16
249

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Facultad de Contaduría y Administración

CONTROL, AUDITORIA Y SEGURIDAD EN INFORMATICA

SEMINARIO DE INVESTIGACION INFORMATICA

Que en opción al Grado de

LICENCIADO EN INFORMATICA

p r e s e n t a

CLAUDIA RUIZ RIVAS

Asesor:
C.P. y M.B.A. José Antonio Echenique García

México, D. F. 1993

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE

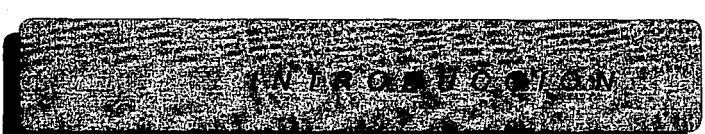
TEMA "CONTROL, AUDITORIA Y SEGURIDAD EN INFORMATICA"

INDICE

INDICE

CAPITULO III

INDICE


UNIVERSITY OF ILLINOIS

I

INTRODUCCION

Antecedentes

Se ha dicho que la Informática constituye la segunda revolución industrial de la humanidad debido a que la sociedad moderna está viviendo un profundo y creciente proceso de "automatización" cobrando una importancia significativa en el desempeño de las actividades de las organizaciones.

Después del elemento humano, el recurso más valioso para cualquier organización es sin duda el de la información, siendo el equipo y los sistemas, elementos que ayudan a incrementar ese valor al mejorar su oportunidad, confiabilidad, uso y almacenamiento.

Sin embargo es necesario tener un conocimiento claro de este importante activo de las organizaciones, ya que, dependiendo del uso que se le dé, puede alcanzar altos niveles de utilidad, o por el contrario puede ser una amenaza potencial para la misma.

Por lo anterior, podemos catalogar a la información como "hechos, datos y opiniones que cambian el grado de incertidumbre en situaciones de toma de decisiones o como la materia prima para el proceso de clarificación de situaciones que hace que la decisión correcta sea más fácilmente identificable". (1)

Durante el proceso normal de generación de la información, llega un momento en que el volúmen es tal, que manejarla en forma manual desde su recopilación y análisis hasta su síntesis, sería demasiado complicado, y es en este momento donde surge un recurso tecnológico: "la computadora".

Este nuevo elemento tecnológico se convierte rápidamente en un factor estratégico por su capacidad de almacenar y procesar gran-

---

(1) Vid. Colegio de Contadores Públicos. Diferentes Enfoques de Auditoría en Informática, México 1991, Pág. 1-2,MIMEO.

des volúmenes de información, pero como en todo, existen riesgos que amenazan el buen funcionamiento de las actividades en una organización. Estos riesgos externos o internos, humanos o naturales, accidentales o voluntarios, así como la posibilidad de pérdida en la capacidad del proceso, la posibilidad de decisiones erróneas y el abuso del computador ocasionan que la información sea vulnerable o susceptible de ser distorsionada, extraviada, destruída o robada. Los efectos de estas vulnerabilidades pueden ser disminuídas, mediante la aplicación y ejercicio de controles. Si estos controles son débiles o inexistentes, la organización estará expuesta a más riesgos, con una mayor probabilidad de ocurrencia y con efectos adversos de mayor repercusión.

El ***Control, Auditoría y Seguridad en Informática*** *son las áreas de la especialidad de Auditoría en Informática que más me interesaron a lo largo de mis estudios profesionales. La Auditoría en Informática es un área de estudio relativamente nueva en nuestro país, por lo que la presente investigación ha sido desarrollada con la finalidad de proporcionar al lector conceptos y lineamientos actualizados que son de utilidad para comprender la importancia de la especialidad que nos ocupa, la cual surge por la necesidad actual de contar con una función encargada de vigilar el entorno computacional, cuyas posibles debilidades inciden básicamente en siete aspectos a mencionar:*

- *Costos organizacionales por pérdida de información*
- *Toma de decisiones incorrecta*
- *Abuso computacional*
- *Valor del hardware, software y personal*
- *Costos elevados de errores de cómputo*
- *Privacidad*
- *Evolución no controlada del uso del computador.*

El proceso de Auditoría informática se puede concebir como la fuerza que ayuda a las organizaciones a lograr sus objetivos, minimizando la materialización de las debilidades y riesgos antes mencionados, además de redituar en el logro de la salvaguarda de

activos, la integridad de datos y la eficiencia y eficacia de los sistemas de información.

Esta función se desarrollará en las organizaciones con base al tamaño, contexto y complejidad de los sistemas.

Hipótesis

Cuando la revisión general de los procedimientos y controles indican que la función de informática es una parte significativa del marco global de control en la organización y que la seguridad y confiabilidad de la información tiene que basarse en la efectividad del desempeño de aquella; se vuelve necesario contar con la participación del especialista dedicado al Control, Auditoría y Seguridad en Informática, quien vigile no sólo la integridad de la misma sino también la eficiencia y eficacia de los sistemas, así como el lugar físico donde se procesan; por medio de la aplicación de Auditorías al desarrollo a los sistemas en operación y a la evaluación de la seguridad física y ambiental que prevalece en los centros de cómputo.

Contenido capitular

La investigación de tesis consta de cuatro capítulos principales y cada uno contiene diversos subcapítulos afines.

Los capítulos inician con una serie de consideraciones preliminares a fin de introducir al lector en el contenido e importancia del capítulo a tratar.

En el contenido de cada uno se proporcionan diversas citas textuales con objeto de proporcionar una bibliografía que sirva de referencia para obtener mayor información y profundizar en el tema que se desee.

El capítulo I introduce a los ***Conceptos Generales*** *que serán tratados y mencionados a lo largo de la investigación, con objeto de formar un criterio y puntos de vista homogéneos; presenta los riesgos a que está expuesta la información y el centro de cómputo; definiciones básicas de control, auditoría, informática y auditoría en informática; así también se propone una ubicación jerárquica del área mencionada en una organización; el idóneo perfil del auditor en informática, y finalmente se identifican las áreas de participación del mismo.*

El capítulo II, ***Auditoría al Desarrollo de Sistemas****, nos introduce a los aspectos relevantes del desarrollo de sistemas, así como a los riesgos que conlleva un inadecuado control sobre esta fase, lo cual justifica la participación del auditor en informática.*

El capítulo III, ***Auditoría a los Sistemas en Operación****, es tratado con mayor profundidad dado que existe un acervo más ámplio de información al respecto y un mayor grado de experiencia y conocimientos en la materia.*

En él se tratan consideraciones preliminares; se presentan los riesgos relativos a las etapas de las aplicaciones (entradas, procesos y salidas), así como los controles para minimizar los posible riesgos que se pudieran presentar; y las herramientas y técnicas asistidas por el computador que el auditor puede utilizar en el desempeño de sus funciones.

La tercera área de participación del auditor en informática es la que se refiere a la Auditoría a centros de cómputo. Debido a que es un tema muy amplio, decidí establecer un alcance y limitación al respecto, por lo que en el capítulo IV, analizo el tema de ***Seguridad Física y Ambiental en los Centros de Cómputo.***

El capítulo presenta consideraciones preliminares las cuales incluye definiciones de un centro de cómputo, privacía, seguridad, disponibilidad e integridad, así como de seguridad física; se examinan las razones para asegurar físicamente un centro de cómputo, y los controles, procedimientos y medidas de seguridad que deben prevalecer en el mismo.

1. CONCEPTOS GENERALES

1.1 CONSIDERACIONES PRELIMINARES

"La última cosa que uno sabe en la construcción de un trabajo es qué poner primero".

BLAISE PASCAL

A fin de familiarizar al lector con los temas a tratar a lo largo de la presente investigación, señalaremos a continuación algunos conceptos de índole general.

1.2 RIESGOS A QUE ESTA EXPUESTA LA INFORMACION Y EL CENTRO DE COMPUTO.

La parte más vulnerable de las organizaciones de hoy en día es el centro de cómputo, ya que es aquí en donde se encuentra no sólo una gran inversión en equipo, sino aún más importante, la información que sirve de base para el funcionamiento normal de las organizaciones y para una adecuada toma de decisiones.

Al no estar la información y el centro de cómputo protegidos ante cualquier contingencia que pudiera presentarse, estarán expuestos a una serie de riesgos que de no ser conocidos o controlados, podrán repercutir en fatales consecuencias para la misma.

Antes de describir el tema con más detalle, se exponen dos definiciones de riesgo:

- *"Es el valor de la incertidumbre de que se presente un desastre o contingencia, medido en términos del número de amenazas posibles". (2)*

---

(2) Cfr. Franco Romo, Alfonso, Et. al., Planeación de la Recuperación Informática en caso de desastre, Facultad de Contaduría y Administración, UNAM, México 1990, pág. 8. MIMEO.

- *"Una acción o evento el cual puede causar una pérdida". (3)*

El auditor en informática tiene como parte de sus funciones y responsabilidades el evaluar la suficiencia de las medidas adoptadas para abatir la posibilidad de que los riesgos se materialicen, y en caso de que suceda tener los seguros y controles adecuados que disminuyan la pérdida, la forma de recuperación de la información y el reestablecimiento de los sistemas.

Por lo anterior es de suma importancia conocer los diferentes riesgos que amenazan a la información y al centro de cómputo. En la siguiente ***Tabla*** *1, presentamos una clasificación de dichos riesgos y una explicación general de los mismos.*

Son dos los tipos de riesgos: ***Riesgos externos y riesgos internos.***

1.1.1 ***Riesgos externos:***

Son todos aquéllos que se presentan en el ambiente físico y social que rodea a un centro de cómputo, los cuales, si bien no se pueden eliminar, si es posible tomar las medidas necesarias que minimicen la probabilidad de pérdida de información o destrucción de las instalaciones. A su vez, los riesgos externos se clasifican en tres tipos: naturales, humanos y materiales.

- ***Riesgos naturales***

a) *Temblor. Se refiere a los movimientos de tierra que pueden afectar la totalidad de los recursos informáticos, incluyendo los edificios en donde se localizan.*

---

(3) Cfr. Weber Ron, ***EDP Auditing. Conceptual Foundations and Practice,*** *Edit. Mc Graw-Hill, 2a. Ed., Pág. 248.*

RIESGOS A QUE ESTA EXPUESTA LA INFORMACION Y EL CENTRO DE COMPUTO			
R I E S G O S	EXTERNOS	NATURALES	- TEMBLOR - INCENDIO - INUNDACION - TORMENTA
		HUMANOS	- ROBO - SABOTAJE - MOTINES SOCIALES - FRAUDE
		MATERIALES	- DESCOMPOSTURA DE EQUIPO - FALLAS DE ENERGIA
	INTERNOS	ROBO	- MATERIAL - RECURSOS - INFORMACION * Programas * Datos
		SABOTAJE DESTRUCCION	- PAROS - RECURSOS * Voluntaria * Involuntaria
		HUELGA FRAUDE	
		ERRORES Y OMISIONES	

TABLA 1

b) *Incendio. Es la propagación de fuego que puede tener como origen el mismo local en donde se encuentra el computador o bien en instalaciones adyacentes.*

c) *Inundación. Fugas o corrientes de agua. Elemento que representa un peligro muy grande para los equipos de cómputo, tomando en cuenta los componente de los mismos.*

d) *Tormenta.- Se relaciona con las descargas de energía eléctrica que traen consigo estos fenómenos físicos, que pueden igualmente destruir un Centro de Cómputo o al menos impedir que éste pueda laborar en condiciones normales.*

Estos riesgos están determinados por la localización geográfica del centro de cómputo y el medio ambiente que los rodea.

- Riesgos humanos

a) *Robo. "...posesión de una cosa ajena, sin derecho y sin consentimiento de la persona que puede disponer de ella...". (4) Motivado por la introducción de terceras personas ajenas a la organización, puede ser de materiales, programas y datos, entre otros.*

b) *Sabotaje. Igualmente provocado por grupos de terroristas, que por personas que tengan conocimiento del tipo de información que se encuentra dentro del Centro de Cómputo.*

El sabotaje tiene aún más una sutileza, esto es la extorsión utilizando los archivos o programas como medio de presión hacia los dirigentes de una organización.

El Código Penal define la extorsión como: "...al que sin derecho obligue a otro a hacer, tolerar o dejar de hacer algo, ob-

teniendo un lucro para sí o para otro y causando un perjuicio patrimonial". (5)

c) Motines Sociales. Nos referimos a la destrucción del Centro de cómputo como resultado de un conflicto social ajeno a la organización.

d) Fraude. "...comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se haya se hace ilícitamente de alguna cosa o alcanza un lucro indebido". (6)

- Riesgos materiales

a) Descompostura de Equipo. Lo que limitaría la producción normal del Centro de cómputo y generaría pérdidas cuantiosas en caso de no obtener los medios necesarios para efectuar las reparaciones pertinentes.

b) Fallas de Energía. Sobrecargas o bien bajas de voltaje que afectan la confiabilidad del sistema o que pueden dañar los componentes internos de la máquina.

1.1.2 Riesgos internos

Son los que se generan dentro de la organización donde se encuentra ubicado el Centro de Cómputo. Estos riesgos son más sencillos de preveer y en consecuencia, perfeccionar las medidas para contrarestarlos. Sin embargo y aún cuando parezca contradictorio, la posibilidad de que éstos se materialicen es muy grande, ya que el conocimiento de los procedimientos operativos y de con-

---

(4) Cfr. Código Penal., Ediciones Dalma, título vigésimo segundo, México 1989, pág. 135.
(5) Ibidem., pág. 143.
(6) Código Penal. Loc. cit., pág. 139.

trol interno de la organización facilitarán el camino a quien desee hacer un daño irreparable.

Los riesgos internos se clasifican en seis tipos: robo, sabotaje, destrucción, huelga, fraude, y errores y omisiones.

- Robo

a) De Material. Es la escala más baja del robo, ya que aquí hablamos del robo de los activos de la organización, tales como: cintas, papelería y discos.

b) De Recursos. En este caso el robo puede alcanzar una pérdida sustancial en tiempo-máquina dedicado a aplicaciones, que en algunos casos, pertenecen a entidades diferentes y completamente ajenas a la organización.

c) De Información. La escala superior en la clasificación de robo es aquélla que trata de la sustracción física de los programas, archivos y en general de los datos que se encuentran en un Centro de Cómputo.

Esto también puede dar lugar a la extorsión o abuso de confianza.

El Código Penal define al abuso de confianza como: "...al que, con perjuicio de alguien, disponga para sí o para otra de cualquier cosa ajena de la que se le haya transmitido la tenencia y no el dominio...". (7)

- Sabotaje

Tiene la misma connotación que el inciso b) de riesgos humanos externos, con la diferencia de que en este caso, éste se puede presentar a través de otros medios como entorpecimiento de la producción sobre carga ficticia de trabajo.

---

(7) Código Penal. Loc. cit., pág. 138.

- Destrucción

a) De datos.- Archivados en medios electromagnéticos, de documentación y de archivos de respaldo, entre otros.

b) De recursos.- Este punto se refiere a la destrucción física de los elementos que se encuentran depositados en un centro de cómputo, tales como las unidades de cintas, discos, unidad central de proceso o cualquier equipo periférico.

Se incluyen también los recursos de papelería y soporte que complementan los elementos de producción de un centro de cómputo.

En este caso encontramos que la destrucción, tanto de los datos como de los recursos se puede dar en forma voluntaria como un ataque directo y con intención predeterminada de daños a la organización, o bien en forma involuntaria debido a errores u omisiones de los operadores o usuarios de un sistema.

- Huelgas

Del personal, que impedirían el funcionamiento del servicio informático ocasionando una detención total del procesamiento de información.

- Fraudes

En este caso hablamos de los desfalcos, robos, abuso de confianza o utilización, sea de los elementos que se encuentran en el centro de cómputo, o de la información que se maneja, a fin de obtener beneficios que se traducen directamente en pérdidas para la organización.

"Hay seis maneras básicas en las cuales "el fraude informático" es cometido:

1.- Desaprovechar el tiempo de computadora o robar recursos computarizados.

2.- Utilizar la computadora como un "chivo espiatorio".

3.- Manipular datos de entrada o introducir intencionalmente datos incorrectos.

4.- Alterar o copiar los registros de la base de datos.

5.- Modificar el software o sustituir programas inválidos para validar información .

6.- Interceptar datos transmitidos sobre los sistemas de comunicación". (8)

- Errores y omisiones

Finalmente nos referimos a la falta de información íntegra y consistente debido a errores y omisiones provocadas por el personal interno en el desarrollo de sus actividades. Este tipo de riesgo constituye el de mayor ocurrencia y es fuente de los principales problemas en el área de sistemas y de la organización en general.

Es importante hacer notar que estos riesgos, en caso de materializarse, no siempre significarán un beneficio para la persona que lo origina, pero invariablemente se traducirán en pérdidas para la organización tomando en cuenta los efectos secundarios

---

(8) Cfr. Cuevas Guzmán, Ma. Teresa de Jesús, Et. al; Control y Auditoría en Centros de Cómputo, TESIS de Licenciatura, Facultad de Ingeniería, UNAM, México, 1987. Pág. 102-103.

que tendrían alguno de los riesgos antes mencionados, por lo que es necesario reconocer su existencia para estar en posibilidades de contrarestarlos. Algunos de los efectos secundarios para la organización podrían ser: pérdida de confianza, vital en cualquier actividad; pérdida de imágen, de activos; y de la imposibilidad penetración en el mercado, entre otros.

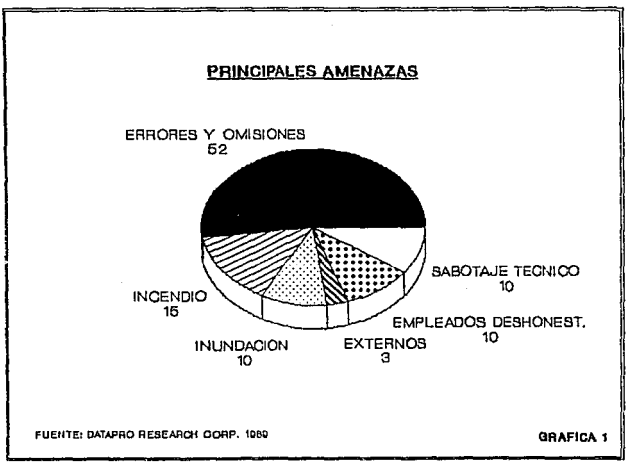
Finalmente, se llevó a cabo una recopilación de investigaciones realizadas en años recientes por instituciones reconocidas, tales como:

1) Datapro Research Corp.
2) Data Processing Management Association.
3) National Center Comp. Crime.

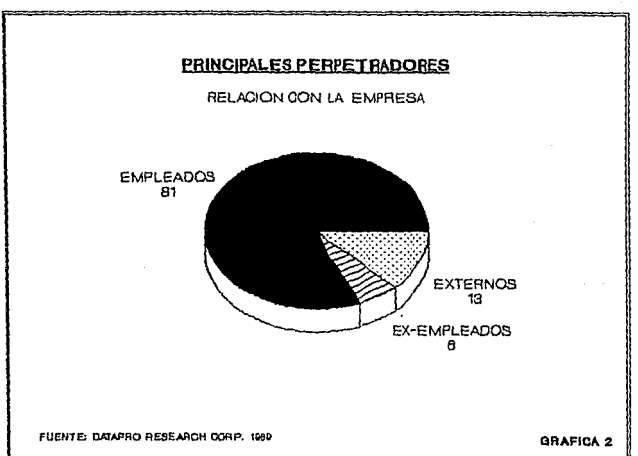
Obteniéndose los siguientes resultados:

*1) **Datapro Research Corp.***

*Estudió las principales amenazas a que está expuesta la información y el Centro de Cómputo, obteniendo los resultados que se muestran en la **Gráfica 1**.*

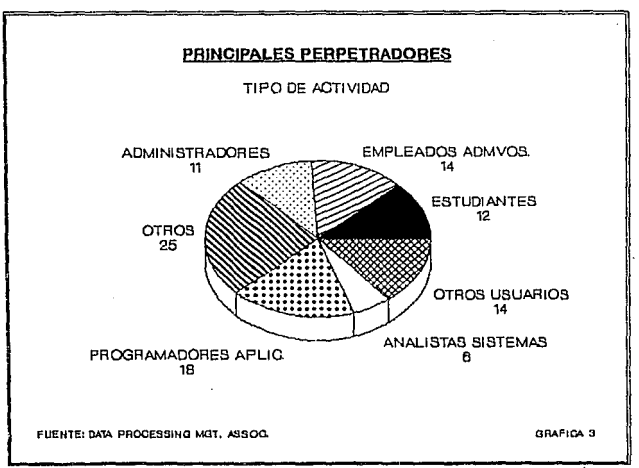


Asi también, se realizó otra investigación con respecto al recurso humano relacionado con la empresa y el resultado de ésta, se muestra en la ***Gráfica 2.***



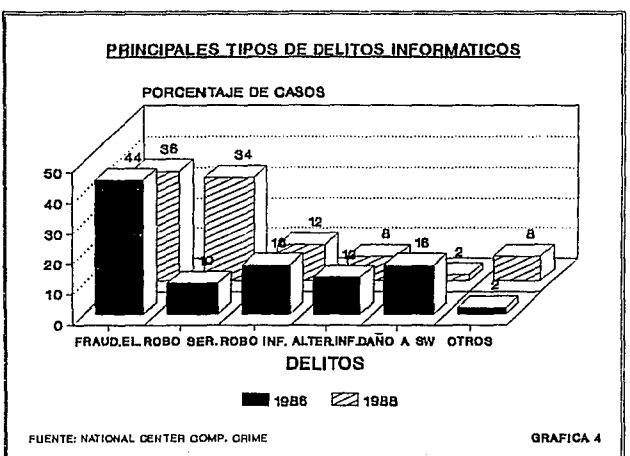
2) Data Processing Management Association

Concluyó en su estudio que los principales usuarios que tienen relación con la función informática y que amenazan la operación e integridad de la información son los que se presentan en la Gráfica 3.



3) National Center Comp. Crime.

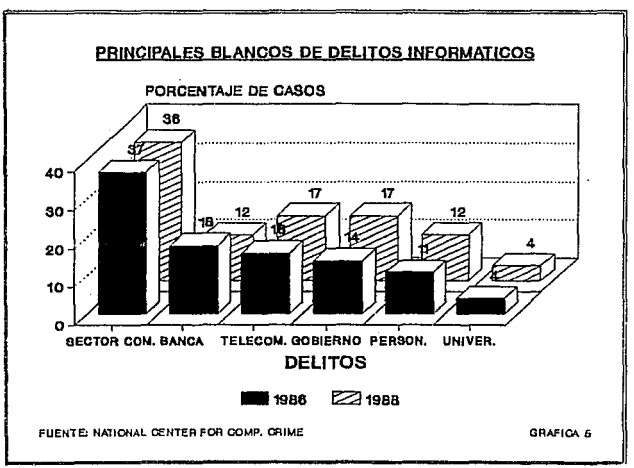
Durante el período comprendido entre 1986 y 1988, la National Center Comp. Crime evaluó los delitos informáticos y concluyó que los principales son: fraude electrónico, robo de servicios e información, alteración de información, daño al software entre otros; los resultados obtenidos se muestran en la ***Gráfica 4.***



FUENTE: NATIONAL CENTER COMP. CRIME

GRAFICA 4

*Finalmente, los sectores afectados por los delitos informáticos fueron: el sector comercial, la banca, las telecomunicaciones, el gobierno, negocios independientes y las universidades, en los porcentajes que se muestran en la **Gráfica 5**.*



1.3 CONTROL

La obtención de resultados en una organización se basa en gran medida en la eficiencia lograda en las diversas áreas que la forman, a través de la estructura de control desarrollada e implantada.

Bajo esta premisa es posible garantizar que la probabilidad de riesgo que pudiera afectar el éxito de una organización, se mantendrá en niveles mínimos y ante la ocurrencia de algún riesgo, se contará con medidas preventivas que permitirán disminuir con oportunidad y eficiencia los efectos que de ésta se deriven.

Luego entonces, se puede afirmar que uno de los propósitos fundamentales de la Auditoría en Informática será el determinar el riesgo existente en la organización y promover la optimización permanente del control o su propia implantación.

1.3.1 Definición

William Mair define al Control como "... todo aquello que tiende a causar la reducción de los riesgos. El control puede lograr reducir, ya sea, los efectos nocivos del riesgo o la frecuencia de su ocurrencia". (9)

---

(9) Vid. Mair, William, Et. al., Control y Auditoría del Computador, Instituto Mexicano de Contadores Públicos, México 1976, Pág. 41.

El incremento directo de controles aumenta la Exactitud, Integridad y Protección (EIP) del centro de cómputo e información, así como su Costo (C).

La mayoría de los controles puedon también incrementar la Efectividad y Eficiencia (EE) del procesamiento en un punto optimo, después del cual la implantación de más controles resultan inútiles. El objetivo de la organización en general es alcanzar el punto óptimo tal como se indica en la Figura 1. La implantación de controles excesivos o muy estrechos decrementa en su curva la (EE) a tal grado que en un punto, tiende a jalar la curva (EIP).

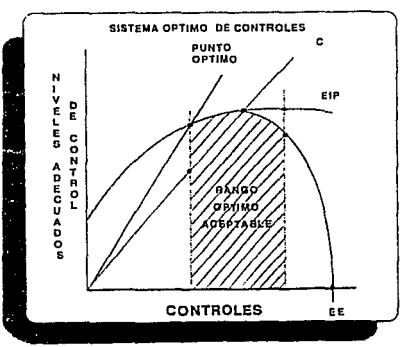


Figura 1

Dentro de la estructura general de controles existe un tipo de Control denominado," Control Interno" que se describe a continuación.

1.3.2 Control Interno

El estudio y evaluación del Control Interno es de suma importancia, debido a que el alcance y la magnitud de las organizaciones ha llegado a un punto donde su estructura jerárquica se ha vuelto tan compleja y extensa que resulta más difícil controlar eficazmente las operaciones.

Asimismo, la responsabilidad de salvaguardar los activos de las organizaciones y preveenir errores y fraudes descansa principalmente en la administración, por lo que un buen control interno le permite depositar mayor confianza en la veracidad de los datos.

Por lo antes expuesto se puede definir el Control Interno como: "El plan de organización y el conjunto de métodos y procedimientos que en forma coordinada se adoptan en una organización para: proporcionar una seguridad razonable de que los activos están protegidos y que la información es oportuna y confiable; para promover la eficiencia en las operaciones; e impulsar el cumplimiento de las políticas de la dirección, las leyes y regulaciones". (10)

De esta definición obtenemos los objetivos propios del Control Interno, los cuales se constituyen en medios para el logro de los objetivos institucionales.

- *La protección de activos del PEI (Procesamiento Electrónico de Información.*

- *Producción de información íntegra, correcta y oportuna.*

---

(10) Vid. Instituto Mexicano de Contadores Públicos, Normas y Procedimientos de Auditoría, Novena edición, México, 1989, Pág. 101.

. *La promoción de la eficiencia y efectividad de los sistemas y operaciones.*

- *Eficiencia, es consumir recursos de manera óptima*
- *Efectividad, es la medida con la cual se cumplen los objetivos para los cuales fue desarrollado el sistema*

. *El cumplimiento de las políticas de la Dirección, las leyes y demás regulaciones.*

En primer término, los activos del PEI representan el total de recursos, bienes y derechos con que cuenta el área de sistemas para realizar sus operaciones.

La información (en cualquier forma que ésta se expresa) es el elemento sobre el que se toman las decisiones operativas y administrativas.

Por otra parte, el aprovechamiento de recursos y tiempo se reflejan en la productividad del área.

Finalmente, los lineamientos obligatorios, internos y externos, fijan el curso de las actividades de la organización dentro del marco social, económico, fiscal y laboral en que se encuentra.

Para controlar se requiere de todo un sistema de Control Interno, el cual permita lograr dichos objetivos.

*1.4 **AUDITORIA***

Para definir las funciones y responsabilidades de Auditoría en Informática es conveniente referirse al papel que juega la Auditoría en general dentro de un esquema de organización.

Una organización como tal, parte de la definición de sus objetivos, los cuales son revisados y actualizados periódicamente de acuerdo con las características del entorno y las de la propia organización en sus aspectos internos.

Una vez definidos estos objetivos, se lleva a cabo la especificación y/o actualización del plan de acción para el logro de los resultados que se deben alcanzar.

Este plan de acción involucra la participación de cuatro tipos de áreas:

- ***Productivas***
- ***de Apoyo***
- ***de Control***
- ***de Evaluación del control***

Las áreas Productivas son aquéllas que tienen participación directa con el giro de la organización y son las que con su acción determinan, principalmente, el éxito o fracaso de un negocio.

*Las áreas de **Apoyo** como tal, no necesariamente participan en forma directa con el giro de la organización, sin embargo su acción es indispensable para el desarrollo adecuado de las áreas operacionales, como sucede con las áreas de Personal, Sistemas o Contabilidad.*

*Las áreas de **Control** tienen características especiales, dado que su responsabilidad se ejerce en forma distribuída, esto es, cada área productiva y de apoyo tiene como parte de su responsabilidad la aplicación de controles adecuados al tipo de función que realizan, sin embargo, existen áreas especiales, cuya responsabilidad básica radica en el establecimiento de controles, como es el caso de las áreas de Contraloría y Seguridad.*

*Por último, existe el área responsable de la **Evaluación del control** en toda la organización, esto es, en Producción, Apoyo y Control, que es el área de Auditoría, la que dadas sus características, debiera estar manifestada dentro de la estructura jerárquica como un apéndice del más alto nivel directivo de la organización, lo cual lo veremos a detalle en el subcapítulo 1.7.*

Por lo tanto, decimos que la obtención de resultados en una organización, se basa en la eficiencia lograda en las áreas productivas y de apoyo a través de la estructura de controles desarrollada, implantada y evaluada periódicamente.

El equilibrio existente entre productividad y control, la armonía en la participación de las áreas involucradas, el adecuado funcionamiento de cada área y la congruencia de los objetivos específicos, deben ser motivo de evaluación permanente por parte del área de auditoría.

Concluyendo, decimos que el propósito de un área de auditoría es determinar el nivel de riesgo que existe en la organización y promover la optimización permanente del control existente.

1.4.1 Definición

Etimológicamente la palabra auditoría proviene de la raíz latina "auditorius", que significa tener la virtud de oir; derivada de los términos "audis", oir y "auditor", el que escucha.

La palabra auditoría ha sido mal empleada ya que es considerada como una evaluación cuyo único fin es detectar errores y señalar fallas. Sin embargo, dicho término tiene un significado más amplio y requiere del ejercicio de un juicio profesional sólido y maduro para juzgar los procedimientos y lineamientos que deben de seguirse para evaluar los resultados obtenidos, ya que de ninguna manera es una actividad que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo sean de carácter indudable.

Para Carlos Slosse, la Auditoría es: "el exámen de la información por parte de una tercera persona, distinta de la que la prepara, con la intención de establecer su razonabilidad dando a conocer los resultados de su exámen, a fin de aumentar la utilidad que tal información posee". (11)

Para efectos de estandarizar el criterio de dicho concepto que trataremos a lo largo de la investigación, propongo la siguiente descripción conceptual:

Auditoría, es una evaluación analítica y sistemática valiéndose de un conjunto de técnicas y procedimientos que aplica el auditor para que por medio de señalamientos de cursos alternativos de acción, proporcione los elementos de juicio necesarios para fundamentar de una manera clara y objetiva, la opinión que emite como resultado de su revisión acerca de la situación de una organización o área en específico.

Para analizar la información antes descrita la podemos dividir en tres ideas principales:

---

(11) Vid. Slosse, Carlos, Et. al., Auditoría. Un Nuevo Enfoque Empresarial, Ed. Ediciones Macchi, segunda edición, Buenos Aires, Argentina, Pág. 4.

1. *Conjunto de técnicas y procedimientos..., mediante la aplicación de métodos de investigación, técnicas formales, procedimientos y pruebas, el auditor puede cerciorarse de la autenticidad y razonabilidad de los hechos e información.*

2. *El auditor obtiene los elementos de juicio necesarios para fundamentar de una manera clara y objetiva su opinión... El auditor durante el desarrollo de su trabajo se debe formar un criterio independiente y cumplir con los lineamientos inherentes a su profesión.*

3. *El objetivo final de la actuación del auditor será el de emitir una opinión sobre la razonabilidad y confiabilidad de la información y área bajo estudio.*

1.4.2 Tipos de auditoría

La auditoría, como cualquier disciplina toma caracterírticas diferentes de acuerdo al campo de acción o área de aplicación en que se desenvuelve.

De acuerdo a las personas que la realizan se pueden reconocer dos tipos de auditoría, la Auditoría externa o independiente y la Auditoría interna.

1. Auditoría externa o independiente

"Es la auditoría que se realiza a solicitud de las organizaciones con el objeto de presentar una opinión profesional independiente acerca de la razonabildiad y confiabilidad de la información y los recursos a examinar expresada bajo los principios y políticas de la misma". (12)

---

(12) Vid. Slosse, Carlos, Auditoría. Un nuevo enfoque empresarial, Op. Cit., Pág. 8.

La labor de auditoría externa implica una competencia profesional singular, caracterizada por una serie de atributos tales como independencia, conocimientos especializados y dedicación al servicio.

El auditor externo está capacitado para brindar cualquier servicio que implique el exámen de información, operaciones, procedimientos, actividades y proyecciones, que necesiten de un juicio profesional independiente dentro de su marco de competencia.

2. Auditoría interna

"Es una evaluación independiente de las operaciones realizadas por los empleados o funcionarios de la organización con propósitos de control". (13)

La auditoría interna es una función gerencial que mide y valora la eficacia de los controles, políticas y procedimientos definidos por la organización para que se cumplan de acuerdo a lo establecido.

Esta auditoría es una actividad apreciativa, independiente de los sectores objeto de revisión. Por lo tanto reporta directamente a los máximos niveles de la organización y de los cuales depende de ellos. Tiene por objeto la revisión de las operaciones para servir de base a la administración. Por este motivo, es un control que se describe como independiente puesto que mide y evalúa la eficacia de otros controles.

La auditoría interna deberá trabajar en forma separada a las operaciones de la organización.

---

(13) Vid. Slosse, Carlos. Pág. 7.

Sus funciones incluyen:

- *Revisión de las operaciones para verificar la autenticidad, exactitud y efectividad con las políticas y procedimientos establecidos por la organización.*

- *Comprobar la confiabilidad de los datos de la administración producidos dentro de la organización.*

- *Evaluar la calidad de desempeño en la ejecución de las responsabilidades asignadas.*

- *Revisión para conocer si los procedimientos fueron aplicados en forma consistente con las normas establecidas.*

Como conclusión podemos decir que estos dos tipos de auditoría deberán trabajar en forma coordinada, ya que el alcance de revisión del auditor externo es inferior al del auditor interno, en razón a su tiempo de permanencia en la organización, por lo cual el primero se deberá apoyar en el trabajo del cuerpo de auditoría de la organización.

En la Figura 2 comparativa mostrada a continuación, se presenta las principales diferencias entre la Auditoría externa e interna.

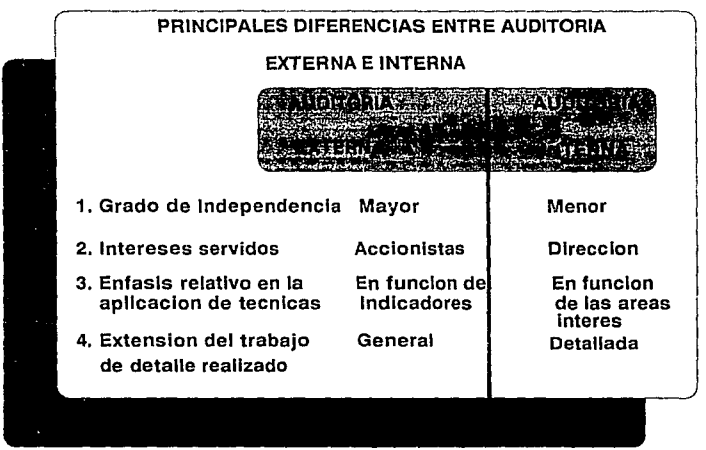


FIGURA 2

De acuerdo al objetivo específico de la auditoría existen tres tipos:

1. Auditoría contable/financiera

Es la auditoría que realiza un Contador Público quien examina los estados financieros de una organización con el fin de dictaminar sobre su razonabilidad y verificar que las operaciones se hayan registrado de acuerdo a principios de contabilidad.

2. Auditoría administrativa/operativa

Antonio Echenique define a la Auditoría administrativa como: "el exámen comprensivo y constructivo de la estructura de una organización, de una institución o cualquier parte de un organismo, en cuanto a sus planes, políticas y objetivos; sus metas y estructura orgánica; funciones; niveles de autoridad y responsabilidad; su forma de operación y sus recursos, sistemas y procedimientos generales". (14)

El objetivo de esta auditoría es la evaluación de la efectividad de la toma de decisiones, apoyándose en las fases del proceso administrativo.

La auditoría administrativa/operativa ayuda a complementar a la administración en determinadas áreas que requieren economías y prácticas mejoras, depurar los medios de control, y pugnar por el mejor uso de los recursos humanos, materiales, financieros y tecnológicos.

---

(14) Cfr. Echenique, José Antonio, Auditoría en Informática, Facultad de Contaduría y Administración, UNAM, México, 1990, Pág. 16.

Cualquier tipo de organización tiene áreas generales sujetas a investigaciones y que permiten obtener una evaluación de la administración.

Finalmente decimos que, la auditoría administrativa/operativa evalúa la forma en que se llevan a cabo los procedimientos para registrar un determinado tipo de operación a fin de detectar posibles carencias de control, esfuerzos duplicados, problemas de funcionalidad, corregir los efectos de las decisiones administrativas o cualquier proceso susceptible de ser optimizado para alcanzar los objetivos establecidos por la Dirección.

*En la **Figura** 3 se muestran las principales diferencias entre la Auditoría contable/financiera, y administrativa/operativa.*

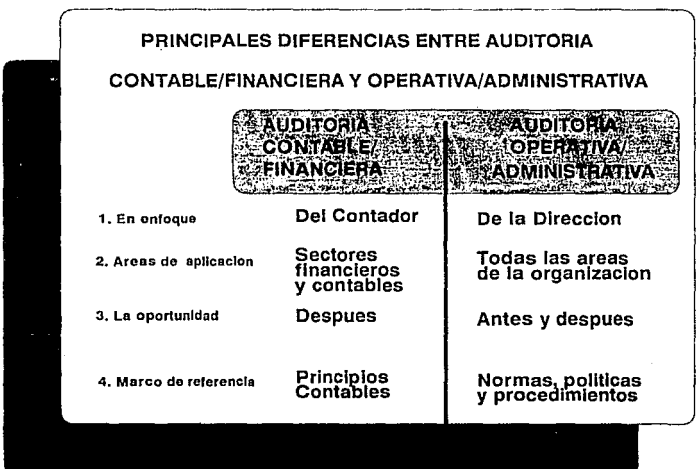


FIGURA 3

1.5 INFORMATICA

1.5.1 Definición

Actualmente no existe una definición de la palabra "informática" que tenga reconocimiento universal. Por lo tanto y basándome en los intentos para definir esta palabra, se propondrá una definición que se apegue lo más posible a las necesidades de esta investigación.

Etimológicamente el concepto informática se deriva de la palabra francesa "informatique" que a su vez se compone de los vocablos "information", información, y "automatique", automática que al unirlas significa Información Automática.

El primer intento serio para definir informática es el de la Academia Francesa quien la conceptualiza como:

"La ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automatizadas, de la información y de la comunicación en los ámbitos técnicos, económico y social" (15).

Durante los años subsecuentes se producen diversos intentos por aclarar y afinar el concepto de informática.

"En 1973 se publica en México una de las primeras obras de habla hispana en la que se pretende presentar una concepción de informática. En este libro se plantea a la informática como el estudio que define las relaciones entre medios (equipo), los datos y la información necesaria en la toma de decisiones, desde el punto

(15) Vid. Molina Ravetto, Enzo, Informática, una nuova ciencia, Academia Francesa, Francia, 1978, pág. 18.

de vista de un sistema integrado". (16)

Posteriormente otros trabajos presentaron definiciones propias, tales como las que se enuncian a continuación.

El Diccionario de la Lengua Francesa, define a la informática como el "Conjunto de técnicas de la colección, clasificación, almacenamiento, transmisión y utilización de la información tratada automáticamente con la ayuda de programas a través de computadoras" (17).

Enzo Molina la define como "la ciencia de los sistemas inteligentes de información. Es la ciencia relativa al estudio de las necesidades de información de los sistemas, mecanismos e insumos necesarios para producirla y aplicarla". (18)

De acuerdo a las definiciones anteriormente citadas, se puede observar que existe un común denominador que las agrupa y les presta una cierta coherencia a pesar de los diversos énfasis y puntos de vista. Este común denominador es la información abarcando a los procesos y sistemas relacionados con el manejo de la misma. Con base en lo anterior, propongo la siguiente definición de Informática:

"Es la ciencia que se encarga del estudio y tratamiento de los sistemas de información utilizando regularmente dispositivos electrónicos de procesamiento". Para analizar la definición se estratificará en los elementos claves que le dan origen. El primer elemento de la definición es el relativo al concepto de Ciencia.

---

(16) Cfr. Lambarri Valencia, Alejandro, Curso de Auditoría Informática, Loc. cit., pág. 20, MIMEO.

(17) Vid. Petit Robert, Diccionario de la Lengua Francesa, Le Robert París, 1981, Pág. 100.

(18) Vid. Molina Ravoto, Enzo, et. al., Introducción a la Informática, Edi. Trillas, México, 1984, Pág. 28.

Los elementos que conforman a la ciencia se apegan al método científico, ya que se orientan a lo objetivo, razonable y sistemático, porque se obtiene mediante razonamiento lógico, el cual incluye sistemas, pasos y etapas para llevarlo acabo. Desde el punto de vista dinámico se considera a la ciencia como un proceso, es decir, como una disciplina o actividad encaminada a mejorar las cosas, predominando el criterio de utilidad práctica.

El segundo elemento de la definición es el de sistema de información; este término en su connotación actual se refiere al conjunto de elementos y procedimientos ordenados, que al ser ejecutados proporcionan información para apoyar la toma de decisiones y el control en la organización.

Finalmente nos referimos a los dispositivos electrónicos en el proceso de información que comprenden el ingreso, proceso, emisión y transferencia de datos; entendiéndose por esto a todos los componentes de una instalación computarizada (equipo físico y sistemas).

1.6 AUDITORIA EN INFORMATICA

1.6.1 Definición

Las definiciones anteriores nos permiten deducir la correspondiente a Auditoría en Informática:

Para Mair William, la Auditoría en Informática es: "la verificación de los controles en las tres áreas de organización:

- Aplicaciones (programas en producción).
- Desarrollo de programas.
- La instalación del centro de cómputo" (19)

Marc Thorin define a la auditoría en informática como: "el examen para obtener un juicio de un sistema de información" (20).

Por mi parte, conceptualizo el término de Auditoría en Informática como "el examen y validación de los controles, técnicas y procedimientos utilizados e implantados en el centro de cómputo y sistemas en operación y bajo desarrollo, a fin de verificar que los objetivos de: continuidad del servicio; salvaguarda de activos, confiabilidad, seguridad, integridad y consistencia en la información, se están cumpliendo en forma satisfactoria y oportuna y de acuerdo a los objetivos y políticas establecidas por la organización".

---

(19) Vid. Mair, William, et. al., Computer Control & Audit, The Institute of Internal Auditors, U.S.A., 1978, Pág. 17.

(20) Vid. Thorin, Marc, La Auditoría en Informática, Masson, Paris, 1981, Pág. 33.

1.7 UBICACION JERARQUICA DEL AREA DE AUDITORIA EN INFORMATICA EN UNA ORGANIZACION.

Cuando nos referimos a la ubicación que debe ocupar el área de Auditoría en Informática, nos encontramos ante una situación polémica, ya que dependerá del tamaño, contexto y complejidad de toda la organización, así como del nivel de automatización de la misma.

Considerando lo anterior, la función o área debe estar ubicada de manera separada a las áreas usuarias; al área de sistemas, así como de la gerencia y dirección donde se realiza la toma de decisiones; esto es a nivel Staff. Esto permite al área el poder contar con autoridad propia y bien definida a fin de realizar sus actividades y actuar con un criterio imparcial e independiente para obtener como producto de sus funciones, resultados objetivos.

A continuación presento en la Figura 4, el organigrama con la ubicación ideal del área de Auditoría en Informática en una organización.

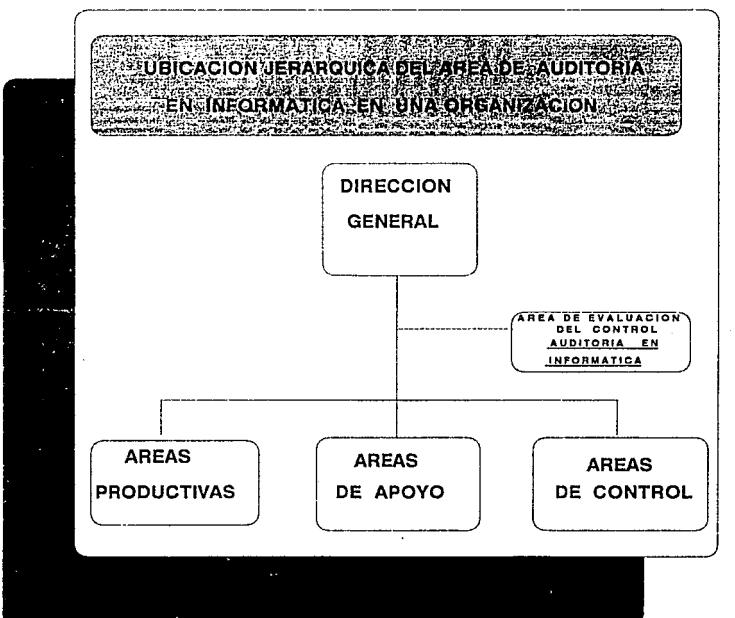


FIGURA 4

1.8 PERFIL DEL AUDITOR EN INFORMATICA

El aspecto fundamental en la definición del perfil más adecuado para llevar a cabo las funciones de Auditoría en Informática, es la controversia entre personal con perfil de informática, al que se le capacita en funciones de control o el perfil de auditor, al que se le dá capacitación en tecnología de cómputo". (21)

Obviamente el perfil más adecuado es el del personal que reúne una mezcla de experiencia y conocimientos en ambos campos, sin embargo, una realidad que debemos enfrentar es la escaséz en el mercado de personal con estas características.

Ante esto, la estrategia que se debe de adoptar en este sentido es la de localizar personal con experiencia y conocimientos en informática, de preferencia en desarrollo de sistemas, que cuente con claras inclinaciones hacia el control, manifestados en la utilización por convicción del proceso de planeación, la aplicación de metodologías, técnicas, estándares y de todos aquellos elementos que constituyen el marco de control, bajo el que debe de operar la función de sistemas.

Por otro lado, como complemento para lograr un equilibrio adecuado entre conocimientos de informática y auditoría, igualmente se debe reclutar personal con experiencia y conocimientos en auditoría que tengan una clara tendencia hacia la sistematización manifestada ésta a través de una precisa idea conceptual de lo que comprende la función de sistemas y la inexistencia de temor al "tabú" hacia los centros de cómputo y sistemas en operación y

---

(21) Cfr. Colegio de Contadores Públicos de México., Diferentes enfoques de Auditoría en Informática, Op. cit. Pág. 13.

bajo desarrollo.

A través de la interacción entre estos dos tipos de elementos es como consideramos que existe la posibilidad de llevar a cabo en forma adecuada la función de auditoría en informática y dado que difícilmente se puede encontrar el elemento ideal en el mercado actual, debemos asumir como un compromiso adicional de la función, el desarrollo y formación de auténticos profesionales en este campo.

Ahora bien, "por perfil de un profesional hemos de entender las características, aptitudes o requisitos mínimos que debe reunir una persona para ejercer una profesión" (22).

El perfil profesional se integra por Características generales y específicas.

*1.8.1 **Características generales***

Las Características generales se encuentran representadas por los requisitos intelectuales y personales que ha de poseer un auditor en informática, con independencia del área en la que se desenvuelve, tales como:

- *Capacidad e interés intelectual, es decir, disposición y aptitudes para captar, comprender, evaluar y aplicar los conocimientos.*

- *Habilidad para evaluar en forma objetiva e independiente. Esto implica un conocimiento funcional de los estándares aceptados en el área de PEI (Procesamiento Electrónico de Información) y*

---

(22) Vid. López, Elizondo, La Profesión Contable. Selección y desarrollo, Edit. ECASA, tercera edición, México, 1984., Pág. 104.

la habilidad para comparar operaciones, funciones y procedimientos existentes con aquellos estándares.

. *Aptitud para reconocer rápidamente problemas claves. Una función importante de la auditoría es la de identificar problemas y deficiencias fundamentales, así como el sugerir medidas adecuadas de corrección.*

. *Capacidad para comunicarse eficazmente. Una cantidad considerable de información es la que se maneja, por lo que es necesario comprenderla para transmitirla razonablemente correcta y oportuna al personal correspondiente.*

1.8.2 Características específicas

Finalmente, las características específicas agrupan a los conocimientos, habilidades, disposiciones y aptitudes deseables que se necesitan para desempeñar la especialidad de auditoría en informática, tales como:

1. Conocimientos y habilidad técnica:

. *Auditoría*
  - *Métodos estadísticos*
  - *Enfoque global de auditoría*
  - *Auditoría asistida por computadora*
  - *Técnicas y procedimientos de auditoría*
  - *Análisis de riesgos*
  - *Elaboración de planes de auditoría*
  - *Planeación y desarrollo de programas*
  - *Control de proyectos*
  - *Normas y procedimientos de auditoría*

. *Administración*

  - *Administración*
  - *Organización*

- *Psicología*

. *Sistemas*
- *Equipo/hardware*
- *Programas elaborados "in-house" y paquetería/sortware*
- *Programas de aplicación*
- *Seguridad física y lógica*
- *Procedimientos operativos*
- *Ciclo de vida de los sistemas*

2. Características del trabajo:

- *Precisión*
- *Juicio*
- *Capacidad para seguir instrucciones*
- *Habilidad para trabajar sin supervisión*
- *Respuesta a situaciones bajo presión*
- *Productividad*
- *Deseo y destreza para desarrollar su trabajo*

3. Características personales:

. *Liderazgo*

. *Delegación*
- *Habilidad para establecer objetivos*
- *Habilidad para distribuir el trabajo eficiente y equitativamente*

. *Entrenamiento*
- *Habilidad para dirigir personal*
- *Habilidad para revisar y evaluar trabajo*

. *Imagen y apariencia personal*
. *Equilibrio y madurez*
. *Confidencialidad*
. *Independencia*
. *Integridad*
. *Honestidad*

1.9 AREAS DE PARTICIPACION DEL AUDITOR EN INFORMATICA

A fin de ubicar el tema principal, objeto de esta tesis, describiremos en los siguientes capítulos II, III y IV, las áreas de participación primordial del Auditor en Informática dentro de la organización, particularmente nos referimos a:

- *Auditoría al desarrollo de sistemas*
- *Auditoría a sistemas en operación*
- *Auditoría a centros de cómputo*
  - *. Controles y medidas de seguridad físicas y ambientales*

CAPÍTULO II

AUDITORÍA AL DESARROLLO DE SISTEMAS

2. AUDITORIA AL DESARROLLO DE SISTEMAS

2.1 CONSIDERACIONES PRELIMINARES

El presente tema titulado "Auditoría al Desarrollo de Sistemas" trata de la importancia y necesidad de la intervención del auditor en informática, tanto en el desarrollo de nuevos sistemas o aplicaciones, como en las modificaciones a los mismos una vez que se encuentran en producción.

Los objetivos particulares que persigue esta área de participación del auditor en informática son los siguientes:

- Ayudar a prevenir la omisión de controles adecuados y verificar la suficiencia de los mismos incorporados a lo largo del desarrollo del sistema.

- Validar la oportunidad y costo-beneficio del desarrollo o modificación del sistema.

- Verificar que el sistema satisfaga los objetivos y requerimientos que le dieron origen.

- Verificar que el sistema sea comprensible, tanto para técnicos, usuarios y terceras personas.

- Tratar que el sistema sea auditable, incorporando controles y pistas necesarias para poder rastrear una aplicación o transacción a lo largo del flujo normal de la operación.

- Verificar que las políticas internas de la organización, así como las externas a ella sean incorporadas en el sistema.

. Verificar que los sistemas se encuentren totalmente documentados por medio de la elaboración de manuales técnicos y de usuario.

. Obtener mayor confianza en los sistemas que se encuentran en una ambiente de operación.

. Lograr un menor esfuerzo para obtener pruebas de los archivos para efecto de auditoría.

2.2. RIESGOS RELATIVOS AL DESARROLLO DE SISTEMAS

El desarrollo de nuevos sistemas está expuesto a una gran variedad de riesgos.

La organización puede interrumpirse temporal o permanentemente a causa de la implantación de una aplicación con diversos tipos de errores de diseño. En forma similar, tales errores pueden también ocasionar que se proporcione información inexacta o incompleta y que se originen decisiones erróneas por parte de la dirección.

La posibilidad de cometerse fraudes puede darse en forma accidental o deliberadamente en el sistema; se puede violar leyes, impuestos o políticas conduciendo a diversos tipos de sanciones internas o externas a la organización.

Las decisiones y especificaciones equivocadas respecto al diseño y posteriormente a las modificaciones pueden hacer que el sistema opere ocasionando trabajo, tiempo y costos excesivos en forma adicional.

Finalmente resumimos en la siguiente lista los riesgos más comunes que se presentan en el desarrollo o modificaciones a los sistemas:

- *Decisiones erróneas*
- *Especificaciones inadecuadas*
- *Personal incompetente*
- *Mínima comunicación*
- *Mal uso de recursos*
- *Aplicaciones que no puedan mantenerse*
- *Costos excesivos*

El personal encargado de desarrollar los estudios para una nueva aplicación o modificación, por su misma formación profesional no está sensibilizado en su mayor parte a los problemas de control y pistas de auditoría, por lo cual es frecuente encontrar que, si bien un sistema es muy eficiente desde el punto de vista operativo (tiempo de respuesta y oportunidad de la información), éste carece de los controles necesarios que permitan garantizar la confiabilidad e integridad de la información, así como los datos necesarios para estar en posibilidad de efectuar la supervisión y recuperación para fines de auditoría.

Hay dos maneras en las cuales el auditor en informática puede participar en esta área:

La primera, como miembro del equipo de desarrollo de sistemas; y la segunda, como evaluador del sistema una vez que ha sido terminado. Los objetivos de auditoría difieren significativamente para cada una.

"Cuando el auditor participa en todo el proceso de desarrollo de sistemas, los objetivos son asegurar que el sistema esté desarrollado sobre una estructura de controles adecuada y suficiente para salvaguardar los activos, asegurar la integridad de los datos y lograr sistemas eficientes y efectivos". (23)

Cuando el auditor lleva a cabo una post-auditoría, los objetivos son evaluar los controles y procedimientos implantados y emitir sugerencias y observaciones derivadas de la evaluación para fortalecer el sistema y su operación.

De igual forma se quiere hacer notar que el auditor deberá tener la habilidad para no sobrecargar un sistema con demasiadas medidas de control, en función a los objetivos e importancia del mismo, ya que si bien se puede llegar a obtener un índice de control y seguridad muy alto, así también se puede perder el objetivo inicial del mismo.

Conseguir un perfecto balance entre controles, seguridad y eficiencia es en mi opinión una de las tareas más difíciles del auditor que realiza esta función.

El auditor debe jugar un rol muy importante en el desarrollo de los sistemas si quiere cumplir cabalmente con sus obligaciones y su compromiso con la administración. Si esto no es hecho puede estar trabajando en un ambiente que no tiene suficientes controles y que es difícil o imposible de auditar". (24)

---

(23) Cfr. Wober Ron, EDP Auditing. Conceptual Foundations and Practice., Op. cit., pág. 107.

(24) Vid. Bank Administration Institute, Auditing the Systems Development Life Cycle, Artículo, Rolling Meadows, III, U.S.A. 1979. Prólogo.

Un punto más que obliga la participación del Auditor en el desarrollo de sistemas es la baja participación, tanto de los directivos como de los usuarios, dando origen a sistemas que son controlados prácticamente por el personal del área de sistemas.

La siguiente figura permite ejemplificar esta situación:

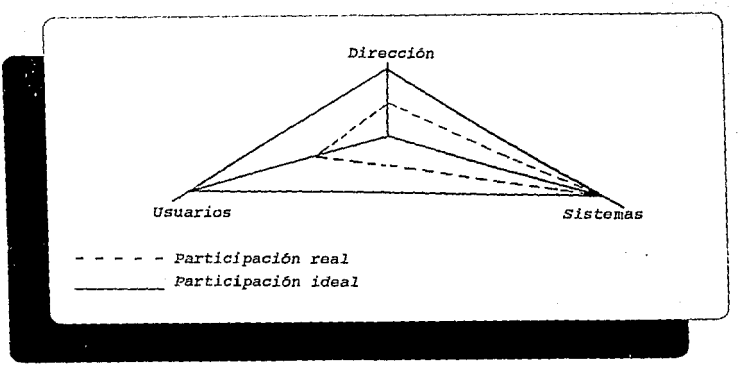


Figura 5

La forma de participación ideal dará como consecuencia sistemas equilibrados que respondan integralmente a las expectativas de la dirección y a las necesidades de los usuarios con la ayuda óptima del área de sistemas y con la tecnología disponible.

En las organizaciones grandes y medianas la comunicación se convierte en un problema significativo, por lo que deberá existir

desde un inicio estrechos vínculos entre la dirección, usuarios, auditores y el área de sistemas, siendo de suma importancia el ir dejando constancia clara y por escrito de las decisiones que se vayan tomando a lo largo del ciclo de vida del sistema con objeto de lograr un mayor entendimiento.

De este modo, la documentación debe garantizar una continuidad en el proceso que asegure la realización del objetivo de las partes involucradas cuando el sistema se convierta en una realidad operativa.

El área de sistemas debe contar con un patrón formal o metodología, es decir con un conjunto de procedimientos sistemáticos que permitan la estandarización en el proceso y la ausencia de numerosas deficiencias, inexactitudes e inconsistencias.

2.3 DESCRIPCION GENERAL DE LOS PRINCIPALES PASOS PARA EL PROCESO DE DESARROLLO DE SISTEMAS

El desarrollo de sistemas es un término amplio, el cual describe la conversión de un proceso manual a una solución automatizada, basada en la necesidad de incrementar la eficiencia y productividad de las operaciones en una organización.

En la **Figura 6** se presenta un conjunto de procedimientos que se pueden definir como una progesión de pasos lógicos para el desarrollo de sistemas. El proceso se inicia con una investigación inicial (principio conceptual) y culmina con un sistema implantado sujeto a mantenimiento sobre la marcha.


PLANEACION
INVESTIGACION
ESTUDIO PRELIMINAR
ESTUDIO DE LA PLANEACION
DECISION GERENCIAL
DESARROLLO
REQUERIMIENTOS DL USUARIO
ESPECIFICACIONES TECNICAS
PLANEACION DE LA IMPLANTACION
PROGRAMACION
PRUEBA
DECISION GERENCIAL
IMPLANTACION
CONVERSION
REVISION POSTERIOR A LA
IMPLANTACION
MANTENIMIENTO
MANTENIMIENTO

Figura 6

"El proceso de desarrollo de sistemas se divide en tres fases principales:

Planeación
Desarrollo
Implantación" *(25).*

En la ***Figura 6*** *los pasos que se encuentran colocados a la terminación de cada uno de las dos primeras fases, indican puntos de revisión importantes previamente establecidos bajo un enfoque denominado "compromiso progresivo", es decir, se va solicitando la autorización de la gerencia para poder continuar con las siguientes etapas.*

Dichas etapas son manejadas por un equipo integrado por usuarios y el departamento de sistemas. Los usuarios desempeñan un papel crítico en la definición de los requerimientos y la identificación de los beneficios. El personal del departamento de sistemas actúa como coordinador y además proporciona apoyo técnico; asimismo se compromete a cumplir con los requerimientos estipulados por los usuarios.

A continuación se describen de manera general cada uno de los pasos que se encuentran integrados en las fases para el proceso de desarrollo de sistemas.

---

(25) Cfr. Hoir, William, Et. al., Computer Control & Audit, Op. cit., pág., 260-261.

Planeación de sistemas

Las actividades iniciales de planeación identifican "...la definición del problema, el establecimiento del alcance y los objetivos del proyecto. También se detalla el costo/beneficio y la presentación preliminar del diseño.

Esta fase corresponde a lo que conocemos con el nombre de Estudio de Factibilidad" (26).

La planeación se cumple:

- *Estudiando los procedimientos existentes dentro de la organización*
- *Determinando las posibilidades y oportunidades de mejoras, automatizando la operación*
- *Evaluando los recursos informáticos disponibles*

La planeación de un sistema de gran magnitud puede ser dividida en tres pasos: investigación inicial, estudio preliminar del sistema y estudio de planeación. En otros casos, estas tres actividades pueden quedar comprendidas en una sola.

El nivel y magnitud del esfuerzo que se invierta deben depender de la naturaleza del proyecto y quedará definido por el alcance.

Esta fase debe ser realizada por niveles directivos altos.

---

(26) Cfr. Electronical Data Processing Auditors Foundation, Inc., CISA Review Manual, Domain 7, U.S.A., 1992, pág. VII-2.

Estas personas deberán tener la madurez y juicio necesario para evaluar las oportunidades y manejar la incertidumbre.

Las actividades de planeación producen dos resultados: un reporte de la planeación del sistema y una decisión gerencial respecto a si se debe continuar con el proyecto.

Especificaciones del usuario

La actividad de especificaciones o requerimientos del usuario está orientada al desarrollo de un planteamiento para resolver los problemas de la organización o de áreas específicas.

Esta actividad se realiza mediante esfuerzos conjuntos de los usuarios y analistas de sistemas como miembros del equipo de trabajo.

Este equipo examina todos los procedimientos manuales y automatizados y estudia las relaciones entre el sistema que se va a desarrollar y otras aplicaciones ya existentes para determinar el impacto de uno sobre otro.

El analista debe comprender las responsabilidades del usuario, sus limitaciones y problemática, así como todos los procedimientos que realiza para el cumplimiento de sus objetivos.

Es necesario obtener la aprobación del usuario por cada elemento funcional y lógico del nuevo sistema, incluyendo los procedimientos manuales, el contenido de los archivos, la lógica de las decisiones, los controles, los documentos de transacciones fuente, los documentos de trabajo y los reportes. Uno de los objetivos de tener acuerdos parciales y procedimientos de aprobación en

cada avance en las especificaciones de usuario es el establecer reuniones formales entre los usuarios y los analistas de sistemas, con lo que se obtiene la seguridad de que ambos discutirán y comprenderán la misma información.

El producto final que se obtiene de esta etapa es un manual detallado que describe políticas, formatos y documentos, criterios que deberán ser cumplidos en la operación y los servicios de procesamiento que deberán ser ejecutados por y para el usuario.

Especificaciones técnias

Los objetivos principales de esta actividad son el desarrollo de decisiones a nivel técnico y de documentación para las partes automatizadas de una aplicación, así como las funciones operativas relacionadas dentro del departamento PEI. Esta documentación es más detallada que la que se prepara durante las actividades anteriores y proporciona las instrucciones que deben seguirse durante la actividad de programación. De la misma forma esta documentación será de vital importancia para dar mantenimiento al sistema una vez implantado.

Las funciones a realizarse durante la actividad de especificaciones técnicas son la definición de módulos y programas, los cuales deben estar relacionados con los archivos que soportarán la aplicación, la selección del lenguaje de programación a ser utilizado y un plan para la elaboración de los programas de la aplicación.

Planeación de la implantación

La planeación de la implantación es el último punto planeado para evaluación, análisis y modificación del sistema antes de ser realmente desarrollado.

Esta actividad tiene como producto un documento de planeación detallado que incluye; la confirmación de los objetivos, el alcance, los costos y los beneficios de la nueva aplicación; el programa de instalación, las responsabilidades asignadas y un informe de avance a los usuarios y a la Dirección.

Programación

La programación se refiere a la codificación del problema a un lenguaje de programación.

El objetivo de esta actividad es interpretar todas las especificaciones del usuario y técnicas a un lenguaje entendible por la computadora.

La programación es una actividad totalmente técnica que se inicia tomando como base la documentación obtenida de las especificaciones técnicas. Esta actividad dá como resultado programas de aplicación terminados que han sido compilados del lenguaje de programación al lenguaje objeto, y que han sido probados.

"Esta actividad debe generar programas documentados y mantenibles" (27).

Procedimientos y entrenamiento del usuario

Simultáneamente a la actividad de programación se preparan procedimientos y material de entrenamiento para que el usuario pueda convertir y operar la nueva aplicación.

---

(27) Cfr. Electronical Data Processing Auditors, Foundation, Inc. CISA Review Manual, op cit, pág. VII-4.

Los esfuerzos de entrenamiento deben llevar a los usuarios hasta un punto en el que puedan efectuar su trabajo normal y eficientemente, los procedimientos puedan evaluarse y los cambios puedan efectuarse en forma adecuada durante la prueba del sistema, la conversión y la operación en marcha.

Prueba del sistema

El objetivo principal de esta fase es que las personas involucradas prueben todas las partes de la aplicación como unidad, incluyendo: los programas, la operación, los archivos de prueba y el personal con la finalidad de efectuar cualquier modificación o ajuste necesario para que la aplicación quede correcta y adecuada para su implantación y uso posterior. Estas pruebas deberán ser desarrolladas, dirigidas y autorizadas por el personal usuario.

Una de las partes importantes de la actividad es llevar un registro, con cierto grado de detalle, para todas las tareas efectuadas. Además, deberá prepararse un reporte de discrepancias encontradas, el cual deberá diseñarse para ser utilizado como control y también como documento informativo.

Conversión

Durante la actividad de conversión, la nueva aplicación llega a su vida útil.

El principal objetivo de esta actividad es lograr que un sistema se encuentre listo para operar.

Dentro de la conversión existen tres tareas que son dignas de mencionarse en términos de su importancia para la auditoría:

1. *Las aprobaciones para la conversión de los archivos son los puntos de partida para operar la nueva aplicación.*

2. *La aprobación de la nueva aplicación debe basarse en un número de ciclos operativos previamente establecidos. El nivel de experiencia deberá asegurar que la aprobación ha sido llevada a cabo totalmente y a satisfacción del usuario y del personal involucrado.*

3. *Deben evaluarse los avisos de discrepancias y programarse las acciones correctivas correspondientes.*

Revisión post-implantación

Una vez que el sistema de aplicación ha sido implantado y se encuentra funcionando debe establecerse una actividad para efectuar una revisión encaminada a comparar los logros alcanzados, contra los planes originales.

La práctica de las revisiones posteriores a la implantación sirve para:

. *Afinar los conocimientos relativos al desarrollo de sistemas.*

. *Identificar posibles áreas de modificación o mejoras.*

. *Sugerir posibles técnicas de control de proyectos, a fin de minimizar los problemas encontrados en los trabajos anteriores.*

Deberán revisarse los avisos de discrepancias, los cambios, y los registros de errores que se hayan preparado desde que el sistema fue implantado.

Adicionalmente deberá haber una comparación entre los controles operativos reales dentro de la aplicación y aquellos que se planearon en la documentación del proyecto.

Mantenimiento continuo

Como último punto, el especificar una actividad y un mecanismo para el mantenimiento continuo de un sistema reconoce que el cambio es una constante en este medio, tanto en la naturaleza de los sistemas como en la tecnología, por lo tanto, cada proyecto deberá producir documentación e integrar la opción de modificar la aplicación implantada conforme cambien los requerimientos.

Las razones para modificar los sistemas de información implantados pueden clasificarse en dos categorías: ***cambios obligatorios y mejoras***

Los ***cambios obligatorios*** *normalmente se inician porque se descubren discrepancias o errores en la aplicación, o bien los requerimientos de la organización exigen modificaciones.*

Estos tipos de cambios se derivan principalmente de regulaciones externas o de cambios en otras aplicaciones adyacentes.

Las mejoras a las aplicaciones se presentan con el objeto de lograr una operación y producción más efectiva y eficiente, así como mantenerse al día o para aprovechar los nuevos desarrollos relativos a los equipos de cómputo o de los programas en operación.

2.4 PARTICIPACION DEL AUDITOR EN EL DESARROLLO DE SISTEMAS

Uno de los principales controles sobre el desarrollo de sistemas de aplicación es que el auditor forme parte del equipo de desarrollo. "Aún cuando el auditor estará interesado en todos los aspectos del nuevo sistema - control, eficiencia, información gerencial, seguridad - su mayor interés estará en el sugerir y evaluar los controles de aplicación. Consecuentemente, su principal contribución es asegurar que las aplicaciones automatizadas recientemente implantadas incluyan características de control sólidas y confiables" (28).

El hecho que el auditor participe en el desarrollo de nuevos sistemas no elimina la necesidad de un examen de los sistemas de aplicación existentes. Lo que hace, en términos generales es ayudar a prevenir que se implanten sistemas de aplicación que tengan riesgos importantes.

El auditor participa revisando y aprobando la documentación generada como producto final de las actividades. Por "aprobar" no quiero decir que el auditor autorice la continuación del proceso de desarrollo o que proporcione una garantía absoluta de que no se ha omitido ningún control, sino simplemente el auditor debe tomar una decisión con respecto a si los productos finales de la documentación son o no adecuados. Todos los miembros del equipo - diseñadores, usuarios, gerencia - deben comprometerse en forma similar.

Al mismo tiempo, el auditor debe seguir siendo independiente, estar consciente de que su revisión tiene limitaciones y continuar informando sobre cualquier riesgos importantes que detecte.

A continuación se describe el papel que debe realizar el auditor en cada una de las fases del desarrollo de sistemas.

---

(28) Vid. Hair, William, Et. al., Control y Auditoría del Computador, op. cit., pág. 341.

Planeación de sistemas

La mayoría de los proyectos de desarrollo de sistemas requieren una participación limitada del auditor durante la fase de planeación. Su revisión de la documentación no incluye ninguna evaluación de los controles, ya que para entonces son demasiados vagos y generales. Su principal interés es familiarizarse con la naturaleza y el impacto del proyecto y planear y programar su participación futura.

El auditor deberá conservar el reporte de planeación que resulte, debido a que la información sobre los objetivos y beneficios proporcionará referencias importantes para el resto del proyecto.

Especificaciones del usuario

Dado que la documentación que resulta de la actividad de requerimientos o especificaciones del usuario describe íntegramente el flujo de la aplicación, el auditor deberá efectuar una revisión detallada. Con base en esto, el auditor deberá esperar que en esta etapa se definan todos los controles, excepto aquellos que dependan de las especificaciones técnicas.

El auditor también puede tener requerimientos para el sistema solicitando la implantación de pistas de auditoría, es decir funciones específicas dentro del mismo para poder rastrear desde un punto determinado la aplicación.

Especificaciones técnicas

La evaluación que el auditor efectúa en las especificaciones técnicas y las producidas en las especificaciones del usuario, deberán proporcionarle una visión completa de todos los controles que van a implantarse en el nuevo sistema.

Las especificaciones finales sobre el contenido de los archivos también será de especial interés, particularmente si el auditor planea utilizar programas de operación de auditoría de propósito general para las pruebas posteriores.

Planeación de la implantación

La revisión del auditor en este momento le servirá de guía para el resto de su participación, así como para su examen después de la implantación.

Los controles de la implantación incluyen aquellos que se relacionan con la creación de nuevos archivos maestros.

Estos pueden abarcar una variedad de ediciones y controles de comparación, así como controlos sobre la corrección de errores.

Programación

Durante esta etapa es probable que surjan errores y malos entendidos en la preparación de la codificación del programa fuente con base en las especificaciones técnicas, lo cual deberá ser corregido por los controles de supervisión existentes.

La función del auditor en la fase de programación dependerá en gran parte, de su nivel de experiencia técnica. Si se encuentra capacitado en cuanto al lenguaje de programación y al sistema operativo que se estén empleando, el auditor podrá verificar la implantación de normas de programación sólidas, así como la de controles de aplicación adecuados, examinando la documentación de la progamación.

El principal control disponible para verificar la corrección de los programas concluídos es la prueba de los sistemas. Normalmente el trabajo del auditor será más efectivo si participa

en la prueba de los sistemas más que en la programación.

Procedimientos y entrenamiento del usuario

El auditor en esta fase se limita en revisar el manual de procedimientos o de operación del sistema, así como verificar si se esta llevando a cabo una adecuada capacitación al usuario por parte del área de sistemas acerca de la operatividad del nuevo sistema.

Prueba de los sistemas

La prueba de los sistemas es un proceso de aceptación por parte de los usuarios incluyendo al auditor. El auditor deberá estar preparado para recomendar a la alta gerencia que la implantación no se lleve a cabo o no continúe si existen riesgos importantes en la aplicación debido a errores u omisiones en las especificaciones originales, o debido a discrepancias en la implantación de las mismas.

La decisión final de implantar una aplicación computarizada corresponde a la alta gerencia.

La actividad de prueba de los sistemas funciona como un control detectivo sobre las fases precedentes del proyecto.

El auditor deberá asegurarse de que los usuarios estén llevando a cabo la prueba, que la información y procedimientos sean completos y suficientes, y que los controles especificados estén funcionando como se pretendía. El auditor también deberá revisar todos los resultados de las pruebas y estar seguro de que las discrepancias importantes sean corregidas y aprobadas nuevamente antes de la conversión del sistema.

La prueba del sistema es la última opción para evitar la implantación de una aplicación que pudiera tener riesgos importantes. Por lo tanto, la participación del auditor en esta actividad es escencial.

Los tres productos finales de esta etapa son de interés primordial para el auditor:

- *La documentación de las pruebas efectuadas*
- *La documentación de las discrepancias reportadas y de las acciones correctivas correspondientes*
- *La aprobación del usuario*

Los datos de prueba utilizados durante esta actividad deben ser conservados por el auditor para su revisión y para utilizarlos en exámenes posteriores de la aplicación implantada. Los reportes sobre discrepancias y correcciones también son valiosos en virtud de que indican la naturaleza de los errores encontrados y proporcionan evidencia suficiente de que se siguieron las acciones correctivas. Por último, la aprobación es importante, ya que indica que los usuarios han tenido un papel activo y han especificado las correcciones y han aprobado los resultados.

Conversión

Los objetivos del auditor en esta fase deberán asegurar que los controles de conversión planeados se implanten adecuadamente, que las excepciones y discrepancias se resuelvan apropiadamente y que la conversión permita una comparación efectiva de los resultados de la aplicación, tanto antes como después.

Los tres productos finales que documenta esta actividad y de importancia para el auditor son:

. La documentación del proceso de edición deberá indicar que la conversión de los archivos ha alcanzado un nivel de calidad satisfactorio. Las cifras control de la aplicación deberán indicar que todos los archivos que existan han sido convertidos.

. La documentación de los resultados deberá revelar los volúmenes de procesamiento y discrepancias, e indicar que la aplicación es capáz de manejar los niveles existentes de procesamiento y corrección de errores.

. Toda la documentación expresará que el sistema fué finalmente implantado con las aprobaciones apropiadas de la gerencia, del usuario y del departamento de sistemas.

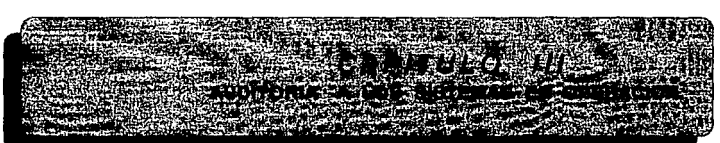
Revisión posterior a la implantación

El auditor deberá participar activamente en la revisión posterior a la implantación. Deberá trabajar con los usuarios y la gerencia de desarrollo de sistemas para verificar que realmente se hayan logrado los beneficios planeados y cubiertos los objetivos que dieron origen al sistema.

Mantenimiento continuo

En esta fase se le deberá informar al auditor de todas las modificaciones que se planean hacer a los programas del sistema en operación. El puede entonces juzgar por sí mismo qué modificaciones podrían crear riesgos significativos y determinar la medida en la cual deberá involucrarse.

Como en el desarrollo de un sistema de aplicación, el mantenimiento continuo deberá ser controlado; primero, mediante la preparación de especificaciones adecuadas y segundo, por la prueba adecuada de las modificaciones concluídas.



3. *AUDITORIA A SISTEMAS EN OPERACION*

3.1 CONSIDERACIONES PRELIMINARES

La Auditoría a sistemas en operación o a aplicaciones se realiza para aquellos sistemas que se encuentran en producción.

La auditoría a aplicaciones esta orientada a validar y verificar los controles y medidas de seguridad implantadas en el flujo de información a través de todo el sistema incluyendo entradas, procesos, salidas, interfases, y afectación de archivos.

Es muy importante que el auditor reconozca el hecho de que un sistema puede ser vulnerable una vez que ha sido liberado en producción y que puede, en un momento dado, no estar procesando la información en forma adecuada y, en consecuencia, no cumplir con los objetivos definidos inicialmente.

Es en esta área de participación de la auditoría en informática es en donde se han desarrollado más técnicas a aplicar, ya que es aquí precisamente donde se encuentra el procesamiento de las operaciones que generan la información, base para la toma de decisiones, por lo que cualquier error o manejo inadecuado en ésta se traduciría en problemas y quizás hasta en pérdidas significativas para la organización.

Los objetivos particulares que persigue el auditor en informática en esta área son los siguientes:

- *Verificar que los controles incorporados a lo largo del sistema sean razonablemente confiables y que no existan puntos débiles que la expongan a riesgos significativos.*

. *Verificar que el sistema sea comprensible.*

. *Validar que el sistema sea auditable, incorporando los datos necesarios para estar en posibilidades de rastrear una operación desde su inicio hasta su fin (pista de auditoría).*

. *Verificar que tanto las políticas internas de la organización como las externas a ella sean consideradas en el sistema.*

3.2 RIESGOS RELATIVOS A LAS APLICACIONES

Los riesgos se derivan de causas activas, directamente de la ausencia de controles. Los riesgos atribuibles a las aplicaciones operadas por el computador pueden encontrarse en las siguientes etapas del flujo normal de un sistema:

- *Entrada*
- *Proceso*
- *Salida*

3.2.1 Riesgos relativos a la entrada

Los riesgos relativos a la entrada existen siempre que una transacción o archivo se sujeta a un nuevo proceso. Este proceso puede ser manual o automatizado. Los principales riesgos relativos a los datos de entrada son:

- *Pérdida de datos*
- *Duplicidad de datos*
- *Contenido incorrecto de los datos*
- *Transacciones no registradas*

3.2.2 Riesgos relactivos al procesamiento

Aun cuando los datos de entrada estén completos, sean exactos y apropiados existe el riesgo de que el procesamiento no sea adecuado.

Los riesgos relativos al procesamiento incluyen:

- *Lógica incorrecta en el programa*
- *Procesamiento con el archivo indebido*
- *Procesamiento incompleto*
- *Procesamiento incorrecto*
- *Pérdida de archivos y programas*

3.2.3 Riesgos relativos a la salida

El que el computador produzca información que sea completa, exacta y útil no constituye el final de la aplicación. Tal información existe para que el personal correspondiente la utilice, por lo que para lograr sus objetivos, debe llegar a los usuarios apropiados y transmitir los resultados de los datos de entrada y el procesamiento de manera legible y aceptable, ya sea en forma impresa, óptica, auditiva u otra. Los principales riesgos relativos a los datos de salida son:

- *Distribución inadecuada*
- *Pérdida de información*
- *Información errónea*
- *Información inoportuna*

3.2.4 Riesgos resultantes

Los riesgos principales al no contar con los controles suficientes a lo largo del flujo general del sistema se resumen de la siguiente manera:

- *Interrupciones de la organización*
- *Decisiones erróneas de la gerencia*
- *Fraude*
- *Sanciones legales*
- *Costos excesivos*
- *Pérdida o destrucción de activos*
- *Desventaja ante la competencia*

3.3 CONTROLES DE APLICACION

Los objetivos de los controles son prevenir, detectar o corregir los diferentes riesgos relativos a las aplicaciones.

El propósito de los controles es asegurar que:

. *Los datos de entrada sean exactos y esten debidamente aprobados para su procesamiento.*

. *No exista pérdida de datos o falta de procesamiento en los mismos.*

. *Los programas estén procesados con los archivos apropiados.*

. *El procesamiento logre el resultado deseado y se ejecute sin error.*

. *La información de salida sea distribuída en forma apropiada al personal autorizado.*

Los controles deben ser evaluados por el auditor para identificar los puntos débiles en el sistema en operación y para permitirle determinar el alcance del examen que se requiere en una situación particular. Este proceso de evaluación requiere no solamente un conocimiento general del sistema a auditar, sino también de la

seguridad mediante pruebas selectivas de que tales controles están operando efectivamente.

Este subcapítulo esboza diversos factores que deben ser considerados por el auditor en su evaluación de los controles de aplicaciones.

El departamento de PEI normalmente actúa como área de servicio y tiene como responsabilidad primaria el procesamiento de datos para otros departamentos en la organización.

Una función separada, comúnmente conocida como la función de control, debe establecerse para verificar que toda la información que se recibe, procesa y distribuye por el departamento de PEI a los propietarios de la información es razonablemente correcta y confiable a las necesidades de la organización. Esta función también debe:

- *Controlar la acumulación y transmisión de la información de entrada al departamento de PEI.*

- *Controlar el flujo de datos que pasan a través del departamento.*

- *Conciliar los datos de control con la información resultante durante el procesamiento y con la salida.*

- *Controlar la distribución de la información de salida a personal autorizado.*

- *Controlar errores presentados durante el procesamiento para asegurar que sean reportados, corregidos y reprocesados.*

Es importante que las transacciones procesadas por el PEI se originen, aprueben y controlen por personas fuera de dicho departa-

mento, con objeto de cumplir con una adecuada segregación de funciones.

La función de control la realiza el departamento usuario quien origina la información y en donde deben comparar los resultados obtenidos del procesamiento con los totales de control establecidos antes de enviar la información al departamento de PEI.

A continuación se presenta los principales controles que el auditor debe considerar en la evaluación de los sistemas en operación:

3.3.1 Controles de entrada

"El proceso para obtener una certeza y confiabilidad de la información procesada en el departamento PEI se inicia con la preparación de la información fuente que servirá como entrada para el sistema" (29).

Es necesario que la información de entrada sea autorizada, completa y precisa.

El auditor debe tener conocimiento de las fuentes de errores y de los controles que pueden emplearse para evitarlos y detectarlos.

Algunos de los controles más comúnmente utilizados para verificar la información de entrada son:

- Controles de validación y edición de datos

Una vez que la información es leída, puede sujetarse a ciertas rutinas de validación y edición para suministrar alguna seguridad en cuanto a su validéz. Estas rutinas usualmente se prac-

(29) Cfr. Price Waterhouse, La Auditoría en un Ambiente de Procesamiento Electrónico de Información, México, 1972, pág. 27.

tican en una corrida preliminar de procesamiento y las excepciones se reporten al departamento usuario para investigación y corrección.

. ***Carácter válido.*** *Cuando solamente ciertos caracteres se usan en un campo de datos específicos, tal es el caso de la razonabilidad de las fechas.*

. ***Transacción válida.*** *El computador puede ser programado para comprobar la validéz del código para las transacciones que hayan de ser procesados. Por ejemplo, la clave de un vendedor que puede ser asociada a la clave de un territorio de ventas específico.*

. ***Prueba de datos faltantes.*** *Es una validación para determinar que todos los campos de datos necesarios sean ingresados. Por ejemplo el salario y nombre del empleado en una nómina.*

. ***Prueba de límite o razonabilidad.*** *Los datos de entrada pueden compararse con límites predeterminados para asegurar que no han sido ingresados montos en exceso del límite autorizado. Por ejemplo el importe total de un pedido contra el límite de crédito autorizado.*

- ***Controles sobre los datos leídos por el computador.***

En caso que la información de entrada sea por medio de dispositivos magnéticos, la lectura de los datos puede utilizarse para comprobar las etiquetas de archivo y verificar que se esta utilizando el archivo apropiado para determinar que los campos que están siendo leídos son válidos y para establecer y comprobar los totales de control. Para determinar que se están usando los archivos de transacciones o los archivos maestros apropiados y que se está procesando con el archivo completo.

- Dígito verificador

Es un valor numérico que se calcula matemáticamente y se adiciona a los datos para asegurar que el dato original no ha sido alternado. Por ejemplo el último dígito de número de cuenta de un estudiante.

- Totales de control de entrada

Los totales de control se utilizan como un método básico para asegurar el manejo correcto de datos de entrada y para la detección de errores. Los totales de control son cantidades numéricas, los cuales se obtienen de la suma de datos significativos de una transacción o documento, por ejemplo en un pedido, un total de control es la suma de cantidades e importes. Este total se obtiene manualmente y se ingresa al computador como cifra control, posteriormente se ingresan los datos del documento y al ser procesado son comparados ambos totales. Debe imprimirse o desplegarse por pantalla un mensaje confirmando la comparación y mostrando los totales aún si estos no coinciden.

- Verificación de ingreso por teclado

La verificación de ingreso por teclado puede ser utilizado como control de la exactitud de los datos ingresados. Con este proceso, los datos críticos seleccionados son reingresados identificando las diferencias entre el primer y segundo ingreso de datos. Luego, se investigan las diferencias y se corrigen las transacciones. "Este tipo de verificación resulta útil para controlar la exactitud del ingreso de datos en sistemas no interactivos, ya que en este tipo de sistemas no se realizan controles de edición y validación hasta un punto posterior del procesamiento" (30)

---

(30) Cfr. Price Waterhouse, Sistemas de Información Computarizados, Serie de Guías de Auditoría, Guía Complementaria, Buenos Aires, Argentina, 1988, pág. 56.

- ***Datos rechazados***

Una aplicación bien diseñada debe controlar cada transacción rechazada manteniendo un registro de la misma hasta que sea corregida. Las partidas rechazadas deben ser incluídas en todos los informes de excepción posteriores hasta que el usuario apropiado tome las medidas correctivas necesarias. "Al ser reingresadas, las transacciones rechazadas deben ser sometidas a los mismos controles de edición y validación aplicables a las transacciones originales" (31).

A continuación se mencionan los posibles controles programados sobre estos datos rechazados:

- *Mantenimiento de un registro de partidas rechazadas y de su posterior reprocesamiento.*

- *Preparación de lotes separados de rechazos corregidos. Este procedimientos nos permite asegurarnos de que todos los rechasos sean investigados y corregidos.*

- *Corrección de los rechazos por errores en los documentos fuente a cargo del departamento usuario emisor de éstos; devolución de los documentos corregidos para su reprocesamiento bajo los controles normales de ingreso, incluyuendo autorización.*

Esto permite a la gerencia determinar si los rechazos son causados por procedimientos de ingreso inadecuados y evaluar el impacto de dichos errores.

"Dependiendo del diseño del sistema de computación, los datos rechazados pueden ser:

---

(31) Ibidem, pág. 56.

. *Aceptados por el sistema e incluídos en un informe de excepciones*

. *Incluídos en un archivo de partidas en suspenso dentro del sistema*

. *Completamente rechazados" (32)*

Por lo general, cuando los datos son rechazados el computador no retiene ningún registro de las partidas y, en consecuencia, los mismos deben ser controlados manualmente.

Las partidas en suspenso pueden ser mantenidas en un sistema en una o más de las siguientes formas:

. *En archivos separados físicamente.*

. *En registros separados dentro de los archivos maestros.*

. *Con los restantes registros de los archivos maestros, pero identificados como un tipo de transacción separada por medio de indicadores.*

Generalmente, el riesgo asociado con la corrección de transacciones inválidas es menor cuando se utiliza un archivo en suspenso que cuando las transacciones erróneas son aceptadas e incluídas en informes de excepción para su posterior corrección.

La corrección de las partidas en suspenso puede ser efectuada automáticamente por el computador o através de ajustes ingresados por el usuario. En ambos casos, el usuario es responsable del correcto procesamiento de los datos.

---

(32) Ibidem, pág. 61.

Los controles de procedimiento utilizados a fin de minimizar los riesgos anteriormente expuestos son:

- ***Etiquetas externas.*** *Los archivos deberán ser etiquetados claramente de manera que el operador puede estar seguro de su contenido. Las etiquetas deberán de indicar la fecha en que fue preparada, el número y nombre del archivo y la fecha en que fue terminada la cinta.*

- ***Anillos de protección de archivos.*** *Se utiliza para evitar borrar la información antes de la fecha en que se indique una cinta ha sido desechada.*

- ***Etiquetas internas.*** *Son utilizadas como pruebas programadas para proteger los archivos contra un uso indebido. Estas etiquetas identifican la cinta y proporciona información que el programa puede comprobar para cerciorarse de que la cinta es la requerida.*

3.3.2. Controles de procesamiento

- Puntos de reinicio

Cuando sea posible, los programas que requieren mucho tiempo de corrida deben ser escritos de manera que un error que ocurra en la parte final de la corrida no requiera que se corra por completo nuevamente el programa. Esto se logra incluyendo puntos de reinicio en el programa. En dichos puntos, todos los resultados intermedios obtenidos hasta ese momento son conservados.

- Controles programados para detección de errores

Los programas que hayan sido apropiadamente depurados y probados deben presentar pocos problemas. Sin embargo, con programas complejos, nuevos o modificados, existe la posibilidad de encontrar

errores latentes que puedan no ser descubiertos en un momento determinado. Pueden incorporarse características de control para descubrir ciertos tipos de errores que pueden permanecer sin detectarse durante la preparación, modificación y depuración del programa. Tales controles pueden ser relativamente sencillos pero muy efectivos para descubrir errores en lógica, procesamiento incompleto y errores introducidos por cambios en el programa. Los controles programados también pueden detectar determinados tipos de errores del operador, tales como alimentación de archivos incorrectos de datos.

- ***Comprobación de las unidades de cinta y las unidades de almacenamiento de discos antes de procesar los datos.***

Los operadores pueden introducir errores en el procesamiento alimentando archivos o lotes de transacciones incorrectos o poniendo archivos de transacciones en una pieza equivocada de equipo. "Los controles de programa normalmente están diseñados para reducir errores del operador mediante el ingreso de instrucciones en el programa a efecto de que se utilice el equipo y se procesen los archivos apropiados" (33).

Un operador de computador debe siempre recibir instrucciones detalladas del programa, especificando el equipo que debe ser usado, y archivo que debe ser procesado. Los mensajes de la consola pueden ser generados por el programa que describa los pasos que deben ejecutarse por el operador durante la corrida del mismo. El programa debe requerir verificación por la vía de la consola en el sentido de que se han seguido las instrucciones correctamente.

---

(33) Cfr. Price Waterhouse, Le Auditoría en un Ambiente de Procesamiento Electrónico de Información, op. cit., pág. 32.

- Verificación de los datos procesados

Los programas de computador pueden ser bastante complejos y requerir un largo tiempo de procesamiento. En tales casos los programas deben requerir una comparación periódica de los datos que están siendo procesados contra controles previamente establecidos o contra totales de lotes determinados al final de una etapa previa en el procesamiento. Si cualquier dato se omite inadvertidamente en algún paso en el procesamiento o se procesa más de una vez, es esencial que el error se descubra tan pronto como sea posible. El costo de encontrar un error después de que los datos han sido procesados frecuentemente exceden en valor al costo de incorporar comprobaciones periódicas de cifras de control en el programa que está siendo usado.

3.3.3 Controles sobre errores y datos rechazados

Los programas del computador deben preveer la preparación de un registro de todas las transacciones incluidas en paros del programa e intervenciones del operador.

Debe mantenerse control sobre los datos rechazados o incorrectos para asegurar su reprocesamiento futuro.

Se debe escribir programas efectivos para que el procesamiento no se vea interrumpido por errores.

Un procedimiento de errores escrito dentro del programa puede proporcionar identificación y listado de ciertas clases de transacciones erróneas. Debe prepararse un reporte de rechazos o errores durante cada rutina de procesamiento y, cuando el error está en los datos originales, debe regresarse al departamento fuente para corrección y reposición. Actuar de otra manera sería eludir el control interno básico sobre el procesamiento de datos.

La información rechazada o incorrecta debe ser controlada de manera que se apliquen las correcciones apropiadas, y los operadores del computador no deben tener facultad de iniciar correcciones.

Sobre datos que son rechazados durante una corrida normal de procesamiento y los procedimientos usados para corregir errores son una parte importante de los procedimientos de control y deben ser revisados cuidadosamente por el auditor.

Debe prepararse un registro de todos los errores anotando su naturaleza, frecuencia y efecto sobre la exactitud de la información de salida, la cual puede indicar deficiencias básicas en algún punto del sistema.

El significado general de todos los errores debe evaluarse periódicamente para determinar su efecto sobre la confiabilidad de la información de salida. Las estadísticas de errores deben revisarse periódicamente por personas independientes del departamento de PEI, tales como los auditores.

- Controles en los cambios en los archivos

Los cambios en los archivos deben ser estrechamente controlados por el departamento usuario que inicia los cambios. Debe suministrarse al departamento que los inicia un aviso o registro de todos los cambios proceados para verificar que tales cambios fueron hechos apropiadamente y para sujetar los cambios a su revisión.

Los archivos completos que contienen información clave deben imprimirse regularmente para ser revisados y actualizados tanto por el departamento que los origina como por el que los usa.

3.3.4 Controles de salida

- Revisión de la información procesada

La información de salida debe ser entregada al grupo de control del departamento de PEI para su revisión, después de completar el procesamiento. Este grupo debe ser responsable de revisar la información en cuanto a que sea razonable, completa y para comprobar totales de control que hayan sido establecidos previamente. Para hacer esto efectivamente el grupo de control debe tener un conocimiento general del propósito fundamental de la rutina de procesamiento y debe saber lo que requieren los usuarios.

- Establecimiento de procedimientos adecuados para controlar la distribución de información.

La distribución de la información de salida debe ser controlada para asegurar que solamente personal autorizado la recibe; puesto que muchos de los datos procesados por el departamento de PEI pueden ser confidenciales. Para asegurar que la información se distribuye apropiadamente, el grupo de control debe mantener un programa de todos los datos a procesar, los informes resultantes, el número de copias que deben prepararse y a la persona responsable y autorizada que se le debe de entregar la información.

Las personas que reciben la información de salida del departamento de PEI son una parte integral del sistema de control interno y representan una fuente importante de descubrimiento de errores.

Debe haber una confirmación de errores proveniente de los usuarios de datos, quienes deben tomar la responsabilidad final de toda la información recibida del PEI. Estas personas deben satisfacerse de que la información está completa, exacta y en forma aceptable antes de usarla. Para lograr estos objetivos toda la información de salida debe ser revisada en cuanto a su razonabi-

lidad por un empleado responsable dentro del departamento usuario.

3.4 HERRAMIENTAS PARA AUDITAR APLICACIONES

Una herramienta de auditoría es un ayuda tangible que asiste al auditar en la implantación de una técnica de auditoría.

A continuación se presenta las principales herramientas utilizadas y recomendadas como apoyo para el autidor en informática en el desempeño de sus funciones:

3.4.1 Cuestionarios

Los cuestionarios estandarizados son una herramienta de auditoría que se ha empleado tradicionalmente para recopilar información sobre los controles internos y procedimientos existentes.

Los cuestionarios relativos a los controles de aplicación deben estar orientados hacia el flujo general de información del sistema: por ejemplo; nóminas, inventarios, y compras, entre otros.

Un cuestionario no se diseña considerando todas las circunstancias especiales que de hecho existen en cualquier sistema de aplicación. Por lo tanto, los cuestionarios deben utilizarse únicamente como guías y recordatorios. Bajo ninguna circunstancia deberá permitirse que sustituyan el análisis minucioso del auditor.

3.4.2 Diagramas de flujo

Una herramienta útil para el análisis de auditoría es un diagrama de flujo analítico, el cual identifica todo el procesamiento manual y computarizado de una aplicación. Este diagrama muestra

todos los archivos y transacciones sujetos a procesamiento. La complejidad de la aplicación determinará qué tan extenso debe ser el diagrama de flujo.

La característica especial de un diagrama de flujo analítico es que se establecen columnas por separado para cada entidad organizacional significativa que se involucra en el procesamiento. Normalmente se asignarán columnas a nivel departamental con base a las responsabilidades sobre el procesamiento, manejo, decisiones y control.

Una vez terminado, el diagrama de flujo analítico presenta una imagen general que ayuda en muchas formas al análisis posterior de la aplicación.

3.4.3 Programas fuente

Los listados del programa en lenguaje fuente es una referencia útil respecto a la información detallada relativa a las funciones y controles de la aplicación programada; sin embargo, requiere un alto grado de conocimientos técnicos. Aun cuando en el desarrollo de la aplicación se preparan diagramas de flujo de la lógica de los programas, a menudo no se actualizan en lo que se refiere a las modificaciones posteriores de los mismos. Este tipo de programas pueden ser empleados por los auditores u otras personas que requieran un conocimiento detallado de la lógica del programa de aplicación.

3.4.4 Programas utiliarios

Los programas utilitarios han sido diseñados para llevar a cabo tareas específicas de procesamiento de datos de naturaleza rutinaria y para que su uso sea sencillo. Estos programas son generalmente provistos pro el fabricante del computador o por proveedores de software, aunque, ocasionalmente, los programadores de sistemas los desarrollen por su cuenta. El usuario proporciona

sus instrucciones al programa utilitario en forma de parámetros que identifican los archivos de entrada y de salida, la función que debe ser realizada y los criterios de selección.

Algunos programas utilitarios típicos son: DFU, Ditto, ZAP y SUPERZAP.

"Las funciones que los programas utilitarios pueden realizar incluyen:

. Clasificación de archivos de datos

. Fusión de varios archivos de datos en uno solo.

. Copia de archivos de datos

. Impresión de todo o parte de los archivos de datos

. Búsqueda en un archivo de datos que contengan determinados valores en un campo de datos dado" (34).

3.4.5 Lenguajes convencionales de programación

El uso de estos lenguajes requiere un alto nivel de conocimientos técnicos para desarrollar y correr los programas, como así también conocer el lenguaje de programación. Se requiere instrucciones de programación detalladas aún para realizar un procedimiento simple. Sin embargo, cuando no se dispone de programas de software de auditoría u otro software, un programa convencional puede ser la alternativa más conveniente.

---

(34) Cfr. Price Watorhouse, Sistemas de Información Computarizados, op. cit., pág. 194.

3.4.6 Generadores de datos de prueba

Uno de los intentos más recientes para optamizar la utilidad de los datos de prueba en sistemas y situaciones complejas son los programas de operación que generan ese tipo de datos. Dichos programas emplean diversas técnicas para generar datos de prueba variables, tales como valores al azar, valores constantes, valores dentro de rangos específicos que han de colocarse en los campos dentro de los registros, o datos que se encuentran en condición de error.

Los datos de prueba ideales deben representar la aplicación que se examina con todas las posibles combinaciones de transacciones.

3.4.7 Programas de recuperación y análisis

El uso de programas de recuperación y análisis puede brindar ventajas sobre los procedimientos manuales tradicionales en cuanto a la eficiencia. Algunas de estas ventajas son:

- La información puede reordenarse en formatos que permitan un uso más eficiente para la auditoría.

- Los datos pueden ser clasificados y seleccionados con mayor rapidez y precisión.

- Un archivo de datos completo puede ser revisado en menos tiempo del que se requiere para seleccionar una muestra pequeña en forma manual.

- Los datos con significatividad de auditoría pueden ser identificados y listados rápidamente para su posterior revisón.

El propósito general del uso de programas de recuperación y análisis es mejorar la eficiencia y efectividad de la auditoría.

"Los programas de recuperación y análisis pueden ser particularmente útiles para:

. Obtener muestras y selecciones de auditoría para las pruebas que realizará el equipo de trabajo.

. Realizar cálculos con los datos.

. Resumir, reclasificar y comparar datos en archivos separados para permitir que el trabajo planeado pueda ser finalizado de la forma más efectiva y eficiente posible". (35)

Algunos ejemplos de este tipo de programas son Focus e Easytrieve.

3.4.8 Paquetes de software de auditoría

Un paquete de software de auditoría es un programa o conjunto de programas diseñados en un lenguaje de programación para auxiliar al auditor y permitirle desarrollar, en forma independiente, rutinas que le faciliten la opción de seleccionar, recuperar y emitir información seleccionada de un archivo o bases de datos.

El uso de paquetes de software de auditoría tiene las siguientes ventajas:

. Generalmente han sido suficientemente probados como para asegurar que funcionan en forma adecuada.

. Han sido diseñados para satisfacer necesidades específicas de auditoría.

---

(35) Cfr. Price Waterhouse, Sistemas de Información Computarizados, op. cit., pág. 198.

. *Frecuentemente se dispone de cursos de capacitación para su uso.*

. *Se puede obtener asistencia técnica para su utilización.*

Sin embargo, existen ciertas desventajas comunes a todos los paquetes de software de auditoría que deberíamos conocer, incluyendo limitaciones en:

. *La cantidad de archivos que pueden ser leídos.*

. *El tipo de estructuras de registros y representaciones de datos en archivos a los que se puede acceder.*

. *La cantidad de selecciones y cálculos de auditoría que pueden especificarse.*

. *El número de informes de auditoría que pueden ser producidos en cada procesamiento de un archivo.*

- *El formato de los informes de salida.*

Ejemplos de paquetes de software de auditoría son: PW Analyzer, PANAUDIT e IDEA.

3.5 TECNICAS PARA AUDITAR LAS APLICACIONES

A medida que los computadores y sistemas se han vuelto más refinados y complejos, el auditor ha tenido que modificar sus procedimientos de auditoría para guardar el paso con los cambios en tecnología y estar en posibilidad de llevar a cabo su examen de una manera efectiva. Si bien el auditor puede en muchos casos auditar con procedimientos manuales, debe considerar cuidadosamente la utilización del computador en cada trabajo ya que esto puede dar por resultado una auditoría más eficiente y efectiva en muchas áreas.

Este subcapítulo contine una descripción de las principales Técnicas asistidas por computador que pueden utilizarse para determinar la existencia de los controles y verificarlos. Existen dos objetivos en cuanto su uso, verificar las operaciones manuales y/o computarizadas y verificar los resultados del procesamiento.

Selección de la técnica

Cualquiera que sea la técnica o técnicas utilizadas, el auditor debe iniciar su examen de los controles que se aplican a los programas identificando los pasos del procesamiento y los controles clave que van a verificarse y posteriormente seleccionar la técnica que mejor se adapte a sus necesidades y limitaciones que se pudieran presentar.

3.5.1. Datos de prueba

Los datos de prueba, comúnmente llamados "lotes de prueba", son conjuntos de datos de entrada que presentan al computador una variedad de transacciones para verificarlas a través del procesamiento real, como medio para detectar resultados que no sean válidos. Los datos de prueba ideales deben representar la aplica-

ción que se examina con todas las posibles combinaciones de transacciones, situaciones de archivos maestros, valores y lógica de procesamiento que podrían encontrarse durante las operaciones.

Para que la verificación de los datos de prueba sea factible, debe contarse con documentación altamente confiable respecto a la aplicación. Esta documentación deberá incluir información detallada y completa de los formatos de las transacciones, los formatos de los archivos maestros, las condiciones de procesamiento y los controles.

En caso de que sea necesario que el auditor cree nuevos archivos maestros para verificarlos mediante el uso de datos de prueba, pueden considerarse dos enfoques alternativos:

- *Los datos reales selectivos pueden compilarse como un archivo de datos de prueba.*
- *El auditor puede crear registros de archivos maestros especialmente para este propósito.*

- Aplicación de la técnica de datos de prueba

Al aplicar la técnica de datos de prueba, el auditor hace lo siguiente:

Define los objetivos

El requisito de una definición formal de objetivos, válido para cualquier técnica de pruebas de auditoría, se aplica para verificar únicamente aquellas características o controles que el auditor designa en forma explícita.

Prepara los datos de prueba

El segundo paso en la aplicación de las técnicas de datos de prueba es obtener o diseñar el archivo maestro y de transacciones con las características apropiadas. La obtención o preparación de todas las condiciones y características que van a probarse.

Caálcula los resultados previstos para el procesamiento

El siguiente paso en el flujo del trabajo asociado con los datos de prueba es el cálculo previo de los resultados previstos para el procesamiento. Esto se hace mediante el uso de datos reales que se incluyen en los registros maestros y en las transacciones relacionadas que constituyen los datos de prueba. Los datos de prueba se determinan con base en la comprensión de la lógica del programa, los métodos de cálculo y las características de control, para compararlos con los resultados del procesamiento por computador.

Procesa los datos de prueba a través del computador

El siguiente punto a considerar es procesar los datos de prueba a través de todos los programas en el flujo general de la aplicación.

Cuando se procesan diferentes tipos de transacciones en distintas etapas de una aplicación, el auditor debe preveer que para llevar a cabo las verificaciones de los datos de prueba pueden requerirse más de un tipo de transacciones y más de un archivo maestro.

Compara los resultados manuales contra los producidos por el computador

Después del procesamiento, el auditor compara los resultados reales con aquellos que se predeterminaron con base a los cálculos

manuales previos. Todas las discrepancias deben identificarse y analizarse para determinar sus causas.

Resuelve las excepciones

Cuando los resultados de la prueba indican verdaderas discrepancias en el procesamiento de los programas de aplicación, el auditor debe identificar sus causas precisas y diseñar procedimientos adicionales para cuantificar los efectos derivados de un procesamiento realizado con programas erróneos.

3.5.2 Método de instalación de prueba integrada (ITF)

*"El método de instalación de prueba integrada (**Integrated Test Facility -ITF**) permite alimentar a un sistema los datos de entrada de prueba seleccionados, junto con, o como si estuvieran mezclados con los datos "reales", y rastrear el flujo de estas transacciones de prueba a través de las diferentes funciones en el sistema, para compararlas con resultados predeterminados" (35).*

Ventajas

Las ventajas de utilizar el método ITF son las siguientes:

- *Se requeire un mínimo conocimiento técnico.*
- *El costo del procesamiento es bajo debido a que los datos de prueba se procesan junto con los datos de entrada normales.*
- *Se evalúa el sistema real, tal como opera normalmente.*

---

(35) Cfr. Mair, William, Et. al., Control y Auditoría del Computador, Op. cit., pág. 175.

. *Todos lo entienden, ya que el auditor utiliza los procedimientos normales que sigue la organización para alimentar los datos.*

Desventajas

Las desventajas del método ITF son:

. *Falta de control al ingresar las transacciones de prueba.*

. *La posibilidad de que se destruyan archivos, debido a que las transacciones afectan archivos reales.*

. *La dificultad para identificar todas las variaciones de las excepciones, para probar el programa.*

. *La cantidad de datos de prueba que el auditor introduce puede verse limitada por la necesidad de alimentar esos datos juntos con los reales.*

. *Las transacciones de los datos de prueba deben ser eliminadas de los registros y archivos inmediatamente de haberse concluido la prueba.*

Aplicación de la técnica ITF

Al aplicar la técnica de instalación de prueba integrada, el auditor hace lo siguiente:

Define objetivos

El requisito de una definición formal de objetivos, válido para cualquier técnica de pruebas auditoría, se aplica para verificar únicamente aquellas características o controles que el auditor designa en forma explícita.

Establece registros "falsos" en los archivos "reales"

El auditor generalmente establece datos de prueba por separado, contra los cuales se procesarán sus transacciones. El método ITF requiere que estos registros se introduzcan en el mismo flujo de operación real; sin embargo, debe implantarse un estricto control del lote de datos de prueba ingresado por medio de una identificación.

Establece el método para eliminar los efectos de los datos de prueba

Debido a que los datos de prueba se encuentran junto con los datos reales y a que las transacciones de pueba se alimentan durante el flujo normal del procesamiento, debe tomarse alguna medida para eliminarlos de los resultados del procesamiento real. Las medidas podrían ser:

- *Reversión manual de los efectos de las transacciones y registros sobre los resultados reportados.*

- *Eliminación de las transacciones y registros en las cifras control, mediante programas*

- *Uso de valores insignificativos para las transacciones y registros, con objeto de que sus efectos puedan ser ignorados.*

Calcula los resultados previstos para el procesamiento

El auditor debe determinar, antes o después de la prueba, qué resultados deben obtenerse de acuerdo con su entendimiento y sus objetivos de auditoría.

3.5.3 Archivo de revisión de auditoría como control del sistema (SCARF)

*El método del archivo de revisión de auditoría como control del sistema (**System Control Audit Review File - SCARF**) implica la incorporación de pruebas de razonabilidad determinadas por el auditor, en los programas del procesamiento normal. Los resultados de esas pruebas se reportan al auditor, en lugar de a los usuarios, para su revisión y posible investigación.*

Implantación de la técnica SCARF

Los pasos que incluye esta técnica son los siguientes:

- *El auditor proporciona sus requerimientos al equipo de desarrollo de sistemas durante la fase de desarrollo relativo a las especificaciones del usuario.*

- *Los requerimientos de selección del auditor se implantan en los programas de aplicación, junto con el resto del desarrollo de la misma.*

- *Una vez que se ha implantado el nuevo sistema, los controles detectivos especificados por el auditor funcionan simultáneamente con los del procesamiento normal de la aplicación, y las excepciones a estas pruebas de auditoría se registran en un archivo.*

- *El archivo de excepciones de auditoría es revisado por el auditor utilizando técnicas manuales o ayudadas por computador.*

- *El auditor sigue la acción que considera apropiada, basado en las excepciones que descubre.*

3.5.4 Archivo de revisión de auditoría por muestreo (SARF)

*Un archvio de revisión de auditoría por muestreo (**Sample Audit Review File - SARF**) es bastante similar a SCARF excepto en que su contenido se selecciona al azar, más que como excepciones a cualquier prueba especial de edición o razonabilidad. El objetivo de esta técnica es obtener un archivo representativo para efectos del análisis de auditoría.*

"La técnica SARF es particularmente apropiada para los auditores externos, a quienes se les requiere que prueben los controles o las transacciones durante todo el año que examinan. Sin embargo, la técnica también es recomendable para los auditores internos que simplemente desean una muestra represetativa" (37).

Implantación de la técnica SARF

Los pasos que se incluyen en esta técnica son similares a los de la la técnica SCARF:

- *El auditor proporciona sus requerimientos al equipo de desarrollo de sistemas, durante la fase de desarrollo relativa a las especificaciones del usuario.*

- *Los requerimientos de selección del auditor se implantan en los programas de aplicación, junto con el resto del desarrollo de la misma.*

- *Una vez que se ha implantado el nuevo sistema de aplicación, la rutina de selección al azar origina que los registros sean grabados en un archivo.*

---

(37) Cfr. Mair, William, Et. al., Control y Auditoría del Computador, op. cit., pág. 180.

. *El archivo representativo de registros es examinado por el auditor utilizando técnicas manuales o ayudadas por computador.*

. *El auditor sigue la acción apropiada en base a las situaciones que detecta.*

3.5.5 Downloading

Los recientes avances tecnológicos proporcionan a los usuarios conexiones entre microcomputadores y computadores centrales. Estas conexiones pueden brindarnos la oportunidad de perfeccionar nuestros procedimientos de auditoría, facilitando el acceso a los datos de los archivos.

Un ejemplo de la forma en que dichas conexiones pueden colaborar en nuestro trabajo incluyen:

. *Transferencia de los archivos a microcomputadores y análisis de datos u otras funciones de auditoría relacionadas ("downloading").*

"Las conexiones entre microcomputadores y computadores centrales facilitan nuestro acceso a los datos y la ejecución de los procedimientos de auditoría. Permiten que el microcomputador se transforme en un mecanismo de ingreso, procesamiento y salida de datos además de ser una unidad independiente" (38).

La mecánica del downloading puede ser resumida de la siguiente manera:

---

(38) Cfr. Price Waterhouse, Sistemas de Información Computarizados, op. cit., pág. 202.

. *Identificación de los datos que serán transferidos desde el computador central al microcomputador.*

. *Determinación del método que se utilizará para transferir datos desde el computador central al microcomputador. (En algunos casos, se establece una conexión directa entre los computadores. En otros, los datos son copiados en una cinta magnética y luego, desde una unidad de cintas se podrán transferir los datos desde la cinta al microcomputador).*

. *Si fuera necesario, conversión de los datos a un formato que pueda ser utilizado por el software de microcomputación. (A menudo, los computadores centrales emplean métodos de representación de datos que difieren de los utilizados por los microcomputadores. Por ejemplo, los computadores centrales de IBM utilizan un método de representación de datos denominado EBCDIC, en tanto que los microcomputadores emplean ASCII).*

3.5.6 Snapshot

La técnica Snapshot es una forma de pista de las transacciones que se estipula únicamente para los datos de entrada seleccionados, los cuales llevan una clave especial. Este es a menudo un enfoque efectivo en sistemas de gran volúmen. Si esta función se implanta por anticipado en el sistema de aplicación, puede añadirse una clave especial a cualquier transacción de entrada para generar una pista impresa de esa partida específica, siguiendo cada paso del procesamiento de la aplicación.

Implantación de la técnica "Snapshot"

Los pasos requeridos para utilizar la técnica Snapshot son los siguientes:

. *El auditor proporciona sus requerimientos durante la fase de desarrollo relativa a las especificaciones del usuario.*

. *El equipo de desarrollo de sistemas implanta la función para obtener una pista selectiva de las transacciones durante los pasos subsecuentes del desarrollo del sistema de aplicación.*

. *Después de la implantación del nuevo sistema puede añadirse una clave adicional especial a los datos de entrada sin afectar ningún otro aspecto del procesamiento de la misma.*

. *Durante el procesamiento de la transacción se producen reportes en puntos predeterminados, a fin de revelar el impacto que la transacción "marcada" tiene sobre los registros maestros y los cálculos posteriores.*

. *El auditor recibe la documentación de la pista de las transacciones.*

. *El auditor analiza la pista de acuerdo con sus objetivos de auditoría.*

La utilización de una pista de transacciones selectiva no es solamente una técnica efectiva para ser usada por el auditor, sino que es especialmente útil para el personal de desarrollo de sistemas y de programación para localizar discrepancias en el procesamiento de la apliación. Además, la gerencia usuaria compartirá los mismos intereses que el auditor.

Consecuentemente, esta técnica se implanta para que el personal de programación depure los programas del computador. Si dicha función se encuentra a disposición del personal de programación,

el auditor y el usuario pueden también emplearla cuando lo deseen.

3.5.7. Simulación en paralelo

La simulación en paralelo consiste en preparar una aplicación computarizada por separado que efectúe las mismas funciones que los programas de aplicación reales utilizadas para el procesamiento diario u otros procesamientos periódicos.

La designación de simulación es apropiada, ya que el programa creado para efectos de auditoría efectúa las mismas funciones de procesamiento que los programas de aplicación normales. Debido a que los programas de computador actuarán en forma consistente (dadas circunstancias idénticas), el auditor puede inferir un alto grado de confianza en que cada vez que se utilicen los mismos programas se obtendrán los mismos resultados.

Una vez procesados los mismos archivos y transacciones por los dos sistemas, los resultados deberán ser idénticos y directamente comparables en lo que se refiere a las funciones y controles de aplicación seleccionados para la simulación en paralelo; es decir, la técnica no necesita reproducir íntegramente las aplicaciones. Más bien, el auditor selecciona los datos y funciones de la aplicación con base a su importancia para la auditoría (en relación con la importancia relativa), y aplica las técnicas de simulación únicamente a esas áreas.

La característica importante de la simulación en paralelo es que se efectúa un procesamiento independiente de la información real en operación. Las técnicas de simulación son más efectivas cuando se aplican a cálculos, decisiones y controles programados. También pueden simularse las funciones de aplicación que mantienen y actualizan los archivos con transacciones.

La simulación de los programas de operación de auditoría procesa transacciones contra los datos de los archivos, creando sus propios archivos de datos de salida, y los compara con los archivos generados por los programas de la aplicación real. La aplicación de programas de operación de auditoría puede incluir que el computador compare los datos producidos por los programas de la aplicación real contra los producidos por la simulación. En tal caso, el reporte entregado al auditor incluye únicamente partidas de excepción.

CAPITULO IV

COSTUMBRES Y NORMAS DE SEGURIDAD FISICA Y AMBIENTAL EN UN CENTRO DE COMPUTO

4. CONTROLES Y MEDIDAS DE SEGURIDAD FISICA Y AMBIENTAL EN LOS CENTROS DE COMPUTO

4.1 CONSIDERACIONES PRELIMINARES

El desarrollo tecnológico, el incremento de aplicaciones y el consecuente manejo de información ha permitido que la computadora sea utilizada en una gran cantidad de organizaciones las cuales concentran la función informática en departamentos, unidades o centros de procesamiento de datos, que se encargan de proporcionar los servicios de cómputo necesarios a la organización.

Dentro de estos centros de cómputo se encuentran, además del equipo y programas que procesan la información, factores muy importantes de cuya integridad y medidas de salvaguarda depende la satisfacción de las necesidades de cómputo de las organizaciones.

La seguridad física efectiva en los centros de cómputo debe garantizar la prevención y detección de los diversos riesgos a los que está expuesta la información y los centros de cómputo, los cuales fueron mencionados y analizados en el capítulo 1.

La existencia de procedimientos y medidas claramente definidas permitirán afrontar con oportunidad un desastre o contingencia ante la interrupción del procesamiento, reestableciendo la continuidad de las operaciones.

El presente capítulo titulado Seguridad Física y ambiental en un centro de cómputo tiene por objetivo analizar los procedimientos controles y medidas adecuadas de seguridad utilizadas en las instalaciones de cómputo.

4.1.1 *¿Qué es un centro de cómputo?*

Antonio Vaquero define al centro de cómputo como: "...una instalación concebida especialmente (climatizada, insonorizada, con piso y techo falsos, etc.,) para albergar computadoras, sus periféricos locales y equipo auxiliar, además de las salas para el personal de servicio" (39).

Por mi parte, defino a un centro de cómputo como un lugar, con características especiales de seguridad e instalación en donde reside el equipo de cómputo, dispositivos periféricos, y equipo humano especializado en donde se procesa la información.

Al centro de cómputo se le conoce también como Centro de Procesamiento Electrónico de Información (PEI).

4.1.2 Privacia, seguridad, disponibilidad e integridad

Analizar las características de privacia, seguridad, disponibilidad e integridad de los recursos en un centro de cómputo son actualmente tópicos de gran importancia, razón por la cual los defino a continuación:

*Se entiende por **privacía**, al derecho de prohibir y evitar el acceso general a cierta información, propiedad de un grupo dentro de la organización.*

*El segundo término, **seguridad**, "es la condición de estar seguros; lo cual significa estar libre, exento de riesgos, daños o males" (40).*

*La **disponibilidad** se refiere a la posibilidad de poder hacer uso y modificación de la información contenida en archivos en todo momento, siempre y cuando se cumplan con las normas de privacía correspondientes.*

*Por último, la **integridad**, se refiere a la característica fundamental de que la información se mantenga consistente, completa y válida durante y después del uso diario de la información. Cuando se cuenta con una alta integridad, se considera que la información es confiable.*

De antemano podemos mencionar que con el fin de tener integridad, se requiere aplicar medidas de privacía y seguridad a la operación diaria de una organización.

4.1.3 Concepto de seguridad física

Seguridad física en un lenguaje común, es la protección de todo aquello que es visible y tangible.

Desde el punto de vista computacional se tienen los siguientes conceptos:

"...Es la protección de hardware y software contra daños o destrucción ocasionadas por incendios, inundaciones o sabotaje". (41)

---

(40) Aguirre Martínez, Eduardo Seguridad Integral en las organizaciones: Actualización para Ejecutivos, Edit. Trillas, México 1986, Pág. 9
(41) Sanders H., Donald, Informática: Presente y Futuro. Edit. McGraw-Hill. México, 1985, Pág. 538.

Por otra parte, decimos que la seguridad física es la implantación de medidas de seguridad adecuadas que permite garantizar la integridad del equipo y recursos en el centro de cómputo con objeto de evitar daños materiales (descompostura de equipo, fallas en instalaciones, daños causados por la naturaleza (temblor, inundación, fuego, etc.), o daños causados por el hombre (robo, fraude, sabotaje, etc.)

4.2 RAZONES PARA ASEGURAR FISICAMENTE UN CENTRO DE COMPUTO

Algunas razones por las que hay que asegurar físicamente un centro de cómputo son las siguientes:

a) Una instalación de cómputo representa una fuerte inversión que es necesario proteger.

b) La vulnerabilidad del equipo de cómputo.

c) El equipo no se puede reemplazar fácilmente.

d) Hay una alta concentración de datos e información en un sólo lugar.

e) La dependencia que tiene la organización del centro de cómputo.

f) Es el lugar físico donde se procesa la información necesaria para la toma de decisiones.

Son dos los objetivos principales que se pretenden alcanzar al asegurar físicamente un centro de cómputo.

a) Reducir la probabilidad de que ocurra algún siniestro y si ocurre, reducir sus efectos.

b) Asegurar la continuidad del servicio que presta el centro de cómputo a la organización.

4. 3 CONTROLES Y MEDIDAS DE SEGURIDAD FISICA A EVALUAR POR EL AUDITOR EN INFORMATICA:

No hay una clara definición respecto a los controles y medidas principales que se deben considerar para tener una adecuada seguridad física y ambiental en un centro de cómputo; sin embargo, de acuerdo a la experiencia en investigaciones realizadas llegué a la conclusión que lo más importante que el auditor debe evaluar es:

1) Ubicación y construcción de un centro de cómputo.

2) Suministro de energía eléctrica.

3) Condiciones del medio ambiente.

4) Seguridad contra incendios.

5) Control de acceso.

6) Planes de contingencia.

7) Planeación para recuperación en casos de desastre.

8) Seguros.

4.3.1 Ubicación y construcción de un centro de cómputo

CONSIDERACIONES PRELIMINARES

Aparentemente el problema de decidir respecto a la ubicación y construcción de un centro de cómputo, es algo sencillo y trivial de resolver; sin embargo, considero que no es así, ya que se involucran una gran cantidad de factores, que de no ser considerados pueden ocasionar resultados de fatales consecuencias.

- UBICACION

Anteriormente se pensaba, que cuando se adquiría una computadora se debía difundir lo más posible. En consecuencia, muchas instalaciones de cómputo se colocaron dentro de atractivas paredes de vidrio con vista al exterior y con un máximo de publicidad. Las serias amenazas que se presentaron contra las instalaciones de cómputo cambiaron rápidamente esta situación. Su ubicación se ha vuelto cada vez más clandestina. La selección del local también se ha vuelto más conservadora, y las computadoras se colocan lejos de las áreas de gran tránsito, tanto terrestre como aéreo.

El centro de cómputo deberá estar ubicado en una área que proporcione máxima protección para que no sufra daños, y alcance el máximo de vida útil.

Los factores a considerar para la elección del lugar donde se ubicará la instalación de cómputo son:

a) Limitaciones físicas del lugar en donde se planea instalar el centro de cómputo, por ejemplo, la capacidad de carga del piso.

b) El tamaño y características del equipo de cómputo a instalar.

c) *Espacio para las salas anexas a la instalación como son: sala de mantenimiento, almacén de medios magnéticos, área para la planta de aire acondicionado, área para la planta auxiliar de suministro de energía, etc.*

d) *Es muy importante considerar la capacidad de energía eléctrica disponible para hacer uso de ella sin pérdida de tiempo.*

e) *Flujo de trabajo hacia otras áreas usuarias.*

f) *Posibilidad de una futura expansión.*

Hay que tomar en cuenta las siguientes recomendaciones:

g) *El centro de cómputo no debe estar ubicado en zonas geográficas con un alto índice de fenómenos naturales (lluvias, inundaciones, sismos, etc.).*

h) *El centro no debe estar ubicado en lugares susceptibles de sufrir inundaciones o fuego, como aquellas áreas adyacentes al sótano o que faciliten la propagación de éste.*

c) *Debe estar localizado lejos de aeropuertos, equipos eléctricos (como radares y microondas), tráficos pesados, y calentadores de vapor.*

d) *Las colindancias no deben ofrecer peligros de incendio, explosiones, derrumbes, escapes de gases tóxicos, o contaminación bacteriana o viral.*

e) *Debe estar alejado de zonas con un alto índice de vandalismo.*

f) *No debe encontrarse a la vista del público.*

g) *Debe estar lo más inaccesible.*

h) *Cuando se trata de un edificio de varios pisos, evitar ubicar la instalación en el sótano, en la planta baja o en un piso alto. Lo recomendable es ubicarlo en el primer piso debido a lo pesado que resulta ser el equipo y lo complicado que es su transportación.*

i) *Debe estar separado físicamente de las otras áreas o departamentos de la organización.*

"La ubicacion mal planeada ha sido la causa principal de problemas que, con un poco más de previsión, se hubieran evitado" (42).

- CONSTRUCCION

Consideraciones preliminares

"En la actualidad, son pocos los arquitectos que son expertos en los principios de diseño de centros de cómputo. Quizá por esto se realizan malos diseños y muchos de ellos no son los más adecuados y seguros". (43)

Es muy importante que se construya un centro de cómputo de tal manera que no sea capáz de llamar ni la mínima atención. Debe ser construido con materiales no combustibles y resistentes al fuego (tiempo mínimo de resistencia 2 horas), y contar con un buen sistema de seguridad contra incendios.

---

(42) Cfr. John G. Burch, et. al., Sistemas de Información: Teoría y Práctica, Edit. Limusa, México 1986. Pag. 382.
(43) Cfr. Leonard H. Fine., Seguridad en Centros de Cómputo, Edit. Limusa, México, 1983 pág. 38.

Paredes, techos y pisos

Las paredes que rodean al área del computador deben ser sólidas para evitar el esparcimiento del fuego o las entradas de agua, así como para que se limite el acceso al área. Para ello, se recomienda el uso de ladrillos o concreto de alta calidad en su construcción. Además, las paredes deben extenderse desde la estructura del piso a la del techo del edificio y no desde pisos elevados (o falsos) a techos falsos, con el fin de impedir una entrada a las áreas sensibles del centro de cómputo.

Se evitará en lo posible que las paredes exteriores a la sala del computador estén expuestas a las condiciones climatológicas, ya que se generaría una carga extra en el aire acondicionado, lo que originaría un incremento en el costo de operación. Cuando no se pueda evitar esta exposición, las paredes exteriores serán tratadas con un asislante término para evitar condensación.

En ocasiones es necesario utilizar paredes y páneles removibles para construir ciertos cubículos dentro del centro, así como para facilitar expansiones futuras, los cuales deben ser construidos con material aislante térmico para limitar la transferencia de calor entre la sala del computador y las áreas adyacentes.

Si las paredes y los pisos son de concreto, hay que sellarlos con pintura resistente al polvo.

Uno de los factores más importantes para limtar los daños por incendio, es el diseño de los pisos y techos para resistir el paso de calor, humo, gases y agua, de un nivel a otro.

Es necesario una altura suficiente (mínimo 3.15 metros) en la sala del computador para obtener una circularización del aire

acondicionado sin restricciones. Una insuficiente altura puede causar problemas con el aire acondicionado y hacer inconfortable el local para el personal de operación. Además, puede violar reglamentos de construcción.

Acceso

Es importante que al diseñar y construir un centro de cómputo se tome en consideración la entrada y salida de personas, así como del equipo de cómputo, ampliaciones, cambios de equipo, mudanzas, etc.

Debe existir un solo acceso en la medida de lo posible y vigilarlo permanentemente.

Es conveniente la instalación de puertas automáticas y con autocerrado en la sala, para minimizar rápidos cambios de temperatura y humedad provenientes de fuentes externas.

Puertas de emergencia

Es vital contar con puertas de emergencia, de tal manera que el personal pueda desalojar la instalación lo más rápido posible. Deben estar estratégicamente colocadas y que puedan ser abiertas de una manera fácil y rápida. Es necesario inspeccionarlas periódicamente con el fin de verificar su buen funcionamiento.

Piso falso

Dependiendo de las características del equipo de cómputo a instalar, como son sus dimensiones y peso, se determinará si es conveniente o no instalar un piso elevado, más conocido como piso falso.

Las ventajas que proporciona el piso falso son:

a) Permite que la instalación del equipo de cómputo sea más flexible.

b) Puedo servir para proteger el cableado, así como para darle un mejor mantenimiento a éste.

c) Permite que el aire acondicionado se inyecte y fluya por el espacio que hay entre el piso cimentado y el falso, para un mejor enfriamiento de la instalación.

d) Brinda un ambiente confortable de trabajo.

e) Permite adiciones futuras de equipo de cómputo con una mayor flexibilidad.

Al seleccionar un tipo de piso falso, se sugiere seguir las siguientes recomendaciones:

a) Que esté construido con un material no combustible, tal como acero o aluminio. Las dimensiones de los paneles no deben exceder de 60 x 60 centímetros.

b) Que al acabado del piso falso se haga con losetas de goma vinílicas u otro material sintético similar. Además que sea recubierto con impermeabilizantes no inflamables de colores claros. Todo esto proporciona una superficie de fácil limpieza y extrema durabilidad.

c) Debe ser antiestático.

d) Debe ser resistente al fuego.

e) Debe soportar el peso y dimensiones del equipo de cómputo.

No es recomendable el uso de alfombras porque son propensas a causar problemas de electricidad estática.

Iluminación

Es importante determinar el nivel adecuado de iluminación dentro de la sala de cómputo, de tal manera que ofrezca protección a la vista de todo el personal que trabaja en él. Asimismo, su distribución en toda la sala deberá ser uniforme.

Es común el uso de tubos fluorescentes alojados en recintos translúcidos dentro del techo falso.

La fuente de alimentación de la iluminación será independiente de la fuente del computador, de manera que una falla en una fuente no altere la otra.

Debe ser evitada la luz directa del sol sobre el equipo de cómputo, sobre todo en las consolas.

Mobiliario

Todo el mobiliario que se requiera dentro de la instalación de cómputo, como son las mesas de trabajo y los gabinetes, deberá cubrir los siguientes requisitos:

a) Debe ser de material no combustible y resistente al fuego.

b) Debe ser de material antiestático (evitar que sea de metal).

c) Debe ser de un material no estropeable.

d) Que sea fácil de limpiar.

Salas Anexas

Algunos ejemplos de salas anexas son las siguientes:

a) *Sala de mantenimiento.*

b) *Sala de almacenamiento de medios magnéticos, como cintas y discos.*

c) *Sala de almacenamiento de materiales diversos, como papel y cintas para impresora.*

d) *Area para la planta auxiliar de suministro de energía.*

e) *Area para la planta de aire acondicionado.*

f) *Despachos.*

g) *Cortado y desencarbonado.*

Las salas anexas deberán ser contiguas al centro de cómputo. Esto con el fin de optimizar tanto la circulación del material necesario (papelería, discos, cintas, herramientas, etc.) como para extender el aire acondicionado sin tener que efectuar un gran gasto.

Las salas anexas deberán ser cuidadosamente planeadas para minimizar espacio y tiempo requerido para moverse en ellas. Otra consideración es que deberán de tener las mismas condiciones ambientales (temperatura, humedad y presión) de la instalación de cómputo, ya que evitará que haya cambios bruscos en las condiciones ambientales de ésta, los cuales podrían afectar seriamente al equipo de cómputo.

En conclusión, la construcción de un centro de cómputo debe hacerse de tal manera que cubra dos objetivos principales:

a) *Garantizar una larga vida al equipo de cómputo manteniéndolo en óptimas condiciones.*

b) *Crear un ambiente confortable de trabajo, sobre todo para el personal encargado de operar el equipo de cómputo. Una razón para hacerlo es que puede influir en el rendimiento del personal que trabaja en el mismo.*

4.3.2 SUMINISTRO DE ENERGIA ELECTIRCA

CONSIDERACIONES PRELIMINARES

Es importante que un centro de cómputo cuente con un adecuado suministro de energía, el cual puede lograrse con una instalación eléctrica confiable. Una instalación deficiente implica apagones pasajeros e inestabilidad en el suministro de energía (fluctuaciones en el voltaje y/o en la frecuencia de la electricidad).

Un suministro de energía inadecuado puede dañar al equipo de cómputo, debido a la alta sensibilidad que caracteriza a éste.

El suministro de energía al equipo de cómputo deberá ser independiente de cualquier carga como, por ejemplo, el equipo de oficina (máquinas de escribir, calculadoras, etc.), o los enchufes de la sala del computador o áreas adyacentes.

- LA INSTALACION ELECTRICA

Resulta necesario planear cuidadosamente la instalación eléctrica de un centro de cómputo. Asimismo, la planeación deberá estar a cargo de personas expertas en la materia.

El cableado

El cableado deberá ser de alta calidad; además, deberá ser inspeccionado de manera periódica para verificar su buen estado.

Hay que evitar que se rocen los cables. Si es necesario, los alambres deben estar soldados o cubiertos. Asimismo, hay que aislar los cables descubiertos.

Tomas de corriente

Se deberá contar con un número suficiente de tomas de corriente, las cuales tendrán la característica de ser de tres cables con uno firmemente conectado a tierra. Con frecuencia éste último se daña y entonces es necesario cambiar el enchufe.

Conexión a tierra

Se tiene que dar especial énfasis a la existencia de un sistema de tierra efectivo y seguro, el cual tiene dos propósitos: limitar el efecto del ruido en la operación del equipo de cómputo y, lo que es más importante, proveer un camino a tierra para las corrientes dañinas que puedan ser producidas por defectos en el sistema eléctrico.

Todo el equipo de cómputo, sin excepción, doberá estar firmemente conectado a tierra.

Continuidad

El suministro de energía para el equipo de cómputo y el aire acondicionado, es importante. En aquellas instalaciones que cuentan con procesamiento en línea o de tiempo real, el suministro de respaldo es imprescindible. Hay que resaltar que cualquier interrupción de energía puede ser crítica y producir muchos efectos no deseados. El respaldo de energía puede hacerse por medio de una planta auxiliar de suministro de energía, la cual se usa para reemplazar el suministro principal en caso de interrupciones prolongadas.

Apagado de emergencia

Será necesario contar con un medio para interrumpir, en caso de emergencia, la corriente eléctrica que se suministra al equipo de cómputo y apagar los ventiladores del aire acondicionado sin afectar la iluminación de la sala de cómputo.

Los medios de interrupción deberán estar localizados cerca de cada una de las salidas de la sala y en lugares fácilmente accesibles al operador.

4.3.3 CONDICIONES DEL MEDIO AMBIENTE

CONSIDERACIONES PRELIMINARES

Para que el equipo de cómputo opere de una manera confiable y satisfactoria se requiere que esté bajo determiandas condiciones ambientales. Por lo consiguiente, la mayoría de los centros de cómputo operan bajo condiciones controladas mediante el uso de equipos de aire acondicionado y eliminadores de humedad.

Una de las razones por la que resulta necesario un ambiente controlado es que los componentes electrónicos del equipo de cómputo son sensibles a cambios bruscos de temperatura. Otra razón es que permite prolongar la vida de los componentes electrónicos del equipo.

Cambios bruscos en las condiciones del medio ambiente pueden causar problemas serios en varias formas, tales como: alteraciones en el funcionamiento del equipo, corrosión en los contactos eléctricos, generación de electricidad estática, etc.

Entre los factores a tomar en cuenta para el cálculo de la carga de aire acondicionado para el centro de cómputo se pueden mencionar los siguientes:

a. Tamaño y características del equipo de cómputo a instalar.

b. Condiciones climatológicas de la localidad.

c. Ubicación y características de construcción del centro.

d. Una posible expansión futura del centro.

Una instalación de aire acondicionado tendrá tres funciones básicas:

a. Controlar y ajustar tanto la temperatura como la humedad.

b. Filtrar y distribuir el aire en circulación.

c. Señalar las condiciones que caen fuera de las tolerancias.

Las condiciones ambientales a considerar son: aire acondicionado, temperatura, humedad, ventilación, presión, luz ambiental, orden y limpieza.

- PLANTA DE AIRE ACONDICIONADO

La planta de aire acondicionado estará situada lo más cerca posible de la sala del computador y preferiblemente adyacente a ella. Esto evitará instalar gran cantidad de ductos, que son quizá la parte más costosa de una instalación de aire acondicionado, ya que hace necesaria una planta mayor para compensar las pérdidas ocasionadas por la longitud de los tubos. El tamaño de la planta dependerá de la cantidad de aire acondicionado requerido y el tipo de equipo de cómputo a instalar.

Hay que resaltar que las instalaciones de aire acondicionado son una fuente de incendios muy frecuentes y también son susceptibles al ataque físico, especialmente a través de los ductos. Por lo que es conveniente instalar en éstos redes de protección,

detectores de incendios y extinguidores, así como monitores y alarmas de sonido efectivas.

Por último, hay que dar mantenimiento y verificar mensualmente todo el sistema de aire acondicionado.

- TEMPERATURA Y HUMEDAD

En un centro de cómputo debe haber niveles apropiados tanto de temperatura como de humedad.

La temperatura ideal para la sala de cómputo es de 22 grados centígrados. Sin embargo, una temperatura considerada aceptable es aquélla que se encuentra dentro del rango de los 18 a los 25 grados centígrados.

El nivel ideal de humedad es aquél que cae dentro del rango del 40% al 60% de humedad relativa (44).

Estos registros de temperatura y humedad proporcionan:

a. *Una comprobación del funcionamiento del sistema de aire acondicionado. Los errores de instalación y pérdida de eficiencia son debidos al mal funcionamiento de alguna parte del sistema.*

b. *Indican todo el tiempo cuando las condiciones ambientales del lugar cumplen las especificaciones de operación del equipo.*

c. *Indican cuando se alcanzan o exceden los límites de temperatura o humedad, para que el operador del computador o cualquier otro personal pueda corregir la anomalía.*

---

(44) HUMEDAD RELATIVA es un índice usado para medir la cantidad de vapor de agua presente en el aire, la cual es expresada como el porcentaje de la humedad existente en el aire con respecto a la necesaria para producir su situación.

d. *Los instrumentos de lectura directa con gráficas de siete días son recomendables para registrar las condiciones ambientales del centro de cómputo.*

La temperatura y la humedad no sufren grandes cambios cuando el equipo de cómputo no está en uso.

- ***VENTILACION Y PRESION***

Debido a que el equipo de cómputo disipa una gran cantidad de calor, es necesario que el centro de cómputo se encuentre ventilado ininterrumpidamente mientras el equipo se encuentre en operación.

Un requisito que debe tener el aire usado para la ventilación es que sea limpio (libre de polvo), y para ello require que sea filtrado antes de llevarlo al centro de cómputo. Si el aire del exterior contiene gases corrosivos, sales y otros contaminantes dañinos en la atmósfera que rodea la instalación, se requerirá además usar filtros especiales. El banco de filtros estará equipado con un dispositivo que indique cuando los filtros necesiten limpieza o deben ser cambiados.

La presión del aire en la sala del computador debe ser ligeramente mayor a la presión del aire de las áreas adyacentes, esto con el fin de reducir la entrada de polvo y basura.

- ***LUZ AMBIENTAL***

Se debe tomar en cuenta la orientación de la sala de cómputo dentro del edificio en que se instalará, procurando que no esté expuesta al sol, ya que esto incrementaría la temperatura, así como los costos de operación del equipo de aire acondicionado.

La iluminación en la sala debe ser de un nivel adecuado para proteger la vista de todo el personal que trabajará en ella. Asimismo, su distribución deberá ser uniforme en toda la sala.

- *ORDEN Y LIMPIEZA*

Se tomará especial cuidado en el orden y limpieza de la instalación de cómputo y áreas adyacentes, ya que no sólo mejora la moral del personal que labora en ellas, sino que evita que se cometan errores u omisiones en el manejo de la información y reduce la posibilidad de fuego. El orden y la limpieza no pueden lograrse si se realizan de manera ocasional; necesita ser algo continuo y darles la suficiente atención.

La sala de cómputo debe ser limpiada todos los días, preferentemente cuando el equipo no esté funcionando. Deberá supervisarse el uso de los materiales de limpieza para evitar el daño al equipo. "Por ejemplo, en cierta instalación un sandwich de queso fué dejado sobre la unidad central de proceso, el calor derritió el queso y éste quedó adherido a dicha unidad; posteriormente el personal de aseo intentó remover el queso con una fibra de metal, y por desgracia se introdujo la fibra en el procesador dejándolo inservible" (45).

Se sugiere limpiar la sala con trapo húmedo, con un sacudidor tratado o con aspiradora. Nunca se use escoba. El objeto de la limpieza es remover el polvo, no esparcirlo.

Hay que evitar el uso de pisos con cubiertas que requieren de pulidores o lijadores debido a la gran cantidad de polvo creado por este proceso. Es adecuado colocar tapetes absorbentes de polvo en la entrada a la sala.

El polvo acumulado en el techo y piso falso debe ser retirado con frecuencia.

---

(45) Cfr. Arn Ramírez Cazarez, et. al., Tesis: Organización y Administración de Centros de cómputo. Universidad Nacional Autónoma de México., Facultad de Ingeniería, México, 1987. Pág.142

Es conveniente reforzar las siguientes políticas:

a. Prohibir comidas y bebidas en la instalación de cómputo.

b. Prohibir fumar. Las cenizas del tabaco pueden dañar cintas y discos magnéticos, el humo puede hacer arrancar las alarmas de detección de humo e incrementar el promedio de cambios de filtros de aire en el equipo de aire acondicionado.

c. Limpiar diariamente el piso, las cubiertas del equipo y las superficies de trabajo.

d. Vaciar las cestas y otros recipientes de basura fuera del cuarto de la computadora con el fin de anular el exceso de polvo.

e. Desempaquetar el equipo y los suministros de papel fuera del cuarto con el objeto de reducir el polvo.

f. Estar seguro que todos los pasillos de entrada, gabinetes y equipo estén limpios antes de entrar al salón del computador.

g. Controlar el número de personas que entren al área estableciendo reglamentos definitivos.

Por último, se recomienda que la limpieza del equipo de cómputo sea llevado a cabo por el propio operador; éste trabajo no debe hacerlo la persona que hace el aseo general.

4.3.4 SEGURIDAD CONTRA INCENDIOS

CONSIDERACIONES PRELIMINARES

Desde tiempos remotos, el hombre ha sido víctima del fuego y sus consecuencias, es por eso que ha tenido la necesidad de desarrollar aplicaciones y medidas de prevención, protección, detección y extinción de incendios.

El fuego es, sin duda un riesgo alto que amenaza a cualquier tipo de organización, aunque sus efectos son más peligrosos en las organizaciones de tipo industrial y comercial.

Eduardo Aguirre Martínez define al fuego como "la oxidación rápida que se efectúa en un material y que se manifiesta en forma de luz, de calor o de ambos, como consecuencia del desprendimiento de partículas de carbono e hidrógeno".

Para que se origine el fuego es necesario que existan tres elementos esenciales:

a. Material combustible.

b. Calor suficiente para que el vapor de los materiales llegue a su temperatura de ignición.

c. Oxígeno.

Si se elimina cualquiera de estos tres elementos, el fuego dejará de existir.

Los incendios ocurren con más frecuencia de lo que se piensa y pueden ser desastrosos. Se debe considerar el fuego causado

accidentalmente, así como los premeditados. Enseguida se listan las causas más frecuentes de incendios (46):

a. "El acto de fumar

b. Los líquidos y gases inflamables, y material combustible.

c. Las instalaciones y aparatos eléctricos.

d. Fuegos abiertos (47) y chispas".

Los incendios que tienen su origen en causas eléctricas, representan una buena porción en el total de los incendios registrados en las organizaciones.

"No hay ningún incendió, ni uno sólo, que en el área urbana y sobre todo en organizaciones, tenga su origen en un hecho que no haya podido preveerse y prevenirse con toda oportunidad. Sin embargo, según los medios de información, para las autoridades mexicanas, bomberos y personas afectadas por los siniestros la mayoría de los incendios se originan en corto circuitos" (48).

Una de las preocupaciones del hombre actual en este sentido, es el poder evitar que estos accidentes ocurran mediante la implantación de medidas adecuadas de seguridad.

La importancia de un sistema de seguridad contra incendios para un centro de cómputo no puede considerarse como exagerada. Si un

---

(46) Eduardo Aguirre Martínez, Seguridad Integral en las Organizaciones: Actualización para Ejecutivos, op. cit., pág. 82

(47) Fuego abierto es aquél que se produce o mantiene sin protección alguna que lo aisle del ambiente. El fuego abierto se manifiesta comunmente en las organizaciones por el uso de quemadores industriales, de estufas o cocinetas, soplotes, velas o veladoras, etc.

(48) Eduardo Aguirre Martínez, op. cit., pág. 87.

incendio es detectado rápidamente, podrá ser extinguido antes de que ocasione cualquier daño serio al centro. Por otro lado, si el incendio se propaga, las consecuencias en términos de pérdidas de información y capital invertido, pueden causar trastornos por meses si no es que por años.

- PREVENCION

Prevenir un incendio implica tomar las medidas que son necesarias para reducir al mínimo las posibilidades de que éste ocurra.

"La prevención es, en su más amplio sentido, un efectivo e indispensable medio de defensa, y debe estar a la vanguardia en la lucha por la seguridad" (49).

"Entre las ventajas que proporciona una organización de seguridad contra incendios figuran las siguientes:

a. Protección de la vida del personal.

b. Posibilidad mínima de que se interrumpa la operación de la organización.

c. Menos posibilidades de un incendio grave.

d. Extinguidores adecuados contra incendios, colocados en lugares convenientes.

e. Conservación del equipo protector contra incendios.

f. Personal adiestrado disponible para utilizar el equipo.

---

(49) Herrera Zogby Luis. La Prevención de Daños por Incendio en Arquitectura, Edit. Limusa, México, 1981, Pág. 13.

g. Mayor eficiencia en otras labores" (50).

Un incendio en un centro de cómputo es más fácil de prevenir que de sofocar por lo cual se deben tomar en cuenta las siguientes normas:

a. Construir y mantener un ambiente no inflamable.

b. Mantener orden y limpieza.

c. No fumar.

d. Conservar en pequeñas cantidades los materiales inflamables usados en el cuarto de la computadora, tales como líquidos limpiadores.

e. Almacenar el papel y otros suministros combustibles, fuera del cuarto de la computadora, a excepción de aquellos que se van a usar inmediatamente.

f. Procurar cestos de basura autoextinguibles en caso de incendio.

g. Desconectar el equipo de cómputo, una vez terminadas las actividades.

h. Una vez concluida la jornada de trabajo, el personal de vigilancia deberá efectuar un recorrido por el centro de cómputo para asegurarse que no ha quedado encendido o conectado el equipo de cómputo. Asimismo, el centro deberá ser vigilado constantemente.

---

(50) Cfr. H. Ronan William. Adiestramiento para combatir incendios, Edit. Hermanos Herrero, México, 1963, pág. 13.

i. Vigilar y mantener el sistema eléctrico en buenas condiciones.

j. Reportar a mantenimiento cualquier desperfecto que se observe en circuitos eléctricos.

- PROTECCION

Anteriormente, expuse algunos de los requerimientos para la protección contra incendios en la construcción de un centro de cómputo. Es importante que estos requerimientos no sólo se apliquen en la construcción del centro, sino también en las áreas adyacentes.

Será necesario contar con lugares especiales de almacenamiento para las cintas y los discos magnéticos que se usan en la instalación, así como para toda la documentación de los sistemas, programas y sistema operativo. Por lo general, se recurre al uso de bóvedas bancarias o cajas fuertes que son resistentes al humo, calor y fuego. Sin embargo, hay situaciones en las que la falta de sentido común hace sentir su peso a este respecto.

"Una compañía compró una caja fuerte excelente para almacenar cintas magnéticas y sintió que había hecho una labor aceptable para conseguir una buena protección de información contra el fuego. Sin embargo una cinta magnética puede ser leída solamente utilizando un computador, y un computador no funcionará sin un programa. Los programas fueron almacenados en un gabinete de acero junto al computador. En caso de incendio, los datos estuvieron seguros, pero no había forma de procesarlos" (51).

Por otra parte, la destrucción de la documentación de los sistemas y los programas pueden imposibilitar el uso de archivos de

---

(51) Cfr. Gordon B. Davis, La Auditoría y el Procesamiento Electrónico de Información, Instituto Mexicano de Contadores Públicos, México, 1972. Pág. 94.

respaldo. En muchas instalaciones protegidas con mecanismos de alta seguridad esta situación se ignora o bien la documentación con que se cuenta es obsoleta. Se deben establecer procedimientos que garanticen la actualización de toda la documentación.

Un fuego intenso, o algún otro desastre como una inundación, también pueden destruir los registros del procesamiento de información en bóvedas a prueba de fuego. Por esta razón, el almacenamiento fuera del local es utilizado para proporcionar una seguridad adicional para registros y archivos escenciales de procesamiento de información.

- DETECCION

Es de suma importancia detectar un fuego de manera oportuna para evitar su propagación.

Actualmente, los medios de que se dispone para prevenir y atacar el fuego han sido perfeccionados a tal grado que no es un grave problema atacarlo si se descubre en los primeros instantes después de iniciado.

Una forma de detectar un incendio es por medios científicos, es decir, utilizando dispositivos sensores, como los termostatos de temperatura fija, que accionan las señales de alarma; éstas se manifiestan de manera visual (focos rojos instalados en techos) o en forma sonora (sirenas). Tales dispositivos sensores responden al humo, calor y fuego.

Existen varios sistemas de detección contra incendios, desde los más sencillos a base de campanas o sirenas de accionamiento manual hasta los sistemas electrónicos de acción automática. El problema de su elección dependerá básicamente de un estudio de las condiciones de seguridad que sea necesario obtener.

Para los dispositivos de detección de incendios hay que tomar en cuenta las siguientes observaciones:

a. *Los detectores se deben de instalar tanto en la sala de cómputo como en las áreas adyacentes a ésta.*

b. *Es necesario colocar detectores en el techo, bajo el piso falso y en los ductos de aire acondicionado.*

c. *El detector de humo que se elija, debe ser capaz de detectar los distintos tipos de gases que desprendan 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 producidos por un corto circuito tal vez no se detectan.*

d. *Ante una contingencia que se llegara a presentar, el sistema automáticamente cortará todos los suministros de energía a la sala del computador, aire acondicionado e iluminación y activará el sistema de extinguidores.*

e. *Las alarmas contra incendios deben estar conectadas con la alarma central, o bien directamente al departamento de bomberos de la localidad.*

f. *Los detectores de incendios deberán de recibir periódicamente un mantenimiento adecuado.*

- LA SEÑALIZACION

En toda organización, debe existir señales indicadoras en caso de incendio, tales como:

a. Evacuación de personal.

b. Circulación de vehículos.

c. Controles de energía eléctrica.

d. Depósitos y almacenes de sustancias inflamables, tóxicas o explosivos.

e. Equipos contra incendio.

f. Gabinetes de guarda de equipo individual contra incendio.

La señalización se puede llevar a cabo por medio de líneas discontinuas con puntos de flecha que indiquen la circulación.

Por último se harán indicaciones por medio de carteles colgantes a una altura aproximada de 2.20 metros o fijos a los muros, con leyendas alusivas.

- EVACUACION

Los pasillos, las escalera y las salidas de emergencia de la instalación de cómputo y de sus áreas adyacentes; invariablemente deberán estar señalados, a fin de permitir una adecuada y rápida evacuación en caso de incendio. Asimismo, hay que comprobar que estén libres de obstrucciones.

Las salidas de emergencia deben de identificarse mediante letreros y señales visibles que indiquen tanto la dirección como la ubicación de las mismas.

Se sugiere poner en las paredes, preferentemente cerca del lugar de los extinguidores portátiles, planos de rutas de evacuación por piso.

- EXTINCION

Por lo general, el fuego que se presenta en un centro de cómputo es de los tipos A y C, por lo que se recomienda hacer uso de cualquiera de los siguientes agentes extintores:

a. Polvo químico ABC o BC.

b. Bióxido de carbono.

c) Gas halón.

El bióxido de carbono tiene la desventaja de tener un efecto letal sobre los humanos. Usualmente es costoso debido a los extensos controles de seguridad que deben ser instalados como parte del sistema. En rolación al equipo de cómputo, este tipo de extintor le produce poco o ningún daño.

El gas halón es el mejor de todos los medios de extinción. Su acción es más rápida que la del bióxido de carbono y no baja la temperatura. Teóricamente, no es dañino al personal, pero como esto no ha sido corroborado por ningún organismo oficial, la evacuación del personal deberá efectuarse antes de activarlo.

Hay que evitar el uso de extintores que sean conductores de electricidad como es el caso del agua y de algunos tipos de espumas. Además, el agua puede producir daños de gran extensión en un centro de cómputo.

Si ya existen rociadores de agua en el edificio donde se ubica la instalación de cómputo, es conveniente quitarlos o volverlos inoperantes, sobre todo los que se encuentran dentro de la instalación y en sus áreas adyacentes.

- ADIESTRAMIENTO AL PERSONAL

Es necesario definir y documentar los procedimientos que se deben seguir en caso de incendio; además se debe adiestrar al personal acerca del uso del equipo de extinción. Se ha comprobado que ésta es una medida débil, sobre todo en instalaciones cuyos índices de cambio de personal son altos. Con frecuencia, muchos empleados no saben exactamente que deben hacer en caso de incendio.

El fuego se combate mejor cuando el equipo que se usa es el apropiado, cuando está disponible con rapidez, y las personas cuentan con adiestramiento suficiente en el uso del equipo, lo cual les permite luchar contra el fuego de manera eficaz y organizada.

Asimismo, el personal debe estar adiestrado para la evacuación ordenada en caso de que suene la alarma contra incendio. Esto implica el saber que hacer y no hacer en cada caso en particular, por ejemplo, no hacer uso de los elevadores.

- SIMULACROS

Los simulacros son prácticas que se realizan ante el supuesto de la declaración de un incendio.

Uno de los objetivos de la realización de simulacros es lograr la organización necesaria del personal y el equipo ante dicha contingencia.

Para que puedan considerarse efectivos los simulacros deben cubrir desde el origen del fuego y su expansión hasta las maniobras de combate del mismo y de salvamento.

"El simulacro se debe efectuar como mínimo cada dos meses y debe comprender:

a. El hipotético sitio del surgimiento del fuego.

b. La detección del fuego.

c. La alarma.

d. La participación del personal de vigilancia.

e. La evacuación de personal.

f. El control de los vehículos.

g. La integración de la brigada de incendios.

h. El uso del equipo individual.

i. El combate de incendios.

j. El informe de los hechos" (52).

- SEGURO

Los riesgos contra los cuales la organización debe estar protegida son principalmente el fuego. Los riesgos derivados del

---

(52) Eduardo Aguirre Martínez, op. cit., pág. 122.

fuego son cubiertos en una variedad de grados por tres diferentes tipos de póliza:

1. *Seguro contra incendio*
2. *Seguro sobre documentación y archivos maestros*
3. *Seguro sobre procesamiento de información.*

El cuadro presenta un resumen de cobertura por riesgos específicos.

TIPO DE RIESGO	COBERTURA EN CASO DE INCENDIO	COBERTURA PARA DOCUMENTACION Y ARCHIVOS MAESTROS	COBERTURA PARA EL PROCESAMIENTO DE INFORMACION
Daño y/o pérdida de equipo ya sea rentado o propio	Costo del equipo	Ninguna	Costo del equipo
Pérdida o destrucción de programas (software)	Costo del material (discos y cintas) y mano de obra No hay cobertura para el costo del diseño de sistemas o programas	La extensión de la cobertura está en duda. Puede excluir: la recuperación por pérdida de datos almacenados en discos, cintas o cartuchos.	El costo de reconstrucción bajo condiciones críticas siempre y cuando se emplee almacenamiento fuera de la organización para archivos y documentación claves.
Pérdida o destrucción cuando la reconstrucción resulte costosa, tardada y difícil	Costo de materiales sobre los cuales los datos fueron registrados	Extensión de la cobertura en duda	Costo de reconstrucción bajo condiciones críticas siempre y cuando se utilice almacenamiento fuera de la organización.
Gastos extraordinarios incurridos para volver a la operación normal	Ninguna	Extensión de la cobertura en duda	Cubierta
Pérdida por interrupción de las operaciones de la organización	Ninguna	Ninguna	Cubierta

En la actualidad existen cuatro compañías aseguradoras que dan seguro para el procesamiento de información. Dos determinan las primas sobre la base de una investigación de ingeniería hecha sobre la instalación y dos cotizan una cuota alzada con cláusula deducible de 5,000 Dlls. En los cuatro casos, las primas reales representan porcentajes de las cuotas normales por seguro contra incendio pagadas por la organización.

4.3.5 CONTROL DE ACCESO

CONSIDERACIONES PRELIMINARES

El control de acceso puede lograrse tomando ciertas precauciones, como son la colocación de vigilantes y la implantación de procedimientos de entrada (registros de entrada/salida, gafetes de identificación, y tajetas de acceso, entre otros).

Los controles de acceso varían según las distintas horas del día. Es importante asegurar que los controles durante la noche sean tan estrictos como durante el día.

- CONTROL DEL PERSONAL

Como observamos en la Gráfica 2 titulada "Principales Perpetradores" presentada en el capítulo 1, el 81% de los delitos que se cometen en perjuicio de las organizaciones parte del propio personal que labora en ellas.

El personal debe ser controlado desde el momento de su reclutamiento, y debe obedecer todas y cada una de las normas específicas de seguridad implantadas por la organización.

En un centro de cómputo, cada empleado debe tener acceso sólo a aquellas áreas que exigen sus trabajo individual; esto se puede hacer, por ejemplo, no permitiendo a los programadores y analistas de sistemas ingresar al cuarto de la computadora y al personal de operación el estar en la cintoteca.

- CONTROL DE VISITANTES

Los visitantes son todas aquellas personas que sin tener relación de trabajo con la organización penetran en los locales de ésta

con cualquier motivo. De tal manera, los visitantes son: los clientes; los proveedores; los trabajadores de aseo, de reparación o mantenimiento que no sean dependientes de la organización, y los profesionales que de manera habitual o eventual tengan tratos con la organización.

El control de los visitantes puede abatir considerablemente el número de delitos cometidos o que pueden cometerse. Este control parte de la identificación del visitante, para lo cual se debe destacar también la identificaicón o identidad del propio personal, ya que la falta de identificación visible propicia el que se confunda con los visitantes o que éstos pasen inadvertidos.

Cada uno de los visitantes deberá ser identificado plenamente; además, deberá ser controlado y vigilado en sus actividades durante su estancia dentro de la organización.

"El control de los visitantes tiene tres objetivos fundamentales:

a. Impedir la introducción de cualquier objeto o cosa indeseable.

b. Impedir la sustracción de cualquier bien propiedad de la organización.
c. Evitar la agresión física " (53).

El control de los visitantes comprende:

a. La señalización del visitante, que consite en la implantación a éste de cualquier marca que demuestre de manera ostensible su calidad de visitante.

b. La anotación en el registro de visitantes indicando la fecha, nombre, propósito de la vista, persona a quien visita, hora de entrada, hora de salida y firma.

---

(53) Cfr. Aguirre Martínez, Eduardo. Op. cit., pág. 146.

c. *La limitación del área de visita.*

d. *El tiempo de permanencia.*

e. *Los objetos que introduzca el visitante.*

- ***FORMAS DE CONTROL***

En la actualidad, los gafetes de identificación y las tarjetas de acceso son formas muy populares de control de acceso.

Los gafetes son utilizados para identificar personal autorizado y a visitantes. Deben estar codificados por color, el cual permitirá distinguir cuales personas son empleados y cuales son visitantes. Además, los gafetes del personal deben portar una fotografía en lugar visible.

Las tarjetas de acceso son probablemente el dispositivo de acceso más eficiente. Las puertas del centro de cómputo se abrirán con tarjetas codificadas óptica o magnéticamente. La autorización de entrada puede ser controlada dinámicamente por puertas individuales, hora del día, día de la semana y clasificación de seguridad de los individuos a quienes se les fué dada la tarjeta. Los estados de abierto y cerrado de las puertas pueden ser monitoreadas, e intentar una entrada no autorizada puede ser detectada inmediatamente.

Es necesario rotar periódicamente las claves, combinaciones y contraseñas usadas para accesar a una instalación de cómputo.

En la actualidad ya existen gafetes que tienen integrados sistemas de tarjetas de acceso.

- EL PERSONAL DE VIGILANCIA

Cuando sea factible y justificable, hay que utilizar un servicio de vigilancia de 24 horas con respecto a la entrada y salida del centro de cómputo.

Dispositivos contra el ingreso físico

Todas las áreas de un centro de cómputo deben estar protegidas contra el ingreso físico. Las alarmas contra robo, las armaduras y el blindaje se deben usar, hasta donde sea posible, en forma discreta, de manera que no llamen la atención sobre el hecho de que existe un dispositivo de alta seguridad. Tales medidas se deben aplicar no sólo en el área de cómputo, sino también en las áreas adyacentes.

Cada uno de los puntos de acceso al centro de cómputo, incluyendo las puertas de emergencia, debe ser vigilados en forma permanente. Las ventanas tienen que estar protegidas con película y material antirrobo.

Ciertos dispositivos como los monitores de circuito cerrado de televisión y las cámaras fotográficas intermitentes son ya muy populares, los cuales puede ser conectados a un panel de control para ser vigilados por personal de seguridad. Son muy efectivos para controlar áreas muy grandes.

- CONTROL DE ACCESO LOGICO

En aquellos sistemas de aplicación en los que el ingreso de datos no es interactivo, la restricción del acceso a las funciones de procesamiento del software de aplicación es relativamente sencilla. Por lo general, ello se logra mediante controles de procesamiento por lotes.

Los recientes avances en la tecnología han ampliado el acceso a los sistemas, por consiguiente, a la información almacenada en los archivos del computador. Con mayor frecuencia se permite el acceso, lectura y uso de datos a los departamentos usuarios. Pero una vez que se otorga el acceso a los sistemas aumenta el riesgo de acceso no autorizado. Por ejemplo, existe el riesgo de que empleados que solamente tengan autorización de lectura puedan:

- *Ingresar transacciones.*
- *Modificar transacciones.*
- *Eliminar datos.*
- *Recuperar datos*
- *Modificar archivos maestros (datos permanentes).*

En esta situación, y dependiendo de la naturaleza de las funciones de procesamiento que puedan realizarse con el software al que se accede, un sólo individuo podría llegar a realizar tareas incompatibles.

En ambientes en los que los datos son ingresados o están a disposición de los usuarios en forma interactiva, el control del acceso resulta más complicado. La efectividad del control dependerá, por lo general, del uso de software que permita el acceso del usuario a ciertas funciones de procesamiento, pero no a otras. Por ejemplo, se puede autorizar a un usuario a leer datos pero no a modificarlos. En realidad, los controles de acceso programados pueden considerarse como una manera de implantar electrónicamente la segregación de funciones.

También se utiliza software y ocasionalmente hardware, para definir qué funciones puede realizar un individuo, a qué datos puede acceder y cómo restringir a esa persona en consecuencia. Se utilizan varios mecanismos para lograr estos controles, incluyendo:

- *Menúes*

- *Normas/Perfiles de acceso*
- *Acceso a los datos por programa*
- *Dispositivos de acceso a los datos/programas*
- *Dispositivos de seguridad de terminales, incluyendo dispositivos de acceso personalizado o "tarjetas inteligentes".*

Existen tres etapas dentro del control de acceso: identificación, autentificación y permiso/rechazo. Las funciones de identificación y autentificación, es decir, identificar al usuario y probar quien dice ser, son realizadas independientemente del acceso a las funciones y datos particulares del procesamiento. Estos aspectos del control de acceso son relevantes al riesgo de acceso no autorizado al sistema más que a las funciones y datos de procesamiento. No obstante, en el proceso de identificación, el usuario ingresa un código único al sistema que se utiliza como clave para determinar a qué funciones o datos de procesamiento puede acceder y, a menudo, las opciones con que contará una vez que haya accedido a los datos.

El permiso/rechazo de acceso a las funciones y datos de procesamiento es logrado a través de rutinas que pueden ser incorporadas al software de sistemas o de aplciación, o a ambos.

4.3.6 PLANES DE CONTINGENCIA

Un plan de contingencias es un conjunto de procedimientos de recuperación para casos de desastres; dicho en otras palabras es un plan formal que describe pasos apropiados que se deberán seguir en caso de un desastre o emergencia. Debe estar orientado a minimizar las pérdidas, así como a recuperarse de un desastre total.

Un adecuado plan de contingencias ayuda a una instalación de cómputo y a la organización en general a minimizar sus pérdidas, en caso de desastre, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

Sin embargo, existen organizaciones que piensan que cuentan con planes adecuados de recuperación en caso de desastres, y que cubren todas las categorías de éstos. La realidad es que un buen número de estos planes son superficiales, no estructurados e inadecuados para afrontar las complicaciones que surgen de un desastre real.

Los procedimientos de planeación contra desastres tienen que considerar cuidadosamente los tipos de riesgos expuestos en el Capítulo 1.

- CARACTERISTICAS DEL PLAN

Hay cuatro grandes áreas concernientes al desarrollo y mantenimiento de una buena recuperación o plan de contingencias:

a) Respaldo de configuración del equipo de cómputo y de la programación (software).

b) Las instrucciones de operación para los procedimientos de recuperación deben ser documentados y almacenados en un lugar externo. Un aspecto importante de la documentación es el entrenamiento de los individuos que se encargarán de las operaciones de recuperación.

c) Los programas deben ser respaldados y almacenados en un lugar seguro y que se pueda disponer de ellos cuando se requieran.

d) Los archivos de datos que sean escenciales para la operación continua de la organización deben ser respaldados y almacenados en una localidad segura.

Es muy importante que el plan de contingencias determine quién debe de tomar las decisiones durante la recuperación del desastre, y establezca la disponibilidad y entrenamiento del personal suficientemente experimentado.

Algunos de los puntos que deben ser considerados en un plan de contingencias se listan a continuación:

a) Procedimientos de recuperación para la reproducción de información.

b) La localización de los medios de respaldo.

c) Quién contacta los medios de respaldo.

d) Qué archivos o base de datos deben ser reconstruídos primero.

e) La configuración del equipo de cómputo similar y su localización, <centro de cómputo alterno o espejo>.

f) En dónde puede encontrarse el software de reemplazo.

g) La localización de otro equipo de apoyo, tal como generadores y aire acondicionado.

h) La ayuda que se puede esperar del proveedor del equipo.

i) La acción a ser tomada en caso de un daño parcial inesperado.

j) Procedimiento para la imposición de controles extraordinarios durante el desastre y hasta que regresen los sistemas a la normalidad.

El plan de contingencias debe estar desarrollado en forma detallada. Es posible anticiparse a la mayoría de las situaciones y éstas deben estar cubiertas en dicho plan.

Lógicamente todo el plan deberá estar por escrito y en un lugar conocido por el personal. Asimismo, se deberá de asignar un responsable que mantenga actualizados los procedimientos de recuperación.

- SIMULACROS DE DESASTRE

Los simulacros de desastres son importantes por las siguientes razones:

a) Se evalúa la conciencia y preparación del personal para afrontar el desastre.

b) Se identifican las omisiones.

El ambiente del simulacro no sólo crea una combinación de circunstancias cercanas a la realidad, sino que las presiones que se producen resaltan las posibilidades no previstas o fallas en los planes.

Una de las grandes objeciones a los simulacros es el costo. Este varía, lógicamente, según la frecuencia con que se realicen estas pruebas. Si se trabaja sobre un promedio de dos a tres veces al año para las instalaciones grandes, el costo no resulta elevado.

Los simulacros se deben realizar de manera esporádica.

4.3.7 SEGUROS

CONSIDERACIONES PRELIMINARES

Desde el punto de vista comercial, el negocio de los seguros existe desde hace mucho tiempo, provisto de criterios y prácticas bien definidas. Sin embargo, cualquier organización que busque asesoramiento y orientación sobre cobertura de sus riesgos de

computación, es probable que se enfrente a dificultades considerables.

"Existen dos problemas principales:

a) Los aseguradores saben mucho sobre riesgos comerciales pero muy poco acerca de computadoras,

b) No hay un entendimiento cabal respecto a los riesgos y sus consecuencias, debido a que la profesión computacional es reciente y a que los antecedentes en relación con las reclamaciones sobre seguros son pocos" (54).

El resultado de lo anterior es que muy pocos usuarios de computadoras gozan de una cobertura adecuada para todos los riesgos. La tendencia es cubrir una o dos áreas de riesgo evidente, como la reposición del equipo y el costo de la reproducción de los datos o el incremento en el costo de operación, casi siempre se pasan por alto.

Es necesario examinar los contratos y, si se requiere, pedir aclaración acerca de la cobertura y los riesgos a los cuales se considera expuesto el centro de cómputo. Hay que poner una mayor atención a las exclusiones que se mencionen en el contrato de seguro, es decir, a aquellos riesgos no asegurables.

"El equipo de cómputo y los medios de almacenamiento externos de datos (discos magnéticos, cintas magnéticas, y demás dispositivos de almacenamiento) se deben asegurar por el valor de reposición y no por su costo" (55).

---

(54) Leonard H. Pino, Op. cit., pag. 52

(55) El valor de reposición es aquella cantidad que exigiría la adquisición de un bien nuevo de la misma especie, clase y capacidad, incluyendo el costo de transporte, montaje, impuesto y derechos aduanales si los hubiera.

La cobertura de seguro debe revisarse periódicamente para tener la seguridad de que es adecuada a las circunstancias.

- RIESGOS ASEGURABLES

"El equipo de cómputo y los medios de almacenamiento externo de datos pueden asegurarse contra daños o pérdidas materiales que sufran en forma súbita e imprevista, que haga necesaria su reparación o reposición, a consecuencia de los riesgos que se citan a continuación:

a) Incendio, impacto de rayo, explosión, implosión.

b) Humo, hollin, gases, líquidos o polvos corrosivos.

c) Cortocircuito, sobretensiones causadas por rayo, tostadura de aislamiento.

d) Errores de construcción, fallas de montaje, defectos de material.

e) Errores de manejo, descuido, negligencia e impericia.

f) Daños mal intencionados y dolo de terceros.

g) Pérdida o daños materiales causados por robo con violencia.

h) Robo sin violencia y asalto.

i) Huelgas, alborotos populares y conmoción civil.

j) Granizo, helada, tempestad.

k) Hundimiento de terreno, deslizamiento de tierra, caída de rocas.

l) Terremoto y erupción volcánica.

m) Ciclón y huracán.

n) Inundación y daños por agua.

o) Gastos adicionales por concepto de flete expreso no aéreo, trabajos en días festivos y horas extras.

p) Gastos por flete aéreo.

q) Daños que se originen en el equipo electrónico asegurado a consecuencia de un daño material indemnizable en el equipo de climatización.

r) Otros accidentes que no se excluyan en la póliza de seguro" (56).

Además, los medios de almacenamiento externos de datos pueden estar amparados contra el costo de reproducción de la información perdida.

Hay otro tipo de riesgo que puede ser cubierto por un seguro: el incremento en el costo de operación del equipo de cómputo. Este incremento se dá en el caso cuando una organización asegurada recurre al uso de un equipo de cómputo ajeno y suplente que le permita continuar sus operaciones debido a que su propio equipo fué destruído o dañado a consecuencia de los riesgos amparados en el contrato de seguro y que las operaciones de procesamiento electrónico de datos fueron interrumpidas o entorpecidas. El incremento del costo de operación incluye el costo de alquiler de una instalación de cómputo ajena y suplente, los gastos adiciona-

---

(56) Según la cobertura de seguro de equipo electrónico y electromagnético de Seguros Monterrey, S. A., MIMEO

les por sueldos de empleados propios o ajenos y gastos de transporte de material, papelería y documentos.

En la sección anterior se hizo mención de que se debe poner especial atención a las exclusiones, o sea a los riesgos no asegurables. "Ejemplos de éstos son los siguientes:

a) Hostilidades, actividades u operaciones de guerra, invasión, rebelión, suspensión de garantías o acontecimientos que originen estas situaciones.

b) Expropiación, requisición, confiscación, incautación o detención de los bienes por las autoridades.

c) Destrucción de los bienes por actos de autoridad.

d) Reacción y radiación nuclear o contaminación radioactiva.

e) Vibración o ruido sónico causado por aviones y otros mecanismos.

f) Saqueo que se realice después de la ocurrencia de algún fenómeno meteorológico o sísmico" (57).

---

(57) Según la cobertura de seguro de equipo electrónico y electromagnético de Seguros Monterrey, S. A., MIMEO.

CONCLUSIONES

CONCLUSIONES

Una finalidad prioritaria en el desarrollo de la tesis es la manifestación de un comportamiento analítico, de síntesis, y el acrecentamiento de un marco crítico adoptando aptitudes convenientes para relacionar, plantear y resolver problemas.

La elaboración de esta tesis es una de las oportunidades más tangibles en un corto plazo para extrapolar conocimientos fuera del ámbito académico, de modo que puedan transferirse para afrontar nuevas situaciones en diversas condiciones.

La tesis invita a la valoración personal de la importancia de vivir la problematica actual en el ambito computacional e incrementa los sentidos de ética y profesionalismo; plantea un posible camino a la participación especializada en provecho del mejoramiento personal y del desarrollo de las organizaciones y del país en general.

La tesis busca, con tales bases, la iniciación y/o el seguimiento hacia la valoración y la formación de una nueva área de especialización en la auditoría.

De una forma particular, el desarrollo de esta investigación es una prueba para nuestra propia formación y calidad profesional, así como para nuestra capacidad que se expresará con resultados y hechos.

Las actuales tendencias tecnológicas originadas por los cambios que constantemente se producen en los equipos y sistemas, utilizados para el procesamiento de información, constituyen para el auditor un elemento de cambio sobre el desarrollo, evaluación y suficiencia de controles; sobre la medición de la eficiencia, eficacia de los sistemas, sus medidas de seguridad y la

integridad de la información procesada; es por ello que el auditor en informática requerirá mantener su mayor esfuerzo para asimilar estos cambios y lograr así la realización de auditorías modernas de alta calidad y acordes a esta evaluación, apoyándose en técnicas y herramientas asistidas por el computador.

Se vuelve importante la participación del auditor en informática en las organizaciones donde los recursos informáticos juegan un papel significativo para la toma de decisiones y la continuidad de la misma.

Debido a que dichos recursos se encuentran expuestos a una serie de riesgos y contingencias latentes, es necesario la participación del especialista con el fin de evitar que estos se materialicen, mediante el desarrollo y en ocasiones la implantación de procedimientos, controles y medidas adecuadas para evitar y contrarrestar lo anteriormente señalado.

Cabe en gran medida mencionar la posibilidad de ampliar la investigación presentada con complementos, tales como, integridad de bases de datos, controles de seguridad en redes y telecomunicaciones, herramientas CASE y de reingeniería, entre otros.

Ello convertiría a todo el marco de evaluación de la auditoría en una adecuada integración para la realidad en la que hoy nos encontramos inmersos.

BIBLIOGRAFIA

BIBLIOGRAFIA

AGUIRRE Martínez Eduardo, Seguridad Integral en las Organizaciones: actualización para ejecutivos, Edit. Trillas, México., 1980, Pp. 720.

BANK Administration Institute, Auditing the Systems Development Life Cycle, Rolling Meadows, USA, 1979, Pp. 42.

BURCH G., John, Et. al., Sistemas de Información: Teoría y Práctica, Edit. Limusa, México, 1983, Pp. 130.

COLEGIO de Contadores Públicos, Diferentes enfoques de Auditoría en Informática, México, 1991, Pp. 370.

CODIGO Penal, Actualizado, Edit. Ediciones Delma, título vigésimo segundo, México, 1989, Pp. 159.

CUEVAS Guzmán, Ma. Teresa de Jesús, Et. al., Control y Auditoría en Centros de Cómputo, tesis de Licenciatura, Facultad de Ingeniería, UNAM. México, 1987. Pp. 130.

ECHENIQUE García, José Antonio, Auditoría en Informática, Facultad de Contaduría y Administración, UNAM, México, 1990, Pp. 260.

ELECTRONICAL Data Processing Auditors Foundation, Inc., CISA Review Manual, Domain 7, USA, 1992, Pp. iii-1.

FINE, Leonard H., Seguridad en Centros de cómputo, Edit. Limusa, México, 1983, Pp. 130.

FRANCO Romo, Alonso, Et., al., Planeación de la recuperación informática en caso de desastres, Facultad de Contaduría y Administración, UNAM, México, 1990, Pp. 90, MIMEO.

GORDON B., Davis, La Auditoría y el Procesamiento Electrónico de Información, Instituto Mexicano de Contadores Públicos, México, 1992, Pp. 347.

HERRERA Zogby, Luis, La Prevención de daños por incendio en Arquitectura, Edit. Limusa, México, 1981, Pp. 170.

INSTITUTO Mexicano de Contadores Públicos, Normas y Procedimientos de Auditoría, Novena Edición. México, 1989, Pp.

LAMBARRI Valencia Alejandro, Curso de Auditoría Informática, UPIICSA, IPN, México, 1989, Pp.85, MIMEO.

LOPEZ Elizondo, Arturo, La Profesión Contable. Selección y Desarrollo, Edit. ECASA, Tercera Edición, México, 1984, Pp. 341.

MAIR, William, Et., al., Computer Control & Audit, The Institute of Internal Auditors, USA, 1978, Pp. 380.

MAIR, William, Et., al., Control y Auditoría del Computador, Instituto Mexicano de Contadores Públicos, México, 1976, Pp. 427.

MOLINA Raveto, Enzo, Infomática, una nueva ciencia, Academia Francesa, Francia, 1978, Pp. 82.

MOLINA Raveto, Enzo, Et. al., Introducción a la Informática, Edit. Trillas, México, 1984, Pp. 230.

PEREZ Morales, Ma. Teresa, Curso de Auditoría en Informática, INAP, México, 1992, Pp. 110, MIMEO.

PETIT, Robert, Diccionario de la Lengua Francesa, Le Robert, Francia, 1981, Pp. 570.

PRICE Waterhouse, La Auditoría en un ambiente de procesamiento electrónico de Información, Fascículo II, México, 1972, Pp. 43.

PRICE Waterhouse, Sistemas de Información Computarizados, Serie de Guías de Auditoría, Gruía complementaria, Buenos Aires, Argentina, 1988, Pp. 400.

RAMIREZ Cázares, Arn, Tesis, Organización y Administración de Centros de Cómputo, UNAM, Facultad de Ingeniería, México, 1987, Pp. 237.

RONAN, William, Adiestramiento para combatir incendios, Edit. Hermanos Herrero, México, 1963, Pp. 87.

SANDERS H., Donald, Informática: Presente y Futuro, Edit. McGraw-Hill, México, 1985, Pp. 420.

SLOSSE, Carlos, Et. al., Auditoría, un nuevo enfoque empresarial, Edit. Ediciones Macchi, segunda edición, Buenos Aires, 1989, Argentina, Pp. 1113.

THORIN, Marc, La Auditoría en Informática, Masson, País, 1981, Pp. 79.

WEBER, Ron, EDP Auditing, Conceptual Foundations and Practice, Edit. McGraw Hill, second edition, USA, 1989, Pp. 999.