UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

SISTEMA UNIVERSIDAD ABIERTA Y EDUCACIÓN A DISTANCIA

AUTOR: JOSÉ DE JESÚS AGUIRRE BAUTISTA

AUDITORÍA EN INFORMÁTICA		Clave: 1664
Plan: 2005		Créditos: 8
Licenciatura: Informática		Semestre: 6°
Área: Informática		Horas Asesoría: 4
Requisitos: Ninguno		Horas por semana: 4
Tipo de asignatura:	Obligatoria (X)	Optativa ( )

Objetivo general de la asignatura

Al finalizar el curso, el alumno será capaz de ejecutar auditorías sobre los recursos informáticos de las organizaciones y tomará decisiones a partir del dictamen.

Temario Oficial (64 horas sugeridas)

1.	Fundamentos de auditoría en informática	08 horas
2.	Muestreo estadístico en la auditoría	12 horas
3.	Metodología general para la auditoría en informática	12 horas
4.	Auditoría de sistemas	08horas
5.	Auditoría del equipo de cómputo	08 horas
6.	Auditoría administrativa para el área de cómputo	08 horas
7.	Interpretación de la información	08 horas

Introducción

La información se ha convertido en uno de los activos más valiosos para las empresas públicas y privadas, ya que es determinante para tomar decisiones cuyos resultados se pueden convertir en beneficios o en perjuicios para las empresas o para quien es responsable de tomar las decisiones.

El uso de Tecnologías de la Información (TI) en las empresas como factor de ventaja competitiva es una realidad. Las TI nos ayudan a acelerar el proceso de toma de decisiones, ya que se acorta el tiempo para transformar los datos en información, siempre y cuando esta cumpla con los atributos de: oportunidad, confiabilidad, veracidad, integridad, confidencialidad y accesibilidad. El uso de las TI no garantiza que la información cumplirá con los atributos necesarios o que estas se utilicen de una forma adecuada, por eso surge la necesidad de tener un control sobre las funciones de la informática en las empresas.

La Auditoría en Informática se ocupa de la revisión del uso de las TI, sus inicios se remontan a las auditorías financieras cuyo objetivo primordial es emitir una opinión profesional acerca de los estados financieros de una entidad a partir de una revisión de estos. Como todas las ramas del conocimiento, la Auditoría en Informática ha tomado su propia dirección, tanto a nivel nacional como

internacional, a través de los diferentes Organismos Internacionales de Auditoría en Informática, así como de las instituciones educativas.

Nuestro objetivo es presentar los conceptos fundamentales de Auditoría en Informática y la importancia que tiene para las empresas. Asimismo, el alumno conocerá la metodología general para ejecutar una auditoría y elaborar un dictamen.

TEMA 1. FUNDAMENTOS DE AUDITORÍA EN INFORMÁTICA

Objetivo particular

El alumno reconocerá:

- El concepto de auditoría en informática y sus diferencias con auditoría administrativa y contable.
- La importancia de la auditoría en informática, sus antecedentes, las áreas por auditar en las organizaciones, así como sus beneficios y limitaciones.

Temario detallado

1.1. Concepto de auditoría en informática
1.2. Diferencias entre la auditoría administrativa, auditoría contable y auditoría en informática
1.3. Importancia de la auditoría en informática
1.4. Antecedentes de la auditoría en informática
1.5. Áreas a auditar en informática
1.6. Beneficios y limitaciones de la auditoría en informática

Introducción

El ser humano puede percibir su entorno por medio de los sentidos del gusto, el tacto, la vista, el olfato y el oído, y es precisamente a través de los oídos que podemos percibir ondas sonoras, donde estas se transforman en vibraciones para después codificarse en el cerebro como información. La facultad de oír del ser humano se queda en el simple acto de percibir los sonidos, pero trasciende cuando a esta facultad se le añade la disposición y el entendimiento, es decir escuchar.

Los orígenes de la palabra Auditoría provienen del latín auditorius cuyo origen etimológico es auditor, precisamente “el que escucha”, nosotros consideramos que un Auditor no solamente se limita a escuchar, el despliegue facultativo que realiza el auditor está encaminado a percibir su entorno con todos sus sentidos, a evaluarlo y a opinar acerca de él.

En un esfuerzo formal la Real Academia Española (RAE) nos define la palabra “auditoría” como: “Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse”.

Como hemos comentado la actividad conocida como Auditoría tiene sus inicios en las prácticas de auditorías financieras y, en este ámbito, México cuenta con el Instituto Mexicano de Contadores Públicos (IMCP) que nos define a la Auditoría de la siguiente manera:

> Representa el examen de los estados financieros de una entidad, con el objeto de que el contador público independiente emita una opinión profesional respecto a si dichos estados representan la situación financiera, los resultados de la operaciones, las variaciones en el capital contable y los cambios en la situación financiera de una empresa, de acuerdo con los principios de contabilidad generalmente aceptados. (2008)

Con lo cual la definición de auditoría va más allá de la simple revisión sistemática y evaluación de una actividad o situación, se hace presente que su finalidad es la de emitir una opinión profesional que sea independiente a la entidad, empresa u organización y que al llevar a cabo dicha auditoría se deben respetar los principios generalmente aceptados por dicha actividad o situación.

En este tema el alumno conocerá los conceptos básicos de Auditoría en Informática.

1.1. Concepto de auditoría en informática

Los orígenes de la palabra informática provienen del idioma francés, *informatique* que se refiere a la información automática, este término fue adoptado entre 1966 y 1967 por la Academia Francesa la cual la elevó al grado de ciencia de la siguiente forma: “Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas de la información”.

Existen diferentes concepciones de la informática, pero todos los esfuerzos convergen en el tratamiento sistemático de la información a través de diferentes recursos tecnológicos.

El concepto de Auditoría en Informática de José de Jesús Aguirre Bautista es el siguiente:

> La Auditoría en Informática se refiere a la revisión práctica que se realiza sobre los Recursos Informáticos con que cuenta una entidad, con el fin de emitir un informe y/o dictamen profesional sobre la situación en que se desarrollan y se utilizan, esos recursos.

La revisión que se lleva acabo sirve para comprobar el aprovechamiento de los Recursos Informáticos que abarcan los siguientes elementos: Información, Aplicaciones (software), Infraestructura (hardware, telecomunicaciones, etc.) y Recursos Humanos. Dicha revisión sirve para describir las circunstancias en que se encuentran los Recursos Informáticos y cómo se utilizan; a esta descripción se le conoce como Informe de auditoría, posteriormente el auditor tiene que emitir una opinión profesional acerca de dicho Informe, esta opinión se conoce como dictamen, que resume los hallazgos encontrados durante la auditoría y el juicio del auditor que puede o no ser favorable a la entidad, empresa u organización.

Aunque en la actualidad se realizan diversos tipos de auditoría, no todos llegan a emitir una opinión sobre algún registro, sistema, operación o actividad en particular o con fines específicos. Para lo cual es necesario revisar la diferencia entre Auditoría Informática y las auditorías Administrativas y Contables.

1.2. Diferencias entre la auditoría administrativa, auditoría contable y, auditoría en informática

Las diferencias básicas de las auditorías es su área de aplicación, revisemos los conceptos de Auditoría Administrativa y Contable.

Auditoría Administrativa	"Revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones" (Muñoz, 2002, p. 16)
Auditoría Contable	"Examen de los estados financieros de una entidad, con objeto de que el contador público independiente emita una opinión profesional respecto a si dichos estados presentan la situación financiera, los resultados de las operaciones, las variaciones en el capital contable y los cambios en la situación financiera de la empresa, de acuerdo con los principios de contabilidad generalmente aceptados" (Comisión de Normas y Procedimientos, en Téllez, 2004, p. 45)

La Auditoría Administrativa tiene como propósito evaluar la administración en todas sus etapas del proceso administrativo: planeación, organización, dirección, integración y control y la auditoría contable evalúa la situación financiera de ambas áreas (administrativa e informática); se complementan con la auditoría en informática ya que los recursos informáticos o las TI son el soporte a las funciones de la administración y la contaduría.

El siguiente cuadro contrapone las tres auditorías para hacer una comparación de diferencias y similitudes según sus propiedades.

PROPIEDADES	AUDITORÍA ADMINISTRATIVA	AUDITORÍA CONTABLE	AUDITORÍA INFORMÁTICA
NATURALEZA	Técnica de control administrativo	Técnica de control administrativo	Técnica de control administrativo
PROPÓSITO/ OBJETIVO	Evaluar y mejorar la administración	Dictamen a los estados financieros	Evaluar los recursos informáticos
ALCANCE	La eficiencia y productividad de el proceso administrativo	El sistema contable	Todas las actividades informáticas
FUNDAMENTO	La ciencia administrativa y la normatividad de la empresa	Principios de contabilidad y normas de auditoría	Normatividad institucional y legal, Estándares Internacionales
METODOLOGÍA	Apoyado en métodos científicos	Técnicas y procedimientos predeterminadas	Técnicas y procedimientos predeterminados
APLICACIÓN	A la empresa y sus funciones básicas	A los estados financieros	A todas las áreas de la empresa
PROYECCIÓN	Hacia el futuro	Hacia el pasado	Hacia el futuro
INFORME	Amplio	Preciso	Amplio y Preciso

1.3. Importancia de la auditoría en informática

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con los que cuenta la entidad, sin embargo, por lo que respecta a la tecnología de informática, es decir, software, hardware, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, etc., ésta representa una herramienta estratégica que significa rentabilidad y ventaja competitiva frente a sus similares en el mercado, en el ámbito de los sistemas de información y tecnología un alto porcentaje de las empresas tiene problemas en el manejo y control, tanto de los datos como de los elementos que almacena, procesa y distribuye.

El propósito de la revisión de la auditoría en informática es el de verificar que los recursos, es decir, información, aplicaciones, infraestructura, recursos humanos y presupuestos, sean adecuadamente coordinados y vigilados por la gerencia o por quien ellos designen.

Durante años se ha detectado el despilfarro de los recursos o uso inadecuado de los mismos, especialmente en Informática, se ha mostrado interés por llegar a la meta sin importar el costo y los problemas de productividad.

1.4. Antecedentes de la auditoría en informática

La actividad de auditoría tiene sus orígenes con los intercambios comerciales que se hacían en la antigüedad, al surgir el registro en papel de todos los movimientos comerciales, también surge la necesidad de verificar dicha acción.

En México los “oidores” de la corona española, que con el paso del tiempo se transformarían en auditores, vigilaban el pago de quinto real a los reyes de España, ellos cumplían con verificar el pago de este impuesto.

De manera formal la auditoría en informática tiene como antecedente más cercano a los Estados Unidos de América. En los años cuarenta se empezaron a dar resultados relevantes en el campo de la computación, con sistemas de apoyos para estrategias militares, sin embargo, la seguridad y el control sólo se limitaba a dar custodia física a los equipos y a permitir el uso de los mismos solo a personal altamente calificado.

Fue en el año de 1978 cuando la Asociación de Auditoría y Control de Sistemas de Información por sus siglas en ingles ISACA (*Information Systems Audit and Control Association*) estableció la certificación CISA (*Certified Information Systems Auditor*) para Auditores en Sistemas de Información.

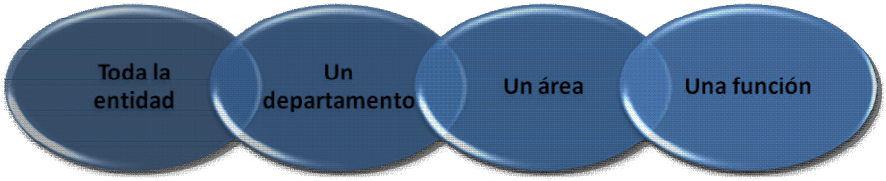
Por otra parte en nuestro país en 1988, el maestro José Antonio Echenique García publicó su libro *Auditoría de Sistemas*, donde establece las bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico-práctico.

Cabe mencionar que en otros países también se han hecho esfuerzos académicos como el realizado por Mario G. Piattini y Emilio Peso en España en el año de 1998 cuando publicaron su obra *Auditoría Informática un enfoque práctico*, donde mencionan diversos enfoques y aplicaciones de la disciplina.

Estos hechos han impulsado a la Auditoría en Informática, misma que se consolida como una actividad estratégica para las empresas.

1.5. Áreas a auditar en informática

Las áreas en donde se puede realizar la auditoría en informática pueden ser:



y se pueden aplicar los siguientes tipos de auditoría:

Sistemas	Evalúa los procedimientos, metodologías, ciclo de vida y el uso de controles en el desarrollo de Sistemas de Información.
Administración de la función de informática	Revisa la aplicación del proceso administrativo en la Informática desde la planeación y control de actividades, la gestión de los presupuestos, costos y adquisiciones, la capacitación del personal y la administración de estándares de operación.
Auditoría a redes	Evalúa el cumplimiento de estándares en la implementación de redes de video, voz y datos, sus topologías, protocolos y funcionamiento así como a su administración, configuración, políticas de acceso y aprovechamiento.
Centros de Cómputo	Revisión de todas las actividades de administración, políticas de mantenimiento, políticas de resguardo y respaldo, políticas de acceso a un centro de cómputo a fin de evaluar el uso de los recursos informáticos.
Seguridad	Evaluación de las protecciones a la Información, Aplicaciones e Infraestructura así como a las actividades preventivas y correctivas. Se puede llevar acabo de manera física y/o lógica.

1.6. Beneficios y limitaciones de la auditoría en informática

El realizar auditorías en informática de una forma periódica y programada nos puede beneficiar de la siguiente forma:

- Evaluar el cumplimiento de planes, programas, políticas, normas y lineamientos.
- Identificar problemas operacionales.
- Proveer oportunidad de mejoras.
- Proveer realimentación para acciones preventivas y correctivas.
- Dictaminar sobre los resultados obtenidos por una empresa, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos.
- Generar confianza internamente a nivel dirección y en los usuarios sobre la seguridad y control de los servicios de TI.
- Generar confianza externamente (clientes y opinión pública).

Por otra parte existen limitaciones como:

- Tiempo. No contar con el tiempo suficiente para ejecutar la auditoría.
- Presupuesto. Tener poco presupuesto asignado para este fin, por lo que se tendrá que recurrir a una auditoría interna.
- Personal. No contar con el personal adecuado y la disponibilidad del mismo es baja.
- Lugar. Dada las dimensiones de área puede sobrepasar en tamaño nuestras capacidades y superar el uso de recursos inicialmente asignados.

Lejos de considerarse una moda entre las entidades, empresas u organizaciones la Auditoría en Informática está justificada por la misma importancia que tiene la información como un factor de ventaja competitiva, el tener el control adecuado sobre los recursos informáticos nos proporciona certeza en la toma de decisiones, nos proporciona confianza y nos asegura el cumplimiento de nuestros objetivos.

Bibliografía básica del tema 1

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Téllez Trejo, Benjamín Rolando. (2004). *Auditoría: un enfoque práctico*. México: Cengange.

Piattini Velthuis, Mario G., Peso Navarro, Emilio del. (1997). *Auditoría Informática: un enfoque práctico*. Madrid: Ra-Ma.

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes]

Cohen, Daniel (2000). *Sistemas de información para los negocios*. (3ª ed.) México: McGraw-Hill.

Sitios electrónicos

(Todos los sitios, consultados o recuperados, de esta asignatura, funcionan al 29/11/11)

Sitio	Descripción
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*
http://www.oocities.org/mx/acadentorno/aui1.pdf	Aguilar Castillo, Gil. (2009). "Capítulo 1" de *Auditoría Informática*, Facultad de Estadística e Informática. Universidad Veracruzana.

Actividades de aprendizaje

A.1.1. Elabora un resumen del tema “Auditoría en Informática en México”

A.1.2. Elabora un mapa conceptual de las diferentes áreas donde se puede aplicar una Auditoría en Informática.

A.1.3. Investiga las diferencias entre Auditoría Interna y Auditoría Externa (indica tus fuentes de consulta).

A.1.4. Elabora un resumen acerca de la certificación CISA.

A.1.5.Construye un cuadro sinóptico acerca de las Normas de Auditoría generalmente aceptadas.

Cuestionario de autoevaluación

Responde las siguientes preguntas.

1. ¿Qué es la auditoría?
2. ¿Cuáles son los recursos informáticos?
3. ¿Cuál es la diferencia entre informe y dictamen de auditoría?
4. ¿Cuál es la diferencia entre auditoría contable y auditoría informática?
5. ¿Cuál es la diferencia entre auditoría en sistemas y auditoría a la función Informática?
6. ¿Cómo defines la importancia de la auditoría en informática?
7. ¿Qué áreas de conocimiento se relacionan con la auditoría?
8. ¿Consideras que la auditoría es necesaria para la seguridad?
9. ¿Cuáles son los beneficios de la auditoría en informática?
10. ¿Cuáles son las características que debe de poseer un Auditor?

Examen de autoevaluación

Elige la respuesta correcta a las siguientes preguntas:

1. Este autor menciona la definición de auditoría en Informática.
   a) José de Jesús Aguirre
   b) Echenique García
   c) Emilio Rosembloth
   d) William Gates

2. Son ejemplos de los tipos de auditoría:
   a) contable, administrativa, informática
   b) externas e internas
   c) públicas y privadas
   d) seguimiento y control

3. Evalúa los procedimientos, metodologías, ciclo de vida y el uso de controles en el desarrollo de Sistemas de Información.
   a) auditoría
   b) control
   c) sistemas
   d) información

4. Una de las propiedades de la auditoría que se refiere a las técnicas es llamada:
   a) objetivo
   b) propósito
   c) naturaleza
   d) alcance

5. Se define como la revisión sistemática a la administración de una empresa, considerando todas las actividades relacionadas con sus operaciones:
   a) auditoría contable
   b) auditoría en informática
   c) auditoría administrativa
   d) auditoría operativa

6. Este tipo de auditoría se encarga de revisar y optimizar los gastos informáticos:
   a) auditoría contable
   b) auditoría en informática
   c) auditoría administrativa
   d) auditoría operativa

7. Se refiere a la cualidad y origen de la solicitud para realizar la revisión de la auditoría en informática.
   a) naturaleza
   b) propósito
   c) alcance
   d) proyección

8. Cuando mencionamos que la auditoría en informática presenta un informe hacia el futuro hablamos de la propiedad de:
   a) proyección
   b) visión
   c) misión
   d) objetivo

9. Proveer oportunidad de mejora es un (a) _____ de la auditoría en informática:
   a) proyección
   b) limitación
   c) misión
   d) beneficio

10. Fue en este año cuando la Asociación de Auditoría y Control de Sistemas de Información por sus siglas en ingles ISACA (*Information Systems Audit and Control Association*) estableció la certificación CISA (*Certified Information Systems Auditor*) para Auditores en Sistemas de Información:
   a) 1980
   b) 1999
   c) 2000
   d) 1978

TEMA 2. MUESTREO ESTADÍSTICO EN LA AUDITORÍA

Objetivo particular

El alumno reconocerá los conceptos básicos del muestreo estadístico utilizado en auditoría, así como los métodos específicos para la auditoría en informática y los riesgos asociados al muestreo estadístico.

Temario detallado

2.1. Conceptos básicos del muestreo
2.2. Métodos de muestreo utilizados en auditoría
    2. 2.1. Muestreo aleatorio simple
    2. 2.2. Muestreo estratificado
    2. 2.3. Muestreo de atributos
    2. 2.4. Muestreo de aceptación
2.3. Inferencia estadística
    2. 3.1. Nivel de confianza y nivel de precisión
    2. 3.2. Pruebas de hipótesis

Introducción

El auditor trabaja o aplica las pruebas para realizar una auditoría a través de muestras, difícilmente se realizarán al 100%, entonces derivado de ello, se auxilia del muestreo estadístico para que el trabajo de auditoría sea más expedito y contundente; asimismo, en este tema se desarrollarán solo algunos ejemplos de lo que es el muestreo y las características de cada uno de ellos.

2.1. Conceptos básicos de muestreo

Hasta el día de hoy la Comisión de Normas y Procedimientos de Auditoría ha emitido el boletín 5020, relativo al muestreo en auditoría que comprende tanto muestreo estadístico como no-estadístico.

El muestreo estadístico es aquél en el que la determinación del tamaño de la muestra, la selección de las partidas que la integran y la evaluación de los resultados se hacen por métodos matemáticos basados en cálculos de probabilidades (véase, IMCP, 2010, p. 392).

	Ejemplo
Población: es el conjunto de todos los elementos de interés en un estudio.	Todas las computadoras adquiridas durante 2010
Una **muestra**: es un subconjunto de una población.	Las computadoras adquiridas en 2010 destinadas para la administración.

2.2. Métodos de muestreo utilizados en auditoría

Existen varios tipos de muestras que se utilizan en auditoría, si bien el IMCP solo menciona el muestreo de atributos y muestreo de variables, existen otros tipos de muestreo, que dependiendo del auditor pueden ser útiles para desarrollar los procedimientos de auditoría, entre ellos encontramos:

- Muestreo aleatorio simple
- Muestreo estratificado
- Muestreo de atributos
- Muestreo de aceptación
- Muestreo por conglomerados
- Muestreo sistemático

- Muestreo por conveniencia
- Muestreo por juicio

2.2.1 Muestreo aleatorio simple

La definición de este método y el proceso de seleccionar una muestra aleatoria simple depende si la población es finita o infinita. Se habla que la población es finita, cuando se puede realizar un conteo de ella y la población infinita es aquella que no se puede realizar un conteo de ella.

Muestreo aleatorio simple (población finita)

Una muestra aleatoria simple de tamaño *n*, de una población finita de tamaño *N*, es una muestra seleccionada de tal manera que cada muestra posible de tamaño *n* tenga la misma probabilidad de ser seleccionada.

La técnica de selección para el muestreo en la auditoría está basada en la selección al azar o aleatoria, que es la que asegura que todas las partidas dentro del universo o dentro de cada estrato tengan la misma posibilidad de ser seleccionadas, por ejemplo, mediante el uso de tablas de números al azar.

Muestreo aleatorio simple (población infinita)

Es aquella que se selecciona de tal forma que se satisfacen las siguientes condiciones:

- Cada elemento seleccionado proviene de la misma selección.
- Cada elemento se selecciona de forma independiente.

Supóngase que una población tiene 400 elementos. Con los tres últimos dígitos de los siguientes números aleatorios de cinco dígitos (601, 022, 448,…),

Determínese los cuatro primeros elementos que se seleccionarán para la muestra aleatoria simple.

98601 73022 83448 02147 34229 27553
84149 93289 14209

2.2.2. Muestreo estratificado

Es aquel en el que se divide la población de *N* individuos, en *n* estratos, atendiendo a criterios que puedan ser importantes en el estudio, de tamaños respectivos *N*1, ..., *Nn*,

En este tipo de muestreo primero se dividen los elementos de la población en grupos llamados estratos, de tal manera que cada elemento de la población pertenece a un estrato. Si los estratos son homogéneos el procedimiento de muestreo estratificado producirá resultados tan precisos como el muestreo aleatorio simple, pero con menor tamaño de la muestra.

Ejemplo
Supóngase que realizamos un estudio sobre la población de estudiantes de la FCA, de la licenciatura en Informática, en el que a través de una muestra de 10 de ellos queremos obtener información sobre el uso de Equipo de cómputo en la Biblioteca.

Lo que procede es hacer un muestreo aleatorio simple, pero en su lugar podemos reflexionar sobre el hecho de que el comportamiento de la población con respecto a este carácter no es homogéneo, y atendiendo a él, podemos dividir a la población en dos estratos:

- Estudiantes masculinos (60% del total);
- Estudiantes femeninos (40% restante).

De modo que se repartan proporcionalmente ambos grupos el número total de muestras, en función de sus respectivos tamaños (6 varones y 4 mujeres). Esto es lo que se denomina *asignación proporcional*.

Si observamos con más atención, nos encontramos con que el comportamiento de los varones con respecto al carácter que se estudia es muy homogéneo y diferenciado del grupo de las mujeres.

2.2.3. Muestreo por atributos

El muestreo por atributos es un método estadístico que se utiliza para calcular la proporción de partidas de una población que contiene una característica o un atributo de interés. Esta proporción recibe el nombre de tasa de concurrencia o tasa de excepción y es la proporción de partidas que contienen el atributo específico en relación con el número total de partidas de la población. La tasa de ocurrencia por lo general se expresa como un porcentaje.

A los auditores les interesa la ocurrencia de los siguientes tipos de excepciones en las poblaciones de datos contables:

- Desviación de los procedimientos del control establecido por el cliente.
- Errores o irregularidades monetarias en los datos de las operaciones.
- Errores o irregularidades monetarias en los detalles de los saldos en las cuentas.

El auditor llegará a la conclusión de que la tasa de excepción de la muestra es el cálculo más probable de la tasa de excepción de la población.

Dado que se basa en una muestra, sin embargo, existe una probabilidad significativa de que la tasa de excepción de la muestra y la tasa de excepción de

la población real difieran. Los métodos estadísticos permiten al auditor indicar la medida en que los dos índices de excepción probablemente difieran y la confiabilidad del cálculo. Lo primero recibe el nombre de precisión y lo segundo riesgo de muestreo. Así pues una vez que se calcula el índice de excepción de la muestra, el auditor determinará la precisión del cálculo, lo sumará y lo restará del índice de excepción de la población. El auditor llegará a la conclusión de que el cálculo del intervalo contiene el índice de excepción real de la población en determinado riesgo de muestreo. El *riesgo de muestreo* se relaciona con la posibilidad de que una muestra debidamente extraída pueda no ser representativa del Universo.

Por ejemplo de un universo de gente en un Mercado se quiere conocer quiénes tienen estudios Universitarios. Así, el universo es el Mercado, el atributo son los estudios universitarios, y el resultado no concluirá que todas las personas de los mercados cuentan o no con estudios universitarios.

2.2.4. Muestreo de aceptación

El muestreo de aceptación está basado en el nivel de confianza y prueba que se determine con base al ensayo que se realice, la propuesta de aceptación o no aceptación la determina el resultado de las pruebas realizadas de acuerdo con parámetros o índices determinados en la planeación de la auditoría, cuando se realizan las pruebas, se cuenta con elementos de indispensables que marcan si las pruebas son aceptadas o no.

Ejemplo
Cuando se han revisado los expedientes del activo fijo, en este caso, de un universo de 100 computadoras, aproximadamente se han revisado 30, y contiene cada uno de ellos lo que es necesario para su control, podemos dar por aceptado el procedimiento de guarda y custodia de los expedientes de computadoras.

Algunos requerimientos son:

- Justificación de uso del área solicitante.
- Requisición o solicitud de compra.
- Cotizaciones.
- Cuadros comparativos.
- Justificación técnica, económica u operativa.
- Factura.
- Entrada y salida del almacén.
- Número de inventario.
- Resguardo de bienes.

Si los 30 expedientes seleccionados cumplen con todas estas características, entonces aceptamos que el procedimiento es válido y con un nivel de confianza elevado.

2.3. Inferencia estadística

Lo que nos otorga la inferencia estadística es la utilidad e interpretación de los de datos, para transformarlos en información que nos auxilie al tomar una consideración o decisión, tomando en consideración el nivel de confianza, que le vamos a otorgar a esos datos utilizados para poder inferir que estos son correctos y útiles.

2.3.1. Nivel de confianza y nivel de precisión

El nivel de confianza para el auditor está basado en el control interno que se ejerza por parte de la administración, es decir entre más y mejores controles existan para las actividades propias que se requieran, menores serán las pruebas realizadas por el auditor, ya que la revisión que se realice va a elevar o disminuir la confianza depositada en nuestras pruebas de auditoría.

Tendremos que elevar el nivel de confianza basado en riesgos, ya que entre mejores procedimientos se obtengan, el resultado es que tienden a disminuir los riesgos, es decir, la posibilidad de que existan errores en la información o, bien, ineficiencia operativa.

Asimismo el nivel de precisión está basado en la totalidad y exactitud que se tenga al elaborar las pruebas, reduciendo al mínimo el margen de error que se pudieran presentar al momento de practicar la auditoría, por lo que el nivel de confianza y el de precisión se encuentran ligados en el accionar de las pruebas de auditoría.

2. 3.2. Pruebas de hipótesis

Es una proposición o supuesto sobre los parámetros de una o más poblaciones.

Tenemos que la hipótesis nula se rechaza o no se rechaza, y se representa así.

Hipótesis nula	:Ho Siempre está el	=	=	<	>
Hipótesis Alterna	:Ha Siempre está el	=	>	>	<

Se tiene que los laboratorios FCA lanzarán un nuevo producto contra todos los virus informáticos solamente si en las pruebas, resulta mejor que los antivirus que actualmente se comercializan. El antivirus actual quita un 78% de virus conocidos, se planea hacer un estudio con 10,000 computadoras con un nivel de confianza del 97.5%.

Ho: El nuevo antivirus no es mejor que los existentes.

Ha: El nuevo antivirus es mejor que los existentes.

El Universo

Es el total de las operaciones que realiza una entidad o bienes tangibles o intangibles que en ella se encuentran, asimismo es un todo de un conjunto que nos interesa en particular al realizar la revisión.

Si fuera el caso de una revisión a la Dirección de Informática, se podría tomar como universo el total de Software que se ha desarrollado en esa Dirección, o el total de software que se ha adquirido.

Riesgo y Certidumbre

Cuando se acepta realizar algún tipo de auditoría, existe como consecuencia de cualquier actividad practicada, la posibilidad de dejar de evaluar algunos aspectos que pueden ser o no relevantes para la aplicación de la auditoría y que, por lógica, repercute en las observaciones e informe del auditor.

Riesgo Inherente

Este tipo de riesgo se da por la práctica misma de la auditoría.

Riesgo de Control

El riesgo de control se da por no contar con los controles internos adecuados al realizar las actividades, ya sea por ausencia, debilidad o incumplimiento de los controles establecidos por la Institución.

Riesgo de detección

Es el riesgo que se tiene implícito al realizar el muestreo de auditoría, ya que al trabajar con pruebas selectivas se puede incurrir en el riesgo de no detectar un hecho importante que pueda traducirse en fraude.

Error tolerable

Es el error que un auditor considera dentro de sus parámetros muestrales, es decir, es el nivel de sesgo máximo permitido para alcanzar resultados satisfactorios que de manera sólida tiene el auditor al realizar sus pruebas de auditoría. Fuera de ese margen se tendrá que aumentar el tamaño de la muestra para elevar el nivel de confianza y se reduzca el margen de error.

Error esperado en el universo

El error esperado se da desde la selección de la muestra, dependiendo del conocimiento de la actividad u operación que se tenga al realizar las pruebas de auditoría, por lo que a mayor conocimiento de la actividad, menor será el error esperado que es el margen de error que puede controlar el auditor y además tiene conocimiento y conciencia de su probable ocurrencia.

Bibliografía básica del tema 2

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2010). Boletín 5020 “El Muestreo en la Auditoría” en *Normas y Procedimientos de Auditoría y Normas para Atestiguar*. México: IMCP, p. 392.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Bibliografía complementaria

Cohen, Daniel (2000). *Sistemas de información para los negocios*. (3ª ed.) México: McGraw-Hill.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

Sitios electrónicos

Sitio	Descripción
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*

Actividades de aprendizaje

A.2.1. Elabora un resumen del tema “Muestreo estadístico en Auditoría en informática”.

A.2.2. Elabora un mapa conceptual de las diferentes áreas donde se puede aplicar el muestreo estadístico en una Auditoría en Informática.

A.2.3. Construye un cuadro sinóptico acerca del boletín 5020 el Muestreo en Auditoría de las Normas y Procedimientos de Auditoría y Normas para Atestiguar.

A.2.4. Supóngase que se está en posibilidad de realizar una auditoría a una Institución que cuenta con 1500 computadoras, su último inventario arrojó que el 30% de ellas tiene tres años de antigüedad, el 25% tiene 4 años de antigüedad y el resto son de reciente adquisición, cada una contiene información importante e indispensable para la Institución.

Se busca verificar que todo el software que utiliza la empresa sea de adquisición legal.

Justifica:

1.- ¿Qué tipo de muestreo utilizarías y por qué?
2.- ¿Cuál sería su nivel de confianza y por qué?
3.- ¿Cuál sería el error tolerable y por qué?
4.- ¿Cuál sería el riesgo de detección y por qué?

Cuestionario de autoevaluación

Responde las siguientes preguntas.

1. ¿Qué es el Muestreo Estadístico?
2. ¿Cuáles son los métodos estadísticos utilizados en auditoría?
3. En qué consiste el muestreo aleatorio simple.
4. ¿Qué es una población?
5. ¿Qué es muestreo estratificado?
6. ¿Qué es el riesgo de auditoría?
7. ¿Qué es el muestreo de aceptación?
8. ¿Qué es el universo?
9. ¿Qué es el error en el muestreo estadístico?
10. ¿Qué es la hipótesis?

Examen de autoevaluación

Elige la respuesta correcta a las siguientes preguntas.

1. La Comisión de Normas y Procedimientos de Auditoría ha emitido el boletín referente al muestreo estadístico.
   a) 3040
   b) 5020
   c) 5030
   d) 3050

2. Son ejemplos de los tipos de muestreo:
   a) aleatorio y estratificado
   b) simple y compuesto
   c) atributos y acelerado
   d) seguimiento y análisis.

3. Es el conjunto de todos los elementos de interés en un estudio.
   a) población
   b) muestra
   c) universo
   d) extracto

4. Es el subconjunto de una población.
   a) población
   b) muestra
   c) universo
   d) extracto

5. Es un método estadístico que se utiliza para calcular la proporción de partidas de una población que contiene una característica en específico.
   a) aceptación
   b) compuesto
   c) estratificado
   d) atributos

6. Es el proceso de inspección de una muestra de unidades extraídas de un lote con el propósito de aceptar o rechazar todo el lote.
   a) aceptación
   b) compuesto
   c) estratificado
   d) atributos

7. Persigue la obtención de conclusiones sobre un gran número de datos
   a) inferencia estadística
   b) nivel de confianza
   c) error tolerable
   d) riesgo por no muestrear

8. El riesgo de que ocurrirán errores importantes también se conoce como
   a) riesgo tolerable
   b) riesgo de control
   c) riesgo de detección
   d) riesgo inherente

9. Es el error máximo en el Universo que el auditor estaría dispuesto a aceptar y a pesar de eso concluir que el resultado del muestreo ha alcanzado su objetivo de auditoría.
   a) error por no muestrear
   b) error tolerable
   c) error permitido
   d) error de asignación

10. Se obtiene a partir de la distribución normal estándar
   a) nivel de atributos
   b) nivel permitido
   c) nivel de hipótesis
   d) nivel de confianza

TEMA 3. METODOLOGÍA GENERAL PARA LA AUDITORÍA EN INFORMÁTICA

Objetivo particular

Diseñar una metodología de auditoría informática a través de los documentos necesarios para su ejecución.

Temario detallado

3.1. Investigación preliminar
3.2. Planeación de la auditoría en informática
3.3. Documentación para la auditoría en informática
    3.3.1. Documentación del software de aplicación, del hardware, y de la biblioteca
    3.3.2. Desarrollo y Manual de estándares
    3.3.3. Organigrama y descripción de puestos del área de informática
3.4. Análisis, evaluación y presentación de la auditoría
3.5. Dictamen de la auditoría en informática

Introducción

Metodología es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado. Generalmente existen diversas formas de obtener un resultado determinado, y de esto se deriva la existencia de varias metodologías para llevar a cabo una auditoría informática, sin embargo veremos una de ellas con características generales.

3.1. Investigación preliminar

La investigación preliminar consiste básicamente en una serie de encuentros con un prospecto de cliente, con el objeto de conocer necesidades y características del trabajo que se va a realizar, asimismo de la Institución auditada; es decir, vamos a realizar un estudio general del escenario planteado por el cliente.

Estudio General

Es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones, a través de sus elementos más significativos para concluir se ha de profundizar en su estudio y en la forma que ha de hacerse, además de inspección física, número de empleados, recursos humanos financieros, y tecnológicos, años de antigüedad, capacidad instalada, etc.

3.2. Planeación de la auditoría en informática

Consiste en la elaboración de los programas de trabajo que se llevarán a cabo durante la revisión a la entidad auditada y puede constar de varias etapas, sin embargo, las más relevantes desde un punto de vista objetivo son las siguientes.

Diagnóstico informático. El Diagnóstico Informático tiene por objetivo, proporcionarnos una panorámica de cómo la empresa percibe y practica la informática, a través de su administración, y de los usuarios primarios y secundarios.

Investigación previa. Aquí conoceremos la infraestructura y capacidad instalada de empresa y de ser posible validaremos la problemática que nos fue expuesta por el cliente o en su defecto redefiniremos la problemática.

Después de esto se estará en posibilidades de hacer una mejor estimación del trabajo, tiempo y de los honorarios, si es que no se pudo hacer en la primera fase.

Elaboración del programa de la AI. Todo buen administrador debe planear sus actividades y el auditor no debe ser la excepción, el programa señala las actividades que han de realizarse, fechas de inicio y término, así como los tiempos.

Actividad	Inicio	Término	Días	Elaboró	Revisó
1.=Planeación	8/01/08	9/01/08	2	ACC/JJAB	PRS
2.= Entrevistas	10/01/08	12/01/08	3	ACC	JJAB
3.=Cuestionarios de control interno	12/01/08	15/01/08	4	ACC	JJAB

3.3. Documentación para la Auditoría en Informática

La documentación es la evidencia suficiente y competente que soporta la opinión de auditor. Debido a la planeación, sabremos qué solicitar al momento de realizar la auditoría. La suficiencia y competencia se refiere a requisitos de cualidad (calidad) y cantidad.

En esta fase se obtendrá toda la información pertinente sobre el caso estudiado, pudiendo recurrir a herramientas como: entrevistas, encuestas, observación, etc., dependiendo del tipo de información que necesite.

Análisis, clasificación y evaluación de la información

El análisis y clasificación de la información podrán realizarse por métodos estadísticos.

Evaluación: es aquí donde se pone a prueba el talento del auditor, porque se requiere para entender e interpretar la información y continuar con el siguiente paso.

3.3.1. Documentación del software de aplicación, del hardware, y de la biblioteca

La importancia de la documentación radica en la obtención de la evidencia del trabajo desarrollado, es decir, que cuando se esté auditando un software, tengamos la documentación comprobatoria como solicitudes del trabajo, autorizaciones, minuta de reuniones, establecimiento de prioridades, licitaciones, estudios de factibilidad y formas de respaldo y resguardo debidamente documentadas por módulo o por sección.

Software de aplicación

Para soportar esta información necesitamos solicitar lo siguiente:

Los manuales se solicitan a los desarrolladores de sistema o al líder del proyecto del ciclo de vida del desarrollo de un sistema o al responsable de sistemas. Ya que ellos son los responsables de realizar cada manual cuando necesiten liberar el sistema.

Solicitar los manuales: de usuario, de sistema y técnico.

Manuales

De usuario

El manual de usuario contiene los requisitos para la instalación del sistema, la introducción, objetivos, módulos, características del sistema, y sus procesos para el uso adecuado del mismo.

De sistema

Este manual se refiere a las características del sistema, los módulos que contiene, el lenguaje utilizado, los comentarios y las versiones del mismo, las pruebas que fueron realizadas, la bitácora y mantenimiento.

Técnico

Se refiere a los recursos técnicos utilizados y que le son útiles para su mantenimiento y soporte.

En algunos casos cuando el software de aplicación es adquirido de forma comercial, ya vienen estipulas las instrucciones de configuración, requerimientos del sistema, etc. Sin embargo cuando el software de aplicación es desarrollado por la entidad auditada o “ad hoc” para las necesidades de la entidad por un tercero, la documentación debe abarcar desde, requerimiento de necesidades, autorizaciones del desarrollo de la aplicación, pruebas, resultados de las pruebas, plan de instalación, requerimientos del sistema, lenguajes de programación, pistas de auditoría, ver si lo que se pretende automatizar esta sistematizado, etc.

Hardware

La documentación del Hardware abarca los siguientes aspectos:

- Necesidades del área solicitante
- Características del hardware
- Solicitud de compra
- Cotizaciones

- Cuadros comparativos
- Justificaciones, técnica, económica, operativa y legal.
- Valores agregados, etc.
- Documentación de bibliotecas.

Biblioteca

Al realizar la programación tendremos que validar las características y documentación integrada de las bibliotecas, y verificar que estas hayan sido incluidas de manera puntual en el sistema. Tendremos que verificar lo siguiente.

Biblioteca Estática

Consiste en un conjunto de rutinas que se copian en una aplicación por un compilado.

Biblioteca Dinámica

Significa que las subrutinas de una biblioteca son cargadas en un programa en tiempo de ejecución, en lugar ser enlazadas en tiempo de compilación, y se mantienen como archivos independientes separados del fichero ejecutable del programa principal.

Básicamente analizaremos y validaremos las características de las bibliotecas.

La **validación** se realiza haciendo pistas de auditoría, con el fin de que las bibliotecas hagan lo que dicen que hace, es decir, que cumplan con la función de compilar y ejecutar los programas, las pistas de auditoría son copias que se utilizan para realizar pruebas.

Además de lo anterior certificaremos las normas internas en cada uno de los procesos de informática.

La **certificación** se da a través de las técnicas de auditoría, así como el estudio y evaluación del control interno, en donde se evalúa, pondera y califica cada proceso de auditoría.

3.3.2. Desarrollo y manual de estándares

Todos los sistemas de información deben ser sostenibles, modificables y auditables y para ello deben contar con manuales, esto debe estar por normatividad, y si no es así, es una falla de control. Los manuales nos ayudan a tener una radiografía del sistema a auditar o que está en ejecución, además todos los sistemas deben tener estos manuales de no hacerlo así, se corre el riesgo de que no se le pueda dar mantenimiento al sistema y caería en la obsolescencia o desuso, lo que se traduce en pérdida de tiempo y esfuerzo para las empresas.

Operación

- Representación gráfica de la estructura del sistema.
- Función de cada programa.
- Requerimientos de equipo.
- Tamaño estimado de archivos (normal y máximo).
- Explicación de los mensajes de la consola, junto con la respuesta adecuada del operador.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Calendarización de procesos.
- Parámetros a alimentar.
- Creación de salida y su distribución.
- Identificación adecuada de las etiquetas de los archivos de salida.
- Puntos de reinicio y recuperación.
- Procedimientos para notificar errores o condiciones defectuosas.
- Procedimientos para casos de emergencia.

Usuario

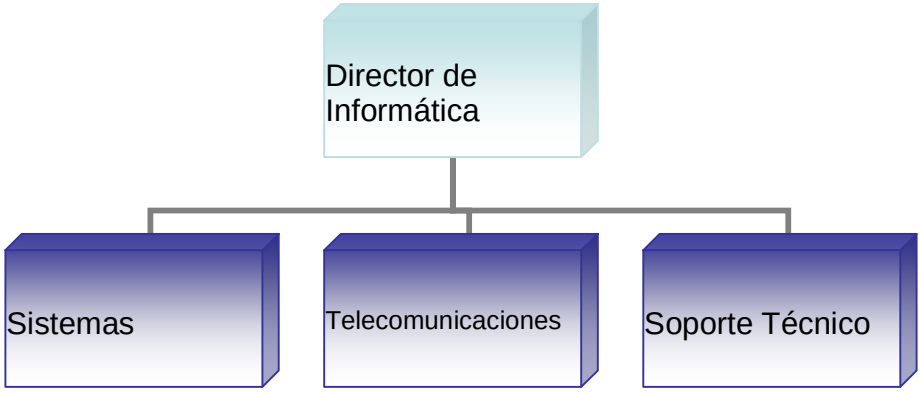
- Representación gráfica de la estructura del sistema.
- Procedimientos de preparación de datos.
- Asignación de prioridades.
- Tiempo probable de respuesta y recepción de productos finales.
- Especificaciones de diseño de entrada de datos (formatos y pantallas de captura).
- Especificaciones de diseño de salida de datos (reportes / pantallas de consulta).
- Controles de usuario.
- Procedimientos para resolver errores e incongruencias.
- Controles sobre la entrada y salida.

Sistema

- Representación gráfica de la estructura del sistema.
- Documentación de cada programa de cómputo.

La revisión de la documentación de una aplicación: involucra identificar su existencia, analizar su contenido y juzgar su oportunidad y disponibilidad. La calidad del mantenimiento de sistemas depende en gran medida de la calidad de la documentación. Además de la claridad y organización de la documentación, debe dedicarse especial atención al tipo de personas a quien va dirigido.

3.3.3. Organigrama y descripción de puestos del área de informática



Este organigrama es sólo de dos niveles, lógicamente esto cambia dependiendo de las características de la Institución y las necesidades de la misma.

Por ejemplo

Para Director de Informática tenemos las siguientes características, siendo estas de manera enunciativa:

Académicos	Título de Licenciatura en: Informática, Contaduría, Administración o Ingeniería.
Laborales	6 años de experiencia en: Auditorías en Informática, tanto en Instituciones privadas como gubernamentales.
Capacidades Gerenciales	Liderazgo y orientación a resultados.
Idioma	Inglés 80%
Calificación Técnica	80
Comentarios	

Para los gerentes

Académicos	Título de Licenciatura en: Informática, Contaduría, Administración o Ingeniería.
Laborales	3 años de experiencia en: Auditorías en Informática, tanto en Instituciones privadas como gubernamentales. Así como proyectos relacionados con la automatización de procesos.
Capacidades Gerenciales	Liderazgo y orientación a resultados.
Idioma	Inglés 80%
Calificación Técnica	80
Comentarios	

Los puestos de jerarquías menores se recomienda que sean pasantes o estudiantes de los últimos semestres de informática, contaduría y administración debidos a los procesos repetitivos de las tareas diarias.

3.4. Análisis, evaluación y presentación de la auditoría

Para realizar el *análisis* de los hallazgos derivados de la revisión es primordial separar lo importante de lo urgente, con el objeto de reconocer qué información es útil y principal y cuál es de soporte y secundaria.

Derivado de lo anterior obtenemos la evidencia suficiente y competente que sirve de base para respaldar nuestro informe, estas etapas se dan desde el inicio de la auditoría y se van supervisando continuamente de manera que no debemos esperar a que finalice la auditoría para realizar esta etapa de la metodología en la auditoría; adicionalmente se deben considerar otros elementos importantes de la presentación y conclusión del dictamen o informe de auditoría.

Informe, elaboración y presentación del informe final
En él se informará de manera clara y concisa, sobre los resultados de la Auditoría en informática (AI). No debemos olvidar que a los ojos de nuestro cliente él paga por recibir un informe, y en este debe encontrar valiosas recomendaciones que habrán de mejorar su administración, el informe aunque es escrito, debe presentarse apoyado en una exposición verbal.

Implementación y seguimiento. Algunos autores consideran esta fase como opcional, que no corresponde al auditor realizarla, sino a la empresa, yo considero que el auditor debe participar, para que se interpreten correctamente sus recomendaciones y no haya lugar a desvíos en las mismas.

3.5. Dictamen de la Auditoría en Informática

El Informe es un documento formal a través del cual, el auditor plasma el resultado del trabajo desempeñado, basado en la Normatividad aplicable para cada situación, y por lo tanto está en posibilidades de emitir una opinión, y se compone de la siguiente estructura:

Principio

- Lugar y fecha de emisión
- Destinatario
- Antecedentes
- Alcance de la auditoría
- Limitaciones al trabajo
- Personal asignado

Cuerpo

- Hallazgos y observaciones
- Secciones o apartados especiales
- Resumen evaluativo de correcciones operadas durante la auditoría

Final

- Opinión y conclusiones del auditor
- Comentarios y puntos de vista de los auditores
- Sugerencias y recomendaciones
- Párrafo de cierre; mencionar las facilidades y atenciones brindadas al auditor
- Firma

A continuación se presenta un ejemplo de un Dictamen corto de Auditoría.

INFORME DE AUDITORÍA EN INFORMÁTICA SOBRE CONTROLES GENERALES

DESPACHO AR INTERNACIONAL S.C.
AUDITORÍA EN INFORMÁTICA
INFORME No 11/JJAB/11

QFB. GUILLERMO GONZÁLEZ VARGAS
DIRECTOR
FACULTAD DE ALQUIMISTAS
UNAM
Presente

Informe de la revisión efectuada a la Facultad de Alquimistas por el periodo comprendido del 1 de enero al 31 de diciembre del 2010, derivada de la intervención realizada del 2 de enero al 30 de abril del 2011 por el despacho AR Internacional S.C.

Hemos examinado los procedimientos de control en informática, específicamente a controles generales al 31 de diciembre de 2010. Dichos controles son responsabilidad de la administración de la dependencia. Nuestra responsabilidad consiste en expresar una opinión sobre los mismos con base en mi auditoría.

Como se menciona en el párrafo siguiente, nuestros exámenes fueron realizados de acuerdo con las normas institucionales, de la propia dependencia y legales, así como el manejo de los

equipos establecidos por los proveedores, referentes a la utilización de recursos informáticos, toda auditoría requiere que sea planeada y realizada de tal manera que permita obtener una seguridad razonable de que el manejo de recursos informáticos y las metodologías auditadas no contengan errores importantes, y de que se están utilizando de acuerdo con las políticas y normatividad internas, así como estándares de uso informático. La auditoría consiste en el examen, con base en pruebas selectivas, de la evidencia que soporta las cifras y revelaciones de los recursos informáticos; asimismo, incluye la evaluación de los bienes informáticos utilizados, de las estimaciones significativas efectuadas por la administración. Consideramos que nuestros exámenes proporcionan una base razonable para sustentar mi opinión.

Debido a que éste tipo de auditorías se revisa por etapas y como auditor de la dependencia, no observé los inventarios físicos de ese año y debido a la naturaleza de los registros de recursos informáticos no pude satisfacerme, a través de la aplicación de otros procedimientos de auditoría, de dichos inventarios. Así como de la deficiencia en las etapas de seguridad física, lógica y plan de contingencias y regular en las etapas de adquisiciones y sistema operativo.

En nuestra opinión, debido a la importancia por el efecto de los ajustes que pudiese haber determinado en el costo de los recursos informáticos, si hubiéramos presenciado los inventarios físicos iniciales de la compañía, como se menciona en el párrafo anterior, la auditoría de controles generales y sus etapas antes mencionadas no presentan

razonablemente en todos los aspectos importantes, la situación informática de la dependencia, por el periodo comprendido del 1 de enero al 31 de diciembre del 2010, y los resultados de sus operaciones, y sus etapas que constan de adquisiciones, sistema operativo, seguridad física, seguridad lógica y plan de contingencias, por el periodo terminado en esa fecha que le son relativos, de conformidad con los estándares nacionales e internacionales existentes para la auditoría de controles generales de recursos informáticos.

México D.F., a 11 de mayo de 2011

L.C y M.AUD. José de Jesús Aguirre Bautista
Director

Bibliografía básica del tema 3

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes]

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

Sitios electrónicos

Sitio	Descripción
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*
http://www.oocities.org/mx/acadentorno/aui.htm	Aguilar Castillo, Gil. (2009). *Auditoría Informática*, Facultad de Estadística e Informática. Universidad Veracruzana.

Actividades de aprendizaje

A.3.1. Elabora un mapa conceptual de las diferentes etapas de la metodología general para realizar una Auditoría en Informática.

A.3.2. Investiga las diferencias entre la metodología para efectuar una Auditoría en Informática y Auditoría financiera (indica tus fuentes de consulta).

A.3.3. Investiga las diferencias que existen entre un dictamen o informe limpio, con salvedad, negativo o con abstención de opinión, de la Auditoría en informática.

A.3.4. Investiga si en México existe un modelo de dictamen en informática para plasmar los resultados obtenidos en su correspondiente auditoría en informática, si fuera afirmativo qué aspectos legales contienen y qué autoridad la regula.

A.3.5. Investiga el informe o dictamen de una auditoría en informática que se practica en otros países y realiza un comparativo entre lo que se presenta en México y lo que investigaste e informa ¿cuál es mejor para ti y por qué?

Cuestionario de autoevaluación

Responde las siguientes preguntas:

1. ¿Qué es Metodología?
2. ¿Cuáles son sus etapas?
3. ¿Qué es Investigación Preliminar?
4. ¿Qué es Planeación?
5. ¿Qué documentación contiene el software de aplicación?
6. ¿Qué es la Biblioteca en informática?
7. ¿Qué contiene un manual informático?
8. ¿Cuál es la estructura de un departamento de informática?
9. ¿Qué es un hallazgo en auditoría en informática?
10. ¿Cuál es la estructura de un dictamen informático?

Examen de autoevaluación

Elige la respuesta correcta a las siguientes preguntas:

1. Es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado:
   a) sistema
   b) metodología
   c) diagnóstico
   d) evaluación

2. Es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones:
   a) estudio general
   b) metodología
   c) diagnóstico
   d) evaluación

3. Consiste en la elaboración de los programas de trabajo que se llevaran a cabo durante la revisión a la entidad auditada:
   a) estudio general
   b) metodología
   c) planeación
   d) investigación

4. Es la evidencia suficiente y competente que soporta la opinión de auditor:
   a) estudio general
   b) metodología
   c) documentación
   d) evaluación

5. En esta etapa es donde se pone a prueba el talento del auditor, porque es indispensable para entender e interpretar la información y así continuar con el siguiente paso.
   a) planeación
   b) metodología
   c) evaluación
   d) estudio general

6. Este manual contiene los requisitos para la instalación del sistema:
   a) manual de usuario
   b) manual de sistema
   c) manual de aplicación
   d) manual de operación

7. Significa que las subrutinas de una biblioteca son cargadas en un programa en tiempo de ejecución, nos referimos a:
   a) biblioteca digital
   b) biblioteca manual
   c) biblioteca dinámica
   d) biblioteca estática

8. Es un documento formal a través del cual, el auditor plasma el resultado del trabajo desempeñado:
   a) documento
   b) papel de trabajo
   c) hallazgos
   d) informe o dictamen

9. Cuando se plasman las limitaciones al alcance del trabajo nos referimos a la estructura del informe o dictamen en cuanto a:
   a) cuerpo
   b) opinión
   c) principio
   d) final

TEMA 4. AUDITORÍA DE SISTEMAS

Objetivo particular

Reconocer las estrategias para realizar una auditoría a sistemas, desarrollando y aplicando los instrumentos requeridos para dar un reporte de los resultados obtenidos.

Temario detallado

4.1. Documentación y estándares
- 4.1.1. Entrada
- 4.1.2. Flujo de información
- 4.1.3. Proceso
- 4.1.4. Salida
- 4.1.5. Archivos
- 4.1.6. Respaldos
- 4.1.7. Controles, operación, mantenimiento y cambios correctivos
- 4.1.8. Control de estándares
- 4.1.9. Integridad de los datos y manejo de cifras de control
- 4.1.10. Controles en el desarrollo de sistemas
- 4.1.11. Controles en base de datos

4.2. Confidencialidad de los sistemas

4.3. Seguridad de los sistemas

4.4. Análisis costo/beneficio pronosticado contra el costo/beneficio obtenido

4.5. Encuestas a usuarios.
- 4.5.1. Ventajas obtenidas
- 4.5.2. Necesidades no cubiertas
- 4.5.3. Desventajas del sistema
- 4.5.4. Limitaciones del sistema

Introducción

La auditoría de sistemas cobra gran importancia debido a que hoy en día los sistemas con que cuenta una Institución son muchos y de características diversas, a pesar de que existen sistemas integrales, estos no son la mayoría, por lo que se debe conocer perfectamente cuál es sistema por auditar y el más esencial para la actividad diaria, asimismo cuál de estos sistemas es el de mayor riesgo y susceptible de que al estropearse o fallar pare las actividades de la Institución.

4.1. Documentación y estándares

Antes de iniciar la revisión de los sistemas debemos saber que para poder automatizar cualquier proceso, es necesario primero reconocer si este proceso está sistematizado, es decir, si lo que vamos a realizar o revisar cuenta con un procedimiento lógico y secuencial y además es estándar, es conocido y reconocido por todos los participantes de la elaboración del sistema.

Es importante señalar que la estandarización en la metodología para la elaboración de los sistemas debe definirse desde el comité de cómputo, si es que existe, y que además es recomendable, o por alguien que tenga conocimiento y jerarquía para hacerlo.

Ya que este debe estandarizar las etapas para la realizar los sistemas, que son: planeación, análisis, diseño, desarrollo e implementación.

Planeación

- Requisición de servicios.

Análisis

- Estudio de factibilidad.

Diseño

- Diseño general del sistema.
- Diseño detallado del sistema.

Desarrollo

- Programación.
- Prueba modular y prueba del sistema integral.
- Desarrollo de manuales.
- Entrenamiento.

Implantación

- Conversión.
- Revisión de la post-implantación.

Ejemplo

a) Planeación

Requisición de servicios

Procedimiento por el cual se requiere el servicio del desarrollo del sistema.

- Justificación. ¿Por qué se realizó?, ¿quién?, ¿cómo?, beneficios, responsables, etc.
- Ambiente en el que se va a operar y quién lo va a operar.
- Alcance. Por módulo, ¿qué se quiso?, ¿hasta dónde llegó?
- Restricciones ¿las hubo? en qué sentido
- Beneficios. ¿Se obtuvieron los resultados esperados?
- Integración del equipo de trabajo y sus responsabilidades.
- Definición de requisitos de información, nuevos y existentes.

- Aprobación del proyecto. Se espera que lo haya realizado el Comité interno de informática.

b) Análisis

Estudio de factibilidad

En esta fase se analizan los diversos escenarios para llevar a cabo el sistema.

- Estudio de los procedimientos existentes. Como el líder del proyecto, diagramas, narrativas, etc.
- Formulación de cursos alternativos de acción. Planteamiento de diversos escenarios, plan A y plan B y en algunos casos plan C.
- Factibilidad tecnológica.
- Disponibilidad de la tecnología que satisfaga las necesidades del usuario, y de la empresa, así como actualización o complemento a los recursos actuales.
- Factibilidad económica.
- Relación costo-beneficio de la alternativa sugerida o planteada, (personal de desarrollo, equipo software, entrenamiento, preparación de la entrada, conversión de archivos de prueba, operación, costo del software, etc.).

Factibilidad operativa

- Determinar ¿qué se operará, utilizará?; tomando en cuenta factores como la resistencia al cambio, debido a su área de comodidad, características del personal, ubicación de las instalaciones, etc.
- Plan de desarrollo informático (puntos de control y calendarización de actividades). Controlados a través de flujogramas. Rutas críticas, etc.
- Personal que lo utilizará, su disponibilidad, carga de trabajo todo ello será el estado general de la función de desarrollo.
- Elección de la mejor alternativa y aprobación del proyecto.

c) Diseño de sistemas

Este debe de realizarse después de haber aprobado el estudio de factibilidad, si no es así, no se puede realizar el diseño.

Diseño general del sistema o de la alternativa elegida.

- Estructura general del sistema.
- Definición y documentación de los requisitos de salida del sistema, datos recientes.
- Contenido y formato de los informes.
- Frecuencia de producción de reportes, quién lo solicita y su uso.
- Lista de distribución de reportes.
- Periodos de retención de informes, es decir vida útil.
- Controles sobre la salida.
- Definición y documentación de los requisitos de entrada. Lógicamente debe estar por escrito.
- Requisitos de edición y validación (control). De todos los datos que se capturan en la computadora.
- Revisiones de seguridad para la protección de los datos. Personal que esté debidamente autorizado para ingresar o modificar datos.
- Controles sobre la entrada.
- Definición y documentación de los requisitos de archivos.
- Definición de los tipos de registros o estructuración de bases de datos. Que puede ser indexada o secuencial.
- Métodos de organización.
- Niveles de seguridad y controles de acceso.
- Periodos de respaldo y retención.
- Cuánto y cada cuándo se deben hacer los respaldos.
- Definición y documentación de los requisitos de procesamientos (manuales y computarizados). Validaremos su tiempo de respuesta.

- Especificación de procedimientos programados de cálculo, clasificación, etc.
- Estimación de tiempos de respuesta.
- Normatividad.
- Interfaces.
- Niveles de seguridad.
- Diseño de documentos fuente.

En esta parte se determinan las especificaciones del usuario, es decir todo aquél que dentro del contexto de la organización se relaciona con el sistema. Existen usuarios primarios y usuarios secundarios.

Usuario primario: Es aquél que usa directamente en sus tareas los resultados del sistema de información y que lo ayudará en la toma de decisiones.

Usuario secundario: Es aquél que introduce datos al sistema.

El analista de sistemas debe comprender las responsabilidades, limitaciones, necesidades, y las acciones que deberán tomar los usuarios y las reglas de decisión por aplicarse. Las especificaciones del usuario involucran el diagnóstico de la problemática y las especificaciones de solución. Las especificaciones de usuario son los antecedentes para todo el equipo de desarrollo. Deben responder a las preguntas, ¿Cómo?, ¿Por qué?, por tanto se deberán quedar diagramados los procedimientos actuales y los esperados.

Otro factor importante por considerar son las relaciones humanas, ya que los sistemas de información pueden cambiar las relaciones interpersonales y las interacciones.

Se debe comprender el estilo organizacional, tomar la organización como un todo, identificar el grado de apertura / restricción:

Permeabilidad. Es necesario identificar si el estilo de liderazgo es autócrata o demócrata.

La recopilación de datos involucra la investigación documental, la realización de entrevistas y la observación. ¿Qué se examinará?, ¿A quiénes se entrevistará?
Principales objetivos de los formatos / pantallas de captura:

- Precisión. Exactitud en la aplicación de datos.
- Facilidad de uso y sencillez.
- Consistencia de las pantallas.
- Controlables (flujo).

Principales objetivos de las salidas:

- Satisfacción del objetivo planteado.
- Adaptada al usuario.
- Adecuada cantidad de información.
- Oportunidad.
- Medio apropiado.
- Medición del grado de confidencialidad.

Diseño detallado del sistema

- Asignación de responsabilidades.
- Diseño de documentos fuente.
- Especificaciones de programas y controles programados, (costo-beneficio).
- Diseño de pistas de auditoría (todos los elementos que permitan reconstruir los hechos).
- Estándares de documentación de programas como:
    - Nombre de la aplicación.
    - Diagrama del sistema.
    - Aspectos generales del programa.
    - Formatos de archivos de entrada.

    - Formatos de archivos de salida.
    - Diseño y muestra de reportes.
    - Diseño y muestra de pantallas.
- Descripción detallada de los principales procedimientos de cálculo, clasificación, etc., incorporados al programa.
- Criterios de selección.
- Procedimientos de conexión de cifras.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Medio de almacenamiento y localización del programa.
- Requerimientos de equipo.
- Listado del programa fuente (última compilación, con comentarios a la lógica).
- Estándares para la prueba de programas y del sistema total.
- Procedimiento para establecer datos de prueba.
- Asignación de responsabilidades para la preparación de datos y evaluación de los resultados.
- Autorización y aceptación escrita.

En estas fases se definen las especificaciones técnicas, es decir las características y definiciones técnicas y operativas del sistema, lo cual es responsabilidad del líder de proyecto en informática. Las especificaciones técnicas incluyen:

- Instrucciones para programación. Todas tienen que tener comentarios.
- Itinerario para el desarrollo de programas / módulos. Calendarización de programas de cómputo.
- Matrices de archivos / programas, módulos / programas.
- Selección de los lenguajes de programación.
- Controles del operador. Es decir que envíe mensajes.
- Instrucciones al operador en caso de interrupciones.
- Procedimientos de respaldo, reinicio y recuperación.

d) Desarrollo

En esta fase ya se debe tener un bosquejo de lo que es el sistema, para pasar a la parte de lenguajes a ejecutables.

Desarrollo y programación

Desarrollo y elaboración de la documentación de programas.

Básicamente se trata de la conversión de especificaciones técnicas a algún lenguaje de programación, estos deben ser documentados y mantenerles con instrucciones de operación.

Prueba modular y prueba del sistema integralmente.

La condición del nuevo sistema debe probarse con los otros sistemas o programas ya existentes para trabajar en paralelo antes de liberarlo por completo y por lo tanto se deben ejercer y realizar ensayos para hacer fallar el sistema. Las pruebas deben efectuarse con volúmenes de datos y bajo condiciones reales de operación. Cualquier error detectado debe ser cuidadosamente analizado y corregido, preparándose un reporte de excepciones: problema, causa y solución, indicando la fecha de corrección. La prueba debe estar bien dirigida, organizada, ser exhaustiva y eficiente, involucrando:

- Los procedimientos manuales.
- Los programas de cómputo y procedimientos de ejecución.
- Archivos de prueba.
- Al personal.

Es importante que se documenten las pruebas y se muestre en ellas la aprobación del usuario.

Plan de instalación

En el caso de proyectos grandes conviene desarrollar un plan de instalación piloto o por módulos, asignando responsabilidades.

4.1.1. Entrada

Todos los controles establecidos se inician con la entrada o acceso de datos, donde estos datos se transforman en información, se sugiere desde la entrada un establecimiento de cifras control, éstas serán de utilidad para saber y conocer la exactitud y totalidad de la alimentación de datos al sistema, cumpliendo con la metodología establecida previamente para ello.

4.1.2. Flujo de información

Su importancia radica en la circulación de los procesos y documentos control que van a alimentar al sistema, reiterando la sistematización de los procesos, con los que se va a contar para alimentar al sistema. Aunado a lo anterior tenemos la oportunidad de la afluencia de la información, así como su real utilidad.

4.1.3. Proceso

El procesamiento electrónico de los datos, debe añadir confianza sobre la certeza y seguridad de que todos los datos capturados serán procesados de forma veraz, confiable, exacta y oportuna, esto es que no sufran ninguna alteración o modificación durante su proceso, ya sea voluntaria o por omisión, en este punto es donde se realza la importancia del establecimiento de cifras control.

4.1.4. Salida

Es el resultado de lo alimentado y procesado, es decir es ya la transformación de los datos a información, cuya característica principal es que esta sea veraz, confiable, útil y oportuna, es decir, que proporcione los datos suficientes para darme un panorama del sistema para que con esa información se puedan tomar decisiones, es entonces cuando demuestra su utilidad, ya que validaremos la efectividad del sistema.

4.1.5. Archivos

El archivo de los sistemas va en función de las versiones que tengamos del sistema, conteniendo resultados y pruebas que se obtiene al echar a andar el sistema en condiciones reales o no.

Los archivos fuente del sistema se deben manejar de forma confidencial y segura, la función del auditor es evaluar el control que se tenga para la salvaguarda de los archivos generados para el sistema.

4.1.6. Respaldos

La importancia de generar respaldos es establecer una alternativa en caso de una contingencia, las contingencias pueden ser involuntarias o voluntarias, sin embargo estos respaldos deben realizarse por procedimiento debidamente establecido, es decir debe existir normatividad en materia de respaldos, así como de su custodia y guarda.

4.1.7. Controles, operación, mantenimiento y cambios correctivos

El establecimiento de controles se realiza con el objeto de salvaguardar los activos de la empresa, de promover la eficiencia en las operaciones, de obtener información veraz, confiable y oportuna, y adherencia a las políticas de la empresa. De tal suerte que cualquier control que establezcamos caerá en cualquiera de estos cuatro puntos de control.

Operación

La operación del sistema lleva un proceso de adaptación e implementación por tal motivo siempre será lo más viable que se trabaje en paralelo y se lleven a cabo pistas de auditoría, para que se trabajen con datos reales e inventados para tratar de reventar el sistema, es decir ponerlo a prueba de cualquier intromisión y por ende validar la fiabilidad de datos y la capacidad de los controles establecidos.

Mantenimiento

Siempre se buscará que todos los sistemas auditados o desarrollados cumplan con los requisitos de mantenimiento y 'auditabilidad' debido a las mejorías que se puedan hacer para obtener lo que se requiera del sistema.

Cambios correctivos

Todos los cambios que se realicen al sistema derivados de su operación deben quedar plenamente identificados y documentados y aprobados por los responsables, ya que éstos se encargarán de la difusión de los mismos, ya que los cambios deben de darse a conocer en tiempo y forma para que sea homogénea la versión de trabajo del sistema para toda la empresa.

4.1.8. Control de estándares

Los proyectos de desarrollo se estructuran como acumulativos, cada actividad o etapa descansa en la precedente. Las actividades del proyecto deben ser evaluadas conforme se realizan y tomar la decisión de continuar con la asignación de recursos y con el programa de trabajo o detenerse a tiempo.

La revisión del ciclo de vida del desarrollo de sistemas parte de los estándares o metodología requerida para el desarrollo de los nuevos sistemas y las modificaciones a los mismos. El propósito de la revisión efectuada por el auditor de sistemas de información es asegurar que la organización tiene y usa la metodología adecuada de desarrollo.

Adicionalmente el auditor de sistemas de información está interesado en asegurar que el proceso de desarrollo se adhiera a los estándares establecidos por la metodología. Su participación puede ser durante el desarrollo del sistema o una vez ya concluido.

4.1.9. Integridad de los datos y manejo de cifras de control

La integridad de los datos se basa mucho en la seguridad tanto física como lógica, debido a ello el estableciendo de controles de acceso de acuerdo con el nivel jerárquico se vuelve parte fundamental del proceso seguro de los datos, porque podemos identificar quiénes cargaron datos, quiénes accedieron a esos datos y quiénes utilizaron la información proporcionada por el sistema, el manejo de las cifras control nos da la garantía de que se introducen todos los datos, su integridad, su totalidad, su exactitud, su autentificación, su autorización, su mantenimiento, su oportunidad y la utilidad de los datos traducidos en información.

4.1.10. Controles en el desarrollo de sistemas

Los objetivos de control del proceso de desarrollo de sistemas son el asegurar que:

1. Los proyectos de desarrollo de sistemas de información son planeados con la suficiente anticipación.
2. Las necesidades y objetivos son definidos adecuadamente.
3. Se evalúan adecuada y suficientemente las desventajas, los aspectos económicos, técnicos, humanos, políticos y de operación.
4. Los sistemas son planeados de acuerdo con estándares.
5. La seguridad física y lógica.

4.1.11. Controles en base de datos

Para el control de las bases de datos se puede desde adquirir sistemas, en específico para su protección, con el objeto de prevenir accesos prohibidos, planes de contingencias, respaldos, controles de acceso a las bases de datos a través de claves de acceso (seguridad lógica), hasta monitoreo constante de los accesos a las bases de acuerdo con el nivel jerárquico correspondiente. Partiendo siempre de la premisa que la información es un activo fundamental de la empresa para la toma de decisiones.

4.2. Confidencialidad de los sistemas

Se debe de tener un número restringido de personas que acceden o que tengan acceso a todo el sistema de forma integral, ya que esto evitará una posible fuga de información, es decir, la administración del sistema debe estar debidamente identificada y delimitada, por claves de acceso restringido, con esto se podrá llevar una bitácora de acceso al sistema de forma controlada dejando un historial debidamente identificado en tiempo y forma.

Además se debe asegurar que las personas que intervienen no divulguen el contenido y especificaciones del sistema desarrollado así como su forma de encriptación o seguridad.

4.3. Seguridad de los sistemas

La seguridad en los sistemas va enfocada principalmente, pero no únicamente, a la seguridad física y lógica del sistema, es decir, en la seguridad de la parte intangible de la informática, con controles como criptografía, claves de acceso irrepetibles y que se cambien por sistema, que tengan fecha de caducidad, etc. Y en la parte física los controles de acceso a los equipos con características críticas o de acceso restringido, así como identificadores para acceder a dichas áreas.

4.4. Análisis costo/beneficio pronosticado contra el costo/beneficio obtenido

El costo-beneficio del sistema se determina desde la fase de planeación del sistema, y se compara en su fase de funcionamiento; los beneficios se verán hasta que ya esté en funcionamiento el sistema, cuando se reproduce la información y se toman decisiones con base en ello. Sin embargo no hay que perder de vista que en los periodos de adaptación se encuentran factores tales como resistencia

al cambio, aunque exista capacitación y manuales respectivos del nuevo sistema, el periodo de adaptación también debe estar contemplado desde la etapa de planeación.

Desde que se determina el desarrollo del sistema se toman en cuenta los estudios de factibilidad económica, tecnológica, operativa y legal, sería muy arriesgado en estos tiempos emprender un proyecto sin contemplar estos estudios de factibilidad, ya que los recursos que son escasos, se deben administrar correctamente y con un máximo grado de eficiencia.

Sin embargo el beneficio se debe traducir en tiempo y esfuerzo, es decir, que los procesos sean más rápidos y la información sea contundente para minimizar riesgos y poder tomar decisiones y mejorar en los controles.

4.5. Encuestas a usuarios

Para la realización de la mayoría de los tipos de auditoría, se emplean las herramientas que trataremos a continuación, ya que son la base de las pruebas que van a sustentar nuestra opinión y son cuestionarios y entrevistas.

Cuestionarios

Las auditorías en informática se realizan recopilando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr que toda la información necesaria para la emisión de la opinión, siempre se ampare en hechos demostrables, es decir, obtención de evidencia suficiente y competente.

Estos cuestionarios deben crearse a la medida de cada empresa y de cada tipo de auditoría. Auditoría al ciclo de vida de desarrollo de un sistema, auditoría a controles generales, auditoría a PC’s aisladas, auditoría a un sistema en

específico, auditoría a redes y auditoría a la administración de la función de informática, ya que cada empresa y cada tipo de auditoría son diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Ejemplo de cuestionario de Aplicado a un centro de computo en la UNAM.

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN.

CUESTIONARIO DE EVALUACIÓN DE CONTROL INTERNO CONTROLES GENERALES

PERIODO DE REVISIÓN DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2010

CALIFICACIÓN: REGULAR

	INICIALES	FECHA	FIRMA
PREPARÓ	JJAB	30-04-2011	
REVISÓ	PRC	02-05-2011	

Pregunta Número	Descripción	Ref. PT	Puntos Óptimos	Puntos Reales	Debilidades de Control
1	Adquisiciones				
1.1	Aspectos generales				
1.1.1	¿Se conoce la normatividad institucional que regula las adquisiciones de hardware?		2	2	
1.1.2	¿Existe normatividad interna (dependencia) que regule las adquisiciones de bienes informáticos (hardware y software?		3	3	
1.1.3	Las adquisiciones efectuadas están		3	3	

	contempladas en el informe enviado al Comité Asesor de Cómputo de la UNAM.				
1.1.4	¿Quién es el responsable de las adquisiciones de bienes informáticos de la dependencia atendiendo al origen de los recursos? (PAPIIT, CONACYT, Fundación UNAM, Fondo Fijo, etc.)		3	3	
1.1.5	¿Se solicitan anticipadamente los requerimientos de información?, se evalúan y documentan.		3	2	
1.1.6	¿Se realizan estudios de factibilidad completos (técnico, operativo y económico) en el que se analicen y evalúen las alternativas más adecuadas para la adquisición de bienes informáticos (hardware y software)?		3	1	Esto no siempre se sigue ya que solo se guían por el factor económico

Entrevistas

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

2. A través de "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

3. Por medio de entrevistas en las que el auditor sigue un método preestablecido , como puede ser que se tengan las preguntas preparadas de antemano, con posibles respuestas de antemano y busca unas finalidades específicas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

4.5.1. Ventajas obtenidas

Obviamente, las ventajas son la obtención de evidencia suficiente y competente, es decir, que se cuenta con información de primera mano y confiable y con estos datos podemos reafirmar nuestro trabajo y opinión.

- Obtención de información veraz, confiable y oportuna al plasmar su firma en la entrevista.
- Conocimiento de viva voz sobre la percepción de las actividades informáticas y su problemática.
- Conocer el ambiente de control que practica la administración referente a los recursos informáticos.

4.5.2. Necesidades no cubiertas

En caso de que esto se dé, solamente se entrega un reporte de sugerencias sobre las debilidades encontradas en el sistema, con respecto a que no cumple los objetivos del usuario secundario de la información, es decir de las personas que obtienen del sistema los datos e informes para poder interpretarlos y poder tomar decisiones basadas en datos reales emanados del sistema auditado.

4.5.3. Desventajas del sistema

Algunas desventajas encontradas durante la revisión son:

- Costos en una proporción inadecuada a los beneficios.
- Incremento en la escala del proyecto.
- Sistemas no integrales o aislados.
- Deficiente comunicación entre usuarios y personal del P.E.D. (Proceso Electrónico de Datos); desconocimiento del papel / responsabilidad de usuarios y dirección.

- Expectativas no cumplidas, insatisfechas de los usuarios.

4.5.4. Limitaciones del sistema

También nos encontramos con situaciones como son las siguientes:

- Ausencia de pistas de auditoría.
- Falta de revisiones técnicas a detalle.
- Entrenamiento deficiente.
- Carencia o incompleta documentación de sistemas (documentación técnica), de operación y/o de usuario.
- Carencia de metodología, o bien de metodología incompleta y no estándar, para el desarrollo de los sistemas, en la que se señalen con precisión actividades, tiempo estimado y responsable.
- Inoportunidad en la transferencia de sistemas en desarrollo a operación normal.
- Desaprovechamiento tecnológico.
- Pruebas del sistema incompletas, inadecuadas, desorganizadas, sin documentar y/o mal diseñadas, las cuales garanticen que los errores e irregularidades se detectan oportunamente por sistema. Pruebas no siempre controladas por usuario.

La revisión post-implantación es una revisión formalmente planeada, que debe realizarse después de transcurridos 3 o 6 meses de la instalación definitiva. La revisión post-implantación normalmente involucra:

- Evaluación del cumplimiento de las necesidades de usuario.
- Análisis de costo-beneficio.
- Efectividad de los controles.
- Control de modificaciones al sistema.

Bibliografía básica del tema 4

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes]

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

Sitios electrónicos

Sitio	Descripción
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*
http://www.oocities.org/mx/acadentorno/aui.htm	Aguilar Castillo, Gil. (2009). *Auditoría Informática*, Facultad de Estadística e Informática. Universidad Veracruzana.

Actividades de aprendizaje

A.4.1. Elabora un flujograma sobre la metodología para realizar un sistema.

A.4.2. Elabora un cuadro comparativo entre una auditoría de sistemas y una auditoría a redes computacionales, señalando diferencias y similitudes.

A.4.3. Elabora un análisis de las problemáticas encontradas al realizar un sistema informático, diferentes a las presentadas en este tema.

A.4.4. Investiga y explica cómo se debe presentar el informe o dictamen de una auditoría de sistemas e investiga cuál es su normatividad aplicable.

Cuestionario de autoevaluación

Responde las siguientes preguntas:

1. Menciona ¿cuáles son las etapas para el desarrollo de un sistema?
2. Menciona en qué consiste la requisición del servicio del Desarrollo de un Sistema.
3. ¿En qué consiste la etapa del Diseño?
4. Menciona los elementos que componen la fase de desarrollo.
5. ¿Que es un estudio de factibilidad?
6. ¿En qué consiste la Factibilidad Operativa?
7. ¿Qué es un usuario Primario?
8. ¿Qué involucra la recopilación de datos?
9. ¿En qué consiste la Prueba modular?
10. ¿Qué son los respaldos?

Examen de autoevaluación

Elige la respuesta correcta a las siguientes preguntas:

1. Es la primera fase del ciclo de vida del desarrollo de un sistema.
   a) planeación
   b) metodología
   c) organización
   d) evaluación

2. La requisición de servicios está contenido en la etapa de:
   a) planeación
   b) análisis
   c) diseño
   d) desarrollo

3. Esta etapa consiste en la elaboración y realización de estudios de factibilidad:
   a) planeación
   b) análisis
   c) diseño
   d) implantación

4. Disponibilidad de la tecnología que satisfaga las necesidades del usuario, y de la empresa, así como actualización o complemento a los recursos actuales se refiere a:
   a) factibilidad económica
   b) factibilidad tecnológica
   c) factibilidad operativa
   d) factibilidad legal

5. En esta etapa se realiza la conversión del sistema:
   a) planeación
   b) análisis
   c) diseño
   d) implantación

6. Su importancia radica, en la circulación de los procesos y documentos control que van a alimentar al sistema, reiterando la sistematización de los procesos, con los que se va a contar para alimentar al sistema:
   a) entrada
   b) flujo de información
   c) proceso
   d) salida

7. Proporciona los datos suficientes para dar un panorama del sistema para que con esa información se puedan tomar decisiones, es entonces cuando demuestra su utilidad, ya que validaremos la efectividad del sistema. Este manual contiene los requisitos para la instalación del sistema:
   a) entrada
   b) flujo de información
   c) proceso
   d) salida

8. Se puede desde adquirir sistemas en específico para su protección, con el objeto de prevenir accesos prohibidos, planes de contingencias, respaldos, controles de acceso a las bases de datos a través de claves de acceso.
   a) controles en la base de datos
   b) seguridad de los sistemas
   c) confidencialidad de los sistemas
   d) análisis costo/beneficio

9. La administración del sistema debe estar debidamente identificada y delimitada, por claves de acceso nos referimos a:
   a) controles en la base de datos
   b) seguridad de los sistemas
   c) confidencialidad de los sistemas
   d) análisis costo/beneficio

10. Ausencias de pistas de auditoría, falta de revisiones técnicas a detalle, entrenamiento deficiente entre otras se refiere a:
   a) ventajas obtenidas
   b) necesidades no cubiertas
   c) desventajas del sistema
   d) limitaciones del sistema

TEMA 5. AUDITORÍA DEL EQUIPO DE CÓMPUTO

Objetivo particular

Identificar el procedimiento a seguir para la aplicación de una auditoría en informática a equipos de cómputo.

Temario detallado

5.1. Documentación y controles
- 5.1.1. De bibliotecas
- 5.1.2. De adquisiciones
- 5.1.3. De respaldos (generación y modificaciones)
- 5.1.4. De resguardo del equipo
- 5.1.5. De equipo
- 5.1.6. De terminales y equipo descentralizado
- 5.1.7. De operación

5.2. Seguridad de los equipos
- 5.2.1. Controles de seguridad
- 5.2.2. Confidencialidad
- 5.2.3. Control de acceso al equipo

5.3. Mantenimiento de los equipos
- 5.3.1. Contratos
- 5.3.2. Preventivo
- 5.3.3. Correctivo

5.4. Orden en el centro de cómputo
- 5.4.1. Aseo
- 5.4.2. Almacén
- 5.4.3. Mantenimiento del centro
- 5.4.4. Mobiliario

5.5. Productividad

5.5.1. Aprovechamiento y uso de la capacidad instalada

Introducción

Una de las áreas de auditoría más conflictivas y sensibles en una Institución es la función de la documentación y controles de equipo de cómputo que, tratándose de recursos informáticos se vuelve por demás interesante, debido a que se tiene que establecer los procedimientos desde una compra simple, hasta una licitación en forma, ya sea por adjudicación directa, por invitación restringida, por licitación nacional o internacional, si se requiere.

5.1. Documentación y controles

La documentación y controles que se necesitan para realizar las actividades en esta auditoría se refieren a la normatividad interna de la institución por auditar, en donde se observe la existencia de comités de informática, políticas, leyes y reglamentos que regulen la actividad informática y su uso.

5.1.1 De bibliotecas

La Biblioteca de Infraestructura de Tecnologías de Información (TI) resulta de gran utilidad para hacer más eficientes las operaciones de cualquier organización involucrada en la entrega, soporte y administración de los servicios de las Tecnologías de la Información (TI), ya sea de forma interna o incluso, mediante *outsourcing*.

¿Qué se busca al auditar las bibliotecas?

- Ser escalable, adaptándose a las particularidades y complejidad de las organizaciones.
- Ser independiente de la tecnología.
- Ser más descriptivo que prescriptivo. (Cossío y Palomino, 2005)

5.1.2. De adquisiciones

Entre los aspectos importantes que tenemos que observar al realizar la auditoría se encuentran:

- Economía y factibilidad del posible proyecto de inversión, para la solución de los requerimientos planteados por la entidad evaluando su efectividad de acuerdo con las metas y objetivos previamente planeados.

- Se debe tener bien establecida la responsabilidad de los proveedores. La responsabilidad de los proveedores en cuanto a garantía de los bienes adquiridos, capacitación si se requiere, servicios adicionales, reemplazo de equipo o software.
- Aspectos legales de la compra. Que los proveedores se encuentren establecidos legalmente, que son distribuidores o concesionarios de los bienes informáticos que ofertan, derechos y obligaciones en las pólizas de garantías, responsabilidad civil y legal.
- Cuadros comparativos. Los cuadros comparativos muestran un resumen de las cotizaciones realizadas por los distintos proveedores, se presentan a través de una matriz que nos auxilie a realizar una toma de decisiones sobre cuál es la mejor oferta tanto técnica, económica, operativa y legal que satisfaga las necesidades del requirente.

A partir del análisis y definición de requerimientos de información o de equipo, si se quiere modernizar o escalar se deberán explorar las diferentes alternativas de solución, realizando un estudio de factibilidad que comprendan los siguientes elementos.

- Factibilidad económica. (estudio de costo-beneficio) involucrando los costos asociados a la adquisición, considerando no solo el desembolso inicial sino los costos por entrenamiento al personal y mantenimiento de los equipos.
- Factibilidad operativa, orientado a evaluar si el equipo tendrá la capacidad de procesar la información con posibilidades de crecimiento probadas.

- Factibilidad Legal, básicamente se tendrán que evaluar aspectos como derechos y responsabilidades de las partes.
- Factibilidad tecnológica, por las restricciones que esto pudiera tener para aprovechar íntegramente la inversión que está realizando. Existen muchos casos en que se obliga a la institución a adquirir otro tipo de dispositivos para poder hacer operativo el equipo inicialmente contratado.

Es importante tomar en cuenta la facilidad que tiene el proveedor para dar mantenimiento en el propio lugar en que se encuentra instalado el equipo o los programas. Ya que esto puede entorpecer la operación en caso de que el proveedor no ofrezca esta posibilidad. Esta condición es aun más importante cuando nos referimos a software especializado.

Con base en lo anterior se iniciará el siguiente paso del proceso que es el envío de solicitudes de propuestas a diferentes proveedores.

En la práctica, se solicita la cotización, abriéndose esta en una fecha determinada ante la presencia de todos los concursantes a fin de que no existan favoritismos en la asignación del periodo y este se canalice hacia la mejor alternativa para la institución.

Estas propuestas deberán incluir todas las especificaciones técnicas, legales y operativas que deberán cumplir para estar en posibilidades de concursar.

Con estas propuestas se realizará la evaluación de los equipos y programas y se efectuarán las pruebas de aceptación previas.

Se sugiere que los resultados de las pruebas se alimenten a un sistema que asignará calificaciones y en forma automática señalará al ganador del concurso.

Es necesaria una revisión minuciosa del contrato con el proveedor (Estudios de factibilidad). Es recomendable solicitar la opinión del departamento legal de la institución o en su ausencia de un especialista externo, que valide la formulación del mismo.

En el caso de adquisición de software es importante definir el nivel de modificaciones que requiere para hacerlo operativo en la realidad. Aceptando que los paquetes responden a necesidades generales pero que requerirán de este proceso de adecuación razonable para hacerlos operativos.

Estos trabajos deberán declararse en forma detallada dentro de los contratos respectivos.

Al término de esta actividad se autoriza la compra mediante la aprobación de la gerencia y se iniciará un sistema de seguimiento del proyecto de tal manera que este se cumpla dentro de las estimaciones de costo y tiempo definidas.

Otro aspecto importante por señalar es la capacitación requerida y ofrecida por el proveedor, tanto en hardware como en software, que también tendrá que formar parte de la propuesta inicial para tener un panorama real de la inversión necesaria.

Es necesario tener claramente especificado de qué activos se trata, de qué manera y cuáles serán los requisitos de autorización necesarios, los cuales pasarán a formar parte de la evaluación del auditor.

Para finalizar, es necesario realizar un seguimiento de los resultados que se obtengan al utilizar las nuevas adquisiciones a fin de comparar las expectativas contra los resultados reales y estar en posibilidades de realizar los ajustes necesarios.

- Objetivos de la revisión
  - Que los recursos y el capital sean efectivas y eficientemente aplicados.
  - Que se cumpla con las políticas y procedimientos establecidos por la institución.

- Aspectos de las adquisiciones.
  - Determinación del presupuesto
  - Consideraciones financieras
  - Requisitos de la aplicación / prioridades
  - Selección de posibles proveedores
  - Petición formal de propuestas
  - Demostraciones
  - Referencias/ pruebas
  - Características de las licencias de uso de software
  - Comparación de propuestas evaluación de riesgos
  - Planificación del local (instalaciones)
  - Plan de instalación
  - Planificación de la conversión
  - Plan de implantación

Estas son solo algunas sugerencias de aspectos por considerar en la revisión de la fase de adquisiciones.

5.1.3. Respaldo (generación y modificaciones)

Los respaldos del software adquirido, así como de los archivos trabajados, son de vital importancia debido a que la aplicación de éstos como política y norma nos ayudará a disminuir el riesgo de que suframos alguna contingencia.

En el caso de resguardos de sistemas nos encontramos con lo siguiente:

- Típicamente el sistema operativo lo proporciona el fabricante al que le adquirimos el equipo en la fase anterior, pero el trabajo de implantación abarca el seleccionar las opciones apropiadas del sistema operativo y "generar un sistema" o sea respaldo, que cumpla con los requerimientos específicos de la institución, tomando en cuenta factores como:

    - Configuraciones de equipos de cómputo (capacidades de memoria, periféricos en uso, etc.)
    - Modo de procesamiento (*batch* o en línea)
    - Otras facilidades que se requieren (comunicaciones)

Este trabajo puede ejecutarse por el proveedor, por cuenta de la entidad o por la entidad misma. En cualquiera de los casos deberá verse involucrado como responsable un funcionario de procesamiento electrónico de datos que ayude a determinar que las opciones se han de seleccionar, probar, documentar e implantar apropiadamente.

El sistema operativo que resulte deberá probarse acuciosamente bajo la supervisión del funcionario responsable, para determinar que se ejecuta de conformidad con los requerimientos de la entidad y que se han implantado apropiadamente todas las rutinas, facilidades y capacidades autorizadas.

Asimismo se deben establecer los procedimientos para la generación de los resguardos respectivos de la información procesada, y estos convienen que sean de forma diaria y obligatoria, y estos resguardos se pueden generar de forma manual o por sistema, sin embargo, el resguardo deberá ser en principio obligación del usuario y posteriormente será de la administración la custodia y guarda tanto física como lógica de la información procesada.

La guarda se puede hacer dentro de la oficina o se sugiere que se realice de forma independiente en un banco, en donde estemos seguros de la integridad tanto física como lógica de la información contenida en los diferentes medios de almacenamiento.

5.1.4. Resguardo del equipo

El resguardo del equipo de cómputo debe formalizarse y llevarse un estricto control del mismo debido a que con esto estaremos cumpliendo con uno de los objetivos de control interno que es la protección de los activos de la empresa.

Esta función la debe realizar, en conjunto, el área de adquisiciones en su sección de inventarios y el encargado del área de cómputo, ya que con esto se pueden y deben realizar compulsas que nos ayuden a determinar si existieran diferencias y aclararlas con la brevedad posible.

El contenido de los resguardos debe contener al menos los siguientes elementos:

- Nombre del usuario
- Ubicación
- Características del equipo
- Componentes del equipo
- Software que incluye el equipo
- Número de inventario
- Garantía
- Nombre del proveedor
- Fecha de adquisición
- Políticas generales de uso
- Responsabilidad por mal uso
- Responsabilidades al asignar el equipo.

- Fecha y firma de quien recibe y quien entrega el equipo

5.1.5. De equipo

Cuando se adquiere el equipo se debe de contar con un archivo por equipo adquirido que contenga como mínimo los siguientes elementos.

- Solicitud de compra
- Autorización de compra
- Invitación a proveedores
- Estudio de factibilidad
- Cuadros comparativos
- Asignación del proveedor ganador
- Inventario del equipo
- Características del equipo
- Factura
- Garantía
- Software integrado al equipo
- Contenido del equipo
- Usos y cuidados

Así como una bitácora de mantenimiento y soporte técnico que haya recibido el equipo.

5.1.6. De terminales y equipo descentralizado

Para la documentación de este tipo de equipos de cómputo, tenemos que llevar a cabo las siguientes consideraciones:

Nunca ha sido tan grande la demanda de la identificación de los usuarios en todos los niveles. En la actualidad, existe cada vez más la tendencia a que los usuarios compartan los recursos de cómputo, por lo tanto el auditor debe preocuparse por:

- Determinar el mecanismo de acceso autorizado es capaz de prevenir accesos no autorizados a los recursos.
- Dadas las capacidades del mecanismo del control de acceso a los sistemas de información, determinar si es suficiente.

Los controles de frontera o controles de acceso establecen la interface entre el usuario de un sistema y la computadora. Su propósito primario es establecer la identificación y la autenticación del que pretende ser usuario del sistema, para lo cual se necesita un mecanismo de control.

Es una realidad que cada vez más los recursos informáticos (equipo, programas y datos) son compartidos por un gran número de personas físicamente dispersas lo cual hace necesario implantar controles que garanticen que el acceso a ellos se realiza de acuerdo con el nivel jerárquico y funciones del personal. Protegiendo a la instalación de:

- Destrucción accidental o intencional
- Mal uso
- Consulta no autorizada de datos

5.1.7. De operación

Para la documentación sobre la operación del equipo de cómputo es muy importante tanto la seguridad física como lógica, sin embargo se le debe dar prioridad a la capacitación del usuario.

Se debe de contar o realizar un manual de usuario y de operación tanto del hardware como del software y quiénes son los responsables de ver que se cumplan en forma todas las especificaciones tanto técnicas como lógicas en la ejecución de los equipos. También, de ser necesario, se deben establecer sanciones y responsabilidades de los usuarios en caso de un manejo inadecuado de los recursos informáticos asignado para realizar su labor.

Los manuales de operación deben contener lo siguiente como mínimo

- Representación gráfica de la estructura del sistema.
- Función de cada programa.
- Requerimientos de equipo.
- Tamaño estimado de archivos (normal y máximo).
- Explicación de los mensajes de la consola, junto con la respuesta adecuada del operador.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Calendarización de procesos.
- Parámetros a alimentar.
- Creación de salida y su distribución.
- Identificación adecuada de las etiquetas de los archivos de salida.
- Puntos de reinicio y recuperación.
- Procedimientos para notificar errores o condiciones defectuosas.
- Procedimientos para casos de emergencia.

5.2. Seguridad de los equipos

5.2.1. Controles de seguridad

La información y los recursos informáticos son activos que deben ser protegidos del acceso no autorizado. La manipulación y la destrucción. La seguridad física debe establecerse para prevenir accesos innecesarios y/o no autorizados y registrar los hechos.

La auditoría a la seguridad física se refiere a la revisión de las medidas de control orientadas a la continuidad del servicio y dependen en gran parte de:

- Los fenómenos naturales: incendio, terremoto, huracanes, tormentas, severas, inundación, fallas de corriente, picos de voltaje, falla de aire acondicionado y cortos circuitos.
- Actos intencionales de ex-empleados, empleados notificados de despido, huelga, empleados adictos al alcohol o drogas, ladrones profesionales, empleados con problemas económicos o descontentos.

Por lo anterior la entidad corre el peligro de:

- Entrada no autorizada
- Daño de equipo
- Vandalismo
- Robo de equipo y documentos
- Copias, consulta o divulgación de información confidencial
- Alteración de equipos sensible
- Cambio no autorización de datos

La seguridad física debe proteger principalmente las áreas de:

- Sala de cómputo
- Consola del operador

- Impresoras
- Equipo de teleproceso
- Fuentes de poder
- Lugar donde se guardan discos duros externos o de respaldo
- Bóvedas de respaldos
- Oficina de control de entradas y salidas
- Closet de comunicaciones
- Microcomputadoras y terminales remotas
- Área de programación

La revisión principalmente abarca la verificación de controles sobre:

- Ubicación del equipo
- Facilidad de acceso. Las áreas extremadamente visibles son muy vulnerables.
- Alimentación de energía eléctrica.
- Líneas telefónicas privadas de respaldo, sobre todo en el caso de teleproceso.
- Índice de delincuencia.
- Empresas vecinas altamente contaminantes.
- Índice de fenómenos naturales: sismos, tormentas, etc.
- Control de puertas. El acceso solo debe permitirse a aquellas personas que opriman la secuencia correcta de botones, sistema de tarjetas, sistemas de gafetes, etc. Tratándose de sistemas digitales generalmente la secuencia es de 6 dígitos. Lo cual proporciona un millón de combinaciones diferentes.
- Guardias de seguridad.
- Cerraduras de combinación, electrónicas o biométricas.
- Cerraduras para terminales.
- Circuito cerrado de televisión.
- Alarmas.
- Puertas blindadas bajo sistemas de doble puerta.

- Registro de visitante y gafetes de identificación.
- Uso de credenciales gafetes con fotografías.

Algunas consideraciones en la selección del sistema de control de acceso son:

- Margen de error. Determinar el porcentaje tolerable de error del sistema por seleccionar; es decir, hasta cuántas veces se aceptará que el sistema niegue el acceso a una persona autorizada o lo permita a una que no lo esté.
- Protección en caso de fallas en el suministro de energía eléctrica.
- Resistencia a la manipulación o sabotaje.
- Mantenimiento del sistema en buen estado.
- Flexibilidad para crecer en relación con el crecimiento institucional.
- Sencillez en su operación desde su instalación hasta su puesta en marcha.
- Cantidad y frecuencia de acceso de acuerdo con el tráfico de entradas y salidas.

Prevención contra fuego y agua

- Existencia mínima de material combustible
- Existencia adecuada de trituradora de papel
- Evitar cables sueltos y contactos en mal estado
- Detectores y alarmas de fuego, humo y humedad
- Extinguidores de agua (áreas administrativas y almacenes) y gas (áreas de equipo) carga, peso, ubicación, cantidad y capacidad
- Tuberías adecuadamente aisladas para evitar filtraciones
- Apagadores automáticos de incendio en ductos de aire acondicionado
- Fundas para los equipos

Extras

- Salidas de emergencias
- Planta de energía, reguladores de voltaje y sistema “no-break”
- Respaldos
- Contratos de mantenimiento preventivo y correctivo a todos los equipos e instalaciones del área de informática.

5.2.2. Confidencialidad

La seguridad lógica se lleva a cabo a través de programas de acceso a:

- Equipos.- A través de contraseñas otorgados por la Institución.
- Programas.- A través de contraseñas que se cambien por sistema o manual de manera periódica.
- Comunicaciones.- Restricción de accesos a equipos de telecomunicaciones y racks respectivos.
- Datos.- Acceso restringido a datos que se traducen en información que puede ser confidencial.
- Facilidades.- Para modificar el sistema para beneficio propio o mal uso del mismo.

Las acciones sobre el acceso de los datos y programas deben restringirse en cuanto a:

- Creación
- Modificación
- Copiado
- Eliminación
- Consulta
- Ejecución

Controles mediante criptografía

La criptografía derivada de dos palabras griegas: “kriptos” (oculto o secreto) y “grafos” (escritura). Es un método de protección de información mediante un proceso en el cual datos entendibles o legibles son transformados en códigos secretos (criptogramas) para prevenir accesos no autorizados y mantener la privacidad de la información por lo tanto la criptografía convierte los datos originales en mensajes que no tienen significados para los que no conocen el sistema para recobrar los datos iniciales.

El análisis criptográfico se refiere a las técnicas para recobrar legalmente datos crípticos incorporados en criptogramas. Los términos de “encripción” y “decripción” son sinónimos descifrados.

La identificación puede definirse como el proceso de distinguir en forma única a un usuario de los demás mientras que la autentificación consiste en determinar si el individuo es quien dice ser. Es auténtico para efectos de la seguridad lógica, un usuario lo constituye cualquier persona que utiliza los recursos informáticos ya pertenezca al área de informática o no.

5.2.3. Control de acceso a equipos

La identificación, autentificación y autorización de los accesos del personal se logran mediante el uso de:

- Información memorizada: contraseñas. ¿Qué conoce el usuario?
- Objetos, tarjetas plásticas con bandas magnéticas, llaves, etc. ¿Qué posee el usuario?
- Características personales: voz, huella digital, retina del ojo, etc.

El medio más común para el control de accesos es la información memorizada o palabras claves; “passwords” y debe reunir las siguientes características:

- No menores de cuatro caracteres
- Alfanuméricos para incrementar el número de combinaciones
- No debe tener el nombre del usuario o cualquier dato personal asignados por el propio usuario
- Debe ser intransferible. Cada usuario es responsable del buen o mal uso.
- No debe permitirse usar palabras anteriormente utilizadas
- Fáciles de recordar, difíciles de recordar
- Número limitado de intentos
- Internamente transformados en un código secreto “encriptados”
- No desplegables en pantalla
- Cambiados periódicamente y de manera automática por el sistema

5.3. Mantenimiento de los equipos

5.3.1. Contratos

Deben establecerse formalmente los procedimientos para dar mantenimiento de los equipos de cómputo, al igual que en las aplicaciones. Un procedimiento conveniente pudiera incluir el que se prepare, revise y autorice adecuadamente una forma estándar de requisición de cambio antes de que se haga la modificación, para ello se debe contar con los contratos respectivos de software y de hardware.

Una vez efectuado el cambio deberán estar en vigor procedimiento de revisión. A efecto de asegurar que la documentación se actualiza de acuerdo con las normas de la entidad.

Después de que los programas modificados se han catalogado, un funcionario de procesamiento electrónico de datos (personal calificado en soporte técnico)

deberá cerciorarse de que se han seguido los procedimientos apropiados para garantizar que se han considerado los aspectos más importantes como son la ejecución del sistema operativo y los cambios que afectan a los usuarios, así mismo se deberán obtener las aprobaciones requeridas y cerciorarse de que el personal implicado ha sido notificado por escrito respecto a la fecha en que entrará en vigor la versión modificada del sistema operativo.

Algunos de los aspectos por incluir en la revisión del sistema operativo son:

- Documentación
- Tablas de configuración del sistema operativo, guías, procedimientos, etc.
- Procedimientos
- Carga inicial del sistema
- Aplicación de actualizaciones o modificaciones.
- Retención del registro de la actividad en consola y contabilidad del trabajo (*job accounting*)
- Restricciones para el uso de comandos críticos.
- Ejecución del sistema (software para monitoreo).
- Tiempo de respuesta en línea.
- Costos/gastos excesivos.
- Sistema operativo.

5.3.2. Preventivo

Los contratos preventivos deben contener el costo, el tiempo y la forma de revisión así como una calendarización de visitas que deben hacer los proveedores del servicio así como en qué consisten dichas visitas.

Debemos tener cuidado con aquellos contratos y proveedores que como mantenimiento preventivo realizan solo limpieza a los equipos, y no realizan el

mantenimiento preventivo por el cual fue contratado, ya que el contrato debe estipular en qué consiste el mantenimiento preventivo.

Un mantenimiento preventivo a equipos nos debe de auxiliar a evitar o disminuir los riesgos de que pueda fallar en algún momento mi equipo en uso o un componente de ellos y que me diga la vida útil del mismo o si es necesario cambiar un componente como puede ser un rodillo en una impresora o la fuente de poder en un equipo, o que detecte que mi mobiliario no es el adecuado para mi equipo de cómputo o que las alfombras producen estática y conservan el polvo lo que puede ocasionarme un corto circuito o un mal funcionamiento en mi equipo.

O que tal vez el software que utilizó esta cada vez más en desuso y se está cambiando por otras tecnologías, etc.

5.3.3. Correctivo

El contrato de mantenimiento correctivo debe contener la reposición de ciertos componentes en cuestión que se desgastan por su uso y ya cumplieron con su ciclo de vida útil.

En el tema de software también debemos de contar con un contrato que avale actualizaciones permanentes y versiones actualizadas, ya sea del propio software que esté cubierto por el contrato y que incluso pueda reponer en caso de falla ya sea accidental o provocada.

Es importante que en todo contrato se especifique el número de equipos que entran dentro del contrato y revisar el costo beneficio del mismo, ya que debemos evaluar también la importancia de los equipos que estén bajo este contrato.

5.4. Orden en el centro de cómputo

El orden y aseo dentro del centro de cómputo o informática se ha vuelto de suma importancia ya que como área de servicio y de la promoción de la buena administración de los recursos informáticos debe predicar con el ejemplo.

5.4.1. Aseo

El aseo dentro del área de cómputo debe realizarse con sumo cuidado y lo deben hacer personas que estén preparadas para ejercer la limpieza de este equipo y lugar, ya que no es un área común donde se pueda limpiar el equipo con una franela mojada, sino que debe hacerse con material especial para no dañar el equipo y que conserve su óptimo funcionamiento, asimismo al limpiar los pisos se debe evitar al máximo levantar el polvo que dañaría los equipos

5.4.2. Almacén

En el almacén donde se puede guardar cableado, o consumibles e inclusive equipo obsoleto o en desuso debe identificarse plenamente, ya sea a través de kardex o de tarjetas de almacén para saber características y en qué condiciones se encuentra, en el caso de consumibles se debe contar con la identificación plena de que la existencia de los mismos sea en proporción al uso y se disminuya el riesgo de poco movimiento u obsolescencia del inventario.

5.4.3. Mantenimiento del centro

El mantenimiento del centro como tal es responsabilidad exclusiva del personal usuario de esa área, debe establecer las medidas de seguridad física y lógica para

reducir el acceso solo a los que realmente deben de estar allí debido al grado de importancia del centro y el grado de confidencialidad de la información que se maneja debe ir en función del control establecido para evitar vulnerabilidad al máximo.

5.4.4. Mobiliario

El mobiliario del centro de cómputo debe contar mínimo con las siguientes características.

- Material de construcción y mobiliario
- Materiales de construcción. Las paredes, techos y pisos deben estar construidas de material difícil de romper, resistente al fuego y no combustibles y que además no genere partículas de polvo, ya que pueden dañar los recursos informáticos.
- Evitar las alfombras ya que causan electricidad estática, sobre todo cuando la humedad es baja.
- Se debe mantener al mismo el número de puertas y ventanas.
- El centro de cómputo debe instalarse dentro de un edificio lejos de ventanas y paredes que den a la calle.
- No deben existir grandes árboles u otras estructuras que pongan en peligro el área de cómputo
- Bóvedas resistentes al calor y humedad.
- Barreras para cortar o aislar incendios.
- Se deben vigilar la instalación de detectores y controles de acceso. Los detectores pueden ser de: humo, calor, agua, combustión, controles de temperatura, controles de humedad, sistemas de detección de intrusos.
- El lugar debe acatarse a los códigos de seguridad.
- Debe evitarse el uso de ventiladores en las áreas en donde se encuentra ubicado el equipo, ya que es un elemento para propagar el polvo con el riesgo de dañar los equipos.

- El mobiliario debe ser resistente al fuego y no se debe permitir fumar alrededor o cerca ya que puede dañar los equipos.
- El mobiliario debe ser resistente al fuego y no se debe permitir fumar alrededor o cerca de los equipos.

5.5. Productividad

En algunos casos la productividad del centro de cómputo va en función de la importancia que se le da al interior de la institución misma.

5.5.1. Aprovechamiento y uso de la capacidad instalada

La experiencia de la mayoría de las empresas nos indica que los resultados obtenidos del proceso de desarrollo de los sistemas de información son deficientes. Mencionaré algunos problemas como ejemplo:

- Costos en una proporción inadecuada a los beneficios.
- Incremento en la escala del proyecto.
- Sistemas no integrales o aislados.
- Deficiente comunicación entre usuarios y personal del PED (Proceso Electrónico de Datos); desconocimiento del papel / responsabilidad de usuarios y dirección.
- Escasez de personal profesional.
- Expectativas no cumplidas, insatisfechas de los usuarios.
- Ausencia de pistas de auditoría.
- Falta de revisiones técnicas a detalle.
- Entrenamiento deficiente.
- Carencia o documentación incompleta de sistemas (documentación técnica), de operación y/o de usuario.

- Carencia de metodología, o bien de metodología incompleta y no estándar, para el desarrollo de los sistemas, en la que se señalen con precisión actividades, tiempo estimado y responsable.
- Administración insuficiente de los proyectos.
- Inoportunidad en la transferencia de sistemas en desarrollo a operación normal.
- Desaprovechamiento tecnológico.
- Pruebas del sistema incompletas, inadecuadas, desorganizadas, sin documentar y/o mal diseñadas, las cuales garanticen que los errores e irregularidades se detectan oportunamente por sistema. Pruebas no siempre controladas por usuario.

Cabe destacar que es sumamente importante que el auditor esté involucrado desde el plan maestro del sistema.

Fundamentalmente al auditor le interesa:

- Que exista una metodología.
- Que la metodología sea la adecuada al entorno tecnológico de la entidad, sea estándar, completa, al día, aprobada, y comunicada a todo el personal.
- Que la metodología se cumpla en el caso de un sistema de información, en particular o en general.

El auditor no siempre ha participado, pero es conveniente que el auditor esté consciente de que él no representa un factor para la toma de decisiones, sino más bien juega un papel de control que contribuye a disminuir riesgos, no a evitarlos. En otras ocasiones la falta de su participación se debe a la escasez de tiempo o personal en cuanto a prioridades.

La mayoría de las organizaciones destinan enormes recursos al desarrollo de nuevos sistemas o a la modificación de los mismos. A la luz del incremento en el porcentaje de fallas en las fechas de terminación, costos estimados y la satisfacción del usuario, las organizaciones deben seguir un enfoque estructurado para el desarrollo de nuevos sistemas y el mantenimiento de los mismos. La combinación de técnicas efectivas de administración del proyecto, la participación activa del usuario y especialistas, y la utilización de una metodología estructurada para el desarrollo del centro de cómputo puede minimizar los riesgos en cuanto a aplicaciones inapropiadas, erróneas, con datos sin uso o bien a las que se efectúan cambios injustificados

Bibliografía básica del tema 5

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes]

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

Sitios electrónicos

Sitio	Descripción
http://www.enterate.unam.mx/Articulos/2005/noviembre/itil.htm	Cossío Ortiz, Saidd Gerardo; Palomino Martínez, Damián F.J. (2005). ITIL: servicios de tecnologías de información. *Entér@te en línea. Internet, cómputo y telecomunicaciones*, UNAM, año 4, Número 44, Noviembre de 2005.
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*.
http://www.oocities.org/mx/acadentorno/aui.htm	Aguilar Castillo, Gil. (2009). *Auditoría Informática*, Facultad de Estadística e Informática. Universidad Veracruzana.

Actividades de aprendizaje

A.5.1. Investiga en tu centro de trabajo o cualquier café Internet, cuál fue el procedimiento que se llevó a cabo para la adquisición de bienes informáticos.

A.5.2. Investiga en tu centro de trabajo, café Internet o centro de cómputo en tu escuela y presenta un informe sobre la documentación y controles con que cuenta ese lugar para la salvaguarda de los bienes informáticos.

A.5.3. Elabora un cuadro comparativo que contenga al menos 3 cotizaciones para abrir un café Internet con 10 equipos de cómputo, y justifica a qué le darías más peso específico, ya sea a la factibilidad técnica, económica, operativa o legal.2

Cuestionario de autoevaluación

Responde las siguientes preguntas:

1. ¿A qué se refiere la documentación y controles en una auditoría de equipo de cómputo?
2. ¿Qué se busca al auditar las bibliotecas?
3. ¿En qué consiste la responsabilidad de los proveedores al adquirir un bien informático?
4. ¿Qué es un cuadro comparativo?
5. ¿En qué consiste la factibilidad tecnológica?
6. ¿Qué elementos debe contener un manual de operación?
7. ¿A qué se refiere la seguridad física?
8. ¿Cuáles son las áreas que debe proteger la seguridad física?
9. ¿Qué es el margen de error?
10. ¿Qué es la seguridad lógica?

Examen de autoevaluación

Elige la opción correcta

1. En este proceso se observa la normatividad interna que rige o regula la actividad informática.
   a) documentación y controles
   b) metodología
   c) biblioteca de TI
   d) adquisiciones

2. La escalabilidad, la independencia tecnológica son algunos aspectos considerados en la:
   a) documentación y controles
   b) metodología
   c) biblioteca de ti
   d) adquisiciones

3. La economía y factibilidad son aspectos considerados dentro:
   a) documentación y controles
   b) metodología
   c) biblioteca de ti
   d) adquisiciones

4. Para la adquisición de bienes informáticos ¿quién es el funcionario responsable de que esto se lleve a cabo?
   a) director general
   b) comité de auditoría
   c) gerente de informática
   d) jefe de adquisiciones

5. Este manual contiene la representación gráfica de la estructura del sistema, la función de cada programa, requerimiento de equipo entre otras cosas.
   a) sistema
   b) operación
   c) usuario
   d) organización

6. Se refiere a la revisión de las medidas de control orientadas a la continuidad del servicio en caso de fenómenos naturales.
   a) seguridad lógica
   b) seguridad física
   c) seguridad de aplicación
   d) seguridad de operación

7. Este tipo de seguridad protege principalmente áreas como sala de cómputo, consola de operador, impresoras, fuentes de poder etc.:
   a) seguridad lógica
   b) seguridad física
   c) seguridad de aplicación
   d) seguridad de operación

8. Este tipo de seguridad se lleva a cabo a través de programas de acceso:
   a) seguridad lógica
   b) seguridad física
   c) seguridad de aplicación
   d) seguridad de operación

9. Es un método de protección de información mediante un proceso en el cual datos entendibles o legibles son transformados en códigos secretos:
   a) ocultación
   b) criptografía
   c) códigos
   d) grafología

10. Este tipo de contratos deben contener el costo el tiempo y la forma de revisión así como una calendarización de visitas que deben hacer los proveedores del servicio así como en qué consisten dichas visitas:
   a) mantenimiento
   b) preventivo
   c) correctivo
   d) detectivo

TEMA 6. AUDITORÍA ADMINISTRATIVA PARA EL ÁREA DE CÓMPUTO

Objetivo particular

Aplicar el proceso administrativo en el área informática a partir de la ejecución de una auditoría, a través de los instrumentos necesarios.

Temario detallado

6.1. Estructura orgánica del área
6.2. Personal
6.3. Capacitación
6.4. Presupuestos
6.5. Costos
6.6. Controles de asignación de trabajo

Introducción

El objetivo de realizar este tipo de auditorías es conocer cómo se ejerce la administración en materia de informática, una de las herramientas por utilizar es el proceso administrativo, ya que se han encontrado a lo largo del tiempo varios problemas por resolver como son:

- Falta de Planeación
- Organización deficiente
- Dirección mal ejercida
- Ausencia o deficiencia de Controles
- Negligencia
- Improvisación

6.1. Estructura orgánica del área

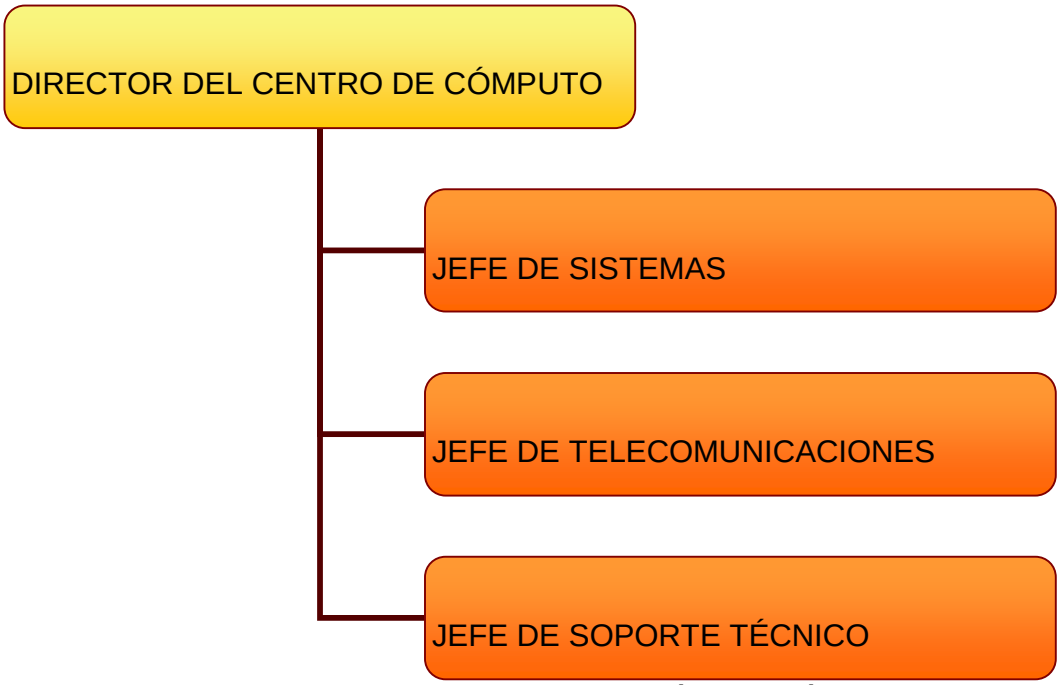


Figura 6.1. Estructura orgánica del área

Este organigrama solo es enunciativo, depende del tamaño y las necesidades de la institución auditada, sin embargo, cada una de las áreas puede inclusive cambiar de nombre y estructura, pero no de funciones. Por ejemplo, en el caso de soporte técnico de los bienes informáticos alguna descompostura o mal funcionamiento; el desarrollo de sistemas atiende a las necesidades de la Institución; el mantenimiento a servidores y a las redes con que cuente la institución, estas funciones se deben de tener de primera mano es decir, permanentemente, ya que se encuentran delimitadas o se deben de encontrar delimitadas en un manual de organización de la entidad o en uno propio del departamento.

6.2 Personal

Antes de realizar la contratación se debe acudir al manual de organización y procedimientos para poder delimitar los perfiles del puesto por desempeñar y la descripción del mismo.

Se deben de realizar los exámenes pertinentes para conocer el grado de conocimiento del personal que realiza la función de informática, si bien se establecen o pueden establecer los exámenes psicométricos y de conocimiento para elegir al candidato idóneo, la última palabra o decisión deberá recaer en el jefe directo o responsable de la función.

En esta fase vamos a evaluar ¿cómo lo va a hacer? Es decir, cuál es el personal con que se cuenta o se reclutará, así como las funciones que debe realizar cada uno de ellos para alcanzar el objetivo previamente trazado.

La organización involucra la estructuración de relaciones:

- Jerarquías: autoridad-responsabilidad
- Funciones: división de actividades
- Obligaciones: por unidad de trabajo y persona.

Cuando en un área de informática no existe una definición de funciones y responsabilidades es muy difícil distinguir los límites del trabajo que deberá cubrir cada área y persona. Por ello es importante que antes de la revisión se deba conocer cuáles son las funciones que realiza cada una de las áreas por auditar.

Áreas de revisión:

- Estructura orgánica
- Situación del personal
- Situación financiera

- Normas, políticas, planes y procedimientos

Para conocer la organización y funcionamiento de las áreas así como el nivel jerárquico de la toma de decisiones, tenemos que conocer la estructura orgánica, ya que esto definirá el alcance de nuestra revisión, y el conocimiento del departamento de informática en cuanto a su estructura.

Al evaluar la estructura orgánica se analiza lo siguiente:

- Los niveles para la toma de decisiones
- La existencia de una clara delimitación de responsabilidades
- Definición de puestos
- Número de empleados
- Personas que reportan a cada nivel
- Conflictos de autoridad

6.3. Capacitación

La capacitación debe darse de forma automática y necesaria, debido al constante evolucionar de la tecnología, y no hay que perder de vista que además es de carácter obligatorio, estipulado en nuestra Constitución y en la Ley Federal del Trabajo.

La capacitación debe darse a través de un plan anual de capacitación que debe hacerse en conjunto con el comité de auditoría (si es que existe) o en su defecto entre quien planea el desarrollo de la empresa y el encargado del desarrollo informático.

La capacitación debe darse en función de las necesidades de la empresa y la proyección misma del área, recordando que la capacitación es una inversión y no un gasto, esta verdad puede marcar el rumbo del centro de cómputo entre lo actual y lo obsoleto, entre ser competitivo o solo participativo, entre disminuir riesgos o vivir pensando que no va a suceder nada, entre la prevención y la corrección.

6.4. Presupuesto

El área debe contar con un presupuesto asignado previamente a la presentación de un plan anual de desarrollo informático, en donde se marcan los distintos escenarios que tiene en función de los objetivos y metas de la empresa.

Se debe evaluar el impacto de la adquisición de nueva tecnología y el desempeño del personal que trabaja en el área, así como la evolución de los resultados obtenidos contra los planeados.

En esta fase verificaremos el cumplimiento de las fases anteriores, es decir, es ver que se haga o se realice y básicamente te enfrentas a la realidad de las cosas y tienes que observar los siguientes principios:

- Coordinación de intereses, es decir que en la asignación presupuestal se privilegie lo importante sobre lo urgente.
- Impersonalidad de mando: Al llevar a cabo esta etapa se debe de cuidar que la asignación presupuestal sea con base en funciones y no a nivel jerárquico.
- Utilización de la vía jerárquica: Que la asignación presupuestal esté autorizada por un funcionario que tenga el nivel de hacerlo.
- Resolución y aprovechamiento de conflictos: Debe existir retroalimentación sobre la problemática detectada tanto con usuarios como con la gente responsable de los bienes informáticos.

La realización eficaz de la dirección incluye:

- Cómo delegar y ejercer autoridad
- Comunicación de órdenes
- Supervisión constante
- Obtención de evidencia suficiente y competente

Es necesario erradicar el fantasma de la informática y la resistencia al cambio, no se pretende crear especialistas en el personal no informático, si no que se conozca la filosofía en informática; para ello nos vamos a auxiliar de la capacitación.

El auditor debe analizar los índices de rotación de personal y sus prestaciones para poder evaluar posible inconformidad del personal y disminuir el grado de ocurrencia de un fraude.

6.5. Costos

El desarrollo informático incluye costos de personal y recursos informáticos, lo que implica la constante verificación de las decisiones tomadas en función del costo-beneficio de cada acción o proceso o sistema desarrollado.

Al realizar el examen del servicio prestado por el área se debe considerar la oportunidad del mismo, por ejemplo se debe entregar un flujograma de actividades y reportes de servicios prestados para evaluar el costo de cada intervención del área o el costo de un sistema desarrollado por esta.

6.6. Control de asignación del trabajo

Es la medición de los resultados obtenidos contra los planeados y aquí vamos a evaluar cómo se hicieron las cosas, con el fin de corregir, mejorar y formular nuevos planes.

La fase del control incluye:

El establecimiento de normas	Conocer los requisitos mínimos para realizar la función de la administración de informática,

	referentes a calidad y eficiencia de las actividades de la Institución por auditar.
Análisis de procedimientos	Consiste en evaluar los procedimientos para realizar la administración de la función de informática, a través de flujogramas, y análisis de procedimientos.
Utilidad del control	Aquí se va a evaluar que los controles establecidos sean oportunos para que detecten el riesgo de ocurrencia.
Seguridad en la acción seguida	Cuando se realizan las actividades cotidianas y se plasman en un manual y estos están debidamente autorizados, actualizados y verificados al llevarse a cabo, se tiene la certeza que la acción seguida en la actividad es adecuada.
Corrección de debilidades	Son los riesgos externos que pueda tener la administración de la función de informática, como enfrentarse a la obsolescencia de los bienes informáticos.
Conocimiento de fortalezas	Es conocer dónde están más fuertes nuestros controles y existe menor riesgo de ocurrencia de un evento.
Mejoramiento de lo obtenido	Es aprender de la experiencia y el riesgo que se haya suscitado al realizar la actividad y reorganizar una nueva actividad o acción para minimizar el impacto de ocurrencia.
Bases para nueva planeación	Todo lo anterior nos debe llevar a mejorar o rearmar nuestra forma de ejercer la administración de la función de informática.

Al terminar la evaluación de éstas fases, estaremos en posibilidad de conocer cómo lleva a cabo la institución la administración de la función de informática y así, poder evaluar su plan de desarrollo informático, si es que existe, o si no, dejar las bases para que se prepare lo más pronto posible.

Control

En esta fase se verifica si se cumplió con los objetivos planeados, analizando los resultados obtenidos.

Solicitar

- Informe anual de actividades del jefe de la División de Informática.
- Último informe de cada departamento con la finalidad de verificar su existencia y periodicidad de realización.
- Registros y bitácoras de actividades desarrolladas por todas y cada una de las personas del área.

Como resultado de este tipo de auditoría daremos un informe de cada fase que compone la auditoría a la función de la administración de informática y podremos identificar en dónde existen debilidades de control para poder emitir las sugerencias pertinentes y poder minimizar el riesgo de la funcionalidad en cuanto a recursos informáticos se refiere.

Bibliografía básica del tema 6

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes].

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

Sitios electrónicos

Sitio	Descripción
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*
http://www.oocities.org/mx/acadentorno/aui.htm	Aguilar Castillo, Gil. (2009). *Auditoría Informática*, Facultad de Estadística e Informática. Universidad Veracruzana.

Actividades de aprendizaje

A.6.1. Elabora un cuadro comparativo entre el proceso administrativo en administración y el aplicado a la auditoría en informática.

A.6.2. Investiga cuál es la estructura orgánica en informática en un Institución que se dedica a la venta de bienes informáticos y una institución educativa y define cuál es para ti la mejor y sustenta tus conclusiones.

A.6.3. Investiga cuál es el perfil del puesto con que debe contar un director de centro de cómputo, asimismo, sustenta cuáles son los artículos constitucionales que hacen obligatoria la capacitación del personal.

Cuestionario de autoevaluación

Responde las siguientes preguntas

1. ¿Cuál es el objetivo de la auditoría administrativa para el área de cómputo?
2. ¿Cuáles son las funciones típicas del área de informática?
3. ¿Qué nivel jerárquico debe tener el responsable de la Administración de la Función de informática?
4. ¿Qué involucra la estructuración de relaciones?
5. ¿Qué se evalúa en la estructura orgánica?
6. ¿Por qué es necesaria la capacitación?
7. ¿En consiste la realización eficaz de la Dirección?
8. ¿Cuáles son los costos que se incluyen en el desarrollo informático?
9. ¿En qué consiste el control?
10. ¿Qué se solicita al jefe de la división de informática?

Examen de autoevaluación

Elige la respuesta correcta a las siguientes preguntas

1. ¿Es la herramienta de la cual el auditor se auxiliará para realizar esta auditoría?
   a) matriz de riesgos
   b) normas de auditoría
   c) procedimientos de auditoría
   d) proceso administrativo

2. En este proceso se observa la jerarquía, autoridad-responsabilidad, funciones son características de la etapa de:
   a) planeación
   b) organización
   c) dirección
   d) control

3. La Constitución Política de los Estados Unidos Mexicanos obliga a los patrones a darle a sus trabajadores:
   a) ropa
   b) herramienta
   c) capacitación
   d) aniversarios

4. La asignación Presupuestal que privilegia lo importante sobre lo urgente se refiere a:
   a) impersonalidad de mando
   b) utilización de la vía jerárquico
   c) resolución y aprovechamiento de conflictos
   d) coordinación de intereses

5. Al llevar a cabo esta etapa se debe cuidar que la asignación presupuestal sea con base en funciones y no a nivel jerárquico.
   a) impersonalidad de mando
   b) utilización de la vía jerárquico
   c) resolución y aprovechamiento de conflictos
   d) coordinación de intereses

6. Que la asignación presupuestal está autorizada por un funcionario que tenga el nivel de hacerlo, se refiere a:
   a) impersonalidad de mando
   b) utilización de la vía jerárquico
   c) resolución y aprovechamiento de conflictos
   d) coordinación de intereses

7. Debe existir retroalimentación sobre la problemática detectada tanto con usuarios como con la gente responsable de los bienes informáticos.
   a) impersonalidad de mando
   b) utilización de la vía jerárquico
   c) resolución y aprovechamiento de conflictos
   d) coordinación de intereses

8. Conocer los requisitos mínimos para realizar la función de la administración de informática, referentes a calidad y eficiencia de las actividades de la Institución por auditar:
   a) Establecimientos de Normas
   b) Análisis de Procedimientos
   c) Utilidad del control
   d) Seguridad en la acción seguida

9. Aquí se va a evaluar que los controles establecidos sean oportunos para que detecten el riesgo de ocurrencia:
   a) Establecimientos de Normas
   b) Análisis de Procedimientos
   c) Utilidad del control
   d) Seguridad en la acción seguida

10. Cuando se realizan las actividades cotidianas y se plasman en un manual y estos están debidamente autorizados, actualizados y verificados al llevarse a cabo, se tiene la certeza que la acción seguida en la actividad es adecuada.
   a) Establecimientos de Normas
   b) Análisis de Procedimientos
   c) Utilidad del control
   d) Seguridad en la acción seguida

TEMA 7. INTERPRETACIÓN DE LA INFORMACIÓN

Objetivo particular

El alumno podrá interpretar los hallazgos obtenidos durante la revisión para plasmarlos en un informe, que sirva de base para prevenir riesgos y en la toma de decisiones.

Temario detallado

7.1. Técnicas para la interpretación de la información
7.2. Evaluación de los sistemas
7.3. Controles
7.4. Presentación del dictamen

Introducción

Se cuenta en la actualidad con numerosas herramientas para interpretar la información que recopilamos durante la auditoría planeada previamente, después viene la fase de la ejecución del trabajo en donde, para realizar un trabajo suficiente y competente nos auxiliamos de las técnica de auditoría emitida por el IMCP, y que podemos adaptar a nuestras revisiones en informática, no obstante podemos adherir las técnicas propias de la informática, a continuación mencionaremos las técnica emitidas por el IMCP, que son Estudio General, Análisis, Inspección, Confirmación, Investigación, Declaraciones, Certificación, Observaciones, Cálculo.

7.1. Técnicas para la interpretación de la información

Clasificación de las Técnicas de Auditoría

Las técnicas son los elementos de ayuda con que el auditor cuenta, debido a que mediante la utilización de las mismas formarán el soporte de los papeles de trabajo que sustentan la opinión final del auditor.

La comisión de normas y procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos, en su boletín 5010 Procedimientos de auditoría, ha propuesto la siguiente clasificación:

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaraciones
- Certificación
- Observaciones
- Cálculo

A continuación se mencionan en qué consiste cada uno de ellos.

Estudio General

Es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones, a través de sus elementos más significativos para concluir se ha de profundizar en su estudio y en la forma que ha de hacerse.

Básicamente con esta técnica se tiene nuestro primer diagnóstico sobre lo que el cliente requiere y las características de la empresa.

Análisis

Es el estudio de los componentes de un todo para concluir con base en aquellos respecto de este. Esta técnica se aplica concretamente al estudio de las cuentas o rubros genéricos de los estados financieros.

Del universo de operaciones que realiza la institución, se determina una muestra que tiene que ser significativa y con base en ella se realizan los análisis correspondientes sobre cada situación especifica que se requiera conocer con detalle.

Inspección

Es la verificación física de las cosas materiales en las que se tradujeron las operaciones, se aplica a las cuentas cuyos saldos tienen una representación material, (efectivos, mercancías, bienes, etc.).

Para el caso de auditoría en informática, es la verificación física de los bienes informáticos, ya sea software o hardware con sus respectivas licencias y usos reales, es decir que los bienes existan.

Confirmación

Es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operación, en la que participó y por la cual está en condiciones de informar válidamente sobre ella.

En el caso de informática se realizará la verificación de licencias de uso de equipo y/o software, y en su caso verificar si existe un contrato para la prestación de servicios.

Investigación

Es la recopilación de información mediante pláticas con los funcionarios y empleados de la empresa.

Para el caso de informática, se realiza esta misma función pero, con los responsables de la función de informática y las áreas usuarias.

Declaraciones y Certificaciones

Es la formalización de la técnica anterior, cuando, por su importancia, resulta conveniente que las afirmaciones recibidas deban quedar escritas (declaraciones) y en algunas ocasiones certificadas por alguna autoridad (certificaciones).

Las declaraciones obtenidas con la técnica de investigación para que sea válida como evidencia tiene que estar firmada por aquella persona que proporcionó dicha información y en caso de ser necesario obtener las certificaciones correspondientes que se incluyen en la protesta de decir verdad.

Observación

Es una manera de inspección, menos formal, y se aplica generalmente a operaciones para verificar cómo se realiza en la práctica.

En informática es percatarse de los procedimientos que se llevan a cabo para realizar una rutina o instrucción y validar si esta se realiza conforme lo establece algún manual, por ejemplo observar que todas las personas que accedan a un área donde se encuentran bienes informáticos claves, o sensibles se registran y se controlan de forma más estricta.

Cálculo

Es la verificación de las correcciones aritméticas de aquellas cuentas u operaciones que se determinan fundamentalmente por cálculos sobre bases precisas. Simplemente es verificar matemáticamente cualquier operación que se requiera para validar alguna cifra o calculo.

Clasificación de acuerdo con el Libro de Normas y procedimientos de auditoría emitida por el Instituto Mexicano de Contadores Públicos. Boletín 5010.

7.2. Evaluación de los sistemas

La evaluación de los sistemas no se refiere únicamente a la metodología para su desarrollo o ciclo de vida de los sistemas, sino a lo que acontece con anterioridad, es decir, en la fase previa, los sistemas son evaluados de conformidad con la planeación de lo que se espera que dé el sistema y nos auxiliamos de documentos que nos permitan conocer el funcionamiento del nuevo sistema.

Además de las técnicas antes mencionadas, nos ayudaremos de los cuestionarios de control interno, y cuestionarios de aplicación general y específica utilizando el modelo que hace referencia a la ponderación de cada etapa de la auditoría en informática y se le da un valor para medir, ya sea la productividad, costo-beneficio, y utilidad de la capacidad instalada, para poder emitir una opinión sobre la razonabilidad en el uso de recursos informáticos, que es finalmente el objetivo de la Auditoría en informática.

Los sistemas finalmente van a ser evaluados por los usuarios de los mismos, donde evaluarán su capacidad y necesidad de información, sobre si se obtiene de ellos lo necesario para la toma de decisiones.

Como todo sistema de información debemos evaluar la seguridad y protección de la información y cumplir con los objetivos de control y salvaguarda de la misma.

Al realizar los hallazgos de auditoría se deben sustentar, es decir la obtención de evidencia suficiente y competente basada en resultados de pruebas de auditoría.

7.3. Controles

Los controles de la información que emanan del sistema deben estar perfectamente establecidos de acuerdo con la utilidad y orden jerárquico de quien lo solicita o emite, se deben evaluar que existan reglas o normatividad clara en materia de emisión, uso y resguardo de los mismos, el resultado final del sistema es la información que de él resulta, recordando que todos los controles deben pasar por los siguientes elementos:

a) Salvaguarda de los activos de la empresa
b) Obtención de información veraz, confiable y oportuna
c) Adherencia a las políticas de la empresa
d) Promoción de la eficiencia en las operaciones.

Todos los controles deben mostrar su valía y existencia con base en su oportunidad y su costo-beneficio. Los controles no deben ser exagerados (en sentido figurado llegar a la ‘controlitis’), ni tan ligeros que darían lo mismo tenerlos o no, es decir llegar a una total ausencia de control, sin embargo de nada valen si no existe una figura que vea que se cumplan todos los controles establecidos para la salvaguarda de la información, que nos ayudará para la toma de decisiones.

7.4. Presentación del dictamen

El dictamen o informe de auditoría va a variar de modelo o presentación dependiendo de hacia quién va dirigido, normalmente cuando la auditoría es de carácter interno se dice que se presenta un informe y cuando es de uso externo se presenta un dictamen. Finalmente lo importante es que se presenta como una radiografía del trabajo realizado basado en hallazgos reales y soportables.

Informe de auditoría

Elementos básicos del Informe de Auditoría

La materialización final del trabajo llevado a cabo por los auditores independientes se documenta en el dictamen, informe u opinión de auditoría. Además, para aquellas entidades sometidas a auditoría legal, este documento junto con las cuentas anuales del ejercicio.

El informe de auditoría independiente deberá contener, como mínimo, los siguientes elementos básicos:

- El título o identificación.
- A quién se dirige y quiénes lo encargaron.
- El párrafo de "Alcance".
- El párrafo de "Opinión".
- El párrafo o párrafos de "Énfasis".
- El párrafo o párrafos de "Salvedades".
- El párrafo sobre el "Informe de Gestión".
- La firma del informe por el auditor.
- El nombre, dirección y datos registrables del auditor.
- La fecha del informe.
- El párrafo legal o comparativo

Objetivos, características y afirmaciones que contiene el informe de auditoría

El informe de auditoría en informática tiene como objetivo expresar una opinión técnica sobre el uso de los recursos informáticos, sobre si esta muestra la imagen fiel del recurso informático, y su aplicación correcta dentro de la Institución que se audite.

Características del informe de auditoría

- Es un documento formal.
- Muestra el alcance del trabajo.
- Contiene la opinión del auditor.
- Se realiza de acuerdo con una normatividad.

Principales afirmaciones que contiene el informe

- Indica el alcance del trabajo y si ha sido posible llevarlo a cabo y de acuerdo con normas de auditoría o de la empresa.
- Expresa si es correcto el uso en los recursos informáticos y que contienen la información necesaria y suficiente y han sido formuladas de acuerdo con la normatividad vigente ya sea interna o externa.

Tipos de opinión

Existen cuatro tipos de opinión en auditoría:

- Opinión Limpia o en blanco o sin salvedades.
- Opinión con Salvedades.
- Opinión Negativa.
- Opinión con abstención.

La opinión favorable, limpia o sin salvedades significa que el auditor está de acuerdo, sin reservas, sobre la presentación y contenido de los procedimientos que se llevan a cabo para verificar la utilización adecuada en los recursos Informáticos.

La opinión con salvedades, significa que el auditor está de acuerdo con los procedimientos y utilización de los recursos informáticos, pero con ciertas reservas.

La opinión negativa significa que el auditor está en desacuerdo con los procedimientos utilizados para el manejo de los recursos informáticos y afirma que éstos no se realizan conforme a estándares nacionales o determinados por la empresa.

Por último, la abstención de opinión significa que el auditor no expresa ningún dictamen sobre el manejo de los recursos informáticos. Esto no significa que esté en desacuerdo con ellos, significa simplemente que no tiene suficientes elementos de juicio para formarse ninguno de las tres anteriores tipos de opinión.

Observaciones

El auditor debe realizar procedimientos diseñados para obtener suficiente y apropiada evidencia de auditoría, en que puedan, todos los elementos hasta la fecha del informe del auditor, requerir de ajustes o exposiciones en las metodologías que hayan sido identificados.

Todos los procedimientos de auditoría emprendidos y las conclusiones alcanzadas deben estar completamente documentados, las hojas de trabajo deben incluir notas, detalladas de reuniones, incluyendo quién estaba presente, los asuntos discutidos y el resto de las discusiones.

El auditor no tiene ninguna obligación de hacer ninguna investigación relacionada con la información de los recursos informáticos, que estos hayan sido omitidos, el informe de auditoría solo se hace responsable de lo presentado por la administración y lo observado por los auditores.

Los objetivos de los procedimientos de finalización de la auditoría para asegurar que:

- Sí ha sido obtenida suficiente evidencia de auditoría para apoyar la opinión de auditoría.
- Todas las decisiones tomadas han sido documentadas.
- El archivo de auditoría ha sido complementado.
- Cualquier tema estratégico ha sido documentado y discutido con el cliente.

Las tareas claves en la terminación de la auditoría son:

- Terminación de cada área de auditoría del archivo.
- Escribir el informe al socio.
- Escribir cualquier revisión estratégica del negocio.
- Revisión de las hojas de trabajo.
- Conclusiones generales de auditoría.
- Realizar una reunión para asegurar que los secretos de la empresa no sean relevados.

Sugerencias

Los programas principales de auditoría deben mostrar claramente el objetivo de auditoría, el trabajo realizado y las conclusiones alcanzadas y ser sustentados por todos los papeles de trabajo de referencia cruzada.

Cada programa principal auditado debe ser comparado con las hojas de trabajo de auditoría relevantes y con las cifras de los recursos ejercidos en informática.

Correctivas

Conclusiones del área de Auditoría:

- Se debe obtener una conclusión para cada área de auditoría.
- Antes de obtener una conclusión, debe asegurarse que el programa de auditoría fue llevado a cabo como se planteó, o que los cambios acerca de las decisiones hechos en la etapa de la planificación están documentados.

- Cualquier problema importante u otros asuntos no aclarados deben ser anotados por la gerencia o incluidos en el informe al socio. Cualquier asunto inusual, aun cuando estén aclarados, deben ser incluidos en el informe al socio en manera de información.
- Cualquier debilidad u otros asuntos relacionados con el área de auditoría, que resulten apropiados reportar al cliente, deben ser resumidos e incluidos en la carta de gerencia.
- Cualquier área donde el auditor haya tenido que depender de representaciones, éstas deben ser incluidas en la carta de representación.

Informe al socio

El informe al socio engloba todos los asuntos que tienen un efecto en la opinión de auditoría, o que necesitan ser discutidos con al cliente.

Dependiendo de la estructura del equipo de auditoría debe ser hecho en borrador por el auditor responsable, para comentar los hallazgos, mientras la auditoría avanza y completado cuando la auditoría termine.

El encargado de la auditoría debe evidenciar la terminación del informe al socio, firmando la primera página y el socio debe refrendarlo.

Aunado a todo lo anterior, el auditor en informática debe tener en cuenta que su trabajo, es profesional y de una fuerte independencia mental ya que al realizar auditorías a información o procedimientos informáticos estos son la médula espinal de la empresa y con riesgos altos.

Y conlleva a que la fragilidad de los sistemas es de alto riesgo y que normalmente las instituciones no le dan importancia a este tipo de auditorías porque no son obligatorios, sino voluntarios y las empresas ven a la auditoría como un gasto y no como una inversión.

El auditor debe, con su trabajo, motivar a que ese supuesto gasto se convierta en beneficios para la empresa y aumente su nivel de confianza en la seguridad de sus recursos informáticos.

Bibliografía básica del tema 7

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes].

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

Sitios electrónicos

Sitio	Descripción
http://www.audit.gov.tw/span/span2-2.htm	Ministerio de la Auditoría General de la República China (NAO). (2004). Auditoría informática
http://www.mitecnologico.com/Main/AuditoriaInformatica	Mitecnológico. (2004). *Auditoría Informática*
http://www.oocities.org/mx/acadentorno/aui.htm	Aguilar Castillo, Gil. (2009). *Auditoría Informática*, Facultad de Estadística e Informática. Universidad Veracruzana.

Actividades de aprendizaje

A.7.1. Busca sobre los diferente tipos de informe que se presentan en la auditoría en informática, en diversos países y continentes, asimismo realiza un cuadro comparativo entre ello y fundamenta ¿cuál de ellos te parece el más completo y por qué?

A.7.2. Analiza la película “Los piratas del Valle de los Silicones” (Martyn Burke, 1999, [TV], 95 min) y analiza su aplicación en el ámbito de la auditoría en informática y en el informe que presenta.

Cuestionario de autoevaluación

Responde las siguientes preguntas:

1. ¿Qué son las técnicas de auditoría?
2. ¿Cómo se clasifican las técnicas de auditoría?
3. ¿En qué consiste el estudio general?
4. ¿En qué consiste la certificación?
5. ¿A qué se refiere la evaluación de los sistemas?
6. ¿En qué consiste el Modelo de Cuestionario del Control interno?
7. ¿Qué es la salvaguarda de los activos de la empresa?
8. ¿Qué deben mostrar todos los controles?
9. ¿En qué consiste el dictamen?
10. ¿Cómo se estructura un dictamen?

Examen de autoevaluación

Elige la respuesta correcta a las siguientes preguntas:

1. ¿Cuáles son los elementos de ayuda con que el auditor cuenta, debido a que mediante la utilización de las mismas formarán el soporte de los papeles de trabajo?
   a) procedimientos de auditoría
   b) normas de auditoría
   c) proceso administrativo
   d) técnicas de auditoría

2. La Comisión de Normas y Procedimientos de Auditoría del Instituto Mexicano de Contadores Públicos emitió este boletín que habla sobre las técnicas y procedimientos de auditoría, es el número:
   a) 3140
   b) 5010
   c) 6080
   d) 5030

3. Básicamente con esta técnica se tiene nuestro primer diagnóstico sobre lo que el cliente requiere y las características de la empresa:
   a) confirmación
   b) análisis
   c) estudio general
   d) inspección

4. Es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operación, en la que participó y por la cual está en condiciones de informar válidamente sobre ella:
   a) confirmación
   b) análisis
   c) estudio general
   d) inspección

5. En informática es percatarse de los procedimientos que se llevan a cabo para realizar una rutina o instrucción y validar si esta se realiza conforme lo establece algún manual, por ejemplo observar que todas las personas que accedan a un área donde se encuentran bienes informáticos claves o sensibles se registran y se controlan de forma más estricta.
   a) observación
   b) cálculo
   c) investigación
   d) análisis

6. Es la recopilación de información mediante pláticas con los funcionarios y empleados de la empresa:
   a) Observación
   b) Cálculo
   c) Investigación
   d) Análisis

7. ¿Por quiénes serán evaluados los sistemas de información una vez terminado este?
   a) dirección
   b) usuarios
   c) sistemas
   d) soporte técnico

8. Tiene como objetivo expresar una opinión técnica sobre el uso de los recursos informáticos:
   a) informe o dictamen
   b) análisis de información
   c) papeles de trabajo
   d) cuestionario de control interno

9. Significa que el auditor está de acuerdo, sin reservas, sobre la presentación y contenido de los procedimientos que se llevan a cabo para verificar la utilización adecuada en los recursos Informáticos:
   a) opinión con salvedad
   b) abstención de opinión
   c) opinión limpia
   d) opinión negativa

10. Significa que el auditor está de acuerdo con los procedimientos y utilización de los recursos informáticos, pero con ciertas reservas.
    a) opinión con salvedad
    b) abstención de opinión
    c) opinión limpia
    d) opinión negativa

Bibliografía básica

Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) e Instituto Mexicano de Contadores Públicos (IMCP). (2009). *Normas de información financiera*. (28ª ed.) México: CNINIF / IMCP.

Echenique García, José Antonio. (2001). *Auditoría en informática*. (2ª ed.) México: McGraw Hill.

Hernández Hernández, Enrique. (2002). *Auditoría en informática*. (2ª ed.) México: CECSA.

Instituto Mexicano de Contadores Públicos. (2008). *Normas y procedimientos de auditoría y Normas para atestiguar versión estudiantil*. (28ª ed.) México: IMCP.

Instituto Mexicano de Contadores Públicos. (2010). Boletín 5020 “El Muestreo en la Auditoría” en *Normas y Procedimientos de Auditoría y Normas para Atestiguar*. México: IMCP, p. 392

Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.

Téllez Trejo, Benjamín Rolando. (2004). *Auditoría: un enfoque práctico*. México: Cengange.

Piattini Velthuis, Mario G., Peso Navarro, Emilio del. (1997). *Auditoría Informática: un enfoque práctico*. Madrid: Ra-Ma.

Bibliografía complementaria

Ayala Rodiles, Sara Isabel. (1996). *Seminario de auditoría en informática* (16 y 17 de junio, FCA), Patronato universitario UNAM [apuntes]

Cohen, Daniel (2000). *Sistemas de información para los negocios*. (3ª ed.) México: McGraw-Hill.

Kell, Walter G.; Ziegler, Richard E. Boynton William. (1995). *Auditoría Moderna*. (2ª ed.) México: CECSA.

RESPUESTAS A LOS EXÁMENES DE AUTOEVALUACIÓN.
AUDITORÍA EN INFORMÁTICA

Tema 1	Tema 2	Tema 3	Tema 4
1. a	1. b	1. a	1. a
2. a	2. a	2. a	2. a
3. c	3. c	3. c	3. b
4. c	4. d	4. c	4. b
5. c	5. d	5. c	5. d
6. b	6. a	6. b	6. b
7. b	7. a	7. c	7. d
8. a	8. d	8. d	8. a
9. d	9. b	9. b	9. c
10. d	10. d		10. d

Tema 5	Tema 6	Tema 7
1. a	1. d	1. d
2. c	2. b	2. b
3. d	3. c	3. c
4. c	4. d	4. a
5. b	5. a	5. a
6. b	6. b	6. c
7. b	7. c	7. b
8. a	8. a	8. a
9. b	9. c	9. c
10. b	10. d	10. a