fin de la auditoría, los auditados entrevistados con indicación de su puesto y los informes parciales entregados.*
- *Definición de ámbito y objetivos.*
- *Enumeración de temas considerados: aplicaciones, ubicaciones, entornos.*
- *Análisis de la situación actual: situación prevista, situación real, tendencias, puntos débiles y amenazas que suponen, puntos fuertes y oportunidades.*
- *Recomendaciones: descripción, plan de implantación, beneficios, plan de seguimiento y control.*

*Las **recomendaciones** deben estar soportadas por datos sólidos y ser viables, claras, específicas, expresadas en términos comprensibles por la Dirección y apoyadas con información técnica (en anexos). Las recomendaciones son opiniones, no datos, por tanto son discutibles y hay que convencer al auditado de su facilidad de implantación y su eficiencia en costo/beneficio.*

El informe final suele acompañarse con un informe resumen para la Dirección, donde en no más de 4 folios, se sintetice el resultado de la auditoría en lo concerniente a las debilidades (en orden de importancia de mayor a menor). Las recomendaciones no se suelen incluir en este documento.



BIBLIOGRAFIA

BIBLIOGRAFIA:

Auditoría en Informática, Lic. y C.P. José Antonio Echenique García. Facultad de Contaduría y Administración , Universidad Nacional Autónoma de México.

Dirección y gestión de los sistemas de información en la empresa, Carmen de Pablos Heredero, Víctor Izquierdo Loyola, José Joaquín López-Hermoso Aguis, Santiago Martín-Romo Romero, Antonio Montero Navarro, José Juan Nájera Sánchez. Universidad Rey Juan Carlos.

Auditoría Informática, un enfoque operacional, Prof. José Dagoberto Pinilla Forero. Facultad de Ciencias Económicas, Universidad Nacional de Colombia.

Auditoría Informática, un enfoque práctico, Mario G. Piattini Velthuis, Emilio del Peso Navarro. Editorial RA-MA, Madrid España, 1998.

Auditoría de los sistemas de información, Rafael Bernal Montañés. Departamento de Organización de Empresas, Economía Financiera y Contabilidad, Universidad Politécnica de Valencia. Oscar Coltell Simón. Departamento de Informática, Universitat Jaume I.

Normas y Procedimientos de Auditoría, Instituto Mexicano de Contadores Públicos. 23ª. Edición.

Auditoría I, C.P. y M.C.A. Juan Ramón Santillana González. Editorial ECASA, 1995.