25

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CAMPUS ARAGÓN

AUDITORÍA EN INFORMÁTICA: TÉCNICAS Y APLICACIONES

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

MARGARITA ZARAGOZA HERNÁNDEZ

ASESOR: ING. JUAN GASTALDI PÉREZ

MÉXICO **1999**

A Dios, por todas las cosas que me ha dado; pero sobre todo por darme la vida

A mi madre, por aguantar y soportar mis malos ratos ¡ Gracias por todo!

A mi padre ✝, por estar siempre a mi lado espero te sientas orgulloso de mi donde quiera que te encuentres.

A Mamá Chucha por esa fuerza y entereza que siempre has mostrado ante la vida.

A mi tía Berhta, por sus regaños y enojos, pero sobre todo por lo que me has dado, esto es solo una muestra de lo mucho que tengo que agradecerte.

A mis hermanos: Andrés, Carlos, Yolanda, Marco Antonio y Susana, porque ustedes me han enseñado lo importante que es tener a alguien con quien contar y sé que siempre estarán a mi lado cuando lo necesite. ¡Gracias a cada uno por todo su cariño!.

A mis Sobrinos: Cynthia, Abigail, Susana, Armando y Marco Sabiani, espero que esto les sirva de motivación, para que logren todo lo que se propongan y que nunca se rindan ante nada para alcanzar su felicidad. Ustedes me han enseñado tantas cosas y son un motivo de orgullo para mí.

A mi familia, porque me han demostrado el verdadero significado de la palabra "UNION".

A mis amigas:

Guadalupe, por todas las locuras que vivimos juntas.

Jeanette, por esos 12 años de amistad y ese cariño que siempre me has dado; ¡Gracias por todo niña!

Cynthia, por lo que nuestra amistad dure muchos años y envejezca con nosotras.

Raquel, tengo que agradecerte tantas cosas, pero la más importante es tu amistad ¡Mil gracias por todo!

A mis amigos de la ENEP, por todos los momentos que compartimos juntos. ¡Gracias Chavos!

A todas aquellas personas que han formado parte de mi vida, porque de todas ellas he aprendido algo.

ÍNDICE GENERAL

INTRODUCCIÓN 1

Capítulo 1. MARCO TEÓRICO

1.1 Auditoría 3
1.1.1 Tipos de Auditoría 4
1.2 Informática 6
1.3 Riesgos 7
1.4 Controles 11
1.5 Control Interno 15
1.6 Seguridad 17

Capítulo 2. AUDITORÍA EN INFORMÁTICA

2.1 Concepto de Auditoría Informática 23
2.1.1 Objetivos y Función 24
2.2 Normas de Auditoría 25
2.2.1 Normas Personales 25
2.2.2 Normas Relativas a la Ejecución del Trabajo 26
2.2.3 Normas de Información 26
2.3 Estructura Orgánica de Auditoría Informática 27
2.4 Metodologías de Auditoría 28
2.5 Áreas de participación 32

Capítulo 3. TÉCNICAS DE AUDITORÍA EN INFORMÁTICA

3.1 Técnicas de Auditoría 36
3.1.1 Procedimientos de Auditoría 37
3.1.2 Herramientas de Auditoría 38
3.2 Técnicas para auditar el Área Informática 39
3.2.1 Auditoría de las Aplicaciones 40
3.2.2 Técnicas para la Administración de la Auditoría 41
3.2.2.1 Selección del Área a Auditar 41
3.2.2.2 Auditoría de Software en Múltiples Localidades 42
3.2.2.3 Auditoría Centralizada 44
3.2.3 Técnicas para la Prueba de Controles en los Programas 45
3.2.3.1 Sistemas en Caso Base Prueba 45
3.2.3.2 Operación Paralela 46
3.2.4 Técnicas de Verificación de Transacciones 46
3.2.4.1 Auditoría desde una Terminal 46
3.2.5 Técnicas para auditar el Desarrollo de las Aplicaciones 47
3.2.5.1 Auditoría de Post-Instalación 47

3.2.5.2 Guías de Control utilizadas durante el Desarrollo del Sistema 48
3.2.5.3 Ciclo de vida del Desarrollo del Sistema 49
3.2.5.4 Grupo de Control y Aceptación del Sistema 50

Capítulo 4. APLICACIÓN DE TÉCNICAS DE AUDITORÍA EN INFORMÁTICA A LA DIRECCIÓN DE CONTROL Y EVALUACIÓN DE LA DIRECCIÓN GENERAL DEL DESTINO DE LOS BIENES DE COMERCIO EXTERIOR PROPIEDAD DEL FISCO FEDERAL

4.1 Solicitud de Autorización para la realización de Auditoría 51
4.1.1 Carta de Solicitud de Autorización 51
4.1.2 Carta de Solicitud de Requerimientos 51
4.2 Análisis General de la Empresa (Dirección General) 51
4.2.1 Antecedentes 52
4.2.2 Objetivo y Funciones 54
4.2.3 Organigrama 57
4.2.3.1 Estructura Orgánica 58
4.3 Área a Auditar (Dirección de Control y Evaluación) 61
4.3.1 Objetivo y Funciones 61
4.3.2 Organigrama 63
4.3.3 Recursos 64
4.3.4 Plano de Ubicación 64
4.4 Definición del Objetivo y Alcance de la Auditoría 64
4.5 Evaluación de Controles 65
4.6 Diseño y Aplicación de Procedimientos de Auditoría 66
4.7 Análisis de Resultados 67
4.7.1 Comparación de Resultados 68
4.8 Obtención de Resultados 70

CONCLUSIONES 71

ANEXOS 72
Anexo 1 73
Carta de Solicitud de Autorización
Anexo 2 74
Carta de solicitud de Requerimientos
Anexo 3 75
Organigrama
Anexo 4 76
Plano de Ubicación
Anexo 5 77
Cuestionarios

Anexo 6 78
Observaciones
Anexo 7 79
Evaluación del Nivel de Riesgo

BIBLIOGRAFÍA 80

FALTAN PAGINAS

De la: 1

A la: 2

Capítulo 1
MARCO TEÓRICO

1.1 AUDITORÍA

La palabra Auditoría proviene del latín "Auditorius", que se deriva de auditor "el que tiene la virtud de oír, pero encaminado a un objetivo".

La auditoria y su finalidad han experimentado una evolución en el transcurso de los años, esta evolución sigue su marcha generando nuevos ámbitos de participación y de servicio.

En la actualidad la auditoría es una función perfectamente identificada tanto en las organizaciones públicas como privadas, y ha diversificado su campo de acción más allá de la revisión de las operaciones y estados contables o financieros, abarcando también aspectos de auditoria operativa, social, y de otros tipos.

El concepto de auditoría debe ser amplio, de tal manera que abarque los distintos tipos que existen actualmente y sus finalidades.

La siguiente definición satisface este objetivo, ya que comprende el proceso y las finalidades:

" Proceso sistemático que consiste en obtener y evaluar objetivamente evidencia sobre las afirmaciones relativas a los actos y eventos de carácter económico; con el fin de determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas. "[1]

Pero a pesar de la diversidad de áreas de aplicación que tiene, los objetivos primordiales que persigue la auditoría son:

1. La revisión y evaluación de la operación de las áreas importantes de las empresa, y de la confiabilidad de la información generada por las mismas, típicamente, las áreas financieras y administrativas.
2. La verificación de la eficiencia y suficiencia de controles en las operaciones de la empresa, así como su cumplimiento.
3. Vigilar que el personal se desempeñe dentro del marco de las políticas y procedimientos establecidos, con honestidad y altos estándares de valores.
4. La generación de los informes correspondientes a las revisiones que desarrolle, en donde se presenten de forma detallada y completa los problemas detectados, sus causas, su posible impacto en la organización y la propuesta de solución a cada uno de ellos.

[1] Boletín del Comité para conceptos básicos de auditoría, Asociación Americana de Contadores, 1973.

1.1.1 Tipos de Auditoría

La auditoría como cualquier disciplina toma características diferentes de acuerdo al campo de acción en el que se desenvuelve, así encontramos que:

De acuerdo a las personas que la realizan, se pueden reconocer dos tipos de Auditoría:

AUDITORÍA INTERNA.

" Es realizada por personal que labora dentro de la propia empresa. Es un control cuyas funciones consisten en examinar y evaluar la adecuación y eficiencia de otros controles."[2]

El objetivo de la auditoría interna es prestar servicio a todos los miembros de la organización en el efectivo desempeño de sus responsabilidades, a través de proporcionarles análisis, evaluaciones, recomendaciones, asesoría e información relacionada con las actividades revisadas.

El alcance de la auditoría interna considera el examen y evaluación de la adecuación y eficiencia del sistema de control interno de la organización y la calidad de ejecución en el desempeño de las responsabilidades asignadas.

La auditoría interna funciona bajo las políticas establecidas por la administración y la alta dirección. El propósito, autoridad y responsabilidad del grupo de auditoría interna debe ser definido por escrito en un documento formal, aprobado por la administración y aceptado por la alta dirección.

Los auditores internos deben ser ajenos a las actividades que auditan. Los auditores internos alcanzan su independencia cuando pueden llevar a cabo su trabajo con libertad y objetividad.

La posición organizacional de la auditoría interna debe ser relevante para asegurar un amplio margen de cobertura de auditoría, y para asegurar acciones efectivas sobre los hallazgos y recomendaciones de auditoría.

AUDITORÍA EXTERNA.

" Es realizada por profesionales contratados exclusivamente para ello, sin ninguna otra relación con la empresa que no sea la que surja de la contratación/prestación de este servicio."[3] Debido a su carácter de ser un servicio contratado, generalmente costoso, se lleva a cabo en un lapso fijo de tiempo y los resultados deben ser presentados en una fecha determinada previamente; lo anterior conduce a que el objetivo principal del auditor externo sea el informe final de

2 Santillana González, Juan Ramón, Conoce las Auditorias, Ed. ECASA, México 1990
3 Alvarez Solis, Fco. Javier, Apuntes de Seguridad y Auditoria en Informática, IPN

resultados, sin importarle si los procedimientos o políticas implementados en la empresa son los adecuados, y tomándolos en cuenta solamente cuando los requiera como apoyo o justificación del dictamen que emita.

De acuerdo área a la cual se aplica, la auditoría se clasifica en los siguientes tipos:

AUDITORÍA FINANCIERA: La auditoría de estados financieros es la más conocida y desarrollada dentro del campo empresarial, su objetivo primordial es el de examinar a los estados financieros de la entidad, asegurándose que dichos resultados presenten en forma razonable la situación financiera y los resultados de las operaciones de conformidad con los principios de contabilidad generalmente aceptados.

AUDITORÍA OPERACIONAL: Es el servicio que presta el contador público independiente, cuando examina ciertos aspectos administrativos, con la intención de hacer recomendaciones para incrementar la eficiencia operacional de la entidad.

AUDITORÍA ADMINISTRATIVA: Puede definirse como un examen completo y constructivo de la estructura organizativa de una empresa, institución o departamento y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales. El objetivo principal que persigue es el de detectar posibles errores, deficiencias o irregularidades en los factores del proceso administrativo.

AUDITORÍA SOCIAL: Es la técnica que evalúa el comportamiento social de la organización, analizando precios, salarios, investigación y desarrollo, publicidad, relaciones públicas, relaciones humanas, relaciones de la organización con la comunidad, y estas en razón directa de la contribución que aportan a los objetivos de la organización.

AUDITORÍA DEL COMPORTAMIENTO: Es la técnica que evalúa por medio de los resultados obtenidos de las estrategias y objetivos, la eficiencia, el rendimiento y toma de decisiones que la alta dirección o gerencia ha establecido. Comparándolos con sus similares en otras empresas del mismo ramo a fin de determinar que tan razonables son, o si requieren de modificaciones.

AUDITORÍA GUBERNAMENTAL: Se encarga de la revisión de aspectos financieros, operacionales, administrativos, de resultados de programas y de cumplimiento de disposiciones legales que enmarcan la actividad de las entidades públicas.

AUDITORÍA FISCAL: Verifica el correcto y oportuno pago de los diferentes impuestos y obligaciones fiscales de los contribuyentes desde el punto de vista físico: Secretaría de Hacienda y Crédito Público, direcciones o tesorerías de hacienda estatales y tesorerías municipales. En está auditoría recae también, por filosofía, las revisiones que llevan a cabo organismos o autoridades con facultades de imponer gravámenes a los contribuyentes; como son, a manera de ejemplo: IMSS e INFONAVIT.

1.2 INFORMÁTICA

En términos concretos, se define a la Informática como:

> "Es el conjunto de técnicas y herramientas relativas al tratamiento y procesamiento eficaz y eficiente de la información mediante el uso de máquinas automáticas y computadoras, con el fin de dotar a esta información de un significado y un valor que la convierta en un elemento estratégico capaz de dar a quien la posee una ventaja competitiva." [4]

El uso de la Informática en las empresas, y en general en cualquier sector de la sociedad, es ahora el principal motor que las impulsa hacia su crecimiento mediante la eficientización de las operaciones de todas sus áreas.

Dada la diversidad de las ramas de la sociedad en que la informática es aplicada, los objetivos que debe cumplir se vuelven innumerables. Sin embargo; la esencia fundamental de la finalidad de su uso se puede resumir en los siguientes puntos:

1. Liberar a las personas de las tareas tediosas, repetitivas y pesadas permitiéndoles ocupar su tiempo en otras actividades más creativas.

2. Automatizar, agilizar y eficientizar la ejecución de tareas, haciendo más confiables los resultados obtenidos.

3. Proporcionar a la alta gerencia de las empresas información relevante para la toma de decisiones estratégicas.

4. Servir como herramienta para la integración de las personas en las empresas y en la sociedad, mediante el intercambio de información a través de aplicaciones de comunicaciones, redes, etc.

5. Servir como herramienta para la creación de nuevas tecnologías y apoyar en las ramas de la investigación científica.

---

4 H. Sanders, Donald, Informàtica Presente y Futuro, Ed. MC-Graw-Hill, Mèxico 1990

1.3 RIESGOS

Podemos definir el riesgo como: "La posibilidad de que ocurra algún evento negativo para las personas y (o) empresas." [5]

Los riesgos que amenazan a los aspectos informáticos y a la información misma se clasifican en dos grandes grupos:

a) RIESGOS INTERNOS

Son los que se generan dentro de la misma empresa. Estos riesgos, por su fuente, son más sencillos de prever. Sin embargo, y aun cuando parezca contradictorio, será más fácil que se presenten, ya que el conocimiento de los procedimientos internos de operación hará más sencillo el camino de alguna persona interesada en dañar a la institución.

Robo

1) De material.- Es la escala más baja del robo, ya que aquí hablamos del robo de los activos de la empresa como: cintas, papelería, discos, etc.

2) De recursos.- En este caso el robo puede alcanzar una pérdida substancial en tiempo máquina utilizado para procesar aplicaciones no autorizadas.

3) De información.- La escala superior en la clasificación de robo es la que trata la sustracción de programas, archivos y datos en general, con el fin de utilizarlos en beneficio propio y en contra de la institución.

Sabotaje

Éste se puede presentar a través de otros medios como entorpecimiento de la producción, sobrecarga ficticia de la operación, etc.

Destrucción

1) De datos.- En medios magnéticos, documentación, archivos, respaldos, documentos fuentes, etc.

2) De recursos.- Aquí tratamos de la destrucción física de los elementos que incluye un Centro de Proceso de Información como unidades de cinta, discos, unidad central de proceso, así como los recursos de papelería y soporte que complementan los elementos de operación.

[5] A. Lambarri. V., Identificaciòn, Evaluaciòn y Control de Riesgos, Toluca, Mèxico, Junio 1988

En este caso se puede decir que la destrucción tanto de los recursos como de los datos, se puede dar en forma voluntaria como un ataque directo o bien en forma involuntaria debido a errores de los operadores o usuarios de un sistema.

Huelgas

Del personal, que impedirían la operación del servicio informático, pudiendo llegar a detenerla totalmente.

Fraudes

Se refiere a la manipulación de la información a fin de obtener un beneficio ilegítimo para la persona que lo realiza.

Esta clasificación nos da en forma natural las áreas de riesgo en el ambiente de la informática. Sin embargo, su identificación requiere de algunos elementos que veremos posteriormente.

b) RIESGOS EXTERNOS

Se definen como todos aquellos que se presentan en el ambiente físico y social que rodea a un Centro de Proceso de Información, los cuales, si bien no es posible eliminar, si es posible tomar las medidas necesarias que minimicen la probabilidad de pérdida de información o destrucción de las instalaciones.

Naturales

1) Temblor.- Se refiere a los movimientos de tierra que pueden afectar la totalidad de los recursos informáticos, incluyendo las instalaciones.

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

3) Inundación.- Fugas o corrientes de agua. Elemento que representa un peligro muy grande para los equipos, tomando en cuenta sus componentes.

4) Tormenta.- Se relaciona con las descargas de energía eléctrica que generan estos fenómenos y que pueden igualmente destruir, o impedir que el Centro de Proceso continúe operando en condiciones normales.

Estos riesgos están determinados por la localización geográfica de centro, el medio ambiente que lo rodea, e inclusive por su diseño y construcción.

Humanos

1) Robo.- Por la intromisión de terceras personas ajenas a la empresa, pueden ser de material, programas, datos, etc.

2) Sabotaje.- Provocado por grupo de terroristas o por personas que tengan conocimiento de la importancia de la información que se encuentra en el Centro de Proceso.
3) Motines Sociales.- En este nivel nos referimos a la posible destrucción o entorpecimiento del proceso, como resultado de un conflicto ajeno a la empresa.

4) Fraude.- Sobre los datos que se manejan cometido por terceras personas.

Materiales

1) Descomposturas de equipo.- Que limitarían la operación normal del centro y que podrían generar pérdidas cuantiosas.

2) Fallas de energía.- Sobrecarga o bajas de voltaje que pudieran afectar la confiabilidad de la información o inclusive dañar los componentes de la computadora.

Una vez que hemos analizado los riesgos que enfrentamos pasaremos al proceso de evaluarlos para definir de igual forma el tratamiento que le daremos.

Esta parte es, quizá la más laboriosa, ya que requiere una metodología para poder llegar a medir el grado de exposición al riesgo en que nos encontramos operando, para lo cual deberemos incorporar como criterios de evaluación los siguientes factores:

Posibilidad de ocurrencia.- Se refiere a la frecuencia de que un riesgo se materialice, estimada en función a estadísticas, experiencia del personal asociado al área de informática o a estudios formales de probabilidad, aún cuando estos últimos requieren de información muy compleja y estadísticas precisas, que en nuestro ambiente no es fácil de obtener.

En base a lo anterior se llegará a la asignación de valores particulares en función a esta frecuencia, como ejemplo tenemos:

1. Extremadamente Remoto
2. Remoto
3. Razonablemente Probable

El siguiente factor de evaluación será el impacto económico y operativo que tenga el riesgo que eventualmente pudiera presentarse, y que al igual que en el elemento anterior presenta dos opciones de evaluación.

La primera asigna valores de 1 a 3 dependiendo de la severidad del evento sin incorporar cifras de pérdidas.

Marginal: En donde no hay daños significativos

Crítico: Los daños son ya considerables

Catastrófico: Pérdida de gran parte de la totalidad de las instalaciones, suspensión del modo operativo y afectación del personal

La asignación de valores a los diferentes riesgos determinados en la Institución nos permitirá orientar directamente nuestras acciones hacia aquellas que se encuentren más expuestas a fin de definir el tratamiento que les daremos.

A continuación mencionaremos las tres formas de administrar los riesgos:

a) Asumir el riesgo

En este caso la Institución reconoce un riesgo dentro de alguna de sus actividades, sin embargo, estamos ante un caso en que el estudio de costo-beneficio muestra que, las pérdidas estimadas, en caso de que este se presente, no justifican la incorporación de controles y (o) medidas de seguridad.

Esta situación deberá estar perfectamente sustentada y ser del conocimiento de la administración de la Institución ya que una decisión tomada sobre bases inciertas pudiera comprometernos, al estar aceptando un riesgo.

b) Minimizar el Riesgo

Bajo este esquema, se definirán nuevos controles y (o) medidas de seguridad orientados a minimizar el grado de exposición al riesgo en que operamos. En consecuencia estaremos hablando de inversiones en beneficio de la confianza de que nuestras actividades no se verán seriamente afectadas ya que las medidas preventivas y correctivas que se incorporen minimizarán los efectos contrarios en caso de que se presente algún riesgo.

Es aquí en donde, quizás, se requiera de un compromiso mayor por parte de la administración hacia la seguridad alrededor de la actividad de informática.

c) Transferir el Riesgo

Este último apartado trata sobre la utilización de seguros, transfiriendo a estas organizaciones el riesgo que estamos enfrentando con las ventajas que esto trae.

Cualquiera que sea la alternativa que tomemos, es necesario realizar evaluaciones periódicas que nos muestren el grado de exposición al riesgo, tomando las decisiones y acciones tendientes a llevarlo a niveles aceptables.

1.4 CONTROLES

"El término genérico de Control se refiere a cualquier acción tomada por la gerencia que eventualmente lleve al logro de los objetivos y metas de la organización." [6] Esta definición de control es amplia e incluye tanto acciones positivas como negativas.

Un control debe de supervisar que las operaciones que se realicen en la empresa, se enfoquen al cumplimiento de los objetivos establecidos por la misma. El control debe de englobar los siguientes aspectos:

1. Establecimiento de normas o estándares
2. Instalación de sistemas de información
3. Comparación de las normas con los resultados reales
4. Corrección de las desviaciones

Debido a que en todas las áreas existen riesgos de todo tipo, es necesario que los controles establecidos disminuyan estos, tratando de eliminar al máximo cualquier desviación dentro de los estándares y normas establecidas por la administración de la empresa.

Existen cinco tipos de controles que pueden ser usados en un ambiente computarizado y son:

[6] The Institute of Internal Auditors, Inc., Systems Auditability & Control Study, Florida 1981

Controles Directivos

Estos controles son acciones gerenciales, políticas, procedimientos, directivas o guías que provocan o promueven la ocurrencia de un evento deseado.

Ejemplos de controles de este tipo son los siguientes:

- Establecer un comité de administración de la seguridad de sistemas

- Asignar, a los empleados la responsabilidad sobre los activos que usen para el desempeño de sus funciones

- Generar conciencia sobre la seguridad, en todo el personal
- Proveer guías para proteger la confidencialidad de los datos y la información

Controles Preventivos

Los controles de este tipo previenen la introducción de errores al sistema o su eliminación después de que son descubiertos. En este tipo de controles encontramos estándares, guías, métodos, prácticas y técnicas manuales o automatizadas que den como resultado sistemas seguros, confiables y de alta calidad.

Tales controles incluyen también el uso de claves de acceso o "passwords" y técnicas estructuradas las cuales, cuando son usadas apropiadamente, pueden eliminar o reducir mucho del mantenimiento actual o futuro de una aplicación computarizada.

Los controles preventivos, también impiden o minimizan eventos no deseados tales como fraudes, robos, desfalcos, errores, omisiones y otras regularidades. Para hacer más efectivos los controles de este tipo, es necesario combinarlos con controles de otro tipo, por ejemplo una alarma, la cual emita un continuo sonido hasta que se lleve a cabo una acción determinada.

Ejemplos de controles de este tipo son los siguientes:

- Implementar buenos programas de seguridad física y control de acceso

- Controlar el acceso al sistema, del personal de servicio de mantenimiento de Hardware y/o Software

- Validar todos los usuarios remotos que pretenden accesar el sistema

- Restringir el proceso de programas de aplicación y el uso de terminales

- Establecer una adecuada separación de responsabilidades

Controles Detectivos

Los controles de este tipo detectan errores pero no permiten la corrección de ellos, hasta que el proceso se ha llevado a cabo en forma completa. Proporcionan una retroalimentación del funcionamiento de los controles preventivos y sus resultados, y detectan si los estándares de seguridad se han logrado.

Estos controles detectan la ocurrencia de eventos no deseados e identifican áreas problema que demandan mejoras en los elementos de control, seguridad y calidad del sistema.

Los controles detectivos incluyen herramientas y técnicas tanto manuales como automatizadas.

Ejemplos de controles de este tipo son los siguientes:

- Uso obligatorio de la credencial del empleado

- Implantar bitácoras de actividades de terminales
- Aplicar técnicas de revisión de las fases del desarrollo de una aplicación

- Controlar los cambios a los programas para asegurar que sólo se hagan los cambios autorizados

- Conducir periódicas auditorías a los sistemas de seguridad

Controles Correctivos

Los controles de este tipo, detectan irregularidades, omisiones y errores e intentan corregirlos inmediatamente a través de procedimientos manuales o automatizados.

Ejemplos de este tipo de controles son los siguientes:

- Producción de reportes anteriores y posteriores a la corrección de errores

- Diseño de reportes de auditoria y de controles para ser revisados por el usuario y los auditores

- Educación y entrenamiento de analistas y programadores para desempeñar en forma eficiente y efectiva sus funciones

- Educación y entrenamiento de usuarios y personal de informática en aspectos de control y auditabilidad de aplicaciones

- Documentación de comentarios que clarifiquen las funciones de las rutinas de un programa

Controles de Recuperación

Los controles de este tipo, facilitan el respaldo y la recuperación de un sistema después de que ha ocurrido una interrupción o una falla en el sistema de cómputo.

Estos controles también promueven un ambiente ordenado en el cual todos los recursos están disponibles para permitir una razonable y suave recuperación, previniendo la interrupción de una actividad específica o de todas las operaciones de una organización.

Los controles de recuperación incluyen el respaldo oportuno y la rotación de los archivos de datos, programas, procedimientos, retención de registros y la planeación de contingencias y de recuperación en caso de desastre.

Ejemplos de controles de este tipo son los siguientes:

- Respaldo periódico de datos y programas y su almacenamiento en una instalación ubicada en otra localidad

- Desarrollo de un plan de contingencia, el cual sea probado periódicamente para asegurar su efectividad

- Provisión de papelería, formas y accesorios requeridos para asegurar la continuidad de las operaciones

- Establecimiento de guias y procedimientos para procesos de reinicio y recuperación de aplicaciones y del sistema de cómputo

- Procedimientos para el manejo de emergencia, documentados y probados periódicamente para asegurar su efectividad

- Contratación de un seguro de cobertura amplia con propósitos de recuperación

- Implementación de programas de retención de registros vitales

Cuando estos cinco tipos de controles son apropiadamente planeados e implementados, dan como resultado sistemas que son usados, controlados, mantenibles, seguros y auditables.

Los controles que previenen errores, eliminándolos del sistema, son mejores que los controles que detectan errores para su posterior corrección.

Los controles que detectan errores e intentan su corrección inmediata, son aún mejores, pero el número de casos en los cuales se puede aplicar controles de este tipo dentro de sistemas comerciales o de negocios, es relativamente bajo. La decisión sobre que tipo de control usar, depende del sistema en particular.

1.5 CONTROL INTERNO

Los controles internos, como su nombre lo indica, son medidas dentro de una organización para asegurar una operación exitosa, protegiendo los recursos contra pérdidas, malos usos, créditos no garantizados, fallas en las adquisiciones, empleados ineficientes y robos. Si el sistema de control es efectivo, asegura a la gerencia que la información sobre las finanzas y operaciones de su empresa, sea confiable y completa.

Sin dichos controles sería muy difícil que una organización operara de una manera eficiente. Es responsabilidad de los directivos y no del auditor, asegurar que existan los controles adecuados. El auditor tiene la responsabilidad de verificar la existencia de dichos controles y hacer recomendaciones en caso de que éstos sean ineficientes.

El sistema de Control Interno se define como: "Los controles internos comprenden el plan de organización y los métodos y medios adoptados en una empresa para salvaguardar sus activos, verificar la exactitud y confiabilidad de su información contable, promover la eficiencia operativa y el apego a las políticas establecidas por la gerencia."[7]

[7] Alvarez Solis, Fco. Javier, Apuntes de Seguridad y Auditoria en Informàtica, IPN

Los controles son necesarios para disminuir riesgos, por lo tanto, antes de evaluarlos es necesario identificar los riesgos que deben prevenir, detectar o corregir. Los controles actúan sobre las causas que hacen que un riesgo se materialice, y no directamente sobre el riesgo.

El Control Interno es una de las más importantes responsabilidades de todo directivo: Jefe de Departamento, Gerente de Sucursal, Gerente de Área, Subdirector y/o Director, etc.

El Control Interno en el ámbito informático, debe de perseguir de manera general:

1. Promover la eficiencia de la operación.

   La función informática debe de enfocar sus esfuerzos y recursos en la entrega y manejo de la información, la cual debe cumplir con características fundamentales que garanticen el buen servicio y la confiabilidad requerida, cubriendo además los objetivos de: totalidad, exactitud, autorización, mantenimiento, oportunidad y utilidad de la información.

2. Adhesión a las políticas predefinidas de la empresa.

   Estas políticas pretenden disminuir diversos riesgos del entorno en el que se desenvuelve una empresa y del manejo interno de esta: disposiciones legales, estándares, políticas internas, etc.

3. Protección de activos.

   Los nuevos riesgos que la informática involucra, no sólo se dan en la pérdida o robo de algunos equipos, sino que los mayores riesgos se presentan en el contenido y la posibilidad de alteración de los registros magnéticos, donde se encuentra el activo principal de toda la organización y que se denomina: información.

Actualmente la mayoría de información de las empresas, es administrada, generada y controlada a través de equipos de cómputo, software y medios de comunicación.

1.6 SEGURIDAD

"Es la administración y protección de los recursos de cómputo que tiene la empresa y que accesan los usuarios."[8] El objetivo es el de proteger el patrimonio informático de la institución, entendiendo por tal, instalaciones, equipos e información, ésta última en todas sus formas (en cualquier dispositivo de almacenamiento magnético como son los disquetes, discos duros, cintas, cartuchos, etc.).

La Seguridad Informática debe de establecer los controles suficientes para *disminuir los riesgos que se generen en el ámbito informático.*

La seguridad informática puede dividirse en:

SEGURIDAD FÍSICA: es un conjunto de lineamientos y procedimientos cuyo objetivo es evitar o disminuir la exposición a riesgos ya sean internos o externos en las instalaciones físicas de cómputo. Las medidas de seguridad física deben tomar en cuenta riesgos como accidentes, desastres naturales, ataque por intrusos, condiciones ambientales, etc.

SEGURIDAD LÓGICA: la seguridad lógica es tan importante como la física, incluye normas para el control del acceso a los datos/información, a fin de reducir el riesgo de transferencia, modificación, pérdida o divulgación accidental ó intencional de éstos. La seguridad física y la lógica dependen, para el éxito de cada una, de la eficiencia y fortaleza de la otra.

Algunas de las principales *aplicaciones de las medidas de seguridad lógica* son:

- Separar de otros recursos del sistema el material al que tiene acceso permitido un usuario.
- Proteger los datos de un usuario de los de otro.
- Controlar el acceso de lugares remotos.
- Definir y poner niveles de control de acceso.
- Monitorear el sistema para detectar cualquier uso impropio.

El sistema integral de seguridad debe comprender:

1. Elementos Administrativos
2. Definición de una política de seguridad
3. Organización y División de responsabilidades

[8] Alvarez Solis, Fco. Javier, Apuntes de Seguridad y Auditoria en Informàtica , IPN

4. Seguridad Física contra catástrofes (incendio, terremoto, etc.)
5. Prácticas de Seguridad del personal
6. Pólizas de seguros
7. Elementos técnicos y procedimientos
8. Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales)
9. Aplicación de los sistemas de seguridad, tanto internos como externos
10. El papel de los auditores, tanto internos como externos
11. Planeación de programas de desastre y su prueba.

SEGURIDAD EN CENTROS DE CÓMPUTO

La seguridad en centros de cómputo debe ser implantada tomando en cuenta dos enfoques:

1) Tipos de Computadora: Mainframe, Minicomputador o Microcomputadora.

2) Aspectos a Implementar: Administración, Seguridad Física, Seguridad Lógica, Operativa de Sistemas y Planes de Contingencia.

Dependiendo del tipo de computadora serán los controles que deben de establecerse, en su mayoría los riesgos son iguales para cualquier tipo de computadora, pero el control a establecerse a efecto de reducir el mismo y garantizar la continuidad del servicio y la integridad de los activos, difiere por las características propias del tipo de equipo.

Dentro de los controles a implementar y de manera general debe de contemplarse lo siguiente:

a) Administración

- Políticas y Procedimientos
- Delimitación de funciones y responsabilidades
- Controles administrativos
- Planes de Contingencia

b) Seguridad Física

- Ubicación del centro de cómputo
- Control de acceso físico
- Construcción del edificio
- Soporte ambiental
- Protección contra fuego
- Protección de registros (respaldos)
- Programa de mantenimiento

c) Seguridad Lógica

- Esquema de seguridad de usuarios
- Esquema de seguridad de recursos
- Uso de claves
- Asignación de claves

d) Operativa de Sistemas

- Cifras control de los sistemas
- Controles administrativos
- Controles de respaldo

e) Planes de Contingencia

El objetivo general que se persigue con el establecimiento de planes de contingencia, es el de contar con procedimientos por escrito y claramente identificados para el manejo de emergencias en caso de catástrofe o amenazas mayores para proteger al personal, minimizar el daño a las instalaciones y equipo de procesamiento de datos y reducir la magnitud de la interrupción del servicio.

Contingencia es toda aquella posibilidad de que una cosa suceda y que a su vez genere riesgos y peligro.

Todo plan de contingencia debe de contener:

1.- Plan de emergencia.- Es el establecimiento de controles para contener el daño, debe de contemplarse todos los desastres naturales y eventos mal intencionados.

Mecanismos: Detectores de humo, de calor, alarmas, circuitos cerrados de tv, etc.

2.- Plan de respaldo.- El plan de respaldo debe de contener el mantenimiento de partes críticas entre la pérdida del servicio y/o recurso y su recuperación o restauración. Para ello deben de tenerse las siguientes consideraciones: Capacidad de respaldo, Ambientes requeridos, Aplicación por aplicación y procedimiento por procedimiento.

Mecanismos: Equipo de respaldo, centros alternos de respaldo, etc.

3.- Plan de recuperación.- El plan de recuperación consiste en la restauración temporal o permanente de una capacidad operacional crítica, para lo cuál es necesario una estrategia de recuperación por cada recurso identificado.

Mecanismo: Planta física, facilidades de comunicación, etc.

4.- Programa de registros vitales.- Es la parte vital en la sección de datos del plan de recuperación, su objetivo es proteger datos esenciales y preservar aquellos registros necesarios para restablecer las operaciones.

SEGURIDAD EN LOS SISTEMAS DE PRODUCCIÓN

Se deben de considerar el control, la integridad y la seguridad de los datos compartidos por muchos usuarios.

Debe instalarse el software que proporcione el acceso, la organización y el control sobre datos compartidos, el sistema de administración de base de datos, debe instalarse y mantenerse de tal manera que asegure la integridad del software, de las bases de datos y de los parámetros de control que definen el ambiente.

SEGURIDAD EN EL DESARROLLO DE SISTEMAS

Objetivo: Implantar medidas de seguridad tendientes a disminuir los riesgos antes de la liberación del producto.

Es común encontrarse con sistemas que no cumplen con ciertos atributos, pues no cuentan con una planeación adecuada, y se desarrollan de una manera desorganizada. Estos sistemas generalmente se desechan antes de concluirse y si llegan a su fin tienen un uso mínimo por no cumplir con las necesidades del usuario, ser muy complicados, defectuosos y costosos. Lo anterior puede ser causa de la falta de atención, desconocimiento o carencia de un adecuado sistema de control de los factores que intervienen en el desarrollo de un sistema y que son necesarios para lograr el éxito mismo.

Los controles presentes en el desarrollo de un sistema tienen como finalidad asegurar el desarrollo de sistemas de calidad dentro de los costos y tiempos estimados, contando con altos niveles de eficiencia y confiabilidad.

Los aspectos de seguridad que deben de abarcarse, son:

1. Participación activa y aprobación tanto de directivos como de usuarios.
2. Estándares y lineamientos de desarrollo.
3. Administración del proyecto.
4. Controles en las pruebas y conversiones.
5. Revisiones de post-implementación.

SEGURIDAD EN REDES Y TELECOMUNICACIONES

La finalidad de establecer aspectos de seguridad en redes y telecomunicaciones es con objeto de garantizar un servicio eficiente, seguro y confiable.

Los aspectos que deben de considerarse son:

Administrativos:

- La función de administración de telecomunicaciones debe de ser lo suficientemente fuerte, para establecer estándares y procedimientos.

- Deben de existir adecuados registros para documentar y controlar los inventarios del equipo de telecomunicaciones y administrar los cambios del equipo.

- Deben de existir procedimientos para monitorear el uso de la red, para hacer ajustes, registrar y resolver cualquier tipo de problemas.

- Deben de existir procedimientos para seguir la pista a los costos de las telecomunicaciones y cargarlos a los departamentos y personas adecuadas.

- La función del administrador deberá de tomar un rol activo en el diseño y desarrollo de las nuevas aplicaciones en línea para asegurar que se sigan los estándares de telecomunicaciones.

Seguridad Física:

- El equipo de comunicaciones deberá de ser mantenido en un área segura para prevenir accesos indebidos.

- Las líneas de comunicaciones deberán de ser debidamente blindadas y protegidas para prevenir "conexiones indebidas".

- El equipo de prueba a las comunicaciones usado para monitorear la red, debe de ser protegido para limitar accesos indebidos.

- El plan de contingencia debe de proporcionar una adecuada atención a la recuperación de las facilidades de comunicaciones de datos.

Seguridad Lógica:

- Deben de existir password y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado para utilizar la red de telecomunicaciones.

- Las facilidades de chequeo de errores deberán de existir para detectar errores en la transmisión y establecer retransmisiones si s apropiado.

- Si están siendo transmitidos datos sensibles, el sistema debería de usar facilidades para establecer nuevas rutas automáticamente, para limitar cualquier conexión a los cables de la señal que no sea autorizada, así como controles para asegurar que las transmisiones solo son para usuarios autorizados.

Capítulo 2
AUDITORÍA EN INFORMÁTICA

2.1 CONCEPTO DE AUDITORÍA INFORMÁTICA

En los últimos años los avances tecnológicos han impulsado el crecimiento que han tenido las computadoras, ocasionando que la gran mayoría, si no es que todas las operaciones de una empresa se realicen a través de medios informáticos. Este avance obligo a la auditoría tradicional a extender su campo de acción, el cual en un principio se limitaba a la revisión de estados financieros, y que ahora incluye al ámbito informático.

Este nuevo campo de acción de la auditoría fue de importancia tal, que significó la creación de una nueva rama de auditoría llamada *Auditoría en Informática*, la cual utiliza muchas de las mismas técnicas y metodologías que otros tipos de auditoría, pero que tiene una característica que la aparta de las demás: que no puede ser llevada a cabo por un auditor común, sino que requiere de mayores conocimientos acerca de los aspectos de informática, es decir, el auditor en informática es un profesional especializado.

José Antonio Echenique[9] define a la Auditoría Informática como:

" La revisión y evaluación de los controles, sistemas y procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio de señalamientos de cursos alternativos se logre la utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones",

De acuerdo con esta definición podemos decir que la Auditoría en Informática es la revisión y evaluación de la suficiencia de controles que se establecen en el ámbito informático, para el uso eficiente de los recursos informáticos con que cuenta una organización, con el fin de establecer dentro de esta misma una efectiva seguridad en el procesamiento, recuperación y restablecimiento de la información la cual debe ser confiable, efectiva y oportuna para una eficiente toma de decisiones.

[9] Echenique, Josè Antonio, Auditoria en Informàtica, Ed. Diana, Mèxico 1980

2.1.1 Objetivos y Función

Ya se ha definido pero, qué objetivos son los que persigue?

Realmente el área de Auditoría en Informática, su objetivo es el de evaluar la suficiencia de controles y efectuar recomendaciones en materia de informática a los niveles directivos, gerencial y operativo que permitan reducir los riesgos a que esta expuesta la misma.

El objetivo fundamental de la función de auditoría informática en las empresas es el de cuidar, revisar, evaluar, informar y sugerir para mejorar.

La auditoría informática funciona como herramienta de retroalimentación para la administración, de forma que esta cuente con los elementos suficientes para la toma de decisiones que dirijan a la empresa hacia el cumplimiento eficaz de sus objetivos y de su misión.

Los aspectos que la auditoría informática debe cuidar para lograr lo anterior son:

1. Que se cumplan satisfactoriamente las normas, políticas, planes, procedimientos, etc.
2. Que todos los anteriores sean acordes con los objetivos que la empresa persigue, es decir, que conlleven a su cumplimiento.
3. Que la estructura orgánica de la empresa, la división de funciones y los métodos de trabajo sean adecuados y eficaces.
4. Que los nuevos planes, políticas, métodos, etc. sean desarrollados con el fin de contribuir al crecimiento de la empresa, o a su mejor funcionamiento.
5. Que existan controles suficientes en la operación diaria, que aseguren el registro correcto y oportuno de todas las actividades desarrolladas.
6. Que la empresa en general esté protegida contra cualquier tipo de riesgo, ya sea financiero, legal, natural, etc.
7. Que los niveles de integridad y veracidad de la información que la empresa maneja sean los óptimos y que esta llegue de manera oportuna a los niveles directivos.

Actualmente, la visión de la existencia de una área de auditoría informática dentro de una empresa debe enfocarse hacia la obtención de información veraz y eficiente, ya que el nivel de calidad que se observe en la ejecución de las operaciones será el reflejo fiel de los servicios o productos que la empresa pueda ofrecer.

Así, la organización puede conocer que áreas pueden representar una ventaja competitiva por el excelente nivel de calidad con que se desempeñan, y cuales áreas requieren de mayor atención, a fin de mejorar la presencia que se tiene en el mercado, y de tener una clara visión de su posición ante la competencia en todo momento.

2.2. NORMAS DE AUDITORÍA

Las actividades que el auditor en informática realiza, así como los aspectos relativos a su calidad moral y del resultado de su trabajo, son reguladas por normas establecidas y aceptadas por institutos nacionales e internacionales de auditoría, o por normas internas que la propia empresa define.

El Instituto Mexicano de Contadores Públicos (IMPC) es el encargado de promulgar estás normas que son adoptadas y aprobadas por sus miembros, las cuales se conocen como *las normas de auditoría generalmente* aceptadas, a continuación se presenta una síntesis de cada una de las categorías y que pueden ser aplicadas a la Auditoría en Informática:

2.2.1 Normas Personales

Se refieren a las cualidades que *el auditor debe tener para* poder asumir, dentro de las exigencias que el carácter profesional de la auditoría impone, un trabajo de este tipo. Dentro de estas normas existen cualidades que el *auditor debe tener antes* de poder asumir un trabajo profesional de auditoría y cualidades que debe mantener durante el desarrollo de toda su actividad profesional.

- Entrenamiento técnico y capacidad profesional.

El auditor antes de ofrecer sus servicios como tal, debe poseer los conocimientos, preparación y capacidad *suficiente para el desarrollo* de su trabajo y así éstas características lo coloquen en condiciones de prestar eficientemente sus servicios.

- Cuidado y diligencia profesional.

El *auditor* debe poner todo su afán, interés, atención, profesionalismo y responsabilidad al realizar su trabajo y emitir un opinión, poniendo siempre toda su capacidad y habilidad profesional. La actividad del auditor como todas las actividades humanas está propensa a fallas, pero estas deben de permanecer dentro de márgenes muy reducidos, por tal motivo se requiere que realice su trabajo con cuidado y dedicación.

- Independencia.

Un auditor no podrá actuar en aquellos casos en los que existan circunstancias que puedan influir sobre su juicio objetivo y por consiguiente reduzcan su independencia mental.

Un auditor debe ser ajeno al área o actividades que audite, está independencia debe permitirle emitir juicios imparciales sin la influencia de algún sentimiento de pertenencia, la cual se logra por medio de dos factores: *Posición organizacional* y Objetividad.

El auditor no debe perder de vista el objetivo de sus actividades, que es el de identificar y sugerir.

2.2.2 Normas Relativas a la Ejecución del Trabajo

- Planeación y supervisión.

El trabajo que se lleve a cabo para realizar la auditoria debe ser planeado anticipadamente por el auditor encargado de tal tarea, además si en la auditoria intervendrán otras personas, este debe de mantener un control sobre sus actividades.

- Estudio y evaluación del control interno.

Se debe realizar un estudio y evaluación previa de los controles existentes en el área a auditar y en base a esto, determinar cual será la profundidad a alcanzar de la revisión que se llevará a cabo.

- Evidencia comprobatoria.

Recabar el mayor número de datos que pudieran ser utilizados como evidencia y tener así una base razonable al momento de emitir el informe final.

2.2.3 Normas de Información

El resultado final del trabajo del auditor es su dictamen o informe. Mediante él, pone en conocimiento de las personas interesadas los resultados de su trabajo y la opinión que se ha formado a través de su examen.

Estas normas se clasifican como normas de dictamen e información. El dictamen del auditor es el documento formal que suscribe el contador público conforme a las normas de su profesión, relativo a la naturaleza, alcance y resultado del examen realizado. La importancia del dictamen en la práctica profesional es fundamental, ya que usualmente es lo único que el público conoce de su trabajo.

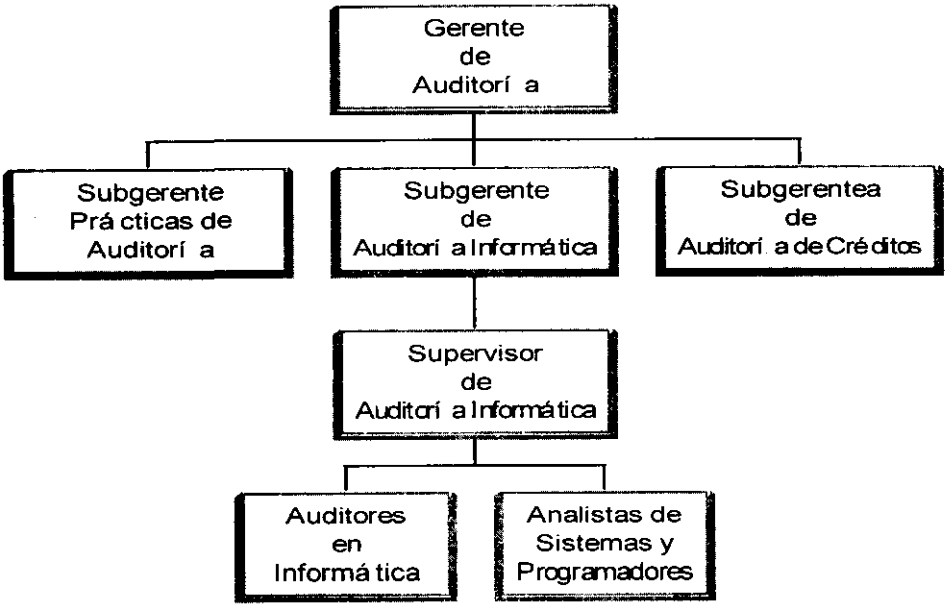
2.3 ESTRUCTURA ORGÁNICA DE AUDITORÍA EN INFORMÁTICA

Al igual que cualquiera de las ramas de auditoria, la especialidad de Auditoría en Informática, deberá depender, en la medida de lo posible, del más alto nivel directivo de la empresa, pudiendo ser del Consejo de Administración a través del Director General o bien de un Comité de Auditoría.

La actividad de auditoría debe conservar una independencia total de la parte operativa que no lo lleve a comprometer sus apreciaciones y que le dé una libertad de acción adecuada, ya que desde esta posición el Auditor en Informática intervendrá en áreas donde las decisiones normalmente son tomadas por los más altos niveles de la organización y, en consecuencia, son éstos quienes podrían objetar y(o) cuestionar las sugerencias, aportaciones y observaciones del auditor en el cumplimiento de su labor.

El respeto y reconocimiento de las áreas de la organización sujetas a la revisión del Auditor en Informática, no se darán en forma automática, sino que, se conseguirá únicamente mediante el conocimiento y profesionalismo que demuestre el comisionado de Auditoría en el ejercicio de su función, pero es innegable que se requiere de un respaldo del más alto nivel para lograr en forma adecuada los objetivos trazados.

La estructura de organización a detalle podrá variar en función a los recursos de la empresa.



En los dos casos la función de Auditoría reporta directamente al Director General, ya que este modelo es el que más se apega a los criterios que mencionamos.

2.4 METODOLOGÍAS DE AUDITORÍA

La Auditoría en Informática para el desempeño de sus actividades debe de contar con una serie de procedimientos integrados en una metodología formal que servirá de apoyo al trabajo de cada auditor en informática. Esta metodología debe ser estructurada de acuerdo al plan de actividades y criterio de cada auditor, además, esta misma debe de apoyarse con técnicas y herramientas propias de esta función, con el objeto de facilitar la adecuada ejecución de sus actividades, y garantizar aún más el éxito de los planes o proyectos realizados por la Auditoría Informática, en cuanto al costo, tiempo y resultados esperados, por lo cual se deben de considerar los siguientes aspectos:

- Examinar detallada y objetivamente todos los informes y datos recabados
- Analizar habilidades y normas personales del auditor en informática
- Tener la suficiente experiencia en conocimientos de auditoría en informática

- Obtener la documentación y actualización de la metodología estructurada de acuerdo al criterio de cada auditor
- Promover la comunicación en todo momento del auditor con el personal a su cargo, y notificar las adecuaciones posibles a la metodología
- Capacitar al personal sobre el uso correcto de la metodología estructurada, de acuerdo a la participación de cada uno
- Verificar la normatividad existente en la organización
- Dar a conocer adecuadamente los métodos, herramientas y técnicas planteadas en la realización de la auditoría
- Verificar aspectos determinados por la organización en la función de la auditoría en informática

Existen diversas metodologías para desarrollar una auditoría, en general todas se pueden considerar como buenas, la aplicación de cualquiera de estas dependerá de la experiencia del auditor, la identificación que tenga hacia esta, o bien del objetivo y alcance de su trabajo en particular.

A continuación se hará mención a las etapas básicas que un auditor debe considerar en la realización de su trabajo, estás pueden ser fácilmente adaptada a cualquier área en la que se vaya a realizar la auditoría.

1. ACTIVIDADES PREVIAS

1.1 Conocimiento general del área a revisar.
Deberá de realizarse una inmersión al área o sistema a revisar, conociendo la cantidad de equipos, tipos de equipos, software utilizado, estructura del área, etc.

1.2 Definición de objetos y alcances.
Al inicio de toda revisión de deben de establecer claramente los objetivos que se pretenden alcanzar y el alcance esperado a cubrirse durante la revisión.

1.3 Preparar el programa de trabajo.
Se deben de establecer las fechas de inicio y final de la revisión, las actividades a cubrir y los tiempos estimados a cada actividad (Gráfica de Gantt).

1.4 De ser necesario, preparar una carta de presentación.
Deberá de realizarse una carta de presentación firmada por el representante del área de auditoría dirigida al responsable del área a revisar, indicando en ella el motivo de la revisión.

1.5 Conocimiento previo sobre las políticas y procedimientos existentes.
Verificar y conocer la existencia de alguna normatividad vigente a donde se dicten la observancia obligatoria de controles y con ello proceder a preparar pruebas de cumplimiento y material de apoyo para revisar el acatamiento de las mismas.

1.6 Preparación de pruebas de cumplimiento.
En ésta fase se deberá de preparar el material suficiente para la realización de todo tipo de pruebas generales y específicas, necesarias para cubrir el alcance de la revisión.

1.7 Preparación de material de apoyo.
En ésta fase, deberá de prepararse los cuestionarios, checklist, etc., que apoyarán durante la revisión.

2. ACTIVIDADES INTERMEDIAS

2.1 Comunicación formal con las autoridades de las áreas a auditar.

2.2 Levantamiento de información.
En ésta etapa el auditor se apoya en el material previamente desarrollado y a su vez se apoya para conseguir la misma aplicando las diferentes técnicas de auditoría. El levantamiento de información, nos permitirá conocer los puntos que nos lleven al objetivo y alcance planteado inicialmente.

2.3 Pruebas de cumplimiento.
En ésta etapa deben de realizarse las pruebas de cumplimiento, definidas con anterioridad.

2.4 Análisis de la información.
En ésta etapa es donde se requiere de mayor experiencia del auditor para detectar debilidades de control. Es aquí donde se debe de identificar las observaciones, a través del análisis de la información recabada (checklist, cuestionarios, pruebas de cumplimiento, etc.) Aquí también es donde se deben de determinar las causas e impactos.

2.5 Papeles de trabajo.
Toda la información recabada que constituye un elemento de evidencia para las observaciones detectadas, deberán de ser referencias en un expediente que se le denominará papeles de trabajo.

2.6 Confirmación de observaciones.
Es contar con la evidencia completa de lo que el auditor observó en su evaluación, en la que se utiliza la cédula de observación, que es la debilidad que se observa y que se plasma en dicha cédula a fin de comentarla con el responsable y obtener su comentario y firma.

3. ACTIVIDADES POSTERIORES

3.1 Identificación de niveles de riesgo.
Al respecto, es necesario identificar el nivel de riesgo a que está expuesta el área que se está revisando, a través de un análisis y un peso a cada una de las observaciones. Los niveles de riesgo existentes, son:

a) Inminente, cuando el problema está presente, ó en su defecto puede generar pérdidas cuantiosas a la institución

b) Potencial, cuando el problema aún no está presente pero es muy probable que ocurra

c) Controlable, es cuando es poco probable que ocurra o puede generar pérdidas mínimas a la institución

El riesgo, viene siendo el impacto de la observación afectada.

3.2 Consolidación de niveles de riesgo.
Después de haber identificado los niveles de riesgo, es necesario consolidar ó agrupar observaciones comunes, con objeto de presentar agrupadas las debilidades y sugerencias, mismas que servirán para generar el informe correspondiente.

3.3 Elaboración del informe correspondiente.
El producto final del auditor es su informe, por lo que éste deberá de elaborarse con objetividad y diligencia profesional.

3.4 Actividades finales de papeles de trabajo.
Los papeles de trabajo constituyen un conjunto de cédulas y documentos que el auditor obtuvo y en los que hará constar la descripción y el resultado de las pruebas realizadas ya que es la única comprobación para soportar lo mencionado en los informes.

2.5 ÁREAS DE PARTICIPACIÓN

La Auditoría en Informática puede estar relacionada con diferentes áreas de la empresa, es decir, puede influir y sugerir no solo en las áreas, sino también en los diferentes procedimientos que se realizan para beneficio de la misma.

Existen diferentes criterios para la determinación de área de participación, algunos criterios son la revisión hecha en base a las funciones, al nivel del sistema, la consecuencia de actividades, la combinación de las funciones, etc.

Sin embargo, un factor importante, independiente al criterio para la clasificación de las áreas de participación, es el alcance que el propio auditor debe darle a su revisión, donde el auditor en informática debe de definir cuál será el área objeto de estudio.

Esta definición puede ser desde luego una área completa de participación, o bien puede concretarse a la revisión de un solo elemento, componente, procedimiento, etc. A continuación se presentan algunas funciones en donde se puede aplicar la función de Auditoría en Informática:

Desarrollo y Modificación de Sistemas: El buen o mal diseño de un sistema de información, determinará su utilidad a la empresa y hará que esta lo integre o lo rechace.

El auditor en informática debe de participar sugiriendo el establecimiento de controles en cada una de las etapas del desarrollo del sistemas.

El objetivo general que persigue es disminuir los riesgos antes de liberar el sistema.

Por lo tanto el auditor en informática debe de conocer las fases en que se desarrolla un sistema de información.

Con este conocimiento previo y de acuerdo al alcance que el auditor le dé a su revisión se podrá participar activamente en está área de la informática.

Algo importante a tener en cuenta es que existen varios métodos de desarrollo de sistemas, cada empresa cuenta o debe de contar con su propia normatividad para el desarrollo de sistemas.

Sistemas de Aplicación: La evaluación y revisión de los controles en los sistemas permite verificar que los datos que se introducen y se actualizan estén completos, exactos y que sean válidos, que el proceso sea el

adecuado y que cumpla con los objetivos de su elaboración y que la información que se obtiene de estos se mantenga actualizada y que ésta sea útil para la empresa. Algunos aspectos que son posibles de implementar por la función de Auditoría en Informática se presentan a continuación:

- Evaluación o revisión de los controles en los sistemas, ya sea en desarrollo o producción
- Preparación de los datos
- Datos de entrada
- Procesamiento de datos
- Datos de salida
- Documentaciones
- Respaldo y recuperación de información
- Controles sobre el personal
- Diseño de controles para los sistemas

Sistemas en Producción: Los sistemas en producción son un conjunto de procedimientos manuales y computarizados interrelacionados entre sí y que persiguen un objetivo común, además de que constituyen un sistema que produce información relacionada con cierto tipo de operaciones o actividades que las empresas requieren.

Los sistemas en producción incluyen la información de las empresas, en cuyo procesamiento interviene una computadora.

En esta área, el auditor en informática deberá de tener un conocimiento general del sistema a auditar (aspectos manuales y aspectos computarizados) antes de iniciar su revisión.

De esta manera se podrá determinar aquellas funciones o módulos críticos a la que habrá necesidad de darle un alcance mayor.

Al auditar los sistemas en producción se deben de perseguir los objetivos de totalidad, exactitud, autorización, oportunidad, mantenimiento y utilidad de la información.

Centros de Cómputo (EDP): Un centro de procesamiento electrónico de datos es la unidad organizacional de una empresa en la cual se realizan actividades de proceso de datos, mediante la utilización de una o mas computadoras.

El auditor en informática deberá de efectuar, entre otras actividades, la revisión a los siguientes rubros:

- Administración.
- Seguridad lógica del equipo de cómputo.

- Seguridad física del equipo de cómputo.
- Operatividad de los sistemas en producción.
- Controles generales y operativos de las comunicaciones.

Redes y Telecomunicaciones: Con la rápida expansión de las telecomunicaciones se ha visto afectada la vulnerabilidad de la información que viaja a través de las redes de comunicaciones.

Este es uno de los aspectos que más se han descuidado en materia de seguridad, aunque ya actualmente se habla de sistemas de control de acceso, protección de datos, etc.

Como uno de los objetivos a seguir es, el control y la revisión continua de accesos a la información sugiriendo el establecimiento de controles en : Identificación, Autorización y Protección.

Como aspectos generales debe de cubrirse: administración, seguridad lógica, seguridad física y planes de contingencia.

Seguridad del Procesamiento de Datos: Se analiza y evalúa la seguridad física, los datos y el software. Se verifica si existen adecuados elementos de protección y salvaguarda para los mismos, como es la instalación de las computadoras, que los archivos no sufran alteraciones en los datos, manteniéndose la información completa, correcta y consistente; que el acceso a los programas sea restringido solo a personal especializado, que el software sea utilizado apropiadamente, etc. Algunos elementos a revisar son los siguientes:

- Revisión de las políticas, procedimientos y estándares de seguridad.
- Evaluación de la seguridad física.
- Evaluación de la seguridad de los datos.
- Evaluación de la seguridad de los sistemas de aplicación.
- Evaluación de la seguridad del software del sistema.
- Evaluación de la seguridad en base de datos.

Planes de Contingencia (Recuperación en caso de desastres):

La revisión de políticas y procedimientos relacionados con la planeación de los procesos en caso de desastre permiten determinar el grado de previsión que una empresa ha tomado para minimizar el riesgo o exposición ante la eventual ocurrencia de un desastre de origen natural o causado por el hombre, que pueda afectar en forma parcial o total las operaciones del

negocio, de forma tal que reduzca la pérdida de información vital, el daño en los equipos y el deterioro de la imagen. Los aspectos a auditar se listan a continuación:

- Análisis y cuantificación de riesgos a que está expuesta la organización en caso de contingencia
- Revisión del Plan de Contingencia
- Listar los recursos de hardware y software que puedan necesitarse para reiniciar las operaciones
- Probar eficientemente los planes de contingencia con respaldos de programas de las siguientes áreas: sistema operativo, software de aplicaciones y documentación.

Capítulo 3
TÉCNICAS DE AUDITORÍA EN INFORMÁTICA

3.1 TÉCNICAS DE AUDITORÍA

Las técnicas de auditoria están orientadas fundamentalmente hacia la auditoría de estados financieros ; sin embargo, estas pueden aplicarse a cualquier tipo de auditoría.

"Las técnicas de auditoría son los métodos prácticos de investigación y prueba que el auditor utiliza para lograr la información y comprobación necesaria para poder emitir su opinión profesional."[10]

Las técnicas de auditoría son las siguientes:

a) Estudio General.- Apreciación sobre la fisonomía o características generales de la empresa, de sus estados financieros y de las partes importantes, significativas o extraordinarias.

El estudio general, deberá aplicarse con mucho cuidado y diligencia, por lo que es recomendable que su aplicación la lleve a cabo un auditor con preparación, experiencia y madurez, para asegurar un juicio profesional sólido y amplio.

b) Análisis.- Clasificación y agrupación de los distintos elementos individuales que forman una cuenta o una partida determinada, de tal manera que los grupos constituyan unidades homogéneas y significativas.

c) Inspección.- Examen físico de bienes materiales o de documentos con el objeto de cerciorarse de la autenticidad de un activo o de una operación registrada o presentada en los estados financieros.

d) Confirmación.- Obtención de una comunicación escrita de una persona independiente de la empresa examinada, y que se encuentre en posibilidad de conocer la naturaleza y condiciones de la operación, y por lo tanto, de informar de una manera válida sobre ella.

Esta técnica se aplica solicitando a la empresa auditada que se dirija a la persona a quien se pide la confirmación, para que conteste por escrito al auditor, dándole la información que se solicita.

e) Investigación.- Obtención de información, datos y comentarios de los funcionarios y empleados de la propia empresa.

[10] Santillana González, Juan Ramón, Conoce las Auditorias, Ed. ECASA, México 1990

Con esta técnica el auditor puede obtener conocimiento y formarse un juicio sobre algunas operaciones realizadas por la empresa.

f) Declaración.- Manifestación por escrito con la firma de los interesados del resultado de las investigaciones realizadas con los funcionarios y empleados de la empresa.

Está técnica se aplica cuando la importancia de los datos o el resultado de las investigaciones realizadas lo amérita.

g) Certificación.- Obtención de un documento en el que se asegure la verdad de un hecho, legalizado por lo general, con la firma de una autoridad.

h) Observación.- Presencia física de como se realizan ciertas operaciones o hechos.

El auditor se cerciora de la forma como se realizan ciertas operaciones, *dándose cuenta ocularmente* de la forma como el personal de la empresa las realiza.

I) Cálculo.- Verificación *matemática de alguna partida.*

Hay partidas en la contabilidad que son resultado de cómputos realizados sobre bases predeterminadas; el auditor puede *cerciorarse de la corrección* matemática de estas partidas mediante el cálculo independiente de las mismas.

3.1.1 Procedimientos de Auditoría

La combinación en la práctica de dos o más técnicas de auditoria da origen a los denominados procedimientos de auditoría.

"Los *procedimientos de auditoría* son el conjunto de técnicas de investigación aplicables a un grupo de hechos mediante los cuales el auditor obtiene las bases para fundamentar su opinión."[11]

Debido a que generalmente el auditor no puede obtener el conocimiento que necesita para fundamentar su opinión en una sola prueba, es necesario examinar cada partida o conjunto de hechos mediante varias técnicas de aplicación simultánea o sucesiva.

[11] Santillana Gonzàlez, Juan Ramòn, Conoce las Auditorias, Ed. ECASA, Mèxico 1990

Naturaleza de los Procedimientos de Auditoría

Los diferentes sistemas de organización, control, hacen imposible establecer sistemas rígidos de pruebas. Por esta razón el auditor deberá, aplicando su criterio profesional, decidir cuál técnica o procedimiento de auditoría o conjunto de ellos, serán aplicables en cada caso para obtener una opinión objetiva y profesional.

Extensión o alcance de los Procedimientos de Auditoría

La relación de las partidas examinadas con el total de las partidas individuales que forman el universo, es lo que se conoce como extensión o alcance de los procedimientos de auditoría y su determinación es uno de los elementos más importantes en la planeación de la propia auditoría.

Oportunidad de los Procedimientos de Auditoría

A la época en que los procedimientos de auditoría se van aplicar, se le llama oportunidad.

En el curso de la revisión debemos poner lo mejor de nosotros mismos, hasta llegar a la certeza moral de obtener una base sólida para fundamentar una opinión; y ese mínimo de seguridad lo ofrece la aplicación de los procedimientos oficialmente aprobados . Sin embargo, habrá ocasiones en que la naturaleza de las operaciones, el tipo de empresa o circunstancias que priven en la revisión, no permitan utilizar los procedimientos aprobados y, en este caso, habrán de utilizarse los recursos de la experiencia, para que a través del uso de diferentes técnicas, se diseñe un procedimiento especial de revisión, adecuado a las circunstancias, hasta obtener la evidencia que permita fundar una opinión.

Bajo este aspecto, se puede concluir que, dado el caso, se puede, durante la revisión, prescindir de algunos procedimientos, adecuar otros a las circunstancias específicas de la revisión o, incluso, en el extremo, diseñar procedimientos especiales aplicables únicamente para el caso especial que se está revisando.

3.1.2 Herramientas de Auditoría

"Es el conjunto de elementos físicos utilizados para llevar a cabo acciones y pasos definidos en la técnica."[12] Antes del auge de las computadoras, así como de otros elementos tecnológicos relacionados con la ingeniería, arquitectura, etc., dichas herramientas eran simples máquinas o utensilios anuales que apoyaban el desarrollo de las tareas de cada uno de los proyectos. Algunos ejemplos de herramientas son los siguientes:

[12] Alvarez Solis, Fco. Javier, Apuntes de Seguridad y Auditoria en Informàtica, IPN

* Procesadores de palabras (documentación, entrevistas, cuestionarios,etc.)
* Diagramadores (diagramas de flujo, organizacionales, etc.)
* Graficadores (estadísticas, estimación de actividades en tiempo, costos, etc.)
* Productos CASE (modelado de datos, modelado de procesos, validación de datos y procesos, generadores de diccionarios de datos, generadores de código, documentación, etc.)
* Microcomputadoras
* Cuestionarios
* CheckList's

3.2 TÉCNICAS PARA AUDITAR EL ÁREA INFORMÁTICA

Los auditores internos tienen adoptados varios métodos de procesamiento para ser utilizados en la Auditoría Informática. El desarrollo de éstas técnicas y herramientas tienen un desarrollo evolutivo que va de acuerdo con el avance de la tecnología y la influencia misma de las demás técnicas.

Tradicionalmente una Auditoría Informática se lleva a cabo en tres etapas.

1. Revisión inicial

En ésta etapa, el auditor se familiariza con el área que va a auditar. Para ello recolecta para su estudio, entre otras cosas, los organigramas, las descripciones de puestos, procedimientos, estructura básica del control de la aplicación, secuencia del proceso, controles, etc. El resultado de esta etapa es un plan específico de auditoría.

2. Revisión detallada y evaluación

Esta fase de revisión y evaluación se realiza sobre los controles internos, procedimientos de proceso, archivos maestros, rastreo de transacciones, análisis de registros y de bitácora de control.

3. Pruebas y reportes

En está etapa se llevan a cabo pruebas para verificar el cumplimiento de los controles establecidos y verificar los registros seleccionados.

Esta fase produce la evidencia del cumplimiento de procedimientos y la evidencia de que los datos han sido procesados con exactitud y en forma completa.

3.2.1 Auditoría de las Aplicaciones

La auditoría de las aplicaciones se llevará acabo en aquellos sistemas que ya se encuentran en operación o explotación normal, estos sistemas pueden haber sido objeto de una intervención por parte del Auditor en Informática, o haber sido desarrollados sin ninguna intervención del mismo, por ser muy antiguos, por falta de coordinación con Auditoría, o por la ausencia de esta en el momento de su desarrollo.

Es en esta área de la Auditoria en Informática en donde se han desarrollado más técnicas, ya que es aquí donde se realiza el procesamiento de las operaciones que generan la información base para la toma de decisiones, por lo que un error se traduciría en problemas y quizás hasta perdidas en la organización.

OBJETIVOS

- Valorar la suficiencia de los controles incorporados en los programas como en los procedimientos que aseguren el nivel de confiabilidad.
- Verificar que el sistema sea comprensible, tanto para los usuarios como para terceras personas.
- Validar que el sistema sea auditable.
- Verificar que las políticas internas, externas y el apego a los estándares de la empresa sean respetados.
- Analizar la flexibilidad del sistema.

TÉCNICAS DE LA AUDITORÍA DE LAS APLICACIONES

Estas técnicas de Auditoria le servirán al auditor para alcanzar los objetivos que persigue y le permitirán decidir sobre la oportunidad de su aplicación.

- ✓ Método de Datos de Prueba.- Este método verifica la calidad del proceso al ejecutar los sistemas, utilizando grupos de datos de entrada especialmente preparados para obtener resultados preestablecidos.

- ✓ Sistema de Valuación de un Caso de Estudio.- Se utiliza para un grupo estandarizado de datos (entradas, parámetros y salidas) para la prueba de un sistema, siendo definidos por el usuario, con la participación del auditor.

- ✓ Prueba Integrada.- Está técnica revisa aquellas funciones de una aplicación automatizada que son internas del computador, permitiendo al auditor examinar el proceso de una aplicación en su ambiente normal de operación.

3.2.2 Técnicas para la Administración de la Auditoría

3.2.2.1 Selección del Área a Auditar

Es una técnica aplicable a organizaciones multidepartamentales; ayuda al auditor a determinar cuales son las principales áreas a ser revisadas.

Consiste en recolectar y evaluar estadísticas de operación de áreas seleccionadas, para identificar variaciones inesperadas. Usa programas para comparar estimados de valores esperados con valores reales, para identificar diferencias potencialmente importantes. Cabe señalar que existe un constante monitoreo a las áreas seleccionadas por medio de indicadores.

Esta técnica es la más aplicada entre las organizaciones con operaciones similares entre sus departamentos. El indicador puede ser comparado con criterios preestablecidos e historial de desempeño por departamento.

La información es mostrada en forma de matriz, permitiendo hacer fáciles comparaciones de los actuales datos de un departamento en particular.

El indicador no puede ser desarrollado para todas las áreas de interés del auditor interno, reconociendo éste último la limitante de ésta técnica.

OBJETIVO

El objetivo de esta técnica es optimizar el uso de los recursos limitados del auditor interno, localizando con toda precisión los posibles problemas dentro de los departamentos, así se hace una directa atención del auditor para esas áreas de mayor interés.

EMPLEO DE LA TÉCNICA

1. Identificar los indicadores que serán usados para evaluar el desempeño de los departamentos. El principal factor a indicar es el que tiene mayor grado de exposición del área funcional.

2. Asignar un determinado valor al indicador.

3. Desarrollar un programa de computadora para la aplicación de la técnica, éste es el que provee los reportes de los resultados del área auditada, que dependen directamente de la accesibilidad y necesidad de los datos.

EVALUACIÓN DE LA EFECTIVIDAD

Auditar por medio de ésta técnica puede significar beneficios para el manejo interno de auditoría y el establecimiento de planes internos, además de un mejor aprovechamiento de recursos. Se puede localizar eficientemente las áreas de mayor riesgo o exposición y pérdida de control.

En organizaciones en las que se tienen múltiples sistemas planeados en operación no se pasa por alto la utilización de ésta técnica.

La efectividad que reporta dicha técnica va en proporción de la cantidad de control que se tenga de las aplicaciones, así como de los recursos de que disponen las mismas.

Una desventaja es que los indicadores utilizados no pueden desarrollarse para todas y cada una de las áreas de interés del auditor, por lo que algunas de ellas deben ser evaluadas por alguna otra técnica.

Todas las aplicaciones y herramientas deben estar colocadas en su sitio para una correcta revisión de las mismas. Las aplicaciones cumplirán con las políticas de desarrollo para poder ser auditadas con precisión.

3.2.2.2Auditoría de Software en Múltiples Localidades

Esta técnica puede ser mejor empleada en organizaciones que tienen centros de cómputo centralizados y sistemas de desarrollo y programación staff.

Es la preparación centralizada del software de auditoría y en su distribución a distintas localidades de la empresa para que sean empleadas por grupos de auditores informáticos descentralizados dentro de una misma organización.

Se desarrolla un sólo paquete de software para ser usado en varios centros de cómputo. De ésta manera se concentra la habilidad y capacidad de desarrollo de software para auditoría interna. Elimina el costo resultante de los esfuerzos de desarrollo independientes y descentralizados. Además, se estimula la práctica consistente de la auditoría en toda la empresa.

OBJETIVO

El objetivo de esta técnica es hacer un mejor uso de los recursos de auditoría y aprovechar la estandarización de herramientas, así como estimular la práctica consistente de la auditoria.

EMPLEO DE LA TÉCNICA

Porque una auditoría puede correrse desde un punto remoto, es importante que la documentación este actualizada, la siguiente narrativa nos describe la forma de uso de ésta técnica.

Requerimos de una breve descripción del paquete de auditoría propuesto, los objetivos y un índice del contenido del mismo. Los nombres de los programas a ser auditados, así como los parámetros y salidas de las funciones de cada programa. Un conjunto de lenguajes de control. La descripción detallada del software de auditoria propuesto. Intrucciones de operación cpmpletas para procesamiento central.

Cuando hablemos de un paquete puede ser un producto derivado de anteriores auditorías o un conjunto de programas hechos a la medida.

Se corre el paquete desde cualquiera de las localidades y se registra y compara con cada uno de los documentos anteriormente citados, de ahí deriva la importancia de la actualización de la documentación. Cuando no concuerdan se elabora un reporte con el que se hará una posterior revisión de las causas por las cuales la información documentada y la que está funcionando es diferente.

El cuidado que debe tenerse es durante los enlaces, ya que la información no debe desvirtuarse de su origen a su destino. Las técnicas para transmisión entre localidades son muchas y muy variadas.

El tiempo empleado para el desarrollo de una aplicación varía en semanas. El tiempo de operación es muy variable y depende de cuánto será extraído y de los reportes requeridos.
Los costos semejantes al desarrollo y esfuerzo son dependientes de la complejidad de los proyectos.

EVALUACIÓN DE LA EFECTIVIDAD

Una ventaja de la utilización de la técnica es que se puede realizar una auditoría corporativa desde cualquier parte de la organización. A la vez resultando una desventaja por los costos de transmisión.

3.2.2.3 Auditoría Centralizada

Una auditoría centralizada está basada en un computador central establecido en un departamento, el cual es el responsable de la ejecución de auditorías a los programas. El computador recibe datos de archivos desde otros departamentos, efectúa la auditoría y distribuye los reportes resultantes a los auditores internos. Esta técnica es aplicable a organizaciones multidepartamentales y cuyas operaciones básicas estén automatizadas.

A través de ésta técnica la auditoría se vuelve centralizada, de ésta forma se eliminan muchos de aquellos problemas que pueden ser encontrados durante la ejecución de software de auditoría en múltiples departamentos.

La capacidad para realizar auditorias se tiene en una instalación o en una sola unidad.

OBJETIVO

Centralizar el desarrollo y ejecución de programas de auditoría, así como eliminar la distribución del software y encaminar el entrenamiento de auditores a una sola unidad de la organización.

EMPLEO DE LA TÉCNICA

Eligiéndose las aplicaciones que van a ser procesadas, se solicita la documentación y aplicación correspondiente. El proceso se lleva a cabo en un procesador central. A cada aplicación se le realizan las pruebas pertinentes con una sola clase de software.

Los resultados de las pruebas se analizan y evalúan, turnándose los posibles errores a los responsables de los sistemas.

El estudio del establecimiento de una auditoría centralizada debe arrojar valores con los que se considere costeable la formación de dicha unidad.

EVALUACIÓN DE LA EFECTIVIDAD

La efectividad de está técnica radica principalmente en el uso de métodos estándares para sus aplicaciones ya que correr sus auditorías desde un sitio central. Las organizaciones utilizan éste tipo de técnicas para participar en la revisión sobre el uso de las herramientas de auditoría durante una operación normal.

3.2.3 Técnicas para la Prueba de Controles en los Programas

Este conjunto de técnicas y herramientas son usadas para probar rutinas, programas o aplicaciones completas para evaluar controles o verificar la exactitud del proceso y el cumplimiento de procedimientos de procesos específicos.

3.2.3.1 Sistema de Casos Base Prueba

Está técnica ejecuta programas usando archivos de prueba desarrollados como parte de un programa completo de pruebas, y verifica la exactitud del proceso, con resultados de datos de datos prueba determinados.

Usa datos prueba desarrollados por los auditores y usuarios en cooperación con el personal de desarrollo de sistemas para lograr una extensa prueba de los programas o aplicaciones.

Un caso base se establece cuando suficientes transacciones han sido procesadas por una aplicación y para asegurar que todas las funciones programadas hayan sido ejecutadas.

El archivo caso base se pretende que sea usado para verificar la correcta operación del sistema antes de su aceptación o producción, así como para verificar periódicamente la integridad del proceso después de la aceptación en producción.

Después del análisis preliminar y la facilidad de asistir a la preparación de los requerimientos de planeación del paquete, se compone un grupo de "base case" integrado por usuarios de departamento y personal de sistemas,

comenzando su participación con la prueba estratégica de procedimientos y aplicaciones específicas.

El grupo desarrollará formatos, planes y otros tipos de prueba que incluyan los códigos de las transacciones y los archivos internos requeridos.

3.2.3.2 Operación Paralela

Está técnica se utiliza para verificar la exactitud de programas nuevos o modificados, procesando archivos o datos de producción, usando tanto los procedimientos existentes y comparando los resultados del proceso para identificar diferencias inesperadas.

Está técnica es ampliamente usada por el personal de informática para verificar programas nuevos o modificados antes de reemplazar los procedimientos existentes.

La verificación de programas debe concentrarse en la forma en que estén estructuradas las aplicaciones, dado que deben funcionar de una manera simultánea dos sistemas produciendo los mismos resultados.

Se deben codificar programas para crear un duplicado de los sistemas en funcionamiento. Estos deberán respetar las condiciones que cumplen las demás aplicaciones.

Las entradas, así como las salidas de los sistemas que han de probarse deberán ser validadas y generar los mismos reportes que los sistemas de operación paralela. Los procesos por lo general no son revisados desde el punto de vista del auditor, sino que a nivel sistemas se evalúan y se identifican los posibles cambios que pudiesen haber ocurrido sin haberse registrado en algún documento.

3.2.4 Técnicas de Verificación de Transacciones

3.2.4.1 Auditoría Desde una Terminal

Al auditar alrededor del computador, los resultados del procesamiento por el computador son verificados manualmente contra los datos fuentes que fueron introducidos al computador. Las pruebas se hacen sobre una base de muestreo o mediante la comparación de saldos totales. Está técnica esta orientada a los resultados obtenidos.

Los productos finales son fácilmente identificados y son utilizados como medida de la confiabilidad del procesamiento.

OBJETIVO

Obtener resultados del procesamiento por el computador para ser analizados y verificados manualmente contra los datos fuente que fueron introducidos al computador. Por lo que su objetivo radica principalmente en la obtención de los resultados.

EMPLEO DE LA TÉCNICA

Para la aplicación de está técnica se debe determinar que existan datos de salida para facilitar el cálculo manual de los procesos y controles que se examinan, así como desarrollar métodos para obtener las muestras representativas de las transacciones para que el auditor verifique manualmente cada control o paso de procesamiento en que desee confiar.

Como toda auditoría, es necesario iniciar una auditoría alrededor del computador definiendo los objetivos específicos del trabajo. Con este enfoque el auditor debe empezar por seleccionar los datos de salida que van a probarse; posteriormente, examinar los datos de entrada correspondientes a la aplicación, para determinar la razón y exactitud de los datos de salida seleccionados. Ya identificados los datos de salida que van a probarse, el auditor debe de obtener los datos de salida correspondientes.

Una vez que se han identificado los datos de salida y obtenido los datos de entrada correspondientes, el auditor está listo para efectuar los cálculos de la aplicación.

EVALUACIÓN DE LA EFECTIVIDAD

Está técnica como su objetivo lo dice, esta orientada a los resultados, por lo que resulta efectiva ya que los productos son fácilmente identificables y pueden ser utilizados como una medida de confiabilidad del procesamiento.

3.2.5 Técnicas para Auditar el Desarrollo de Aplicaciones

3.2.5.1 Auditoría de Post-Instalación

La técnica de Auditoría de post-instalación describe los procedimientos estándares y formales que se deben llevar a cabo al examinar las aplicaciones una vez que éstas se han liberado en una producción normal. Al hecho de haber incorporado algunos controles durante el desarrollo del sistema no garantiza que vayan a funcionar adecuadamente una vez que éste se encuentre en operación.

Esta técnica proporciona un método adecuado y sistemático para que los auditores examinen la efectiivdad de estos controles en un ambiente operacional.

Las auditorías de post-instalación se deben realizar periódicamente, sin embargo el momento ideal para ejecutar es dentro de los tres a seis después de que el sistema se ha liberado. En este punto los problemas de inicio ya se han superado y el personal de operación se encuentra familiarizado en el sistema.
El objetivo de esta técnica es verificar el apego y cumplimiento de políticas y procedimientos y determinar si el sistema está obteniendo los resultados para los cuales fue desarrollado.

Esta técnica no se limita a los programas de computadora sino que incluye las interfaces manuales a través del sistema por lo que cubre todas las operaciones desde la preparación del documento fuente hasta la utilización de las salidas reflejadas en reportes.

En consecuencia, esta técnica incluye las funciones manuales relativas al sistema.
El alcance de la auditoría de post-instalación puede ser extenso o bien limitado dependiendo de los objetivos de la auditoría, en cualquier caso estos objetivos deberán ser definidos previo al inicio del trabajo.

3.2.5.2 Guías de Control utilizadas durante el Desarrollo del Sistema

El momento ideal para el auditor de incorporar controles en una aplicación de computadora es durante la fase de desarrollo del sistema. Durante esta fase, los cambios y adiciones al Sistema de Control Interno pueden ser realizados con un costo y esfuerzo considerablemente menor, no así cuando el sistema se ha liberado.

Los auditores ya han comenzado a involucrarse en la fase de diseño. Su participación pretende asegurar que el Sistema de Control Interno especificado por el analista proporcione confianza en la integridad de la aplicación.

En este trabajo es de vital importancia que el auditor conserve su total independencia por lo cual éste no depende estructuralmente de los líderes de proyecto y no especifica controles, sino que revisa y hace recomendaciones para mejorar el nivel de control planeado.

Se puede tener como apoyo guías de control que indiquen el marco de referencia en al cuál se deben enmarcar los sistemas institucionalmente.

El auditor al revisar los controles del sistema durante las etapas de desarrollo, tiene la oportunidad de interactuar con los diseñadores del sistema cuando es menos problemático y costoso el realizar cambios. La Auditoría tradicional solicitará una revisión una vez que el sistema ha sido liberado lo que ha probado ser demasiado costoso en la eventualidad de cambios a sugerencia del cuerpo de Auditoría.

El auditor recibe copias de la documentación del sistema, participa en las juntas de trabajo del cuerpo de desarrollo y tiene la oportunidad de sugerir controles y modificaciones.

Las guías de control tienen dos ventajas:

- Ayudan a asegurar que el grupo de desarrollo incorpore controles importantes para la empresa.

- Ayudan a evitar las interrupciones y gastos de modificaciones una vez que el sistema se encuentra en producción.

3.2.5.3 Ciclo de vida del Desarrollo de Sistemas

Esta técnica codifica la estructura intrínseca del proceso de desarrollo de sistemas en fases, e identifica puntos de Control de Calidad al final de las tareas críticas en las fases.

En estos puntos los auditores observan y evalúan el avance y los productos para asegurarse de la auditabilidad del sistema y de que los controles previstos son adecuados y han sido ejecutados de la misma forma. Un ejemplo de las fases a seguir es el siguiente:

⇒ Definición del proyecto
⇒ Diseño del sistema
⇒ Diseño detallado y programación
⇒ Prueba del sistema
⇒ Conversiones

Cada fase es posteriormente dividida en tareas. Al final de cada tarea crítica y al final de cada fase, se hace una revisión detallada para determinar si los objetivos del sistema se siguen cumpliendo.

En los puntos de intervención del auditor, éste revisará la organización del proyecto, el apego a la planeación y avance en cada fase, la obtención de costos, el diseño de documentos fuente, la estructuración de los archivos, los controles incorporados, las necesidades de recursos máquina, el apego a estándares, la integración y resultados de las pruebas y mostrará sus conclusiones en un reporte que señale sus resultados.

Estimando el tiempo en porcentaje de intervención del Auditor en Informática en cada una de las fases, éste quedaría como sigue:

FASE	PORCENTAJE DE TIEMPO DEL AUDITOR
Definición del proyecto	20%
Diseño del sistema	30%
Diseño detallado y programación	20%
Prueba del sistema	20%
Conversión	10%

3.2.5.4 Grupo de Control y Aceptación del Sistema

Cuando el auditor determina probar el proceso de desarrollo de sistemas, se enfrenta al reto de cómo realizar de mejor forma esta revisión. A pesar de que la esencia de la revisión no cambia, el Auditor en Informática puede seleccionar entre hacer la revisión el mismo o descansar en los esfuerzos de otro grupo.

Realizar la revisión por si mismo, es la opción seleccionada por muchos auditores, a pesar de que se requiere de un entrenamiento y esfuerzo sustancial para hacer un buen trabajo. El hecho de que mucho de este entrenamiento tiene que ver con el procesamiento de datos en lugar de Auditoría en Informática, entre otros factores, ha llevado a utilizar un grupo especial de control y aceptación para crear y mantener estándares efectivos de desarrollo, particularmente en la auditabilidad del sistema.

Este grupo forma parte del Desarrollo de Procesamiento de Datos y su función es la de revisar y monitorear continuamente el desarrollo de aplicaciones significativas.

Capítulo 4
APLICACIÓN DE TÉCNICAS DE AUDITORÍA INFORMÁTICA
A LA DIRECCIÓN DE CONTROL Y EVALUACIÓN DE LA DIRECCIÓN GENERAL DEL DESTINO DE LOS BIENES DE COMERCIO EXTERIOR PROPIEDAD DEL FISCO FEDERAL

Hasta ahora se ha dado un marco teórico que nos da una idea general de la importancia y de los beneficios que se pueden obtener al aplicar una Auditoría en Informática.

Y para comprobar dichas aseveraciones se realizó una Auditoría a la Dirección de Control y Evaluación, en la cual se tomo como guía la metodología propuesta en el capítulo dos, utilizando en cada una de las etapas las técnicas y herramientas para Auditoría. A continuación se presentan las actividades y resultados obtenidos en cada una de las etapas.

4.1 SOLICITUD DE AUTORIZACIÓN PARA LA REALIZACIÓN DE AUDITORIA

4.1.1 Carta de Solicitud de Autorización

Se elaboró una carta de presentación en la que se solicitó autorización para el acceso y realización del trabajo de Auditoría a la Dirección de Control y Evaluación de la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal -DGDBCEPFF-. (ver anexo 1)

4.1.2 Carta de Solicitud de Requerimientos

Una vez aceptada la carta de presentación, para recabar información general de la empresa y del área a auditar, se elaboró un documento donde se requirió a la Dirección de Control y Evaluación una serie de elementos, tales como: antecedentes de la empresa, objetivo y funciones, organigrama, políticas y procedimientos del área, descripción de puestos, etc. (ver anexo2).

4.2 ANÁLISIS GENERAL DE LA EMPRESA (Dirección General)

El primer paso a dar, previo al inicio de un trabajo de auditoría, y cualquiera que sea el tipo de ésta, es el de allegarse de un conocimiento o "identificación" con la entidad que estará sujeta a auditoría, independientemente del área o funciones que vayan a ser revisados. Esta acción es indispensable para detectar el origen,

planes, condiciones y objetivos de la entidad; así como en específico, de la unidad de trabajo. A continuación se presenta un resumen de la información obtenida.

4.2.1 Antecedentes

Derivado de las atribuciones que emanan de la Ley Orgánica de la Administración Pública Federal, la Ley Aduanera y el Reglamento Interior de la Secretaría de Hacienda y Crédito Público, se han conferido facultades para determinar el destino de las mercancías de comercio exterior que pasen a propiedad del Fisco Federal.

El primer antecedente de reglamentación existente dentro de la Administración Pública Federal para determinar el destino de las mercancías que pasen a propiedad del Fisco Federal, es el Acuerdo del 29 de junio de 1983, publicado en el Diario Oficial de la Federación el 14 de julio de 1983, el cual se emitió con fundamento en el artículo 4o. de la Ley Reglamentaria del segundo párrafo del artículo 31 de la Constitución Política de los Estados Unidos Mexicanos.

El citado artículo disponía que las mercancías de importación prohibida que se introdujeran en el país, pasarían a propiedad del Fisco Federal y a control de la Secretaría de Hacienda y Crédito Público, asimismo señalaba que se procuraría la venta de las mismas fuera del país, por lo cual fue necesario la emisión del referido Acuerdo, el cual pretendía reglamentar el destino de automóviles, vehículos de carga, aeronaves y embarcaciones, concediéndosele al entonces Subsecretario de Inspección Fiscal dentro de esta Secretaría, las facultades de ceder, asignar, o venderlos a las dependencias y entidades oficiales.

Como complemento del Acuerdo antes mencionado, se promulgó la Convención entre México y los Estados Unidos de Norte América para la recuperación y devolución de vehículos y aeronaves robados en materia de disposición ilícita, firmada entre ambos gobiernos el 15 de enero de 1981, aprobada por la Cámara de Senadores del H. Congreso de la Unión el 3 de diciembre de 1981, y finalmente ratificada por ambos países el 28 de junio de 1983, Convención que tuvo como antecedente su similar pactada en el año de 1936.

Con base en la Convención vigente se concretó la obligación de ambos países de notificar a su similar la detección de vehículos reportados como robados, los requisitos para proceder a su devolución, así como el compromiso de no establecer impuestos, multas o sanciones sobre los vehículos, tomándose en consideración para las determinaciones adoptadas en el destino de los mismos.

Con fecha 9 de marzo de 1989 es publicado en el Diario Oficial de la Federación el Acuerdo, a través del cual se dispone de un órgano encargado de establecer las reglas para determinar el destino de las mercancías que pasen a propiedad del Fisco Federal.

El acuerdo dispuso que la ejecución la realizaría una institución fiduciaria que actuaría por cuenta y orden del Gobierno Federal a través de esta Secretaría por medio de un Grupo Coordinador, integrado por diversos funcionarios como el Oficial Mayor, el titular de la Unidad de Contraloría Interna, y el Director General de Aduanas, así como sendos representantes de la Coordinación de Asesores del Secretario de la Procuraduría Fiscal de la Federación y de la Tesorería de la Federación.

Además del establecimiento del Grupo Coordinador, otro punto legal trascendente fue la posibilidad de licitar las mencionadas mercancías en el interior del país, para lo cual, se fijaron reglas y criterios. El mencionado Acuerdo sufrió modificaciones a través de las reformas publicadas en el Diario Oficial de la Federación los días 1 de diciembre, y 14 de mayo de 1990, en las cuales se reguló la venta directa de mercancías y se dio intervención a la entonces Dirección General de Servicios y Recursos Materiales de la Secretaría.

Posteriormente, es publicado en el Diario Oficial de la Federación del 26 de abril de 1994, el Acuerdo por el que se crea el Consejo Asesor para la Determinación del Destino de las Mercancías que pasen a Propiedad del Fisco Federal, y reformado el mismo, el 9 de enero de 1995. Dicho Acuerdo, establece las bases de integración del Consejo y da formalidad a su actuación para opinar y asesorar a la Secretaría en la determinación del destino de las mercancías de comercio exterior que pasen a propiedad del Fisco Federal.

Así también, las disposiciones reglamentarias que facultan a la Secretaría de Hacienda y Crédito Público para determinar el destino de las mercancías de comercio exterior, previstas en los artículos 116, 116-A y 126 de la Ley Aduanera, son reformados por los relativos 144, 145 y 157 respectivamente, y se adiciona el artículo 32, publicados en el Diario Oficial de la Federación del 15 de diciembre de 1995.

Derivados de lo anterior, el C. Oficial Mayor podrá asignar en forma temporal o definitiva las mercancías de comercio exterior propiedad del Fisco Federal para uso de la propia Secretaría o bien para otras dependencias del Gobierno Federal, Entidades Paraestatales, Entidades Federativas y Municipios; así como, a los Poderes Legislativo y Judicial que lo soliciten.

Para llevar a cabo los destinos de donación y venta, la propia legislación aduanera establece que la Secretaría de Hacienda y Crédito Público deberá asesorarse de un Consejo integrado por instituciones filantrópicas y representantes de las Cámaras y Asociaciones de contribuyentes interesadas en la producción y comercialización de mercancías idénticas o similares a aquéllas.

Finalmente, con fundamento en el ordenamiento estipulado en el artículo 8o. del Reglamento interior de la Secretaría, por la atribución conferida al Oficial Mayor para determinar el destino de las mercancías, tanto de las que han pasado a propiedad del Fisco Federal, como de aquellas que habiendo sido objeto de

embargo precautorio, no se hubiere comprobado su legal estancia o tenencia en el país, en términos de los plazos fijados en la Ley Aduanera y hasta en tanto se pronuncia la resolución definitiva del procedimiento; se crea un órgano auxiliar de administración adscrito a la propia Oficialía Mayor, denominado Secretariado Ejecutivo del Consejo Asesor para la Determinación del Destino de las Mercancías de Comercio Exterior que pasen a Propiedad del Fisco Federal.

En virtud de la importancia de las responsabilidades y funciones asignadas al Secretariado Ejecutivo del Consejo Asesor, para instrumentar y ejecutar las acciones derivadas de la determinación de las mercancías de comercio exterior; el 30 de junio de 1997, mediante decreto que reformó, adicionó y derogó diversas disposiciones del Reglamento Interior de la Secretaría, en su artículo 69-A publicado en el Diario Oficial de la Federación, se transformó adscribiéndose orgánicamente como unidad administrativa bajo la denominación de Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, dependiente de la Oficialía Mayor, formalizándose sus facultades para el despacho de los asuntos de su competencia.

4.2.2 Objetivo y Funciones

Objetivo

Dirigir, planear y organizar las actividades necesarias para el control, administración y destino final de los bienes de comercio exterior que prevé la legislación aduanera, puestos a disposición de esta Dirección General, mediante la instrumentación de los acuerdos adoptados por los plenos del Consejo Asesor para la Determinación del Destino de las Mercancías que pasen a propiedad del Fisco Federal y del Comité de Asignación de Bienes al Sector Público, relativos a las operaciones de donación y venta de bienes; así como, de asignación, enajenación de excedentes detectados a maquiladoras o empresas con programas de exportación autorizados, destrucción, devolución, resarcimiento y pago de incentivos a entidades federativas adheridas en materia de Coordinación Fiscal, con sujeción al marco jurídico vigente.

Funciones

- Definir las políticas, procedimientos y criterios para la planeación, control y administración del destino de los bienes de comercio exterior que han pasado a propiedad del Fisco Federal, así como de aquellos que habiendo sido objeto de embargo precautorio, no se hubiere comprobado su legal estancia o tenencia en el país, de conformidad con los plazos fijados en la Ley Aduanera y en tanto se pronuncia la resolución definitiva del procedimiento administrativo instaurado.

- Instrumentar los criterios de opinión que determine el Pleno del Consejo Asesor, para seleccionar los bienes que han pasado a propiedad del Fisco Federal y/o puestos a disposición, que convenga sean donados a instituciones filantrópicas o no lucrativas autorizadas por la Secretaría para recibir donativos deducibles en el impuesto sobre la renta y, los que se consideren para su enajenación.

- Proponer e instrumentar las políticas, lineamientos y criterios sobre el destino de los bienes que han pasado a propiedad del Fisco Federal, así como las mercancías perecederas, de fácil descomposición o deterioro, de animales vivos o de automóviles y camiones, que sean objeto de embargo precautorio y que dentro de los diez días siguientes a su embargo, o de los cuarenta y cinco tratándose de automóviles y camiones, no se hubiere comprobado su legal estancia o tenencia en el país, puestos a disposición de esta Dirección General, que apruebe el Comité de Asignación de Bienes al Sector Público, para su asignación definitiva o temporal a las dependencias del Gobierno Federal, entidades paraestatales, entidades federativas, municipios y a los Poderes Legislativo y Judicial, así como en la destrucción de bienes.

- Resarcir o indemnizar por bienes dispuestos por esta Dirección General, en cumplimiento de resolución o sentencia que cause ejecutoria emitida por autoridad administrativa o judicial, mediante la devolución del mismo bien, y ante la imposibilidad práctica de esto, la entrega de un bien sustituto con valor similar, o en su caso, mediante el pago pecuniario que determine la autoridad competente, información que se hará del conocimiento posteriormente al Comité de Asignación de Bienes al Sector Público.

- Coordinar las acciones y operaciones de asignación definitiva de vehículos que pasen a propiedad del Fisco Federal, como pago de incentivos a las entidades federativas adheridas al Sistema Nacional de Coordinación Fiscal que tengan celebrados convenios en materia de colaboración administrativa, así como autorizar la venta de vehículos inutilizados permanentemente para su circulación, conforme a los establecido en la Ley de Coordinación Fiscal.

- Determinar y proponer la enajenación a la propia empresa objeto del embargo, de los bienes que hayan pasado a propiedad del Fisco Federal como consecuencia de excedentes detectados a maquiladoras o empresas con programas de exportación autorizados por la Secretaría de Comercio y Fomento Industrial, informando de ello al Comité de Asignación de Bienes al Sector Público.

- Integrar las carpetas de asuntos que serán sometidos a consideración de los plenos del Consejo Asesor y del Comité de Asignación de Bienes al Sector Público, previa revisión y aprobación del C. Oficial Mayor; así como efectuar las convocatorias para las reuniones de los mismos.

- Ordenar y practicar la identificación, recepción, traslado, maniobras, entrega, custodia, almacenaje y administración de los bienes de comercio exterior puestos a disposición de esta Dirección General; así como de todas aquellas actividades o actos necesarios para llevar a cabo el destino final de estos bienes.

- Coadyuvar al desalojo y movilidad de bienes de comercio exterior en los recintos fiscales y fiscalizados para evitar la saturación de éstos, el dispendio de los recursos y el decremento en la captación de los aprovechamientos en el caso de almacenes autorizados o concesionados, informando a estos últimos a través de las autoridades aduaneras, sobre los bienes en abandono que no serán sujetos de destino por parte de esta Dirección General.

- Controlar y supervisar los bienes de comercio exterior, que por su naturaleza de perecederos, animales vivos u otros, requieran de un destino inmediato, o bien, su destrucción por ser nocivos para la salud, prohibidos, representar riesgo, peligrosidad o toxicidad, en estado de descomposición, con apego a las disposiciones y reglamentación específica en materia aplicable, informando posteriormente al Consejo Asesor o al Comité de Asignación de Bienes al Sector Público.

- Dar seguimiento a los acuerdos adoptados por los plenos del Consejo Asesor y del Comité de Asignaciones de Bienes al Sector Público, de las operaciones de destino; así como, informar el estado que guardan para su cumplimiento.

- Establecer coordinación con las autoridades que directa o indirectamente estén involucradas con motivo del ejercicio de las facultades de esta Dirección.

- Instruir a la unidad administrativa que corresponda, se ponga a disposición de esta Dirección General, las mercancías de comercio exterior que han pasado a propiedad del Fisco Federal, así como aquellas perecederas, de fácil descomposición o deterioro, animales vivos o automóviles y camiones, que sean objeto de embargo precautorio y que dentro de los diez días siguientes a su embargo o de los cuarenta y cinco tratándose de automóviles y camiones, no se hubiere comprobado su legal estancia o tenencia en el país, así también requerir la documentación que sea necesaria para constatar la situación legal y administrativa que guardan los procedimientos instaurados y la integración de los expedientes.

- Instrumentar la comercialización de bienes, en forma directa, a través de un fideicomiso, o mediante mandato otorgado a una institución de crédito y ordenar la práctica de avalúos de los bienes de comercio exterior puestos a disposición, así como supervisar estas actividades.

- Instruir, dirigir y asegurar que los ingresos obtenidos por la comercialización de las mercancías de comercio exterior se depositen en la Tesorería de la Federación de conformidad con la legislación aduanera y aplicar contra el fondo que se constituya los pagos por resarcimiento o indemnización pecuniaria, y los gastos derivados de la ejecución directa en la destrucción de bienes.

- Instrumentar jurídicamente los actos de los que se genere derechos y obligaciones para la Dirección General y, vigilar que el ejercicio de las operaciones de destino se ajuste al marco legal y administrativo existente.

- Dirigir y coordinar la instrumentación de entrega de bienes a los beneficiarios aprobados por las operaciones de asignación, donación, destrucción y ventas, verificando el cumplimiento de objetivos en el destino final de los bienes, de acuerdo con la normatividad y demás disposiciones en materia aplicables.

- Informar a la unidad administrativa o instancias que correspondan, de los hechos de que tenga conocimiento con motivo de sus actividades, que pueden constituir delitos fiscales o delitos de los servidores públicos de la Secretaría en el desempeño de sus funciones; así como coadyuvar en la esfera de su competencia, con la unidad administrativa que corresponda, en la investigación de hechos presumiblemente delictivos.

- Integrar y mantener actualizados los registros y documentación generada por el destino de bienes, para garantizar la transparencia, seguridad y custodia de las operaciones efectuadas por la Dirección General.

- Formular informes periódicos y anuales para el Oficial Mayor relativos al resultado de las operaciones de destino de bienes efectuadas; así como de los inventarios pendientes a disponerse.

- Administrar los recursos humanos, financieros y materiales asignados a la Dirección General del Destino de los Bienes de Comercio Exterior Propiedad del Fisco Federal, de acuerdo a los lineamientos fijados y de conformidad con las disposiciones emitidas por la Oficialía Mayor.

4.2.3 Organigrama

Para que el auditor pueda darse cuenta cabal de la estructura orgánica de la empresa, así como del equipo humano del área sujeta a revisión deberá empezar por obtener un organigrama detallado de la misma, ¿No lo tiene la entidad?; o, si lo tiene , ¿Está actualizado? razón de más para que el auditor lo elabore y en su ejecución encontrará la magnífica oportunidad de empezar a conocer la operación organizacional del área que será revisada y, sobre todo, las personas involucradas.

En este caso la empresa si cuenta con un organigrama actualizado y detallado el cuál cubre la descripción de las funciones que se tienen establecidas dentro de la misma. (ver anexo 3).

4.2.3.1 Estructura Orgánica

Dirección General

Secretario Particular

Dirección Administrativa

Subdirección de Recursos Humanos y Materiales
Departamento de Recursos Humanos
Departamento de Recursos Materiales

Subdirección de Recursos Financieros
Departamento de Recursos Financieros
Departamento de Análisis y Estudios
Departamento de Correspondencia y Archivo
Departamento de Control y Gestión

Dirección de Informática

Subdirección de Desarrollo de Sistemas
Departamento de Desarrollo de Sistemas

Subdirección de Soporte Técnico
Departamento de Soporte Técnico

Dirección General Adjunta Operativa

Dirección de Almacenes
Subdirección de Control de Bienes
Departamento de Mercancías y Vehículos

Dirección de Inventarios Norte

Subdirección de Inventarios Noroeste y Norte-Centro
Departamento Zona Noroeste 1
Departamento Zona Noroeste 2
Departamento Zona Norte Centro 1

Subdirección de Inventarios Noroeste
Departamento Zona Noroeste 1
Departamento Zona Noroeste 2
Departamento Zona Noroeste 3

Dirección de Inventarios Centro

Subdirección de Almacenes Fiscalizados
Departamento de Almacenes Fiscalizados 1
Departamento de Almacenes Fiscalizados 2

Subdirección de Inventarios Centro 1
Departamento Zona Metropolitana 1
Departamento Zona Metropolitana 2
Departamento Zona Bajío

Subdirección de Inventarios Centro 2
Departamento Zona Golfo Pacífico
Departamento Zona Occidente

Dirección de Inventarios Sureste

Subdirección de Inventarios Sureste
Departamento Zona Sureste1
Departamento Zona Sureste 2

Subdirección de Registro y Control de Inventarios
Departamento de Registro y Control de Inventarios Norte
Departamento de Registro y Control de Inventarios Centro
Departamento de Registro y Control de Inventarios Sur

Dirección General Adjunta de Destino de Bienes

Dirección de Ventas y Destrucciones

Subdirección de Ventas
Departamento de Control y Registro de Ventas
Departamento de Operación de Ventas

Subdirección de Análisis
Departamento de Apoyo en Análisis

Subdirección de Destrucciones

Departamento de Control de Destrucciones
Departamento de Operación de Destrucciones

Dirección de Donaciones y Asignaciones

Subdirección de Registro y Análisis
Departamento de Registro de Solicitudes
Departamento de Análisis de Solicitudes
Departamento de Atención al Sector Público e Instituciones Filantrópicas

Subdirección de Operación de Donaciones y Asignaciones
Departamento de Programación de Donaciones y Asignaciones
Departamento de Operación de Donaciones y Asignaciones

Subdirección de Seguimiento de Donaciones y Asignaciones
Departamento de Seguimiento de Donaciones
Departamento de Seguimiento de Asignaciones

Dirección General Adjunta Jurídica y de Control

Dirección Jurídica

Subdirección Jurídica
Departamento Jurídico de Mercancías
Departamento Jurídico de Vehículos

Subdirección de Normatividad y Consultoría
Departamento de Normatividad
Departamento de Consultoría

Dirección de Control y Evaluación

Subdirección de Control y Operación
Departamento de Control Interno
Departamento de Revisión y Seguimiento de Acuerdos
Departamento de Control de Información

Subdirección de Seguimiento de Acuerdos
Departamento de Integración y Seguimiento de Acuerdos

Subdirección de Evaluación de la Gestión
Departamento de Integración y Registro
Departamento de Evaluación

Subdirección de Supervisión
Departamento de Supervisión Operativa
Departamento de Supervisión Administrativa

4.3 ÁREA A AUDITAR (Dirección de Control y Evaluación)

Una vez que el auditor se ha "identificado" plenamente con la entidad que será objeto de una intervención de auditoría procederá, enseguida, a efectuar un análisis específico de la función que vaya a auditar.

Para llevar a cabo esta etapa de trabajo, el auditor se auxiliará de técnicas con las que revisará absolutamente todas las actividades de la función sujeta a auditoría, así como el personal que las realiza y con qué elementos las lleva a cabo.

4.3.1 Objetivo y Funciones

Objetivo

Dirigir, coordinar y supervisar el registro automatizado de las operaciones y asesorar en la elaboración de los informes financiero-presupuestales y de modernización que deban rendirse; coordinar la elaboración de las Carpetas de Acuerdos de los Plenos del Consejo Asesor y Comité de Asignación de Bienes al Sector Público, verificando el cumplimiento de los acuerdos adoptados; así como supervisar el establecimiento de medidas de planeación, organización, control interno y de evaluación de resultados de la Dirección General a través de estándares e indicadores de gestión.

Funciones

- Dirigir la instrumentación, aplicación y evaluación de las metodologías de modernización administrativa, que permitan determinar el grado de cumplimiento de los programas, en términos de calidad, desempeño y resultados.

- Dirigir y coordinar medidas de control interno que fortalezcan e integren el funcionamiento de la estructura organizativa, operativa y administración de la Dirección General.

- Verificar la elaboración de diagnósticos de operación y administración por áreas de la Dirección General para establecer la aplicación de medidas de control preventivas y correctivas.

- Administrar la aplicación del sistema de estándares e indicadores de gestión para evaluar el impacto, cobertura, eficiencia y calidad de los servicios y resultados, así como mantener la adecuación y actualización de los mismos.

- Verificar la congruencia y compatibilidad de los sistemas automatizados de destino de bienes con los demás de operación y administración aprobados.

- Coordinar el análisis, evaluación y reportes de información sobre la aplicación, desarrollo y avance de los programas operativos de destino de bienes.

- Coordinar y supervisar la elaboración, actualización y aprobación de la estructura orgánica, de los manuales de Organización Específico y de Procesamiento de la Dirección General.

- Establecer y supervisar las actividades de planeación y los programas de trabajo de las áreas de la Dirección General, así como evaluar el cumplimiento de los mismos.

- Vigilar y dirigir las metodologías e instrumentos para la formulación e integración de las carpetas de Acuerdos de las reuniones del Pleno del Consejo Asesor y del Comité de Asignación de Bienes al Sector Público que convoque el Oficial Mayor.

- Verificar el seguimiento y cumplimiento de los acuerdos, políticas y medidas adoptadas en las plenarias, para efectos de la gestión operativa que proceda en cada caso.

- Supervisar, controlar y dirigir las reuniones de trabajo y preparatorias que se lleven a cabo con representantes de los cuerpos colegiados del Consejo y Comité, para la instrumentación de acuerdos que requieran la participación coordinada de sus integrantes.

- Guiar la integración y elaboración de informes especiales y ejecutivos sobre los resultados y desempeños alcanzados por la Dirección General en el cumplimiento de las funciones encomendadas.

- Diseñar un plan maestro de supervisión por funciones encomendadas a la Dirección General, observando las normas, disposiciones, políticas y procedimientos en materia aplicables.

- Supervisar la correcta ejecución de los programas y proyectos, así como de resultados obtenidos en observancia de los procedimientos establecidos para cada una de las áreas.

- Coordinar la verificación del cumplimiento en el destino de los bienes, comprobando por diversos mecanismos que lleguen a los destinatarios finales y cumplan el objetivo por el cual fueron solicitados y autorizados, en beneficio de la sociedad.

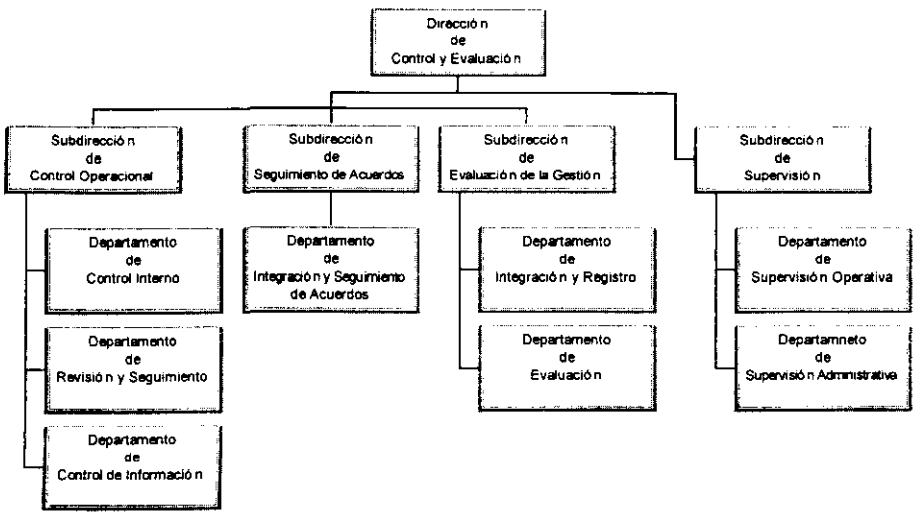
- Proporcionar asesoría en materia de control operacional a las diferentes áreas operativas y administrativas que integran la Dirección General.

- Instrumentar las normas, lineamientos y mecanismos de control que emitan las diferentes dependencias y áreas controladoras para establecer las medidas de control interno necesarias.

- Mantener la relación inter e intrasectorial de atención y apoyo con las autoridades de control gubernamental para el desahogo de las observaciones y recomendaciones de los programas de control y auditoría que se apliquen en el ámbito de su competencia.

- Participar en las reuniones de confronta convocadas por las autoridades de control y fiscalización.

4.3.2 Organigrama



4.3.3 Recursos

Para alcanzar sus objetivos, está dirección cuenta con los siguientes recursos:

RECURSOS HUMANOS

1 Director
3 Subdirectores
7 Jefes de Departamento
4 Analistas
1 Secretaria

RECURSOS MATERIALES

La dirección cuenta con 12 equipos de PC's 386, 486 de las marcas IBM, ACER y HP con diferentes velocidades, disco duro, monitores a color, 2 Modem marca Motorola y 3 impresoras Laser Jet.

RECURSOS TÉCNICOS

Cuentan con licencia de uso de varios paquetes como son: Microsoft Office, Windows, Harvard Graphics, etc. y los sistemas operativos DOS y NOVELL.

4.3.4 Plano de Ubicación

A través de la primera visita a las instalaciones de la Dirección de Control y Evaluación, se hicieron algunas observaciones acerca de su ubicación y la manera en que se encuentra distribuida el área. (ver anexo 4).

Para la operación de cada equipo se tiene asignada a una o dos personas como responsables de su uso.

4.4 DEFINICIÓN DEL OBJETIVO Y ALCANCE DE LA AUDITORÍA

De acuerdo a la información que se obtuvo, se determino el objetivo y alcance de la Auditoría a realizar, mismos que se presentan a continuación.

Objetivo

Identificar y evaluar la suficiencia de controles existentes en la Dirección de Control y Evaluación de la DGDBCEPFF, con el fin de determinar acciones que optimicen su seguridad y operación.

Alcance

La revisión se llevará a cabo de acuerdo a las normas y procedimientos de Auditoría, con la finalidad de contar con los elementos suficientes para opinar sobre la eficiencia y productividad de la Dirección de Control y Evaluación, evaluando los siguientes aspectos:

- Seguridad Física
- Seguridad Lógica

4.5 EVALUACIÓN DE CONTROLES

Una vez que se conoció la información general del área, se procedió a identificar y evaluar los puntos críticos de los controles establecidos dentro de las actividades normales de la Dirección de Control y Evaluación.

Las actividades que a continuación se enlistan sirvieron de base para la revisión de controles, de acuerdo al objetivo y alcance anteriormente definidos.

1. Administración sobre usuarios (acceso, privilegios, huellas o pistas de auditoría), por medio de la obtención de la siguiente información:

- Lista de usuarios del equipo
- Niveles de acceso y privilegios por cada usuario
- Registro de las operaciones mediante la clave de usuario (USER-ID) a fin de determinar huellas o pistas para auditoría
- Procedimientos en caso de intentos de violación de acceso o de privilegios

2. Evaluar aspectos para seguridad física lógica tales como:

Seguridad Física

- Distribución del equipo
- Niveles de aprovechamiento del equipo
- Corriente controlada
- Seguridad de acceso al área
- Equipo de corriente ininterrumpida
- Control de cintas, cartuchos, accesorios, etc.

Seguridad Lógica

- Control de passwords
- Bitácora de fallas
- Bitácora de respaldos
- Controles en la transmisión y transformación de la información
- Generación de copias de respaldos para salvaguardar la información
- Verificar terminación correcta de procesos

3. Analizar todo lo relacionado a la prevención y recuperación en caso de desastres

- Planes de recuperación y restauración de información
-Planes de acción probados por las áreas involucradas, delimitando responsabilidades y participación por cada una
- Realización de simulacros para poner en práctica los puntos anteriores
- Infraestructura instalada, probada y funcional contra inundación, explosión, terremotos, salidas de emergencia, alarmas, etc.

4.6 DISEÑO Y APLICACIÓN DE PROCEDIMIENTOS PARA LA AUDITORÍA

Con los datos obtenidos del área auditada hasta esta etapa, fue posible elegir las técnicas y diseñar las herramientas necesarias para apoyar las actividades de campo de la auditoría, estructurándose de la siguiente manera:

CHECK LIST

- PLANEACIÓN DE LA AUDITORÍA.

  - Definición de Objetivo y Alcance
  - Elaboración del Plan de Trabajo
  - Identificación de Medidas de Seguridad
  - Elaboración de Cuestionarios y Entrevistas

- LEVANTAMIENTO DE INFORMACIÓN.

  - Aplicación de Cuestionarios y Entrevistas
  - Obtener de Información Documental
  - Obtener de Pistas de Auditoría

- OBTENCIÓN DE RESULTADOS.

  - Selección de la Información
  - Análisis de Resultados
  - Realización de Tabla de Riesgos
  - Elaboración de Propuestas
  - Determinar Conclusiones

ENTREVISTAS

Se efectuaron varias entrevistas para obtener la información complementaria a la auditoría realizada, que sirvieran de apoyo para el cumplimiento del objetivo y alcance planteado. Las entrevistas permitieron conocer información con respecto a:

- Funciones del personal
- Operación del área
- Características del equipo
- Organización del área
- Seguridad dentro del área

CUESTIONARIOS

Se formularon diversos cuestionarios para aplicarse a los usuarios y al Director del área auditada, en donde se consideraron los siguientes aspectos:

- Seguridad Física

  - Control de acceso
  - Ubicación del área
  - Mantenimiento preventivo del equipo
  - Protección de registros
  - Plan de contingencia

- Seguridad Lógica

  - Respaldo de información
  - Accesos a la información
  - Administración de usuarios
  - Detección de virus

La estructura de los cuestionarios, se pueden consultar en el anexo 5.

4.7 ANÁLISIS DE RESULTADOS

Los puntos más importantes y relevantes que se detectaron durante la revisión a la Dirección de Control y Evaluación se detallan de acuerdo al siguiente criterio de evaluación:

- Observación
- Causa
- Impacto
- Sugerencia

(ver anexo 6)

4.7.1 Comparación de Resultados

Es la evaluación de los resultados que se obtuvieron durante la Auditoría, esta se va a representar por medio de una tabla en la cual se establece: un valor de riesgo representado por un valor numérico del 1 al 4 dependiendo de la característica aplicable a cada observación y así poder establecer un nivel de riesgo.

TABLA DE NIVELES DE RIESGO

VALOR DEL RIESGO	CARACTERÍSTICAS	NIVEL DE RIESGO
1	Existe medida de prevención y se aplica	Normal
2	Existe medida de prevención, pero no se aplica	Controlable
3	No existe medida de prevención	Potencial
4	Se desconoce el impacto del riesgo	Inmimente

RESULTADO DE LA EVALUACIÓN DE RIESGOS

En base al criterio de los parámetros registrados en la tabla anterior, se determinó el nivel de riesgo que corresponde a cada una de las observaciones realizadas (ver anexo 7).

El siguiente cuadro muestra el promedio de los valores de riesgo asignados a cada observación por área auditada.

CUADRO COMPARATIVO DE RESULTADOS

ÁREAS	PROMEDIO DEL VALOR DE RIESGO	NIVEL DE RIESGO
Seguridad Lógica	2.68	Controlable (con tendencia a potencial)
Seguridad Física	3.0	Potencial

NIVELES DE INCREMENTO EN LA EFICIENCIA Y SEGURIDAD

Una vez que se evalúo el nivel de riesgo en los puntos definidos en el alcance que para efecto del caso práctico fue: Seguridad Física y Seguridad Lógica. Se procederá a proyectar un incremento en la eficiencia de la operación y seguridad del área.

La siguiente tabla identifica el nivel de riesgo en el que se encuentra la Dirección de Control y Evaluación la cuál determina el porcentaje de incremento que va a ir en función de las acciones que se tomen para corregir las desviaciones observadas. Esto es, en la medida en que se procure el establecimiento de medidas preventivas, su aplicación y adecuado funcionamiento tenderá a aumentar la eficiencia de las operaciones y la seguridad del área.

NIVEL DE INCREMENTO EN LA SEGURIDAD	DESCRIPCIÓN	TIPO DE RIESGO
0 - 25%	Se desconoce el impacto del riesgo	Inminente
26 - 50%	No existe medida de prevención	Potencial
51 - 75%	Existe medida de prevención, pero no se aplica	Controlable
76 - 100%	Existe medida de prevención y se aplica	Normal

De acuerdo a los parámetros definidos en la tabla anterior se determina el incremento en la seguridad:

Al encontrarnos en un nivel 0 se dice que se desconoce por completo el impacto de este riesgo, una vez que se adquiere el conocimiento de su prevención se puede llegar a un 25%.

Cuando se comprende la necesidad de su prevención se encuentra en la escala del 26%, una vez que se plantea la medida de prevención se puede llegar a un 50%.

Por otra parte, cuando se define la medida se pasa de un 51 a un 75%.

Y por último cuando ésta medida se aplica se alcanza un 76% y en la medida que se lleven a cabo simulacros de su aplicación se tenderá a lograr un 100%.

4.8 OBTENCIÓN DE RESULTADOS

A continuación se presentan los resultados obtenidos de este caso práctico de auditoría.

Como resultado de la aplicación de las técnicas de Auditoría a la Dirección de Control y Evaluación se pudo determinar que el nivel de riesgo en el que a la fecha se encuentra es ***Potencial***; es decir, que no existen medidas para la mayoría de las anomalías encontradas. Lo anterior se determinó en base a la calificación correspondiente para cada una de las observaciones detectadas en la revisión.

Con la tabla de identificación del nivel de incremento en la seguridad, se proyecta el beneficio que se obtendrá con la corrección de las desviaciones detectadas; esto es, en la medida en que se tomen las acciones pertinentes para corregir las anomalías y contar con la existencia de los controles necesarios, se incrementará la seguridad y la eficiencia en general del área; ya que si las medidas preventivas que se tomen son deficientes, el incremento no resultará significativo pero, si por el contrario se implementan adecuadas medidas y controles el incremento será notorio. Y si por otro lado dichas medidas se establecen formalmente por la institución o entidad, son sometidas a pruebas y regularmente revisadas obviamente su incremento tenderá a ser mucho mayor.

Con las técnicas utilizadas en este trabajo y el análisis hecho para la realización del caso práctico, se comprueba la importancia de la Auditoría Informática dentro de la empresa.

CONCLUSIONES

Por muy grandes o complejos que sean nuestros sistemas, lo más importante es normalizar técnicas y procedimientos que los controle.

Para establecer una función efectiva de Auditoría, el margen de responsabilidad debe ser presentado y aprobado por la Alta Dirección. Aunque la primera auditoría debe ser el procesamiento de datos, es imperativo que una relación de trabajo adecuada tiene que ser establecida y formalizada por escrito. Áreas con conflictos potenciales deben ser discutidas para asegurar que con una planeación previa se prevengan futuros problemas.

Debe ser desarrollada una definición formal de las responsabilidades del área de Auditoría en Informática. Aunque las descripciones de la función son parte integral de la Auditoría del área de Procesamiento de Datos, también son una guía para controlar las responsabilidades del Auditor en Informática.

Hay un gran campo de actividades que pueden ser realizadas por los Auditores en Informática. Un departamento que empieza no puede atender todas las responsabilidades asociadas con su función. Para esto, selecciona dos o tres áreas donde los riesgos de la empresa sean mayores y donde el impacto de Auditoría en Informática pueda ser de gran ayuda.

Dentro de las actividades principales que realiza un auditor tenemos las siguientes:

- Revisión y establecimiento de controles
- Garantizar la incorporación de las medidas de seguridad adecuadas
- Establecer políticas y procedimientos dentro de las actividades del área

Estas actividades se integraran en un procedimiento de auditoría, cuyo desarrollo estará complementado con una serie de técnicas y herramientas que le servirán de apoyo a la realización de su trabajo.

Por todo lo anterior se puede concluir que la Auditoría en Informática es una herramienta indispensable para la correcta administración y aprovechamiento de los recursos informáticos de una empresa y que su adecuada aplicación la convierte en una fuente de información estratégica de apoyo para la toma de decisiones importantes en la organización, impulsando su crecimiento y desarrollo y mejorando la calidad con la que se lleven a cabo sus funciones.

ANEXOS

ANEXO 1

México, D.F. a 18 de Diciembre de 1998.

C.P. Gustavo Altamirano Vega
Director General del Destino de los Bienes
de Comercio Exterior Propiedad del Fisco Federal.
Presente

La presente tiene como fin, obtener la autorización para realizar un caso práctico de una Auditoría a la Dirección de Control y Evaluación, considerando los siguientes aspectos: Seguridad Física y Seguridad Lógica.

La Auditoría se realizará de acuerdo con las técnicas, procedimientos y la aplicación de la metodología presentada en este trabajo.

La práctica consistirá en analizar e investigar algunas de las funciones de la organización, es decir, sus antecedentes, objetivo y funciones, organigrama general, etc., además todo lo relacionado con el área a auditar, su objetivo y función que nos servirán para detectar posibles errores o deficiencias, para que finalmente se sugieran alternativas de solución.

La práctica de la auditoría tomará un tiempo estimado de 10 días, en los cuales se realizarán las siguientes actividades principales:

- Levantamiento de la Información
- Análisis de la Información
- Elaboración de resultados

El inicio de la práctica será el día 18 de Diciembre y terminará el 8 de Enero del año en curso.

Agradeciendo de antemano la oportunidad para llevar a cabo el caso práctico.

A t e n t a m e n t e

C. Margarita Zaragoza Hernández

ANEXO 2

México, D. F. a 18 de Diciembre de 1998

Asunto: Solicitud de Elementos.

Lic. Rodolfo Zúñiga Romero
Director de Control y Evaluación
Presente

Con el propósito de iniciar el trabajo de Auditoría solicitamos a usted nos proporcione los elementos que a continuación detallamos:

Información de los antecedentes y objetivos de la empresa

Organigrama de la empresa

Objetivo y funciones de la Dirección de Control y Evaluación

Políticas y procedimientos del área

Descripción de puestos y funciones

Manuales Operativos

Plan de capacitación

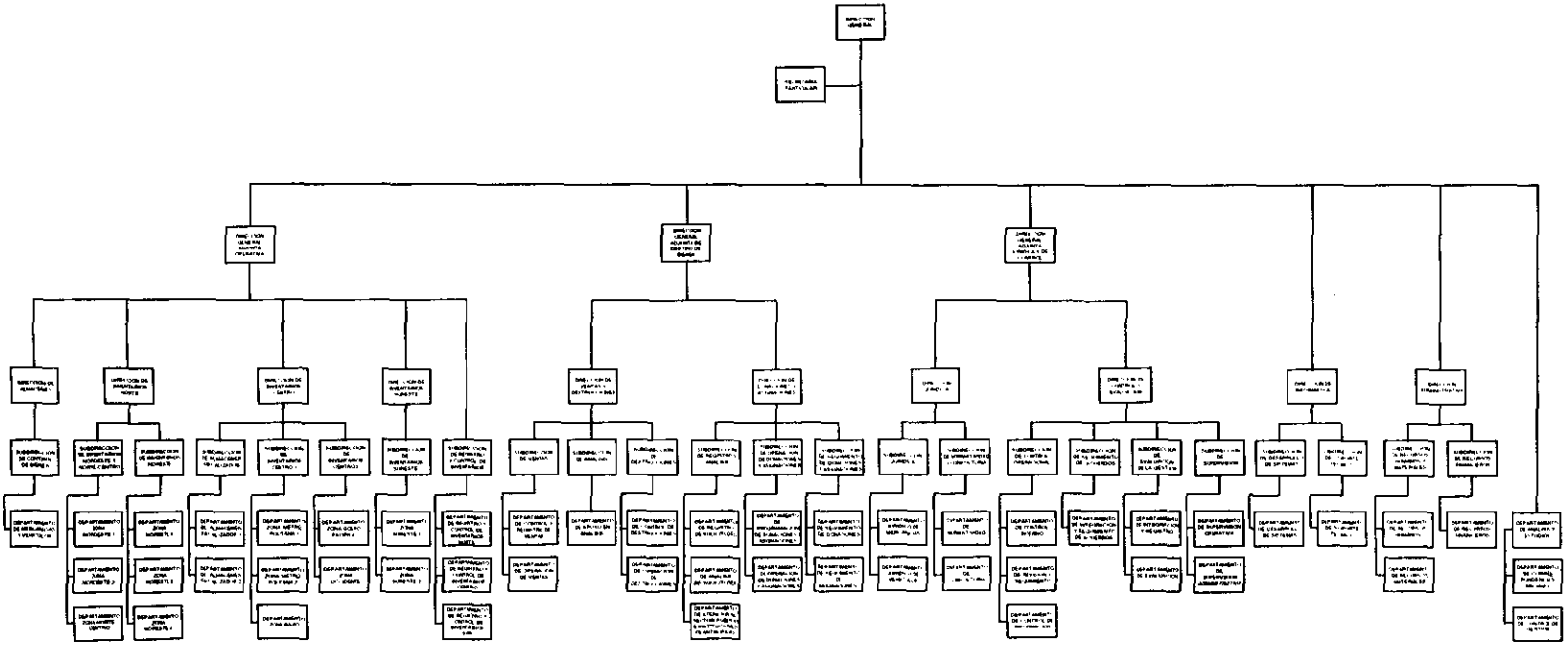
Plan de contingencia

Plano de ubicación

A t e n t a m e n t e

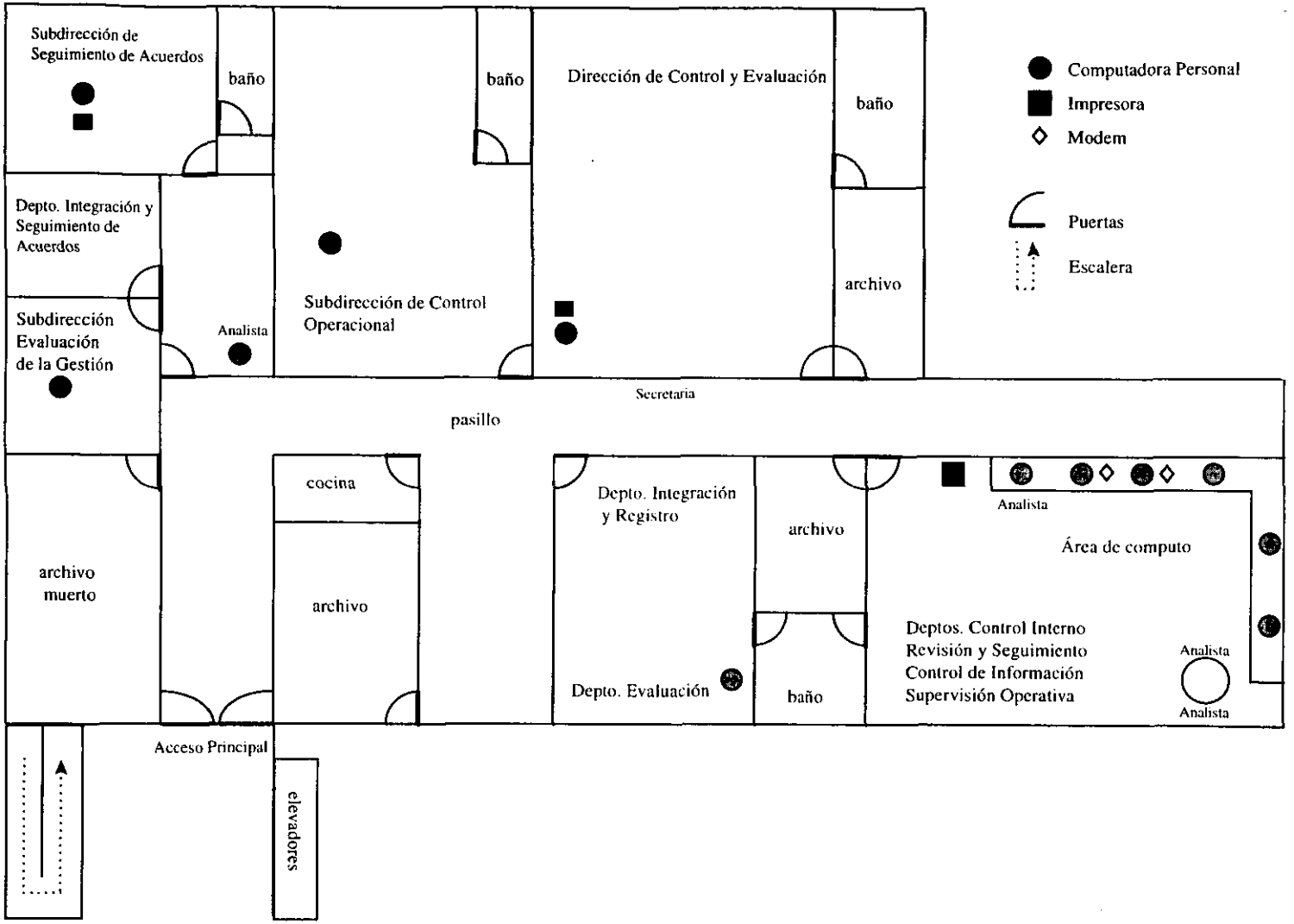
C. Margarita Zaragoza Hernández

ANEXO 3



ANEXO 4

PLANO DE LA DIRECCIÓN DE CONTROL Y EVALUACIÓN



ANEXO 5

CUESTIONARIO

SEGURIDAD FÍSICA

PREGUNTA	SI	NO	OBSERVACIONES
¿Las entradas al área están vigiladas?			
¿El acceso de personas es controlado por medio de cualquiera de los siguientes métodos? - Por una recepcionista - Guardias - Monitores de televisión - Gafetes - Otros			
¿Existe un registro de entradas y salidas para todo el personal del área?			
¿El área siempre cuenta con vigilancia, aún en días inhábiles?			
¿Son adecuadas las medidas de seguridad con que cuenta el área en caso de que no exista vigilancia?			
¿La capacitación que recibieron los guardias está dirigida a proteger las instalaciones del área?			
¿Se inspeccionan los maletines, cajas de herramientas, paquetes y otros elementos similares que portan las personas al entrar y salir de las instalaciones?			
¿Existen gafetes de identificación y se usan permanentemente por el personal que ahí labora?			

Nombre del Auditado: _____

Puesto: _____

Área: _____

PREGUNTA	SI	NO	OBSERVACIONES
¿Existen fugas de agua dentro del área?			
¿El área cuenta con salidas de emergencia?			
¿Las salidas de emergencia se encuentran ubicadas en lugares estratégicos, bien señalizados y están en operación libres de elementos que impidan su apertura y libre tránsito?			
¿Existen detectores de calor-humo, agua y magnetos?			
¿Existe alarma audible que permita alertar al personal en caso de siniestro?			
¿Existe una adecuada limpieza en las instalaciones?			
¿Se encuentra prohibido el consumo de alimentos y bebidas dentro del área?			
¿El personal se encuentra capacitado y cuenta con el entrenamiento necesario que le permita emprender acciones inmediatas en caso de emergencia?			
¿Se vigila que el mantenimiento del equipo se efectúe en las fechas programadas en el calendario?			

Nombre del Auditado: _____

Puesto: _____

Área: _____

SEGURIDAD LÓGICA

PREGUNTA	SI	NO	OBSERVACIONES
¿Utilizan sistemas de protección (passwords)?			
¿Los usuarios poseen passwodrs de entrada a las aplicaciones de arranque?			
¿El usuario es libre de manipular sus passwords?			
¿Utiliza passwords para proteger sus documentos?			
¿Se le ha proporcionado capacitación para el buen uso y confidencialidad de: • La información? • Passwords?			
¿Existe un documento formal que contenga las políticas y procedimientos a seguir en el proceso de: • Acceso a otras estaciones de trabajo • Acceso a archivos • Delimitación de funciones y responsabilidades			
¿Existen mecanismos para comprobar que la clave de acceso fue proporcionada bajo la normatividad establecida por la empresa?			
¿Las claves asignadas pertenecen únicamente a personal activo de esa área?			
¿Está limitado el número de intentos fallidos para accesar a los archivos?			

Nombre del Auditado: _____

Puesto: _____

Área: _____

¿Se detectan virus en las computadoras o en diskettes?			
¿Posee algún programa especializado y actualizado que le permita detectar virus? ¿Cuál?			
¿Se le ha prohibido la utilización o uso de software o dispositivos de dudosa procedencia?			
¿Mantiene una política formal para la revisión de la información? • En cada estación de trabajo?			
¿Esas políticas son del conocimiento de la empresa?			
¿Cumple con las normas establecidas por la empresa para la realización de sus funciones?			

Nombre del Auditado: _____
Puesto: _____
Área: _____

ANEXO 6

SEGURIDAD FÍSICA

➢ **OBSERVACIÓN 1.**

Acceso fácil al área

CAUSA:

- La vigilancia al área no es constante

IMPACTO:

- Pérdida de información propiedad del gobierno
- Pérdida de equipo de trabajo

SUGERENCIA:

- Implementar buenos programas de seguridad física y control de acceso
- Ubicar guardias a la entrada de las instalaciones
- Uso obligatorio de la credencial del empleado

➢ **OBSERVACIÓN 2.**

No existen extintores de fuego dentro del área

CAUSA:

- Falta de un plan de contingencia adecuado

IMPACTO:

- Pérdida de recursos materiales y humanos

SUGERENCIA:

- Es necesario instalar dispositivos de prevención contra incendios

➢ **OBSERVACIÓN 3.**

No existe un programa de capacitación y entrenamiento en caso de desastre

CAUSA:

- No cuentan con el personal adecuado para realizar este tipo de programas

IMPACTO:

- Imposibilidad de actuar adecuadamente ante una contingencia
- Pérdida de recursos

SUGERENCIA:

- Es necesario la creación de un comité que se encargue del entrenamiento y realización de simulacros en caso de desastre

➢ **OBSERVACIÓN 4.**

No se da mantenimiento preventivo al equipo, en forma periódica

CAUSA:

- Falta de responsabilidades por parte de los encargados de este trabajo

IMPACTO:

- Mal funcionamiento del equipo
- Tiempo improductivo por la interrupción de operaciones

SUGERENCIA:

- Es necesario realizar las gestiones necesarias a fin de contar con el mantenimiento adecuado

➢ **OBSERVACIÓN 5.**

No se localizaron procedimientos formalmente establecidos sobre entrada y salida de equipo

CAUSA:

- Falta de estándares propios y actualizados de seguridad

IMPACTO:

- Pérdida o extravío de equipo y accesorios de cómputo propiedad del gobierno

SUGERENCIA:

- Es fundamental que se lleve un control del equipo, estableciendo políticas y procedimientos formales para su administración

➢ **OBSERVACIÓN 6.**

No se respetan las señalizaciones que indican la prohibición de fumar, beber o ingerir alimentos dentro del área

CAUSA:

- Falta de conciencia del personal

IMPACTO:

- Accidentes innecesarios e incendios

SUGERENCIA:

- Es necesario generar conciencia en el personal para que respetan los señalamientos establecidos dentro del área

➢ **OBSERVACIÓN 7.**

Se permite la entrada al personal fuera de su horario de trabajo

CAUSA:

- Falta de un sistema de seguridad más eficiente

IMPACTO:

- Pérdida o malversación de información propiedad del gobierno

SUGERENCIA:

- Es necesario establecer procedimientos de control que ayuden a regular el acceso del personal

➢ **OBSERVACIÓN 8.**

No existen salidas de emergencia

CAUSA:

- No se han percatado de este problema

IMPACTO:

- Imposibilidad de evacuar el área en caso de suscitarse una emergencia
- Pérdida de recursos humanos y materiales

SUGERENCIA:

- Realizar un estudio para promover el adecuado sitio de salidas de emergencia

➢ **OBSERVACIÓN 9.**

No existen alarmas que indiquen la presencia de un siniestro

CAUSA:

- Falta de plan de contingencia adecuado

IMPACTO:

- Imposibilidad de una reacción pronta y adecuada ante una contingencia
- Pérdida de recursos humanos y materiales

SUGERENCIA:

- Realizar las gestiones correspondientes a fin de contar con un sistema que indique la presencia de un siniestro

SEGURIDAD LÓGICA

➢ **OBSERVACIÓN 1.**

Uso inadecuado de passwords

CAUSA:

- Falta de un sistema de seguridad eficiente

IMPACTO:

- Mal uso de la información
- Robo de información propiedad del gobierno

SUGERENCIA:

- Implementar buenos programas de seguridad lógica y control de acceso a los archivos
- Salir del sistema si el usuario intenta un passwords inválido más de un número predeterminado de veces

➢ **OBSERVACIÓN 2.**

No cuentan con un plan de contingencia en caso de pérdida de información

CAUSA:

- Falta de personal para la ejecución del plan

IMPACTO:

- Pérdida de información

SUGERENCIA:

- Contratar al personal adecuado que se encargue de desarrollar de un plan de contingencia, el cual sea probado periódicamente para asegurar su efectividad

➢ **OBSERVACIÓN 3.**

Obtención de información por personal no autorizado

CAUSA:

- Falta extrema de pistas de auditoría

IMPACTO:

- Pérdida de información

SUGERENCIA:

- Establecer procedimientos para limitar y detectar cualquier intento de acceso no autorizado
- Promover guías para proteger la confidencialidad de los datos y la información

➢ **OBSERVACIÓN 4.**

No existe un control de respaldos de información

CAUSA:

- Falta de procedimientos adecuados para la retención de registros vitales

IMPACTO:

- Imposibilidad de una reacción pronta y adecuada ante una contingencia
- Pérdida de información

SUGERENCIA:

- Definir y seguir procedimientos adecuados de respaldo de la información que sea importante para la empresa
- Deben mantenerse respaldos que contengan los archivos suficientes para recuperar la información dañada o destruida y que garanticen la posibilidad de continuar con el servicio y operación de la empresa

ANEXO 7

SEGURIDAD FÍSICA

➢ **OBSERVACIÓN 1.**
Acceso fácil al área

CAUSA:
- La vigilancia al área no es constante

IMPACTO:
- Pérdida de información propiedad del gobierno
- Pérdida de equipo de trabajo

EVALUACIÓN DEL RIESGO: (2)

SUGERENCIA:
- Implementar buenos programas de seguridad física y control de acceso
- Ubicar guardias a la entrada de las instalaciones
- Uso obligatorio de la credencial del empleado

➢ **OBSERVACIÓN 2.**
No existen extintores de fuego dentro del área

CAUSA:
- Falta de un plan de contingencia adecuado

IMPACTO:
- Pérdida de recursos materiales y humanos

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:
- Es necesario instalar dispositivos de prevención contra incendios

➢ **OBSERVACIÓN 3.**
No existe un programa de capacitación y entrenamiento en caso de desastre

CAUSA:
- No cuentan con el personal adecuado para realizar este tipo de programas

IMPACTO:

- Imposibilidad de actuar adecuadamente ante una contingencia
- Pérdida de recursos

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:

- Es necesario la creación de un comité que se encargue del entrenamiento y realización de simulacros en caso de desastre

➢ **OBSERVACIÓN 4.**

No se da mantenimiento preventivo al equipo, en forma periódica

CAUSA:

- Falta de responsabilidades por parte de los encargados de este trabajo

IMPACTO:

- Mal funcionamiento del equipo
- Tiempo improductivo por la interrupción de operaciones

EVALUACIÓN DEL RIESGO: (2)

SUGERENCIA:

- Es necesario realizar las gestiones necesarias a fin de contar con el mantenimiento adecuado

➢ **OBSERVACIÓN 5.**

No se localizaron procedimientos formalmente establecidos sobre entrada y salida de equipo

CAUSA:

- Falta de estándares propios y actualizados de seguridad

IMPACTO:

- Pérdida o extravío de equipo y accesorios de cómputo propiedad del gobierno

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:

- Es fundamental que se lleve un control del equipo, estableciendo políticas y procedimientos formales para su administración

➢ **OBSERVACIÓN 6.**

No se respetan las señalizaciones que indican la prohibición de fumar, beber o ingerir alimentos dentro del área

CAUSA:

- Falta de conciencia del personal

IMPACTO:

- Accidentes innecesarios e incendios

EVALUACIÓN DEL RIESGO: (2)

- **SUGERENCIA:** Es necesario generar conciencia en el personal para que respetan los señalamientos establecidos dentro del área

➢ **OBSERVACIÓN 7.**

Se permite la entrada al personal fuera de su horario de trabajo

CAUSA:

- Falta de un sistema de seguridad más eficiente

IMPACTO:

- Pérdida o malversación de información propiedad del gobierno

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:

- Es necesario establecer procedimientos de control que ayuden a regular el acceso del personal fuera de su horario

➢ **OBSERVACIÓN 8.**

No existen salidas de emergencia

CAUSA:

- No se han percatado de este problema

IMPACTO:

- Imposibilidad de evacuar el área en caso de suscitarse una emergencia
- Pérdida de recursos humanos y materiales

EVALUACIÓN DE RIESGOS: (4)

SUGERENCIA:

- Realizar un estudio para promover el adecuado sitio de salidas de emergencia

➢ **OBSERVACIÓN 9.**

No existen alarmas que indiquen la presencia de un siniestro

CAUSA:

- Falta de plan de contingencia adecuado

IMPACTO:

- Imposibilidad de una reacción pronta y adecuada ante una contingencia
- Pérdida de recursos humanos y materiales

EVALUACIÓN DEL RIESGO: (4)

SUGERENCIA:

- Realizar las gestiones correspondientes a fin de contar con un sistema que indique la presencia de un siniestro

SEGURIDAD LÓGICA

➢ **OBSERVACIÓN 1.**

Uso inadecuado de passwords

CAUSA:

- Falta de un sistema de seguridad eficiente

IMPACTO:

- Mal uso de la información
- Robo de información propiedad del gobierno

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:

- Implementar buenos programas de seguridad lógica y control de acceso a los archivos
- Salir del sistema si el usuario intenta un passwords inválido más de un número predeterminado de veces

➢ **OBSERVACIÓN 2.**

No cuentan con un plan de contingencia en caso de pérdida de información

CAUSA:

- Falta de personal para la ejecución del plan

IMPACTO:

- Pérdida de información

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:

- Contratar al personal adecuado que se encargue de desarrollar de un plan de contingencia, el cual sea probado periódicamente para asegurar su efectividad

➢ **OBSERVACIÓN 3.**

Obtención de información por personal no autorizado

CAUSA:

- Falta extrema de pistas de auditoría

IMPACTO:
- Pérdida de información

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:
- Establecer procedimientos para limitar y detectar cualquier intento de acceso no autorizado
- Promover guías para proteger la confidencialidad de los datos y la información

➢ **OBSERVACIÓN 4.**

No existe un control de respaldos de información

CAUSA:
- Falta de procedimientos adecuados para la retención de registros vitales

IMPACTO:
- Imposibilidad de una reacción pronta y adecuada ante una contingencia
- Pérdida de información

EVALUACIÓN DEL RIESGO: (3)

SUGERENCIA:
- Definir y seguir procedimientos adecuados de respaldo de la información que sea importante para la empresa
- Deben mantenerse respaldos que contengan los archivos suficientes para recuperar la información dañada o destruida y que garanticen la posibilidad de continuar con el servicio y operación de la empresa

BIBLIOGRAFÍA

1. *Asociación Mexicana de Contadores.* **"Boletín del Cómite para Conceptos Básicos de Administración, México 1973**

2. *Rodríguez, Luis Angel,* **"Seguridad de la Información en Sistemas de Cómputo" Ediciones Ventura México,1995**

3. *A. Lambarri V.* **"Identificaciòn, Evaluación y Control de Riesgos", Toluca, Mèxico, Junio 1988**

4. *Richard W. Lott.* **"Auditoría y Control del Procesamiento de Datos" Editorial Norma México, 1984**

5. *William C. Mair, Donald R. Wood, Keagle W. Davis,* **"Computer Control & Audit" Editorial The Institute of International Auditors , Inc.,1980**

6. *Gómez M. Pilar, Vazquez T. Fernando, Alvarez S. Fco. Javier* **"Auditoría y Seguridad Informática" Editorial SPANTA México, 1998**

7. *Instituto Mexicano de Contadores Públicos A.C.,* **"Normas y procedimientos de Auditoría " Programa del libro de texto universitario México, 1984**

8. *H. Sanders, Donald,* **"Informática Presente y Futuro" Editorial Mc. Graw Hill México, 1990**

9. *Pérez Toraño, Luis Felipe,* **"Elementos de Auditoría Contemporánea" Facultad de Contaduría y Administración México, 1985**

10. *Sánchez Curiel, Gabriel.* **"Auditoria Operacional" Editorial ECASA México, 1987**

11. *Santillana González, Juan Ramón,* **"Conoce las Auditorías" Editorial ECASA México, 1990**

12. *Ron Weber*, **"EDP Auditing Conceptual Foundations and Practice Editorial McGraw Hill , 1986**

13. *The Institute of International Auditors, Inc.* **"Systems Auditability & Control Study, Florida, 1981**

14. *Apuntes de Seguridad y Auditoria en Informática.* **Alvares Solis, Fco. Javier, IPN**

15. *Echenique, José Antonio* , **"Auditoria en Informática" Editorial Mc Graw Hill Interamericana**