UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
DIVISIÓN SISTEMA UNIVERSIDAD ABIERTA Y EDUCACIÓN A DISTANCIA

APUNTE ELECTRÓNICO

Auditoría en Informática

Licenciatura en Informática

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

COLABORADORES

DIRECTOR DE LA FCA
Dr. Juan Alberto Adam Siade

SECRETARIO GENERAL
Mtro. Tomás Humberto Rubio Pérez

– – – –

COORDINACIÓN GENERAL
Mtra. Gabriela Montero Montiel
Jefe de la División SUAyED-FCA-UNAM

COORDINACIÓN ACADÉMICA
Mtro. Francisco Hernández Mendoza
FCA-UNAM

– – – –

AUTOR
Mtro. José de Jesús Aguirre Bautista

REVISIÓN PEDAGÓGICA
Mtro. Joel Guzmán Mosqueda

CORRECCIÓN DE ESTILO
Mtro. Carlos Rodolfo Rodríguez de Alba

DISEÑO DE PORTADAS
L.CG. Ricardo Alberto Báez Caballero
Mtra. Marlene Olga Ramírez Chavero

DISEÑO EDITORIAL
Mtra. Marlene Olga Ramírez Chavero

Dr. Enrique Luis Graue Wiechers
Rector

Dr. Leonardo Lomelí Vanegas
Secretario General

Dr. Juan Alberto Adam Siade
Director

Mtro. Tomás Humberto Rubio Pérez
Secretario General

Mtra. Gabriela Montero Montiel
Jefa del Sistema Universidad Abierta
y Educación a Distancia

Auditoría en Informática

Apunte electrónico

Edición: noviembre 2017

D.R. © 2013 UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Ciudad Universitaria, Delegación Coyoacán, C.P. 04510, México, Ciudad de México.

Facultad de Contaduría y Administración
Circuito Exterior s/n, Ciudad Universitaria
Delegación Coyoacán, C.P. 04510, México, Ciudad de México.

ISBN: En trámite
Plan de estudios 2012, actualizado 2016.

"Prohibida la reproducción total o parcial por cualquier medio sin la autorización escrita del titular de los derechos patrimoniales"

"Reservados todos los derechos bajo las normas internacionales. Se le otorga el acceso no exclusivo y no transferible para leer el texto de esta edición electrónica en la pantalla. Puede ser reproducido con fines no lucrativos, siempre y cuando no se mutile, se cite la fuente completa y su dirección electrónica; de otra forma, se requiere la autorización escrita del titular de los derechos patrimoniales."

Hecho en México

OBJETIVO GENERAL

El alumno comprenderá y aplicará los conceptos fundamentales y las metodologías más importantes para realizar una auditoría informática.

TEMARIO OFICIAL

(64 horas)

	Horas
1. Fundamentos de auditoría y auditoría informática	6
2. Control interno	6
3. Metodologías para la auditoría en informática	8
4. Áreas de evaluación de la auditoría en informática	10
5. Planeación de la auditoría informática	12
6. Evaluación de los recursos informáticos	14
7. Informe de auditoría	8
Total	**64**

INTRODUCCIÓN

El constante evolucionar en los recursos tecnológicos nos obliga a evaluar cuál es su función en el desarrollo de una empresa o institución, así como su participación en el logro de sus objetivos. Se busca que los recursos tecnológicos nos proporcionen, además, una garantía razonable sobre la administración de los recursos informáticos, la cual será una función esencial del departamento de auditoría en informática, si es que existe o, en su defecto, del comité de auditoría, que debe ser un órgano de establecimiento de estándares para fortalecer la función de auditoría, y proporcionar a los directivos un adecuado aseguramiento y asesoría en cuanto a las estrategias y políticas que garanticen que los recursos de tecnología de la información (TI), apoyen a la institución a través de la promoción de la calidad, eficiencia, eficacia y reducción de costos de sus procesos, que serán la base para buscar las certificaciones de calidad en todos los ámbitos, si es que la visión de la institución se proyecta hacia la calidad y competitividad internacional, y, derivado de lo anterior, tenemos la estandarización y requerimientos de información propios de los informes internacionales de control.

Los informes de control interno especializados están cada vez más solicitados como área de conocimiento, por ello la difusión de los trabajos e investigaciones de auditorías con características especiales va en aumento; en este caso hablaremos de la importancia de la auditoría en informática.

Los diferentes tipos de auditoría en informática conocidos auxilian cada vez más a las instituciones, ya que se preocupan por el uso de los recursos informáticos; sin

embargo, es el tratamiento de la información y su origen, lo que nos lleva a conocer estos tipos de auditoría.

Siempre han existido las auditorías; ahora, en este mundo globalizado, se nos induce a tomar en cuenta la tecnología ya que, inclusive, el Instituto Mexicano de Contadores Públicos (IMCP), emite el boletín 3140 de Normas y Procedimientos de Auditoría y Normas para atestiguar (NAGAS), llamado “Efectos de Tecnología de Información (TI) en el Desarrollo de una Auditoría de Estados Financieros” y, aunado a esto, existe un informe internacional, llamado Objetivos de Control para la Información Pública y Tecnología Relacionada (COBIT), alineado con estándares de control y auditoría.

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la entidad; sin embargo, por lo que respecta a la tecnología de información, ésta es una herramienta estratégica que representa 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.

La *administración* deberá además optimizar el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos.

Para cumplir con esta responsabilidad, así como para alcanzar sus objetivos, la administración debe entender el estado de sus propios sistemas de tecnologías de información y decidir el nivel de seguridad y control que deben proveer estos sistemas.

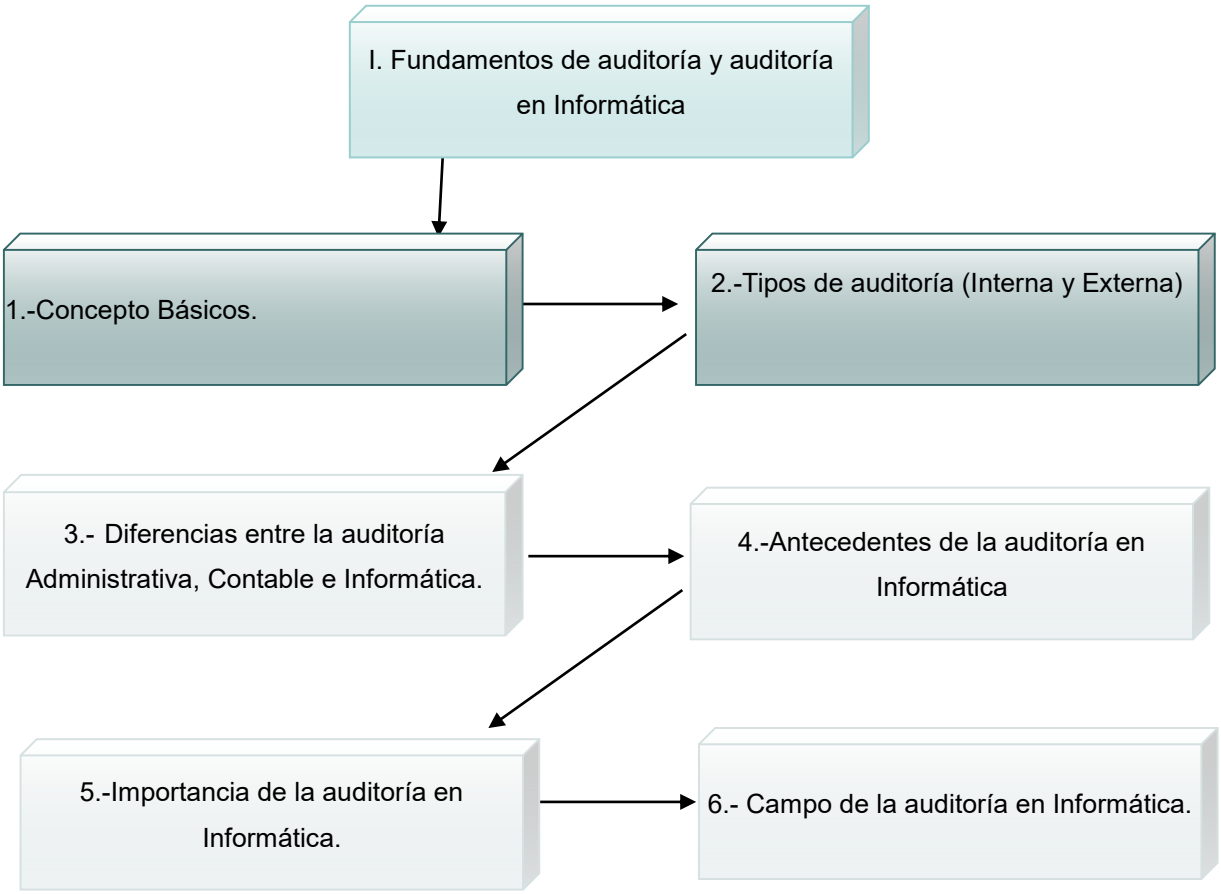
Una parte sustantiva de la auditoría en informática es el conocimiento de los tipos de auditoría que en la vida práctica se han llevado a cabo a diferentes instituciones,

ya sean públicas o privadas, siendo éstas de carácter enunciativo, más no limitativo, y considerando que esta clasificación puede variar con respecto a cada persona que practique este tipo de auditoría. Se listan a continuación los tipos de auditoría:

1. Auditoría al Ciclo de Vida del Desarrollo de Sistemas (ACVDS).
2. Auditoría a un Sistema en Específico o en Operación (ASE/O).
3. Auditoría de Gestión de Tecnologías de Información (AGTI).
4. Auditoría a Redes (AR).
5. Auditoría a Telecomunicaciones (AT).
6. Auditoría a Controles Generales o de Gestión (ACG/G).
7. Auditoría a Computadoras Autónomas (ACA).
8. Auditoría a la Función de la Administración de Informática. (AFAI).

La mayoría de los estudios sobre la temática se basan en la obtención de información; sin embargo, esta situación ha tenido que evolucionar pues hoy, lejos de ser una solución, más parece un problema ya que ahora tendremos que analizar toda esa cantidad de información para poder discriminarla y saber cuál es la que vamos a utilizar y que sea realmente importante. Y debido a la diversificación de la auditoría y sus áreas de aplicación se desarrolla este trabajo de auditoría en informática.

ESTRUCTURA CONCEPTUAL



UNIDAD 1

Fundamentos de auditoría y auditoría informática

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno conocerá las características de la auditoría en informática y las diferencias con los demás tipos de auditoría.

TEMARIO DETALLADO

(6 horas)

1. Fundamentos de auditoría y auditoría informática

1.1. Conceptos básicos
1.2. Tipos de auditoría (externa e interna)
1.3. Diferencias entre la auditoría administrativa, auditoría contable y auditoría en informática
1.4. Antecedentes de la auditoría en informática
1.5. Importancia de la auditoría en informática
1.6. Campo de la auditoría informática

INTRODUCCIÓN

La auditoría en informática nace como un órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico-financiera, aun y cuando todavía no se le da la importancia requerida; las instituciones que frecuentemente solicitan este tipo de servicios son los bancos y otras instituciones financieras.

Las actividades realizadas por el Departamento de Auditoría, sin ninguna duda deben ser independientes, ya que esa es una de sus características plasmadas en las normas personales y establecidas en los gobiernos corporativos de cada institución. Sin embargo, al desempeñar las labores propias de auditoría se evalúa el control interno en materia de recursos informáticos, con la modalidad de que las auditorías que en la actualidad se realizan están basadas en riesgos, el trabajo final del auditor culmina con la emisión de un informe o dictamen en donde se plasman las cédulas de sugerencias, observaciones y consecuencias sobre los hallazgos realizados durante su revisión y que tienen que darlas a conocer en un preinforme y realizar las aclaraciones pertinentes con el auditado antes de presentar el informe definitivo.

El conocimiento técnico y capacidad profesional, así como el cuidado y diligencia profesional que practique el auditor y su grupo de trabajo, en el cual debe haber profesionistas heterogéneos más que homogéneos, dado que nos auxiliamos de contadores, administradores, abogados, etc. Esto nos da garantía de contar con visiones que conllevan a realizar un trabajo integral y multifacético dentro de la auditoría, y, por lo tanto, podremos diagnosticar las áreas de riesgo y de mejora continua que podamos sugerir a la institución auditada.

Recordando que el auditor sólo puede emitir un juicio global o parcial basado en hechos, no en suposiciones, y de los cuales podamos obtener la evidencia suficiente y competente para que, partiendo de esta situación, podamos sustentar nuestra opinión.

Es importante precisar que la obtención de información, veraz confiable y oportuna es un elemento indispensable en el control interno como auxiliar en la toma de decisiones. Esta característica, aunada a los beneficios de las tecnologías de información y comunicación, juega un papel importante en la transformación de los procesos hacia la calidad como medida eficiente de mejora continua y competitividad.

1.1. Conceptos básicos

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”.

Véase: http://lema.rae.es/drae/srv/search?id=jHIksgNjM2x53A2fZYh

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 las 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 (IMCP, 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.

A continuación, se presentan algunas definiciones de diversos autores, sobre el concepto de auditoría en informática.

> “Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.” (Weber, 200: 15).

> “Consiste en emitir una opinión sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple con las condiciones que le han sido prescritas.” (Hernández, 2001: 4).

> Es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que, por medio del señalamiento de los cursos alternativos, se logre una utilización más eficiente y confiable y segura de la información que servirá para una adecuada toma de decisiones. (Echenique, 2001: 18).

> El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que circula por el área se maneja con los conceptos básicos de integridad, exactitud y confiabilidad, etc. (Hernández, 2001, p. 15).

El concepto de auditoría en informática de José de Jesús Aguirre es el siguiente:

> La auditoría en informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una institución, con el fin de emitir un informe y/o dictamen profesional sobre la situación en que se desarrollan y se utilizan, esos recursos, con base en la normatividad existente ya sea interna, externa o ambas.

1.2. Tipos de auditoría (externa e interna)

La auditoría interna

Esta puede ser realizada por personal que puede o no formar parte de la organización; si es realizada con recursos materiales y personas que pertenecen a la empresa auditada, se le conoce como auditor dependiente.

Los auditores internos pertenecen a la institución donde realizan la revisión, y, por lo tanto, son dependientes de ella; sin embargo, esto no es impedimento para que se vea coartada su independencia mental al momento de realizar su trabajo, la capacidad y necesidad de este departamento estará en función de las necesidades de la institución y su evaluación o permanencia estará sujeta a los resultados que presente.

Esta auditoría se refiere a la revisión permanente de los recursos de la institución a la que pertenecen con el objeto de emitir un informe sobre el funcionamiento y aprovechamiento de los mismos, así como el establecimiento de controles y su revisión la realizan basada en riesgos.

La auditoría externa

Esta labor es realizada por personal ajeno a la institución, ya sea una persona física o moral, que son contratadas para realizar una revisión en específico, y entre las ventajas que esto representa para la institución es el aseguramiento de la

objetividad al realizar su labor, ya que no existe una dependencia económica directa hacia la institución, otra de las ventajas de la auditoría externa es la no existencia de conflicto de interés, debido a su independencia.

Esta auditoría se puede realizar a cualquier área funcional de la institución con el objeto de emitir un dictamen sobre la razonabilidad de la administración de recursos a disposición de la institución.

La existencia del departamento de auditoría interna en una institución representa ventajas que con el tiempo muestran sus beneficios, entre ellos se encuentra la oportunidad de realizarla, el conocimiento de la institución así como del *software* y *hardware* existente, aunado a lo anterior la existencia de un comité de informática que establece las prioridades en cuanto al desarrollo informático de la institución. Basado en lo anterior, el informe de resultados que presenta debe de contar con una cédula que concentre la observación, la sugerencia y la consecuencia de no hacer caso a nuestras recomendaciones; ya que muchas veces, al exponer el informe, les impacta más el rubro de consecuencias que de la sugerencia misma, ya que en muchas ocasiones el impacto de las recomendaciones no es tan importante para los auditados, pero cuando se le hace mención de las consecuencias o el riesgo que corren, tienden a hacerle más caso a nuestro trabajo.

En una empresa, los responsables de la informática escuchan, orientan e informan sobre las posibilidades técnicas y los costos de cualquier desarrollo informático o del uso de los recursos informáticos. Normalmente se sugiere que exista un comité de informática.

Es además conocido que los informáticos tratan a veces milagrosamente de satisfacer lo más adecuadamente posible aquellas necesidades que surgen de la actividad diaria. La empresa necesita controlar sus recursos informáticos y que su gestión esté sometida a los mismos procedimientos, normas y estándares que el

resto de la empresa. La necesidad de esto recae en la figura del auditor interno informático.

En cuanto a la creación de un departamento de auditoría en informática dentro de la empresa, normalmente sólo las empresas denominadas grandes la poseen, el resto no creen tener la necesidad de contar con dicho departamento, porque no es un requerimiento oficial, y cuando llegan a tener necesidad de ello, recurren a auditores externos, creyendo que esto es más beneficioso para sus necesidades.

Puede darse el caso, que algún profesional en informática sea trasladado desde su puesto de trabajo para realizar la labor de la auditoría en informática interna de la empresa, si es que se quiere crear o ya existe previamente.

Definitivamente, el propio departamento de informática requiere de control interno, y es por ello que se debe crear este departamento para aumentar la confianza en su labor.

Hoy en día, es bien sabido que existe un encargado de la labor informática dentro de cada departamento o área dentro de la misma empresa, y con diverso grado de autonomía, situación que no facilita en nada la labor del departamento de informática y, por ende, al realizar la auditoría en informática esto sale a relucir.

Una empresa que cuenta con auditoría en informática interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

- Necesidad de añadir confianza a la labor realizada por el departamento de auditoría en informática interna.
- Realizar auditoría a todos los recursos informáticos para verificar cumplimiento de estándares y normativa vigentes, que se hayan establecidos por la empresa.

- Verificar que no se haya perdido la independencia mental al interactuar de manera diaria con los usuarios.
- Evaluar los controles establecidos por el departamento de auditoría en informática interna en informática para validar su oportunidad y grado de cumplimiento.

El departamento de auditoría interna debe contar con un área para realizar la auditoría en informática, estas auditorías deberán estar avaladas por el comité interno de auditoría que, con base en los distintos tipos de auditoría en informática, se aprestará a realizar al menos una al trimestre, al menos es lo que se recomienda, debido a que estas auditorías tienen esa duración en promedio cuando se realizan internamente; sin embargo, es recomendable que se realice una revisión por auditores externos que añadan confianza al trabajo realizado por la auditoría interna, para tener una visión desde fuera de la empresa, para verificar que éste no haya perdido su objetividad ni exista conflicto de intereses.

Una de las normas de auditoría nos indica la necesidad de contar con independencia mental al emitir una opinión sobre la razonabilidad en la utilización de los recursos informáticos, las auditorías internas en informática deben estar avaladas por el comité interno de auditoría, con el objeto de contar con todo el apoyo de la institución al realizar nuestro trabajo ya sea como auditor interno o como auditor independiente. La función de auditoría en informática, se debe realizar de acuerdo a un plan de auditorías previamente establecido, por iniciativa del propio órgano, o a instancias de la propia administración o cliente.

1.3. 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*.

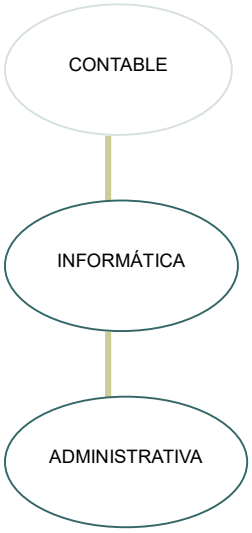
Auditoría administrativa	"Revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones" (Muñoz, 2002: 16).
Auditoría contable	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: 45).
Auditoría en informática.	La auditoría en informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una institución, con el fin de emitir un informe y/o dictamen profesional sobre la situación en que se desarrollan y se utilizan, esos recursos, con base en la normatividad existente ya sea interna, externa o ambas (José de Jesús Aguirre Bautista).

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 del proceso administrativo	El sistema contable	Todas las actividades informáticas
FUNDAMENTO	La ciencia administrativa y la normativa de la empresa	Principios de contabilidad y normas de auditoría	Normativa institucional y legal, estándares internacionales 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

1.4. Antecedentes de la auditoría en informática

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 éstos. 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.



Elaboración propia.

Elaboración propia.

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 su antecedente más cercano en 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 limitaron a dar custodia física a los equipos y a permitir el uso de los mismos sólo 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, que se consolida como una actividad estratégica para las empresas.

Desde siempre ha existido la figura del auditor, que en teoría ha servido para añadir confianza sobre aspectos de pago o cobro de tributo, comercio, impuestos, etc. Esta figura cobra gran importancia en la actualidad, sobre todo a raíz de los más sonados escándalos financieros, como Enron, *Waste Management*, WorldCom, Tyco, Parmalat, etc. Y muchos otros en casi todos los países del mundo, cuando las leyes y regulaciones locales o federales son deficientes o poco exigentes en su cumplimiento y favorecen actuaciones fraudulentas.

Pero aun con todas las deficiencias en las leyes o controles de una empresa, el auditor tiene oportunidad de crear normas internas y un control efectivo, incluyendo la acción de los comités de auditoría en informática.

Ahora bien, sí nos enfocamos a los antecedentes de la auditoría en informática, ésta surge con la misma creación de las primeras computadoras y sus diferentes usos

que tuvieron en sus inicios, así como la verificación de la seguridad de los sistemas que se iban desarrollando sobre todo para el área militar y para usos a nivel macro en los países, tales como censos u otros usos.

En México, la auditoría en Informática ha ido desarrollándose en una serie de esfuerzos aislados, al haber diversificación de carreras universitarias y técnicas que en apariencia, y sólo en apariencia, saben y realizan exactamente los mismo, como ingenieros en sistemas, ingenieros en computación, licenciados en informática, técnicos en informática, etc. Además, la difusión de algunas instituciones gremiales es poco difundida, lo que no sucede en la carrera de *Contaduría y Administración* con sus institutos reconocidos mundialmente.

Uno de los principales precursores de la auditoría en informática es el maestro José Antonio Echenique García, desde que fue titular del Centro de informática de la Facultad de Contaduría y Administración de la UNAM (CIFCA) y, posteriormente, director de la misma FCA, y con la presentación de su libro en 1988, que se llamó *Auditoría de sistemas*, en el cual se mencionan las principales bases para el desarrollo de la auditoría de sistemas computacionales y, a continuación, su libro de *Auditoría en informática,* que aborda cómo realizar una auditoría, auxiliándose de herramientas administrativas para su revisión.

También en el boletín 5080 “Efectos del procesamiento electrónico de datos (PED) en el examen del control interno” recientemente derogado y sustituido a partir de enero del 2006 por el boletín 3140 “Efectos de la tecnología de información (TI) en el desarrollo de la auditoría de estados financieros” que son emitidos por el Instituto Mexicano de Contadores Públicos (IMCP). Han contribuido al desarrollo e importancia de la auditoría en informática.

A nivel internacional, nos encontramos con algunas asociaciones que se han preocupado por regular esta parte de la auditoría en informática y sólo se mencionan como referencia:[1]

INFOSEC Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (*Advisory Committee for IT Security Matters to the European Commission*).

ISACA Asociación para la Auditoría y Control de Sistemas de Información. (*Information Systems audit. and Control Foundation*).

ISACF Fundación para la Auditoría y Control de Sistemas de Información. (*Information Systems audit. and Control Foundation*).

ISO Organización de Estándares Internacionales. (International Standards Organization) (Con oficinas en Génova, Suiza).

ISO9000 Estándares de manejo y aseguramiento de la calidad definida por ISO.

ITIL Biblioteca de Infraestructura de Tecnología de Información. (*Information Technology Infrastructure Library*)

ITSEC Criterios de Evaluación de Seguridad de Tecnología de Información (*Information Technology Security Evaluation Criterial*). Combinación de los criterios de Francia, Alemania, Holanda y Reino Unido, soportadas consecuentemente por la Comisión Europea (ver también TCSEC, el equivalente en los Estados Unidos).

NBS Departamento Nacional de Estándares de los Estados Unidos (*National Bureau of Standards of the U.S.*).

[1]Comité directivo de COBIT y el IT Governance Institute®

NIST (antes NBS) Instituto Nacional de Estándares y Tecnología. (*National Institute of Standards and Technology*), con base en Washington D.C.

OECD Organización para la Cooperación y el Desarrollo Económico. (*Organization for Economic Cooperation and Development*).

OSF Fundación de *Software* Público (*Open Software Foundation*).

PCIE Consejo Presidencial de Integridad y Eficiencia. (*President´s Council on Integrity and Efficiency*).

SPICE Mejoramiento del Proceso de *Software* y Determinación de la Capacidad (*Software Process Improvement and Capability Determination*) un estándar pare el mejoramiento del proceso de *software.*

TCSEC Criterios de Evaluación de Sistemas Computarizados Confiables. (*Trusted Computer System Evaluation Criteria*), conocido también como "*The Orange Book*". Criterios de evaluación de seguridad para sistemas computarizados definidos originalmente por el Departamento de Defensa de los Estados Unidos.

TickIT Guía para la Construcción y Certificación de Sistemas de Administración de Calidad. (*Guide to Software Quality Management System Construction and Certification*).

1.5. Importancia de la auditoría en informática-

En las organizaciones siempre ha existido la preocupación porque los recursos existentes sean optimizados, pero en cuanto al uso del *software y hardware*, sistemas de información, innovación en la investigación tecnológica, redes locales, implementación de bases de datos, ingeniería de *software*, telecomunicaciones, etc., representa una herramienta estratégica que es rentable y tiene ventaja competitiva en el mercado. En el ámbito de los sistemas de información y tecnología, existe un alto porcentaje de empresas que tienen ciertas dificultades y problemas en el manejo de control, ya sea en la gestión de datos, como en los elementos que almacena, procesa y distribuye.

La revisión de la auditoría en informática, tiene como propósito verificar que los recursos, tanto la información, las aplicaciones, infraestructura, los recursos humanos y presupuestos, sean coordinados y vigilados por la gerencia o por quienes sean designados como responsables.

Se ha detectado, durante mucho tiempo, el despilfarro de los recursos o el uso inadecuado de los mismos; sobre todo en informática, se ha mostrado interés por llegar a la meta, sin importar el costo y los problemas de productividad.

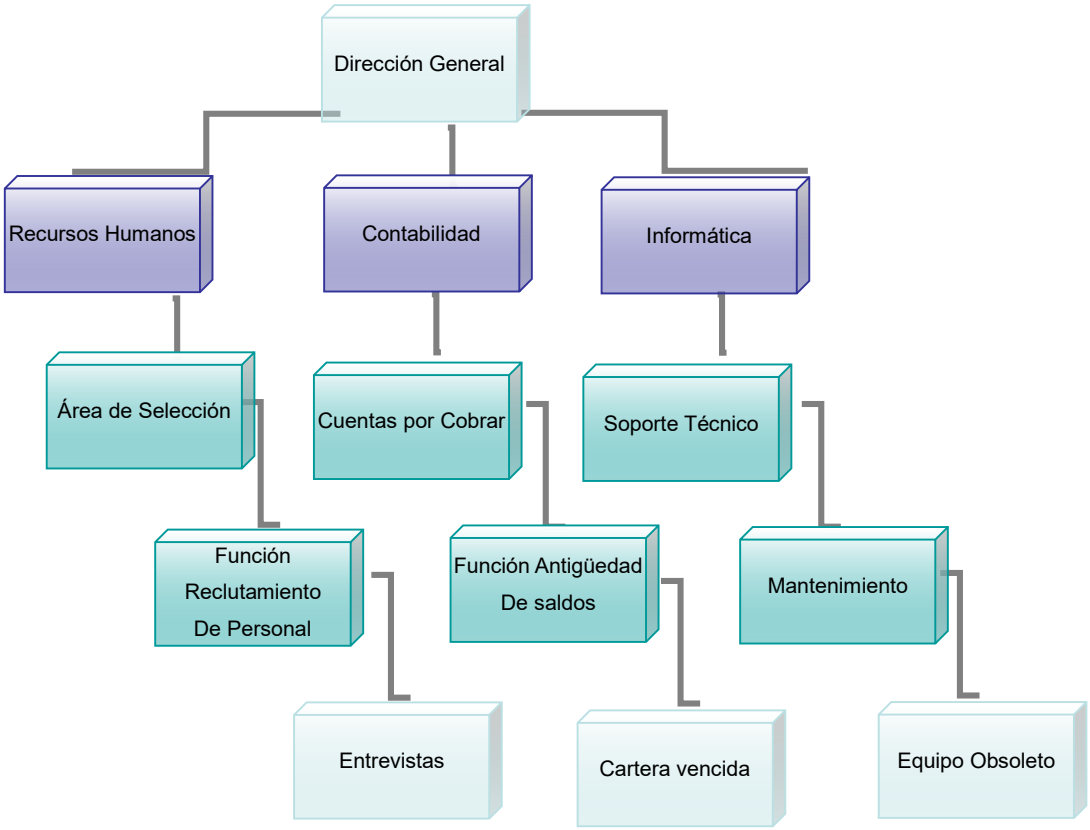
Elaboración propia.

No todas las empresas están dispuestas a invertir en realidad sobre este particular, la mayoría se están haciendo sobre el ensayo y error; es decir, de forma empírica y no le dan la real importancia a los recursos informáticos, en tiempo y forma, y sólo se limitan a automatizar, sin saber que para automatizar, primero debes sistematizar y no a la inversa, porque derivado de ello, se trunca la importancia de la auditoría en informática.

1.6. Campo de la auditoría informática

Las áreas a auditar en donde se puede realizar la auditoría en informática, puede ser:

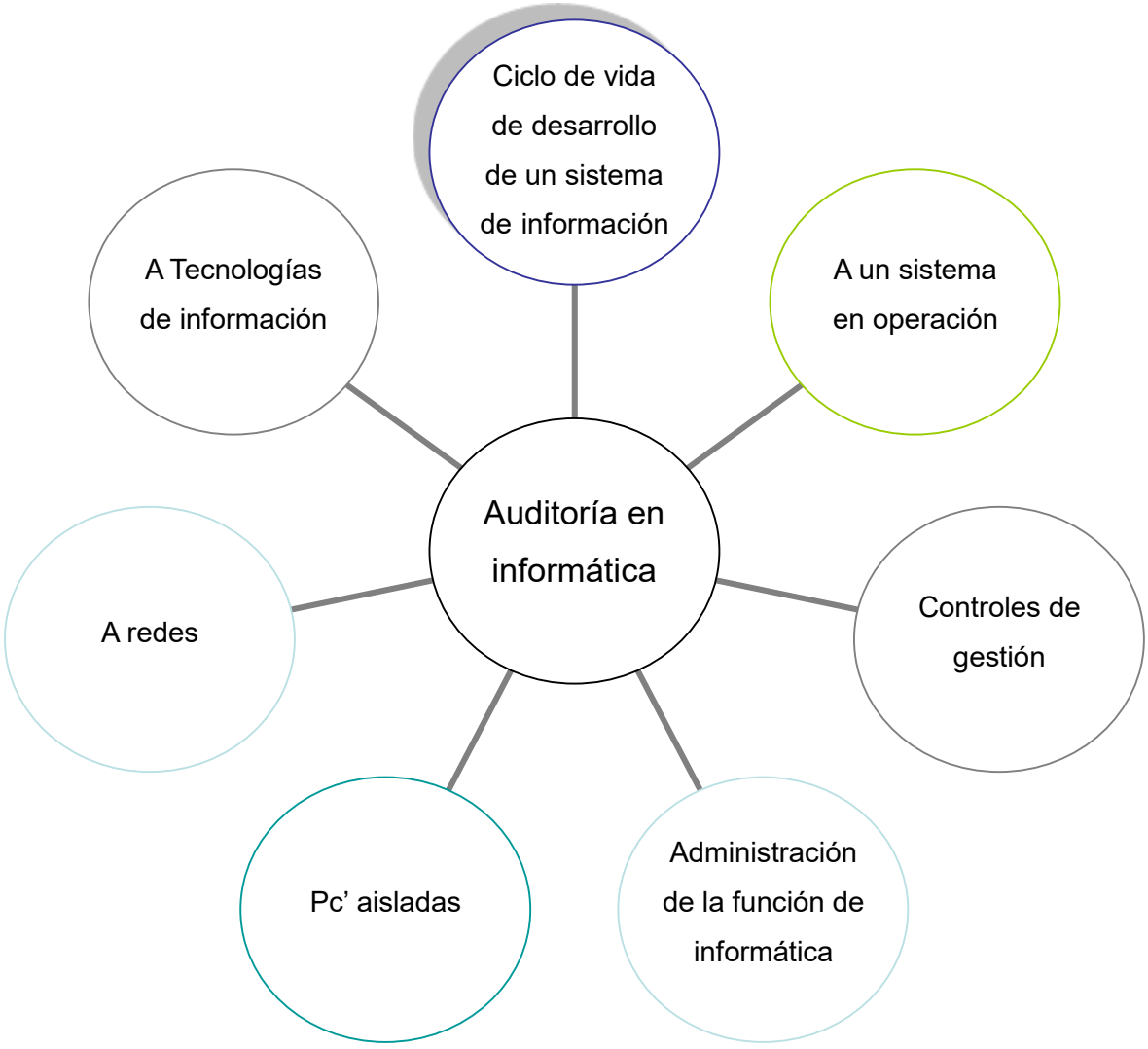
- A toda la entidad. De forma integral.
- A un departamento, en específico al departamento de sistemas o cualquier otra.
- A un área, en específico al área de mantenimiento y soporte técnico.
- A una función, programa de mantenimiento sobre las computadoras más antiguas.
- A una subfunción. Dentro de las más antiguas puede ser sólo en las que se realizaron limpieza o aspirado.



Elaboración propia.

De acuerdo a las necesidades de cada institución, se realiza esta división de los tipos de auditoría en informática; sin embargo, esto no quiere decir que sean los únicos, pero sí los más comunes:

- Auditoría al ciclo de vida del desarrollo de un sistema.
- Auditoría a un sistema en operación.
- Auditoría a controles generales (gestión).
- Auditoría a la administración de la función de informática.
- Auditoría a microcomputadoras aisladas.
- Auditoría a redes.
- Auditorías a TI.



Elaboración propia.

En este esquema, podemos observar los diferentes tipos de auditoría que se pueden realizar en la informática, esta distribución de auditoría es sólo de carácter enunciativo, por lo tanto, no limitativo.

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 a cabo de manera física y/o lógica.

RESUMEN

La necesidad de maximizar los recursos, así como el control de los mismos y la confianza de nuestros procesos nos lleva a desarrollar cada día estrategias de control que conlleven a ofrecer una seguridad razonable sobre la utilización de recursos informáticos, para ello nos auxiliamos de la auditoría que va a añadir confianza a la utilización de los recursos informáticos.

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 institución.

Por ello, se derivan dos clases de auditoría, como son la interna y la externa, que se diferencian una de la otra por la clase de información que presentan mientras la primera rinde un informe, la segunda presenta un dictamen. La primera lo realiza personal que puede o no formar parte de la institución, pero cuyo accionar puede verse coartado por existir dependencia económica, mientras que, en la segunda, se da ampliamente la independencia mental.

Los trascendentales cambios operados en el mundo moderno, caracterizados por su incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora en alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio campo de amenazas; tales como las cibernéticas; la escala y los costos de las inversiones actuales y futuras en información así como en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las instituciones y las prácticas de investigación.

Crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoría, en particular a la auditoría en informática y los informes característicos de cada institución.

La auditoría en informática justifica su existencia y reciente aparición en función de presentar la utilidad de ésta, sobre la fiabilidad e integridad de datos, así como la funcionalidad de la relación de costo/beneficio resultante de las inversiones y los controles en *hardware* y *software* y de la utilidad de ellos en la toma de decisiones.

Asimismo, se mencionan las diferentes clases de auditoría, que son interna y externa, así como los diferentes tipos de auditoría, como son contables, administrativas e informáticas.

Aunado a lo anterior, se especifican la importancia y el campo de acción y alcance de la auditoría en informática.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

Autor	Capítulo	Páginas
José de Jesús Aguirre Bautista.	I Fundamentos de auditoría en informática.	10-20
Echenique García, José Antonio. (2001). *Auditoría en informática* (2ª ed.). México: McGraw Hill.	1.- Concepto de auditoría en informática y diversos tipo de auditorias	2-22
Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales,* México, Pearson Educación.	*1.- Conceptos generales*	3-50

Bibliografía Básica

Piattini, Mario y Emilio del Peso (2001). *Auditoría informática, un enfoque práctico* (2da edición). Madrid: Alfa-Omega.

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.* (28ª ed.) México: IMCP.

Comité directivo de COBIT y el IT Governence Institute®

Bibliografía Complementaria

Solís Montes, Gustavo Adolfo (2002) *Reingeniería de la auditoría en informática*. México: Trillas.

Weber, Ron (1998) *EDP Auditing: Conceptual Foundations and Practice*. New York, McGraw Hill.

Sitios de Internet

Sitio	Descripción
Véase: http://lema.rae.es/drae/srv/search?id=jHIksgNjM2x53A2fZYh	Diccionario de la lengua española.
fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf	Conceptos de auditoría en informática.
www.eumed.net/cursecon/libreria/rgl-genaud/1x.htm	Conceptos generales de auditoria.

UNIDAD 2

Control interno

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno aplicará los mecanismos del control interno como apoyo en la realización de la auditoría informática.

TEMARIO DETALLADO
(6 horas)

2. Control interno

2.1. Concepto de control interno
2.2 Función del control interno
2.3 Importancia del control interno dentro de las organizaciones
2.4 Tipos de control interno
2.5 Metodologías de control interno
2.6 Relación con la auditoría informática

INTRODUCCIÓN

En este capítulo conoceremos la importancia del *control interno*, las dos clases de auditoría en informática: la interna y la externa; asimismo, enunciaremos los diferentes tipos de auditoría aplicados en la auditoría en informática; aunado a lo anterior, es prioritario, para desarrollar con éxito la auditoría, la realización del estudio y evaluación de control interno, específico para cada tipo de auditoría, ya que de ello depende el mapeo de proceso que debemos efectuar para localizar con atingencia las debilidades de control interno por cada área funcional de la institución auditada.

Dentro de los tipos de auditoría que podemos realizar y revisar, se encuentran las siguientes:

Auditoría a un sistema en específico o en operación (ASE/O).
Auditoría a redes (AR).
Auditoría al ciclo de vida de desarrollo de un sistema (ACVDS).
Auditoría de controles de gestión o generales (ACG/G).
Auditoría de computadoras autónomas (ACA).
Auditoría a la función de administración de informática (AFAI).

Como se mencionó anteriormente, en los años cuarenta, se empezaron a dar resultados relevantes en el campo de la computación, con sistemas de apoyos para estrategias militares. Con el paso de los años, la informática y todos los elementos tecnológicos, periféricos, han desarrollado necesidades de estar siempre a la vanguardia, en cada sector económico y social, derivado de lo cual se está obligado a crear también soluciones de respuesta pronta que permita dar satisfacción al

usuario, ya que esto redituará en mejor calidad de servicios y clientes, que demandarán cada día tecnología más eficiente y barata, durable y sencilla.

Lo que conlleva una enorme responsabilidad en el establecimiento de controles, cuyos objetivos son:

- Protección de los activos de la empresa, ya sea *software* y/o *hardware* e información.
- Adherencia a las políticas de la empresa, ya sea de uso y manejo de equipo e información.
- Promoción de la eficiencia en las operaciones, que el uso de *hardware* y *software* sea maximizado.
- Obtención de información veraz, confiable y oportuna, esto con el fin de que se tomen decisiones adecuadas con la mayor información posible.

Existen varios modelos de control interno aplicables a las instituciones, entre ellos, se encuentran el COSO (Comisión Estándar Internacional de Control Interno en los Negocios).

2.1. Concepto de control interno

Es un proceso realizado por la administración de una institución, avalado por el gobierno corporativo, con el propósito de llevar a cabo la consecución de metas para lograr el cumplimiento del o de los objetivos generales y específicos de cada institución (José de Jesús Aguirre).

Es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

Véase: www.ic.coso.org

2.2. Función del control interno

La función del control interno es tratar de disminuir el riesgo de ocurrencia en una situación dada, con el objeto de volver a la normalidad con el menor costo posible en un tiempo mínimo, entiéndase costo en cualquiera de los recursos de la institución.

El control demuestra su funcionalidad y eficacia cuando es exacto y preciso; es decir, la efectividad se da con base en la oportunidad.

Por ejemplo:

Escenario 1

Supongamos que tenemos una institución dedicada a la venta de papelería y artículos escolares y que se presenta un incendio en el almacén de papelería; nuestro control consiste en una cubeta con agua, si bien tengo un control para hacer frente a un incendio, el mismo no es suficiente para encarar el riesgo materializado; es decir, tenemos un control deficiente y no oportuno.

Situación que conlleva a la pérdida de un activo importante para la institución; es decir, verá disminuido fuertemente su actividad debido a esta situación que se traduce en retrasos de surtimiento de pedidos o ingresos que sirven para hacer frente a sus compromisos, como son pago de salarios a sus trabajadores, pago a proveedores, etc.

Por lo tanto, el control establecido no cumple con su función.

Escenario 2

La misma situación que el escenario anterior, pero en este caso, la institución cuenta para hacer frente a este riesgo de incendio, con detectores de humo y fuego, que al presentarse el hecho inmediatamente se activa y apaga el incendio casi instantáneamente, disminuyendo así los daños ocasionados por el siniestro, entonces sabremos que el control implantado ha sido el correcto y por la tanto la función de este control en específico, ha cumplido su función.

Escenario 3

El mismo caso, sólo que ahora contamos con detectores de humo y fuego, hidrantes para ocuparse en caso de incendio por los bomberos, adicional se cuenta con 5 carros cisterna en las instalaciones, así como 10 tinacos, 10 cisternas y 80 tambos con agua, además de extintores cada metro del almacén que mide aproximadamente 500 metros cuadrados; así como 25 cámaras de vigilancia en el almacén, además de rondines de cada 10 minutos por parte de vigilancia (3 personas) para verificar que no exista humo, así como ponerse un traje especial para entrar al almacén.

En este escenario el control es excesivo y caemos en la “controlitis”, lo que conlleva a pensar que la función de control no es la idónea para tratar de minimizar el riesgo de ocurrencia.

Asimismo, siempre que se establezca un control, debemos conocer qué queremos controlar, y si ese control guarda una adecuada relación de costo-beneficio.

El establecimiento de controles, desde mi perspectiva, va en función de la confianza, entre más controles se establezcan en una institución, menor confianza se tiene sobre las acciones y el personal que labora en la misma.

Tanto es perjudicial el tener “controlitis” como ausencia de controles; sin embargo, en el caso de la auditoría en informática, los controles añaden una seguridad razonable sobre el comportamiento y utilización de los recursos informáticos.

2.3. Importancia del control interno dentro de las organizaciones.

La importancia del establecimiento de los controles internos, radica en la oportunidad de los mismos; es decir, que funcionen cuando un hecho suceda, que auxilie a minimizar el impacto al llevarse a cabo la ocurrencia del acto.

Cuando un hecho sucede, el control entra en funcionamiento y auxilia en la continuidad de las operaciones de la institución para el caso de la auditoría en informática, la función del establecimiento de funciones, tiene que ver con el aprovechamiento de los recursos informáticos con base en la administración del riesgo.

- Protección de los activos de la empresa, ya sea *software* y/o *hardware* e información.
- Adherencia a las políticas de la empresa, ya sea de uso y manejo de equipo e información.
- Promoción de la eficiencia en las operaciones, que el uso de *hardware* y *software* sea maximizado.

- Obtención de información veraz, confiable y oportuna, esto con el fin de que se tomen decisiones adecuadas con la mayor información posible.

Cualquier control que se establezca invariablemente tocará alguna de las cuatro situaciones mencionadas, puede ser como mínimo una, y, en la mayoría de los casos, en dos, tres o hasta en las cuatro situaciones.

2.4. Tipos de control interno

Los tipos de control interno se pueden determinar con base en las estructuras departamentales que tenga cada institución, por ejemplo:

El control interno contable

Se refiere básicamente al establecimiento de controles para el mejor registro de las transacciones diarias que tiene una entidad, con el objeto de obtener información confiable y oportuna para el auxilio de la toma de decisiones.

Control interno administrativo

Este se refiere básicamente al control en el proceso administrativo, que, dependiendo el autor, tiene varias fases; el más utilizado es el de Planeación, Organización, Dirección y Control, que lleva la institución por cada una de las fases del proceso mismo.

Control interno informático

Este control se refiere a establecer y vigilar los procedimientos que auxilien en utilizar de la mejor forma posible los recursos informáticos; ya sea *software*, *hardware* y *humanware* que nos ayuden a optimizarlos en pro de alcanzar los objetivos institucionales.

Sin embargo, podemos establecer con toda seguridad, que estos controles van de la mano de los objetivos generales de la empresa y de su normativa. Por lo que se está en posibilidad de establecer para cada área o procedimiento el tipo de control interno que se requiere utilizar.

En el ámbito informático, los controles procuran que los recursos se utilicen de forma razonable e íntegra, con autentificación adecuada.

Los controles deben demostrar su efectividad de acuerdo a su oportunidad y, así, 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. Es decir, el documentar cada procedimiento va a asegurar la no dependencia de alguna persona para darle mantenimiento preventivo, detectivo y correctivo al sistema cuando éste lo requiera. En consecuencia, vamos a disminuir el riesgo en un alto porcentaje debido a que tenemos soporte documental de los pasos a seguir en cada situación ordinaria o extraordinaria que se presente.

2.5. Metodologías de control interno

La función de la auditoría u órgano de control interno, si es que existe, será la de desarrollar el establecimiento de estándares para fortalecer el correcto funcionamiento de los sistemas de información. La función de auditoría; además, es proporcionar a los directivos una adecuada asesoría en cuanto a las estrategias y políticas a seguir, y garantizar que los recursos asignados a las tecnologías de información o PED van a auxiliar a la minimización de los riesgos inherentes a su utilización, apoyar a la institución a través de la promoción de la calidad, eficiencia, eficacia y reducción de costos de sus procesos, que serán la base para buscar las certificaciones de calidad en todos los ámbitos, si es que la visión de la institución se proyecta hacia la calidad y competitividad internacional, ya sea una empresa grande o PYME y, derivado de lo anterior, tenemos la estandarización y requerimientos de información, mencionadas en los informes internacionales de control.

Desarrollado por ISSACA y por IT *Governance Institute*. Es realmente reciente.

En la actualidad, es imprescindible utilizar tecnologías de la información y comunicación en los servicios diarios de las instituciones. Planear, diseñar, desarrollar, implementar y dar mantenimiento a las tecnologías de la información son actividades que se deben efectuar durante el impulso informático, las cuales se encaminan al desarrollo de competencias que propicien la solución de problemas o al análisis de situaciones en su contexto.

Por ello, el hablar de metodologías de control interno en materia informática, nos lleva a pensar en el aprovechamiento y uso de las tecnologías de la información y comunicación en pro de lograr el objetivo.

El control interno en informática es mucho más que un proyecto real que requiere la integración completa de los recursos informáticos en la institución auditada; por lo tanto, involucra costos importantes. Por otro lado, su implementación en la institución, exige cambios significativos en los hábitos laborales de una gran parte de los empleados. No obstante, los beneficios que generaría al facilitar la eficiencia operacional de la Institución auditada.

¿Qué se espera al auditar el control Interno?

Obtener la lista de verificación que permita comprobar el cumplimiento de las acciones encaminadas a la implementación de los elementos que constituyen el control interno.

Todos los controles internos, así como cualquier actividad a realizar, requieren de los siguientes pasos metodológicos.

Planeación

Consiste en determinar qué es lo que se va a controlar o qué se quiere cuidar, siempre tenemos que separar los controles importantes de los urgentes. En esta etapa, se establecen los lineamientos generales para establecer los controles que habrán de regir en la institución y toca al auditor evaluar la oportunidad de esos controles internos.

Diagnóstico

Esta etapa consiste en determinar con base en la aplicación de un cuestionario de control interno la problemática evidente en los controles informáticos establecidos en la institución.

Desarrollo

Consiste en aplicar las acciones planeadas para validar la oportunidad de los controles internos evaluados; el auditor desarrollara su actividad con base en el objetivo de la revisión.

Informe

En esta etapa, se presenta el resultado de la evaluación de los controles internos revisados con base en su eficiencia y oportunidad.

A continuación de manera enunciativa se presentan metodologías diferentes al control interno informático.

COSO (Por las siglas del Comité que patrocinó los estudios que lo produjeron) (USA)

Tiene como objetivo estandarizar los conceptos de control interno; ayudar a la organización a evaluar de mejor manera sus sistemas de control y gestión y tomar decisiones de cómo mejorar estos sistemas.

COCO (Criterios de Control) (CANADÁ)

Se diferencia de COSO porque establece criterios de aplicación y da un enfoque humanístico; es decir, el éxito de su aplicación recae en todas las personas y no en unas cuantas como lo menciona el informe COSO.

Este informe fue emitido en el Reino Unido por el Consejo de Información Financiera, la Bolsa de Londres, entre otros.

a) Incluye normas que considera de práctica aconsejable sobre los siguientes temas:
b) Responsabilidades que les competen a los directores y administradores para revisar e informar a los accionistas y otras partes interesadas.
c) Composición, rol y desempeño de los comités de auditoría.
d) Responsabilidades de directores y administradores en el control, el alcance y el valor de la auditoría.
e) Establece los puntos de contacto entre accionistas, directores y auditores.
f) Otros temas vinculados.

CÓDIGO DE MEJORES PRÁCTICAS CORPORATIVAS (MÉXICO) Consejo Coordinador Empresarial.

Que en su mayoría adopta la esencia del control interno y algunos aspectos de todos los informes anteriores.

En esencia, todos estos informes pretenden promover la creación e importancia de la existencia de un gobierno corporativo, que auxilia a obtener la excelencia y transparencia en las Instituciones, los valores éticos en las prácticas profesionales, las responsabilidades en conjunto de las personas encargadas de la administración y uso de la información.

El tener toda la información no sirve, si no la aprovechamos para que los demás sepan qué es lo que se pretende alcanzar con esa información, y lejos de pensar que el que tiene la información tiene el poder, debemos pensar que quien comparte la información y sabe qué espera de las personas, esa persona en realidad tiene el poder, el secreto es compartir. Ese compartimiento de información conlleva un grado de compromiso y responsabilidad, además de solidaridad en la toma de decisiones (Aguirre, 2007: 6-7).

2.6. Relación con la auditoría informática

La relación que guarda el control interno con la auditoría en informática básicamente se refiere al establecimiento de indicadores para evaluar el grado de seguridad en la información procesada y que se corra el menor riesgo posible, o dicho de otra manera, alcanzar el mayor grado de fiabilidad como sea posible, con el objeto de aportar una seguridad razonable sobre las actividades que se desarrollan normalmente.

Una herramienta para verificar y evaluar al control interno es la siguiente:

MATRICES DE CONTROL/CUESTIONARIO DE CONTROL INTERNO.

Las matrices de control son una nueva clase de herramientas para evaluar los riesgos en los sistemas de información computarizados y el grado de cobertura de los objetivos de control.

Ventajas sobre los cuestionarios de control interno:

- Son más flexibles.
- Presentan más claramente el panorama de control en el sistema.

Se deben preparar matrices de control para evaluar por separado las fases de entrada, la de proceso y al de salida de datos. Los controles de frontera se describen y evalúan en un documento narrativo.

REGISTRO DE DEBILIDADES DE CONTROL (RDC)

El propósito del RDC es encontrar en un solo documento:

- La descripción de todas las debilidades importantes.
- Las repercusiones de la debilidad.
- Las alternativas de solución sugeridas.
- El resultado de la discusión de dichas debilidades, y nombre y puesto del responsable.

Cada debilidad incluida en el RDC debe ser referenciada a la matriz de control/cuestionario de control interno, o al resultado de las pruebas de cumplimiento.

RESUMEN

El control interno lo podemos definir de la siguiente forma:

Un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables

Asimismo, la función del control interno es tratar de disminuir el riesgo de ocurrencia en una situación dada, con el objeto de volver a la normalidad con el menor costo posible en un tiempo mínimo, entiéndase costo en cualquiera de los recursos de la institución.

Aunado a lo anterior, la importancia del establecimiento de los controles internos radica en la oportunidad de los mismos; es decir, que funcionen cuando un hecho suceda, que auxilie a minimizar el impacto al efectuarse la ocurrencia del acto.

Además, los tipos de control interno se pueden determinar con base en las estructuras departamentales que tenga cada institución. La función de la auditoría u órgano de control interno, si es que existe, será la de desarrollar el establecimiento de estándares para fortalecer el correcto funcionamiento de los sistemas de información.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

Autor	Capítulo	Páginas
Piattini, Mario y Emilio del Peso (2001). *Auditoría informática, un enfoque práctico* (2ª. Edición). Madrid: Alfa-Omega.	2.Control interno y auditoría en informática.	80-125
Muñoz Razo, Carlos. (2002). *Auditoría en sistemas computacionales.* México: Pearson Educación.	*1. Control interno.*	95-118

CONTROL OBJECTIVES: (1992) *Controls in an Information Systems Environment: Control Guidelines and Audit Procedures***:** *EDP Auditors Foundation (now the Information Systems Audit and Control Foundation),* Fourth Edition, Rolling Meadows, Illinois.

COSO: (1994). *Committee of Sponsoring Organizations of the Treadway Commission. Internal Control – Integrated Framework. 2 Vols.* New Jersey: American Institute of Certified Accountants.

Bibliografía Básica

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

Comité directivo de COBIT y el IT Governance Institute®

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

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: NBS Special Publication 500-153: National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

INFOSEC. Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (Advisory Committee for IT Security Matters to the European Commission).

Piattini, Mario y Emilio del Peso (2001). *Auditoría informática, un enfoque práctico* (2ª. Edición). Madrid: Alfa-Omega.

Bibliografía Complementaria

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

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

ISO 9000-3 (1991). *International Organization for Standardization. Quality Management and Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software*. Geneva, Switzerland.

ITIL IT Management (1989). *Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and telecommunications Agency (CCTA)*. London.

Muñoz Razo, Carlos (2002). *Auditoría en sistemas computacionales*. México: Prentice Hall.

Sitios de Internet

Sitio	Descripción
www.ic.coso.org	Página Oficial de COSO.

UNIDAD 3

Metodologías para la auditoría en informática

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno conocerá los diferentes mecanismos para auditar las áreas de sistemas de una organización.

TEMARIO DETALLADO
(8 horas)

3. Metodologías para la auditoría en informática
3.1. Introducción a las metodologías
3.2. Metodologías de evaluación de sistemas
3.3. Conceptos fundamentales
3.4. Las metodologías de auditoría informática
3.5. Definición, alcance y objetivos de la auditoría informática
3.6. Definición de recursos
3.7. Plan de trabajo
3.8. Actividades de auditoría
3.9. Informe final
3.9.1. Carta de presentación y carta de manifestaciones
3.10. Herramientas de auditoría

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 sólo una de ellas con características generales.

3.1. Introducción a las metodologías

Cuando hablamos de metodología, tenemos que pensar en la organización de un conjunto de elementos que reunidos entre sí nos puedan auxiliar a realizar mejor un procedimiento que permita resolver o llevar a cabo una tarea específica, cada individuo o entidad tiene su forma particular de evaluar y llevar a cabo su metodología.

Las metodologías de aplicación de la auditoría varían de acuerdo a la aplicación de los diferentes tipos de auditoría en informática a realizar; sin embargo, como metodología general podemos presentar la siguiente.

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 en 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.

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.

3.2. Metodologías de evaluación de sistemas

Cada sistema de información tiene sus principales áreas o fases sujetas a control durante el proceso del ciclo de vida del desarrollo de sistemas y se dividen de la siguiente forma:

A. Planeación.
B. Análisis.

C. Diseño.
D. Desarrollo.
E. Implantación.

El que las empresas auditadas conozcan que hay un ciclo de vida para el desarrollo de sistemas, será el primer paso para su control; para el auditor el hecho de dividir el desarrollo en fases permite predecir el proyecto íntegro, analizar y evaluar cada parte con mayor concentración y monitorizar continuamente la calidad y avance del trabajo.

Evaluaremos que cada área controle las fases que involucran sus actividades, responsabilidades y productos finales. 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.

3.3. Conceptos fundamentales

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

- Toda la entidad.
- Departamento.
- Área.
- Función.
- Subfunción.
- Proceso.

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 su administración, configuración, políticas de acceso y aprovechamiento.
- **Centros de cómputo.** Revisión a 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 efectuar de manera física y/o lógica.

3.4. Las metodologías de auditoría informática

No se ha estandarizado la metodología específica de la auditoría en informática; sin embargo, con base en la experiencia y de forma general y enunciativa, mas no limitativa, se establecen estos pasos para realizar la auditoría en informática.

- Planeación. Consiste en la creación de los programas de trabajo que se llevarán a cabo durante la revisión a la institución auditada, que incluye tiempo, recursos y personal a utilizar durante la revisión; normalmente, para ello, utilizamos un cronograma de actividades.

    - Trabajos preliminares.- Consisten básicamente en una serie de entrevistas con nuestro cliente, sobre si tiene la idea de lo que quiere que auditemos o quiere que se le realice un diagnóstico sobre el trabajo a desarrollar, ya que es importante determinar la situación actual de la institución y que el cliente desee algún tipo de auditoría en informática, en particular.

    - Diagnóstico.- Tiene por objetivo proporcionarnos una panorámica de cómo la institución lleva la administración y distribución de los recursos informáticos.

    - Investigación.- Aquí conoceremos el ambiente de la institución y, de ser posible, validaremos la problemática que nos fue expuesta por el cliente o la que se determinó en el diagnóstico.

    - Elaboración del programa de la AI.- El auditor en informática debe planear y llevar a cabo el programa de auditoría, donde señala las actividades que han de realizarse, fechas de inicio y término, así como los tiempos, y personas que ejecutarán el trabajo, además de quien supervisa cada etapa del plan original.

- Obtención de la información

- En esta fase se obtendrá toda la información pertinente, suficiente y competente, sobre la auditoría a realizar, pudiendo recurrir a herramientas como: entrevistas, encuestas, observación, etc. Derivado de una relación de solicitud de información que se puede pedir vía electrónica o en papel solicitada por el auditor.

❖ Análisis, clasificación y evaluación de la información

- El análisis y clasificación de la información podrá realizarse por métodos estadísticos, o por rubros de información con base en características similares, o por montos financieros.
- Evaluación. Es aquí en donde debe lucir el trabajo realizado por el auditor, porque para entender e interpretar la información, los auditores deben reconocer y separar qué información es importante y cuál es urgente.

❖ Informe, elaboración y presentación del informe final

- En él se informará de manera clara y concisa, pero sobre todo con sentido sobre los resultados de la auditoría en informática. No debemos olvidar que a los ojos de nuestro cliente él paga por recibir un informe, que le ayude a tomar decisiones, corregir errores y minimizar el riesgo, y en él debe encontrar valiosas recomendaciones que habrán de mejorar el desarrollo de la institución; el informe se presenta por escrito; sin embargo, debe existir un preinforme que deberá realizarse de forma verbal, con el objeto de evitar alguna discrepancia entre auditor y auditados.

- 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. Definición alcance y objetivos de la auditoría informática

Definición.

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.

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 racionalmente esos recursos.

La revisión que se lleva a cabo 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; en esta descripción se le conoce como **informe de auditoría**. Posteriormente, el auditor tiene que emitir una opinión profesional acerca de este 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, todos nos llevan a emitir una opinión sobre algún registro, sistema, operación o actividad en particular o con fines específicos.

Alcance

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría en informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el informe final, de modo que quede perfectamente determinado hasta qué puntos se ha llegado. La indefinición de los alcances de la auditoría compromete el éxito de la misma.

Las áreas a auditar en donde se puede realizar la auditoría en informática, puede ser:

- A toda la entidad.
- A un departamento.
- A un área.
- A una función.
- A una subfunción.

Y se pueden aplicar los siguientes tipos de auditoría:

- Auditoría al Ciclo de Vida del Desarrollo de Sistemas. (ACVDS)
- Auditoría a un Sistema en Específico o en Operación. (ASE/O)
- Auditoría de Gestión de Tecnologías de Información. (AGTI)
- Auditoría a Redes. (AR)
- Auditoría a Telecomunicaciones. (AT)
- Auditoría a Controles Generales o de Gestión. (ACG/G)
- Auditoría a Computadoras Autónomas. (ACA)
- Auditoría a la Función de la Administración de Informática. (AFAI)

Objetivo

El objetivo fundamental de la auditoría en informática, es el verificar que los recursos; es decir, información, energía, dinero, equipo, personal, programas de cómputo y materiales son adecuadamente utilizados, coordinados y vigilados por la administración de la empresa, ya que empieza de una forma cualitativa y termina de forma cuantitativa.

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con 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 , bases de datos, ingeniería de *software*, telecomunicaciones, etc., ésta representa una herramienta estratégica que representa 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.

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.

Los principales **objetivos** que constituyen a la auditoría Informática son:

- El **control** de la función informática.
- El **análisis** de la eficacia del sistema informático.
- La **verificación** de la implantación de la normativa.
- La **revisión** de la gestión de los recursos informáticos.

3.6. Definición de recursos

Para la realización de la auditoría es importante conocer y contar con personal calificado en el ramo a auditar; es decir, no forzosamente todos los auditores en informática deben intervenir en todas las revisiones. O sea, va a depender de cada institución y de cada revisión, así como del tipo de auditoría a realizar la utilización de los perfiles del personal que intervenga en cada actividad de auditoría.

Aunado a lo anterior, estableceremos las necesidades de *hardware*, *software* y *Humanware*, que ocuparemos para cada revisión en específico.

Por ejemplo:

Para director de informática tenemos las siguientes características, siendo éstas 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.

Procede, como parte de la planeación de la auditoría a realizar, la aplicación del cuestionario de control interno de cada una de las fases de auditoría de controles generales.

3.7. Plan de trabajo

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

A continuación, presentamos un ejemplo de ello:

Actividad	Inicio	Término	Días	Elaboró	Revisó
1.=Planeación	8/01/2014	9/01/2014	2	JJAB	PRC
2.= Entrevistas	10/01/2014	12/01/2014	3	JJAB	PRC
3.=Cuestionarios de control interno	12/01/2014	15/01/2014	4	JJAB	PRC
4.-Aplicación de pruebas selectivas	16/01/2014	31/01/2014	16	JJAB/JAAR	PRC/DPAR
5.-Junta de preinforme o informe preliminar y aclaraciones	01/02/2014	03/02/2014	3	DPAR	PRC
6.-Entrega de informe final	04/02/2014	04/02/2014	1	DPAR	PRC

Esta auditoría se realizaría en 29 días, y se utilizarían de 2 a 4 personas para realizar cada una de las actividades señaladas en el programa de auditoría.

3.8. Actividades de auditoría

Las actividades de auditoría, se refieren a las acciones que realiza el auditor, para llevar un control sobre las mismas, referenciadas en procesos, acompañadas de fechas reales, estimadas; así como de iniciales de las personas que participan en la auditoría.

AUDITORÍA EN INFORMÁTICA DE CONTROLES GENERALES.

NÚM.	ACTIVIDAD	PERSONAL.	⊢	MARZO 2014
				1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
1	**Planeación de la auditoría y solicitud de información preliminar.**	**Director y Gerente de Auditoría**	E	
			R	
2	**Entrevistas**	**Director y Gerente de Auditoría**		
3	Cuestionarios de Control Interno	**Gerente de Auditoría y Auditor**	E	
			R	
4	Aplicación de pruebas selectivas.	**Auditores**	E	
			R	
5	Informe preliminar y aclaraciones.	**Gerente de Auditoría y Auditor**	E	
			R	
6	**Informe Final de Auditoría**.	**Director y Gerente de Auditoría**	E	
			R	
			R	
				0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

	M		
	SAB.-DOM.	***SIMBOLOGÍA:***	PERSONAL ASIGNADO: José de Jesús Aguirre Bautista
		T: TIEMPO	Perla Reséndiz Campos
	A ***ASUETO***	*E: ESTIMADO*	Jesús Adolfo Aguirre Reséndiz
		R: REAL	Diana Perla Aguirre Reséndiz
	ESTIMADO		
		P: PLANEACIÓN	
	x ***REAL***	*G: REVISIÓN EN GABINETE*	
		I: INFORME	

Otro ejemplo es el siguiente:

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

PROGRAMA DE TRABAJO DE AUDITORÍA EN INFORMÁTICA CONTROLES GENERALES
PERIODO DE REVISIÓN DEL 1 DE ENERO AL 31 DE DICIEMBRE DEL 2014

	INICIALES	FECHA	FIRMA
PREPARÓ	JJAB	19-03-2014	
REVISÓ	PRC	11-05-2014	

Objetivo:

1.- Analizar y evaluar la función de controles generales de la administración de informática en la dependencia.

2.- Verificar el aprovechamiento de la capacidad instalada de los recursos informáticos; así como evaluar los controles emitidos para tal fin.

REFERENCIA	PROCEDIMIENTOS	FECHA DE REALIZACIÓN		RESPONSABLE
		DEL	AL	
Adquisiciones	**1.-** Verificar si se aplica la normativa institucional para las adquisiciones de bienes informáticos.			
	2.- Solicitar las adquisiciones de bienes informáticos para 2014, y verificar que estén contempladas en el informe enviado al Comité Asesor de Cómputo.			

	3.- Solicitar el procedimiento de adquisiciones de los bienes informáticos verificando lo siguiente: **a)** Identificar al responsable de las adquisiciones de los bienes informáticos. **b)** Si los requerimientos se solicitan anticipadamente. **c)** Que los requerimientos estén justificados. **d)** Verificar que los proveedores seleccionados estén inscritos en el padrón de la D.G.P. **e)** Quién y cómo distribuye los bienes adquiridos.			
Sistema Operativo	**4.-** Solicitar los contratos y/o convenios de mantenimiento a *software* y *hardware*, y determinar lo siguiente: **a)** Cuántas modificaciones y/o adaptaciones se han realizado al *software*. **b)** Determinar qué tipo de mantenimiento se le da al equipo (preventivo o correctivo) y con qué periodicidad. **c)** Se contemplan todos los requerimientos para mantener los equipos en buenas condiciones. **d)** Quién lo elabora y si contiene el V.o B.o del abogado general.			
	5.- Solicitar el análisis de los requerimientos del sistema operativo en redes con el objeto de conocer si es el idóneo para las necesidades de la Facultad.			

Seguridad Física	**6.-** Investigar y verificar con qué medidas de seguridad física se cuenta en el área de cómputo.			
	7.- Verificar que se tengan asegurados los bienes informáticos (*hardware* y *software*).			
	8.- Identificar si existe algún responsable de establecer medidas de seguridad y su vigilancia.			
	9.- Verificar físicamente todas las instalaciones del área de cómputo y validar la información proporcionada.			
Seguridad lógica	**10.-** Aplicar el cuestionario correspondiente y plasmar las observaciones que así procedan con el soporte documental suficiente.			
	11.- Identificar si existe un área o un responsable de establecer controles a PC.			
	12.- Solicitar el inventario del *software* instalado en el equipo asignado a las áreas administrativas, clasificado por nombre del paquete o sistema, número de CDS y si es original o copia.			
	13.- Plasmar en cédula de trabajo la información anterior y seleccionar la muestra de nuestra revisión con el objeto de verificar: **a)** El control sobre el uso de los sistemas y/o paquetes instalados. **b)** Si los sistemas y/o paquetes instalados corresponden a las funciones que desarrolla el área. **c)** Si existen respaldos de los sistemas y/o paquetes. **d)** El lugar donde se custodian.			

	14.- Identificar si la información generada en cada PC es confidencial y verificar el control que se tiene sobre el uso de ésta.			
	15.- Verificar si se tienen controles que garanticen que no existan archivos de datos ajenos a las funciones propias del área y de la dependencia.			
	16.- Buscar dentro de las PC, que efectivamente no se tenga información ajena al área y a la Dependencia.			
	17.- De la muestra seleccionada verificar físicamente: **a)** Limpieza del área y de los equipos. **b)** Colocación de los equipos y su cableado. **c)** Estado físico de la instalación eléctrica. **d)** Si se cuenta con reguladores y/o *No-break* adecuados.			
	18.- Verificar que existan medidas adecuadas de control sobre la prohibición de fumar o ingerir líquidos cerca de los recursos informáticos.			

3.9. Informe final

El Informe es un documento formal a través del cual el auditor plasma el resultado del trabajo desempeñado, basado en la normativa 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.
- Periodo que abarca.
- Destinatario.
- Antecedentes.
- Procedimiento realizado.
- Alcance de la auditoría.
- Limitaciones al trabajo.
- Personal asignado.

Cuerpo

- Hallazgos y observaciones.
- Comentarios sobre el hallazgo.
- Secciones o apartados especiales.
- Aclaraciones del auditado.
- 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/15

L.I. JESUS ADOLFO AGUIRRE RESÉNDIZ
DIRECTOR
FACULTAD DE CONTADURIA

Presente

Informe de la revisión efectuada a la Facultad de Contaduría por el periodo comprendido del 1 de enero al 31 de diciembre del 2014, derivada de la intervención realizada del 2 de enero al 30 de abril del 2015 por el despacho AR Internacional S.C.

Hemos examinado los procedimientos de control en informática, específicamente a controles generales al 31 de diciembre de 2014. Dichos controles son responsabilidad de la administración de la dependencia. Nuestra responsabilidad consiste en expresar una opinión sobre los mismos con base en nuestra 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 normativa 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 nuestra opinión.

Debido a que este tipo de auditorías se revisa por etapas y que, como auditor de la dependencia, no se observaron los inventarios físicos de ese año, aunado a la naturaleza de los registros de recursos informáticos, el proceso no fue satisfactorio a pesar de aplicar otros procedimientos de auditoría a dichos inventarios.
Se observó que son regulares las etapas de adquisiciones y sistema operativo, no así las etapas de seguridad física, lógica y el plan de contingencias.
Considerando, que si se hubieran observado los inventarios físicos de la compañía mencionados anteriormente, la auditoría de controles generales y sus etapas, habrían presentado razonablemente en todos los aspectos importantes, la situación informática de la dependencia, durante el periodo comprendido del 1 de enero al 31

de diciembre de 2014; de acuerdo con los estándares nacionales e internacionales existentes para la auditoría de controles generales de recursos informáticos.

México D.F., a 11 de mayo de 2015

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

El informe positivo o en blanco

Se presenta cuando no existe ninguna falla o desviación en el cumplimiento de normas o leyes específicas para cada Institución.

Informe con salvedad

Se refiere a cuando la desviación de la norma no es significativa para que el informe no se considere razonable.

Informe negativo

Se refiere a cuando existen desviaciones considerables en el cumplimiento de la norma y que hacen que se exprese una opinión no razonable.

Informe con abstención de opinión

Se presenta cuando no tenemos los elementos para sustentar nuestra opinión.

(1) Clasificación según el Instituto Mexicano de Contadores Públicos.

3.9.1. Carta de presentación y carta de manifestaciones

Normalmente, la carta de presentación contiene elementos en donde ponemos de manifiesto nuestro interés en participar u ofrecer nuestros servicios profesionales de auditoría. Pero además existe la misma carta con otro propósito, que es el de informar de forma ejecutiva los hallazgos determinados durante la práctica de la auditoría o durante la elaboración de un diagnóstico y, asimismo, manifestamos nuestro interés en seguir participando con esa institución ahora presentando nuestros servicios de seguimientos de hallazgos o riesgos determinados.

La carta no dista mucho de la carta de presentación de un dictamen, sólo que en esta carta se resalta también aspectos positivos encontrados en la institución.

Ejemplo:

Carta de presentación de resultados de la auditoría en informática.

México D.F. a 19 de marzo de 2014.

Asunto: Presentación del Informe de auditoría.

Gobierno Corporativo.
Miembros del Comité de Auditoría.

P r e s e n t e.

PICHACHE SA DE CV

Estimados Miembros:

El propósito de la presente tiene como base la presentación de los hallazgos realizados durante la práctica de la auditoría en informática al rubro de Controles Generales aplicados a las distintas áreas que conforman el Departamento de Informática de esa institución.

Si bien es cierto que encontramos fortalezas, también detectamos riesgos en la operación de las áreas operacionales de informática.

Se ha presentado a los Miembros de la Junta de Gobierno un análisis detallado de los riesgos con que cuenta la Institución, asimismo se les ha hecho llegar la propuesta de asesoría y corrección de muchas de las debilidades y riesgos de control determinadas durante nuestra revisión y el riesgo latente de ocurrencia si no se toman las medidas correctivas y preventivas en tiempo y forma.

En espera de vernos favorecidos como siempre con nuestra petición, esperamos poder contar con una cita para comentar nuestro informe final.

Sin más por el momento reciban un cordial y afectuoso saludo.

Atentamente.

L.C. Perla Reséndiz Campos.
Directora General del Despacho AR Internacional S.C.

Carta de Manifestaciones

Básicamente, de lo que trata esta carta es donde se mencionan aspectos cualitativos que son importantes tanto para el auditor como para la institución auditada, ya que aquí la institución pondrá de manifiesto todas las circunstancias y accesorios que le son presentadas al auditor, para que el auditor lo tome como cierto, por ejemplo: que la administración ha presentado toda la documentación correspondiente al sistema a auditar y que no se ha guardado nada, ni existen otros documentos referidos al sistema, entonces una vez tenida esta manifestación podríamos inclusive incluirla como una prueba de auditoría que auxilie en el mejor desempeño y certeza en nuestra actividad de auditoría.

3.10. Herramientas de auditoría

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
- Entrevistas
- *Checklist*
- Trazas y/o huellas

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.

Para esto, se les envía a las empresas que contesten algunos cuestionarios, que se envían a las personas concretas que el auditor cree adecuadas, o en su defecto a quien solicita la auditoría y éste se encargará de distribuirlo a los responsables de cada departamento, área o actividad, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios deben ser creados a la medida de cada empresa y de cada tipo de auditoría, 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.

ENTREVISTAS

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información. El auditor informático, entrevista al auditado siguiendo el cuidado y diligencia profesional, el entrevistado de ser posible debe conocer los puntos a tratar en esa reunión y básicamente consiste en que el

auditado conteste sencillamente una serie de preguntas variadas, esa preguntas deben de tener una preparación que nos sirva para obtener lo que consideramos importante en la auditoría; es decir, obtener información relevante que auxilie al cumplimiento de los objetivos de la auditoría y de la entrevista misma.

CHECKLIST

El *Checklist* se utiliza básicamente cuando ya se tienen preestablecidos una serie de lineamientos o catálogo de opciones que creemos que se pueden aplicar para cada tipo de auditoría, básicamente son preguntas que se responden con un sí o no.

El *Checklist* o lista de chequeo nos sirve para obviar ciertos aspectos de la revisión, esta lista se crea con preguntas que se enriquecen en cada revisión y que se realizan para cada entidad o institución en particular, ya que va a depender del tamaño de la empresa para saber el grado de profundidad y extensión de estas listas de chequeo.

No existen *Checklist* estándar para todas y cada una de las áreas informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar. Existen además, varios tipos de *Checklist* con diferentes opciones de respuesta; dependerá de cada auditor desarrollar el que mejor cree que se le aplique.

TRAZAS Y/O HUELLAS.

Las trazas se aplican para confirmar que los sistemas y equipos realicen las funciones para lo que fueron adquiridas, con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras.

RESUMEN

Los pasos para guiar en la aplicación metodológica de la auditoría en informática son los siguientes:

- Planeación
- Análisis
- Diseño
- Desarrollo
- Implantación.

Las áreas a auditar en el ámbito de la informática son:

- Toda la entidad
- Departamento
- Área
- Función
- Subfunción
- Proceso.

La palabra informática, de acuerdo a su origen, se refiere a la información automática. Las diferentes concepciones que existen, se centran en el tratamiento sistemático de la información con el apoyo de recursos tecnológicos.

La auditoría en informática consiste en revisar los recursos informáticos con que cuenta una entidad y emitir un informe y/o dictamen sobre la situación en que se desarrollan, así como la utilización y optimización de dichos recursos.

En la actividad de la auditoría, es importante contar con personal calificado en el ramo a auditar.

Para la elaboración del programa de AI, es importante considerar la planeación, dicho programa indica las actividades a realizar, fechas de inicio y término, los tiempos y el personal que interviene.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

Autor	Capítulo	Páginas
José de Jesús Aguirre	TEMA 3. Metodología general para la auditoría en informática	36-50
Instituto Mexicano de Contadores Públicos	Conclusiones y dictamen de auditoría	971-1074

Bibliografía Básica

David Gallo, Facundo (2011). *Inseguridad informática*. España: 2010-2011.

Piattini, Mario y Emilio del Peso (2001). *Auditoría informática, un enfoque práctico* (2ª Ed.) Madrid: Alfa-Omega.

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

Instituto Mexicano de Contadores Públicos (2013). *Normas y procedimientos de auditoría y Normas para atestiguar y otros servicios relacionados*. (3ª ed.) México: IMCP.

Bibliografía Complementaria

Solís Montes, Gustavo Adolfo (2002). *Reingeniería de la auditoría en informática.* México: Trillas.

Weber, Ron (1998). *Auditing: Conceptual Foundations and Practice*. Ed. New York: McGraw Hill.

Sitios de Internet

Sitio	Descripción
www.imcp.org.mx	Sitio del Instituto Mexicano de Contadores, conceptos de auditoría y dictámenes o informes.
http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf	Conceptos de auditoría en informática.

UNIDAD 4

Áreas de evaluación de la auditoría en informática

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno identificará las áreas de la organización en las que se puede aplicar la auditoría informática utilizando las metodologías vistas anteriormente.

TEMARIO DETALLADO

(10 horas)

4. Áreas de evaluación de la auditoría en informática

4.1. Auditoría de sistemas
4.2. Auditoría de datos
4.3. Auditoría del equipo de cómputo
4.4. Auditoría de procesos
4.5. Auditoría de seguridad

INTRODUCCIÓN

La determinación de las áreas funcionales a auditar mediante la auditoría en informática se debe basar en la importancia y capacidad instalada de cada área; sin embargo, y por obvias razones, el departamento de informática es el que naturalmente concentra la administración del *software* y del *hardware*.

Asimismo, los diferentes tipos de auditoría que pueden ser practicados a una institución dependerán del diagnóstico elaborado por el auditor para determinar cuál es la auditoría que más se adecua a las necesidades del auditado.

4.1. Auditoría de sistemas

Las diferentes situaciones que se viven ahora en casi todas las empresas que llevan a cabo el desarrollo de los sistemas de información, presentan deficiencias que pueden tener su origen en los siguientes escenarios observados durante las revisiones que se han efectuado:

a) Poco o escaso aprovechamiento tecnológico, así como rezago del mismo.
b) Pruebas del sistema de información desorganizada, poco o nada planeadas, incompletas, mal diseñadas o sin documentar; tales pruebas deberían garantizar que los errores o irregularidades se detectaran oportunamente por sistema.
c) Pruebas no siempre controladas por el usuario.
d) Costos en una proporción inadecuada o muy por encima de los beneficios.
e) Falta de revisiones técnicas a detalle.
f) Entrenamiento deficiente.
g) Incremento en la escala del proyecto.
h) Sistemas no integrales o aislados.
i) Deficiente comunicación entre usuarios y personal de P.E.D.; desconocimiento del papel –responsabilidad de usuarios y de la dirección.
j) Carencia o incompleta documentación de sistemas (documentación técnica, de operación y de usuario).
k) Metodología incompleta o ausencia de ella y no estándar, para el desarrollo de los sistemas en la que se señalen con precisión actividades, tiempos estimados y responsables.
l) Administración insuficiente de los proyectos.

m) Inoportunidad en la trasferencia de sistemas en desarrollo a la operación normal.
n) Ausencias de pistas de auditoría.
o) Escasez de personal profesional.

Es importante señalar la relevancia que tiene la participación del auditor en el desarrollo del plan maestro de sistemas, ya que le interesa conocer los siguientes aspectos:

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

Los sistemas de información se deben desarrollar para servir al usuario, proporcionándole capacidades para el proceso de datos y reportes.

Cada sistema de información tiene cuatro principales fases sujetas a control durante el proceso del ciclo de vida del desarrollo de sistemas.

- Planeación.
- Análisis y diseño.
- Desarrollo.
- Implantación.

El hecho de dividir el desarrollo en fases, permite predecir el proyecto íntegro, analizar y evaluar, cada parte con mayor concentración y monitorizar continuamente la calidad y el avance del trabajo.

Cada área de control se divide en fases que involucran diversas actividades y responsabilidades así como productos finales.

Los proyectos de desarrollo, se estructuran como acumulativos, cada etapa o actividad 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, el propósito de la revisión del auditor en sistemas, es asegurar que la organización tiene y usa la metodología adecuada de desarrollo, adicionalmente se debe asegurar que el proceso de desarrollo de sistemas se adhiera a los estándares establecidos por la metodología, su participación puede ser durante el desarrollo del sistema o una vez ya concluido.

Objetivo de la auditoría

La meta es verificar que se desarrollen sistemas útiles, auditables, seguros y controlables, que produzcan resultados consistentes para satisfacer los requerimientos del usuario.

Fases del ciclo de vida del desarrollo de sistemas:

1. Planeación A) Requisición de servicios. B) Estudios de factibilidad.
2. Diseño A) Diseño general del sistema. B) Diseño detallado del sistema.
3. Desarrollo A) Programación. B) Prueba modular y prueba del sistema integral.

C) Desarrollo de manuales. D) Entrenamiento.
4. Implantación A) Conversión. B) Revisión de la post-implantación.

1. PLANEACION

A) Requisición del servicio

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

Definición del proyecto:

Justificación.
Ambiente.
Alcance.
Restricciones.
Beneficios.

Integración de equipos de trabajo y sus responsabilidades.
Definición de requisitos de información nuevos y existentes.
Aprobación del proyecto.

B) Estudio de factibilidad:

Estudios de los procedimientos existentes.

Formulación de cursos alternativos de acción.

a) Factibilidad tecnológica (métodos aplicables de P.E.D)

Disponibilidad de la tecnología que satisfaga las necesidades de los usuarios, además de la actualización o complemento de los recursos disponibles.

b) Factibilidad económica

Costos actuales *vs* costos de cada alternativa (personal de desarrollo, equipo, *software*, entrenamiento, preparación de la entrada, conversión de archivos de prueba, operación, etc.).

Identificación y cuantificación de beneficios

c) Factibilidad operativa

Determinar qué se operará o utilizará tomando en cuenta factores tales como la resistencia al cambio, características del personal, ubicación de las instalaciones, etc.

Plan maestro del proyecto (puntos de control y calendarización de actividades).

Estado general de la función de desarrollo.

Aprobación del proyecto.

ANÁLISIS Y DISEÑO DE SISTEMAS.

2. DISEÑO.

A) Diseño general del sistema.

Estructura general del sistema.

Definición y documentación de los requisitos de salida.

- Contenido y formato de los informes.
- Frecuencia de producción de reportes.
- Lista de distribución de reportes.
- Periodos de retención de informes.
- Controles sobre la salida.

Definición y documentación de los requisitos de entrada:

- Requisitos de edición y validación (control).
- Revisiones de seguridad para la protección de la exclusividad.
- Controles sobre la entrada.

Definición y documentación de los requisitos de archivo.

- Definición de los tipos de registros o estructuración de bases de datos.
- Métodos de organización.
- Niveles de seguridad y controles de acceso.
- Periodos de respaldo y retención.

Definición y documentación de los requisitos de procesamientos (manuales y computarizados).

Especificación de procedimientos programados de cálculo, clasificación, etc.

Estimación de tiempos de respuesta.
Normativa.
Interfaces.
Niveles de seguridad.
Diseños de documento fuente.

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

Usuario primario. Es aquel que usa directamente en sus tareas los resultados del sistema de información.

Usuario secundario. Es aquel que introduce datos al sistema.

Las decisiones que tiene que tomar los usuarios de un sistema de información se pueden dar en tres niveles:

a) *Nivel de administración estratégica*. Guían al nivel medio y operativo de administración, actúan en un clima de incertidumbre, postulan metas, estrategias y políticas.

b) *Nivel medio de administración.* Toman decisiones sobre planeación y control a corto plazo, trabajan en un ambiente de baja certidumbre y las decisiones carecen de alto grado de estructuración.

c) *Nivel operativo de administración.* Apoyan sus decisiones en reglas preestablecidas, operan en nivel de alta certidumbre y, fundamentalmente, consiste en la supervisión de detalles operativos.

Nivel de Dirección Estratégica	Características	Nivel de control Operativo
a) Amplia	Visión de la información	Estrecha
b) General	Nivel de detalle	Muy detallada
c) Resumido	Nivel de resumen	Datos primarios
d) Antigua	Antigüedad de la información	Muy antigua
e) Estimaciones	Precisión de la información	Precisión
f) Más cualitativa principalmente externa	Tipo de información	Más cuantitativa, principalmente fuente interna.

Es muy importante que, durante la recopilación de datos, se realicen encuestas, entrevistas, cuestionarios, etc., es decir, cualquier técnica de auditoría; se debe echar mano de todas las herramientas de auditoría que conozcamos para realizar nuestra labor.

Objetivos de los formatos pantalla/ Captura	Objetivos de salida
Precisión	Satisfacción del objetivo planteado
Facilidad de uso y sencillez	Adaptación al usuario
Consistencia	Suficiente cantidad de información
Flujos	Oportunidad
	Medio apropiado
	Grado de confidencialidad

B) Diseño detallado del sistema

- Especificaciones de programas y controles programados.
- Diseño de pistas de auditoría.

- Estándares de documentación de programas.
    - Nombre de la aplicación.
    - Diagrama del sistema.
    - Aspectos generales del programa.
    - Formatos de entrada y salida.

En esta etapa se definen las especificaciones técnicas, es decir, las características y definiciones técnicas y operativas del sistema, lo cual es responsabilidad del líder del proyecto de informática, aquí se incluyen:

- Instrucciones para programación.
- Itinerario para el desarrollo de programas / módulos.
- Matrices de archivo/ programas, módulos/ programas.
- Selección de los lenguajes de programación.
- Controles del operador.
- Instrucciones al operador en caso de interrupciones.
- Procedimientos de respaldo, reinicio y recuperación.

3. DESARROLLO

A) Programación

Desarrollo y elaboración de la documentación de programas.

B) Prueba modular y prueba del sistema integralmente

Se deben realizar pruebas de todo tipo, pero estas deben ser planeadas y dirigidas por el auditor líder del proyecto para que se deje evidencia del resultado de las mismas, y con ello poder hablar sobre la efectividad del sistema, tenemos que provocar reacciones al sistema metiendo datos erróneos intencionalmente, para validar además su eficacia.

- Instalación.

Cuando se realice la instalación de un sistema, y éste sea de considerable tamaño, debe implantarse por sección o módulos, para ir validando su eficiencia y su capacidad de trabajo y efectividad, ya que, si implantamos todo el sistema, puede ser que no sepamos cuál módulo no funciona y nos llevaría mucho tiempo detectar una falla.

C) Desarrollo de manuales

- De operación
  - Representación gráfica de la estructura del sistema.
  - Función de cada programa.
  - Punto de reinicio y recuperación.
  - Requerimientos del equipo, etc.
- De usuario
  - Representación gráfica de la estructura del sistema.
  - Procedimiento de preparación de datos.
  - Asignación de prioridades.
  - Tiempo de respuesta.
  - Controles del usuario.
  - Procedimiento para resolver errores, etc.
- Del 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 del sistema depende en gran medida, de la calidad de la documentación. Además de la claridad y organización de la documentación, debe dedicarse especialmente al tipo de personas al que va dirigido.

D) Entrenamiento

- Métodos de enseñanza
- Evaluación del aprendizaje

4. IMPLANTACIÓN

A) Conversión

- Identificación de las fuentes de información.
- Recopilación de la información.
- Revisión de la exactitud de los documentos previos a la conversión.
- Evaluación de los resultados de la conversión.

La etapa de conversión significa abandonar el sistema actual, manual o computarizado, para emigrar a uno nuevo y conciliar los resultados.
Los controles en la etapa de conversión consiguen y persiguen el aseguramiento de los archivos iniciales, proporcionan un punto de arranque adecuado y oportuno marcando: Itinerarios, compromisos, condiciones de éxito. Normalmente la conversión requiere del desarrollo de programas de conversión de archivos de un formato a otro.

B) Revisión de la postimplantación

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 postimplantación normalmente involucra:

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

Mantenimiento del sistema.

Debido a que lo único constante en sistemas es el cambio, en esta etapa se analiza y evalúa cómo ha sido el mantenimiento de sistemas para proteger la instalación de cambios incorrectos, no autorizados o decisiones equivocadas.
"El primer cambio surge el día que se instala el sistema".

El mantenimiento de sistemas se origina por los siguientes factores:

- Cambios en normativa interna y externa a la entidad.
- Desarrollo tecnológico.
- Comportamiento del entorno, competencia.
- Costos excesivos.

Normalmente, los cambios obligatorios se efectúan con menos controles, por la presión implícita, mientras que los cambios por mejoras (refinamiento, creatividad, ventajas tecnológicas) se atienden más controladamente.

Al auditor le preocupa que haya un sistema para administrar los cambios, por ejemplo, hacer los cambios por grupos o lotes pertenecientes a un mismo módulo/programa. La documentación de los cambios debiera mostrar:

- Control numérico.
- Fecha de implantación.
- Persona solicitante.
- Persona que efectuó el cambio.
- Justificación.
- Descripción narrativa.
- Documentación de las pruebas.
- Autorización formal.

Todo cambio debiera originar la actualización de la documentación correspondiente.

La conciencia de la calidad, seguridad y control, debe iniciarse en las áreas de desarrollo, contemplando un balance adecuado con la productividad de los sistemas.

4.2. Auditoría de datos

Las actividades que se realizan para la alimentación de datos, frecuentemente involucran de manera importante la intervención humana.

Los controles en esta etapa buscan que la información de entrada sea validada y que cualquier error detectado sea controlado, de manera que la alimentación de datos al computador sea auténtica, exacta, completa y oportuna.

Controles de entrada

Técnicas

Se usan para identificar errores en los datos antes de ser procesados y son ejercidos durante el flujo de la información.

Niveles del ejercicio de los controles de entrada

- Dato o campo.
- Registro.
- Lote.
- Archivo.

Verificaciones sobre campos

- Datos requeridos.
- Tipo de caracteres.
- Rangos.
- Constantes.
- Dígito verificador.
- Contra archivos maestros.
- Tamaño.

Verificaciones sobre registros

- Signo.
- Secuencia numérica.

Verificaciones sobre lotes

- Totales de control.
- Tipo de transacciones.
- Número consecutivo de lote (único).
- Secuencia numérica de partidas.
- Tamaño límite del lote.
- Fecha de preparación del lote.
- Información de errores detectados.
- Espacio para firmas de quién preparó, verificó, procesó, etc.

Verificaciones de archivo

- Etiqueta interna.
- Número de generación.
- Fecha de expiración.
- Totales de control.

El auditor debe estar interesado en los siguientes aspectos de las validaciones programadas:

- Cómo se validan los datos.
- Cómo se manejan y reportan los errores.

Documentación, archivos de errores, sistema general de entrada de datos.

ETAPAS EN ENTRADA DE DATOS

- Capacitación u obtención de datos.
- Preparación de datos.

- Alimentación de datos.

CAPTACIÓN U OBTENCIÓN DE DATOS.

Se refiere a la identificación y registro de los eventos que son relevantes en la organización para la adecuada operación de la misma.

Métodos de captación u obtención de datos

- Documental.
- Directo.
- Híbrido.

CARACTERÍSTICAS DEL MÉTODO DOCUMENTAL

- Fácil y flexible
- Intervención humana substancial. Costo sujeto a errores humanos.

Adecuado diseño de documentos fuente

- Aumenta la velocidad y exactitud del registro de datos.
- Controla el flujo del trabajo.
- Facilita la preparación de datos en forma legible por la máquina.
- Facilita el chequeo subsecuente.

Análisis de documento fuente

- Qué datos contendrá.
- Cómo se obtendrán los datos.
- Quién obtendrá los datos.
- Cómo se introducirán al computador.

- Cómo se manejará, almacenará y llenará el documento.

Estructura y estilo de los documentos fuente

- Preimprimir documentos.
- Prenumerar los documentos.
- Proporcionar títulos, encabezados, notas e instrucciones.
- Usar técnicas de énfasis de diferencias.
- Clasificar los datos para facilitar el uso.
- Proporcionar respuestas múltiples a preguntas para evitar omisiones.
- Utilizar encuadres para identificar el tamaño del dato.
- Combinar instrucciones con preguntas.
- Proporcionar espaciado adecuado.
- Diseñar correctamente para fácil tecleo.
- Conformarlo de acuerdo a los estándares de la organización.
- Proporcionar espacio para correcciones y firmas.
- Entrenamiento de los responsables en el llenado de los documentos fuente.

CARACTERÍSTICAS DEL MÉTODO DIRECTO

Se refiere al registro inmediato de un evento cuando ocurre, usando un dispositivo de entrada (terminales, teléfono, etc.).

- Menor intervención humana.
- Inmediata retroalimentación del sistema.
- Costosa en *hardware* y *software.*

CARACTERÍSTICAS DEL MÉTODO HÍBRIDO

Se refiere a la combinación del método de documentos y el directo para la captura de datos. Los documentos contienen parcialmente información preimpresa (datos constantes) acerca del evento a registrar (documentos de ida y vuelta, cheques, marbetes de inventario, etc.)

- Menor intervención humana.
- Costoso en *hardware* y *software.*

Dispositivos de alimentación de datos

- Dispositivos de reconocimiento de tinta magnética (MIRC) principalmente en bancos:

  - Lectura rápida.
  - Almacenamiento al tiempo de lectura.
  - Cierta validación.
  - Fácil para el ser humano.
  - Impresoras de gran calidad y tinta en buen estado.

- Dispositivos de reconocimiento de caracteres ópticos (OCR):

- Para altos volúmenes de entrada.
- Costosos y no muy confiables.
- Información preparada en máquina de escribir, *offset*, impresa por computadora o manualmente.
- Sujeta a errores de codificación.
- Dispositivos de censores para marcas ópticas (OCR).
- Leen marcas en lugar de caracteres alfanuméricos.

- Las marcas pueden ser: preimpresas, escritas en máquina de escribir, manualmente o por computadora.
- Útil para bajos volúmenes de información de entrada.
- La posición de las marcas en el documento indica su valor alfabético y numérico.
- Cierta información se imprime en el documento (horas laboradas, cantidad perdida, etc.).
- La preparación es fácil y sujeta a pocos errores.
- No adecuado cuando los datos a capturar varían muy frecuentemente.

Adecuado diseño de pantallas de entrada

- ❖ Organización de la pantalla.
- ❖ Ordenadas.
- ❖ Simétricas.
- ❖ Delimitadores e instrucciones de llenado.
- ❖ A imagen del documento fuente o conforme se obtiene los datos.
- ❖ Consistencia.
- ❖ Distinguir información ofrecida por el sistema de la solicitada al usuario.
- ❖ Evitar salto automático al siguiente dato.
- ❖ Rápido tiempo de respuesta, *help*, uso de códigos.
- ❖ Mensajes de error (cortos, significativos, corteses, neutrales).

PREPARACIÓN DE DATOS

Cuando en el proceso de obtención (captura) no se registran los eventos inmediatamente de una forma legible por la máquina, se requiere de las actividades de preparación de datos.

Pista de auditoría.

Mantiene la cronología de los eventos acerca del origen de la transacción y su futuro proceso, así como la cronología de los eventos desde que los datos son validados hasta que son corregidos (cuando hay errores) y se consideran aceptables para continuar en el proceso.

CONTROLES SOBRE EL PROCESO DE DATOS

La etapa de proceso es la responsable de calcular, clasificar, ordenar y sumar los datos.

Principales problemas en el proceso

- Estilo de programación.
- Manejo del redondeo.
- Intervención del operador.
- Manejo de "*overflow*".
- Manejo de cifras corrida a corrida.
- Manejo del signo.

Principales riesgos

- Intervención de programadores incautos o inexpertos.
- Falta de estándares.
- Utilización de la versión correcta del programa.
- Caídas del sistema.
- Desconocimiento de políticas y procedimientos (normativa).

Por tanto, se requieren controles para:

- El adecuado manejo del redondeo. La impresión de totales corrida a corrida.
- Minimización de la intervención del operador.
- Establecimiento de cálculos redundantes en el caso de campos de resultados sensibles o importantes.
- Evitar el traslape de longitud (*overflow*).
- Verificación de la razonabilidad de los resultados (pago neto).
- Conciliar totales de corrida a corrida.

Los programas de aplicación contienen las instrucciones requeridas por el usuario para el registro y control de la información y pueden existir errores o irregularidades.

Se debe impedir la entrada de datos vía consola del operador.

Debe haber un control de las interrupciones.
Se sugiere la verificación de etiquetas internas de los archivos.
Deben existir chequeos sobre datos numéricos para asegurar la totalidad, exactitud y autorización de los cálculos, el tipo de chequeo varía debido a la diversidad del proceso.
Los problemas en el manejo del redondeo pueden ocurrir porque el nivel actual de precisión no es igual al requerido. Por ejemplo, en el caso de los intereses de un banco.
Durante cada paso de trabajo es deseable que se generen totales de control, lo cual proporciona evidencia de la totalidad y actitud del procesamiento de datos. Un ejemplo en la actualización de un archivo maestro: saldos anteriores, más registros adicionados, menos registros dados de baja debe ser igual a los saldos finales. Otro ejemplo: el total de registros leídos debe ser igual al total de registros grabados.

El minimizar la intervención del operador disminuye la probabilidad de errores. Se sugiere que se efectúe una validación de las acciones tomadas por el operador.

Otra sugerencia es evitar rutinas cerradas; es decir, cuando el programa asume una condición si no existe alguna de las esperadas. Por ejemplo, cuando se busca uno de cuatro valores y en su defecto se asume un quinto valor, sin esperar algo diferente.

Verificaciones a nivel de campo.

- Cláusulas de control de "*overflow*".
- Chequeo contra rangos de valores permitidos para un dato.

Verificaciones a nivel de registro.

- Razonabilidad. Por ejemplo, el total de deducciones por empleado de acuerdo a su categoría.
- El tipo de registro puede determinar el signo de un campo.

Verificaciones a nivel de archivo.

- Totales de control separados para campos relacionados. Por ejemplo, la suma del pago neto por empleado debe ser igual al pago neto usando importes globales.
- Totales de corrida a corrida.

Pista de auditoría

Mantiene la cronología de los eventos desde que el dato es recibido en la entrada hasta el tiempo en que es enviado a un archivo o reporte.

CONTROLES EN LA 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, o sea, 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, y se valida la efectividad del sistema.

Controles de presentación

- Contenido.
- Medio.
- Formato.
- Estructura.
- Tiempo de ida, vuelta y respuesta.
- Establecimiento de estándares de diseño.
- Establecimiento del mecanismo de monitoreo para evaluar la calidad de las opciones elegidas.

Controles sobre contenido

ATRIBUTO	IMPACTO EN LA CALIDAD DE LA SALIDA
Exactitud	Escala conocida y aceptada
Relevancia	Importancia en relación a la decisión a ser tomada
Sumarización	Estadísticas globales
Filtros	Reportes ejecutivos, pero incompletos probablemente, con información oculta.

Medios de salida

- Papel
- Desplegado en pantalla

Formato

- Tablas
- Gráficas

Controles sobre la salida, Sistemas en *Batch* (por lotes)

Controles sobre el diseño de reportes

- Nombre del reporte.
- Fecha y hora de producción.
- Periodo de proceso cubierto.
- Programa que lo produjo.
- Número de página.
- Encabezado de campos.
- Marcha de fin de trabajo.
- Clasificación de seguridad / confidencialidad.
- Lista de distribución.
- Fecha de retención.
- Método de destrucción.

Controles sobre papelería y accesorios

- Inventario.

- Almacenamiento seguro.
- Control de acceso a operadores.
- Formas preimpresas.
- Formas prenumeradas.

Controles sobre los programas para producir reportes

- Uso de la versión correcta.
- Evitar alteraciones efectuadas por el operador vía consola.
- Puntos de chequeo y reinicio.
- Impresión del reporte en una impresora remota.

Control sobre archivos para impresión
(*spooling/ printer files*).

Diseñados para asegurar que:

- El contenido de los archivos no se altera.
- No se emiten copias no autorizadas.
- Los archivos se imprimen una sola vez.
- No se utilizan respaldos de archivos para efectuar copias no autorizadas.

Controles sobre la recolección y distribución de reportes

- Lista de reportes a producirse.
- Lista de usuarios autorizados.
- Establecimiento de periodos de recolección.
- Existencia de lugares y mobiliario seguro.
- Firma y fecha de recepción de los reportes.
- Etiqueta en el reporte para cada usuario.

Controles sobre la destrucción de reportes

Otro aspecto de gran importancia es el procedimiento de destrucción de los reportes que se tenga establecido, el ideal es mediante trituradoras de papel (suficiencia, correcta ubicación, etc.).

Controles de verificación de la salida
(Mesa de control)

Búsqueda de errores evidentes, formatos erróneos, datos faltantes, valores irrazonables, etc. Revisión al azar de los datos.

Controles sobre la salida en sistemas en línea

- Encriptación.
- Localización de todas las terminales.

Estructura de las pantallas de consulta.

- Orden y clasificación.
- Cuántos datos por pantalla.
- Dónde colocar los datos.
- Área de encabezados.
- Área principal.
- Área de diagnóstico.
- Área de respuestas.

Controles de tiempo.

- Tiempo de respuesta empleado para resolver problemas.

- Puntos de chequeo y reinicio.

Controles de distribución

“Privacidad”

Pista de Auditoría

Mantiene la información acerca de los eventos que ocurren desde el momento en que el contenido de la salida es determinado hasta que es entregado a los usuarios.

4.3. Auditoría del equipo de cómputo

Una de las áreas de auditoría más conflictivas y sensibles en una institución es la función de adquisiciones que, tratándose de recursos informáticos, se vuelve por demás interesante y muy sensible, debido a que se deben establecer los procedimientos de adquisición de los bienes informáticos, que van 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.

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 a las metas y objetivos previamente planeados.

- Se debe tener bien establecida la responsabilidad de los proveedores

Equipo / *software.*

A partir del análisis y definición de requerimientos, 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 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.

- Factibilidad legal, por las restricciones que pudiera tener el proveedor conforme a garantías, servicio, copias ilegales, etc.

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 aún 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 ésta en una fecha determinada ante la presencia de todos los concursantes a fin de que no existan favoritismos en la asignación del periodo y éste se canalice hacia la mejor alternativa para la institución.

Estas solicitudes de propuestas deberán incluir todas las especificaciones técnicas 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 realizarán las pruebas de aceptación previas.

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

Es necesaria una revisión minuciosa del contrato con el proveedor. 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 (customización) 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 éste se cumpla dentro de las estimaciones de costo y tiempo definidas.

Otro aspecto importante a 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 obtenidos 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 efectiva 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.

4.4. Auditoría de procesos

Concepto

Un sistema de información se define como un conjunto de procedimientos o procesos manuales o computarizados entrelazados y que constituyen un sistema que produce información sobre algo en particular.

El origen de los recursos se refiere a la fuente o causa que da inicio a la obtención de un bien o servicio y la aplicación se refiere a la ubicación de la cuenta que refleja en donde se ejerce el recurso.

Ejemplo, un sistema de contabilidad incluye los siguientes elementos:

Origen de recursos	Aplicación de recursos
Facturación	Cuentas por cobrar
Compras	Cuentas por pagar
Inventario	Activo fijo

Nómina	Contabilidad general
Cheques	Ahorros
Valores	Fondos de inversión

El auditor de sistemas necesita conocer y evaluar el control interno para determinar el alcance, naturaleza y oportunidad.

CONTROLES

Definición

Es un proceso para asegurar que los sistemas o controles de seguridad satisfagan la calidad de información y sirvan de base para la adecuada toma de decisiones.

Objetivo

Este tipo de auditoría se realiza con el fin de evaluar ya un sistema en funcionamiento y ver su grado de efectividad y uso, así como la seguridad del mismo.

Tipos de control

Preventivos: Se anticipan a la presencia del error, es decir, lo previenen.

Detectivos: Identifican la presencia de un error y avisan mediante una señal sonora o simplemente visible en la pantalla del monitor de la computadora o en un reporte.

Correctivos: Presentan las medidas establecidas para corregir los errores detectados por los del tipo anterior.

OBJETIVOS BÁSICOS DEL CONTROL

Para poder evaluar un sistema, el auditor debe tomar básicamente en cuenta aspectos que garanticen la viabilidad y funcionamiento del sistema en operación, para ello debe de verificar y validar los siguientes elementos:

A. Integridad. Registro inicial, suministro, alimentación, actualización, datos generados por la computadora.
B. Precisión. Registro inicial, alimentación, actualización, datos generados por la computadora.
C. Autorización. Adecuada al puesto.
D. Continuidad. Total, exacta e importante.
E. Oportunidad. Para comprobar su efectividad.
F. Beneficio. Porcentaje de utilización y servicio.

Básicamente, nuestro objetivo será dar una opinión sobre la confiabilidad de la información que se procesa electrónicamente, tomando en consideración lo siguiente con respecto a los controles.

- Si no disminuye el riesgo, es procedimiento operativo.
- Si se disminuye el riesgo, es procedimiento de control.

A. Integridad

Este objetivo persigue que todas las operaciones:

- Se registren íntegramente.
- Se suministren al sistema.
- Actualicen los diferentes archivos manejados en la aplicación.
- Se consideren en los procedimientos de cálculo, totalización, etc.

Es importante considerar la retroalimentación de errores, omisiones y correcciones para cada fase.

B. Precisión

Este objetivo persigue que los datos importantes de cada operación o actividad sean correctos:

- Al momento de capturarlos en la computadora, ya sea de manera manual o automática.
- Al actualizar los diferentes archivos manejados en la aplicación.
- Al considerarse por los procedimientos de cálculo, totalización, categorización.

C. Autorización

El control primario de una operación dada, es el acto de su autorización, la que consiste en que alguien, comparándola con los planes, condiciones, limitaciones o conocimiento general de lo que constituye una operación correcta, decide si es o no válida; el acto debe ser ejecutado por una persona reconocida en el sistema establecido como quien tiene la facultad y el nivel jerárquico para hacerlo.

D. Continuidad

Este objetivo persigue que las operaciones / actividades permanezcan completas y exactas en el tiempo.

E. **Oportunidad**

Este objetivo persigue que el registro de las operaciones / actividades y la información que se produce sea oportuna en su registro y en la emisión de reportes para la toma de decisiones.

F. Beneficio

Este objetivo persigue que la información que se produce sea útil para la toma de decisiones.

PRINCIPALES TÉCNICAS DE CONTROL

a) Chequeo de secuencia numérica

En sí de lo que se trata es del establecimiento de cifras control o controles de gestión.

El mejor medio para asegurarse de que al procesar las operaciones no se escape alguna de ellas, es numerarlas y, después de procesadas, compararlas (se numeran previamente los documentos / operaciones).

- Chequeo de uno por uno, reportes de cómputo contra documentos fuente.
- Comparación contra datos pre-registrados.

El documento de una operación puede anexarse a otro originado independientemente, como evidencia de su validez. Por ejemplo, la factura del proveedor puede acompañarse con los informes de recepción y la orden de compra.

Algunos datos pueden compararse con estándares predeterminados o listas de normas establecidas. Básicamente lo que haremos es la realización de un cruce de auditoría.

- Comparación de totales de control.
- De documentos.
- De renglones.
- De importes.
- De cualquier campo numérico (número de cuenta, folio, número de parte, unidades, etc.).
- Dígito verificador.

El totalizar ciertos números claves antes y después de procesar todo un grupo de operaciones, es una forma tradicional de asegurarse de que todas se han procesado. Por supuesto, subsiste la posibilidad de errores compensados, pero esta posibilidad es un tanto remota.

Algunas medidas de control consisten en comparar una cifra con otra que se ha determinado independientemente, lo que con frecuencia requiere también una conciliación.

Conciliaciones bancarias, la conciliación de la suma de los saldos detallados del auxiliar con el saldo global de la cuenta de control (de mayor); los recuentos físicos de caja (arqueos), de valores, de inventarios o de otros activos; y, finalmente, la confirmación directa de saldos de deudores y acreedores.

El cálculo del dígito verificador involucra la multiplicación de cada uno de los dígitos del código original por cierto factor de ponderación, la suma de éstos resultados y luego la división de ésta suma por un número que representa el valor del módulo. Finalmente, se resta el valor del módulo del residuo de la división anterior. El analista de sistemas elige la ponderación y el módulo a utilizar.

Los tipos de errores que puede detectar son:

- Sustitución de dígitos.
- Transposición de dígitos.

El enfoque de dígito verificador es útil cuando los códigos originales son de cinco o más cifras y nos auxilian a lo siguiente:

- Verificación de razonabilidad.
- Rangos. Por ejemplo, tabuladores de sueldos.
- Constantes. Por ejemplo, femenino / masculino, si / no, etc.
- Verificación del formato, sintaxis (naturaleza: campos numéricos, alfabéticos, alfanuméricos y longitud de campos).
- Chequeo de generaciones de archivos (abuelo, padre, hijo).
- Reproceso selectivo de partidas.

b) Control de pendientes

Otra verificación bastante común de que todo se registra, consiste en listar las operaciones o conservar un expediente con copia de los documentos que las originan y tachan de las listas o retirar los expedientes, las operaciones que se van procesando.

Sin embargo, estos archivos o expedientes de asuntos no terminados o pendientes requieren, para su funcionamiento efectivo y para que constituyan una medida de

control, ser revisados periódicamente para tomar las medidas procedentes y no dejar en ellos asuntos pendientes por demasiado tiempo.

c) Lista de recordatorio

Ejemplos típicos de estas listas son los archivos de facturas o cuentas por pagar. Por fecha de vencimiento o los calendarios de obligaciones fiscales.

A tres actividades de control se les ha dado la categoría de “disciplinas”, incluyendo los controles básicos y sus resultados.

La disciplina es importante porque ofrece una razonable seguridad de que las operaciones básicas y de control funcionan o se ejercen tal como fueron diseñadas.

Las disciplinas sobre los controles básicos son aquellos aspectos de un sistema que aumentan la confianza de que los controles básicos operan adecuadamente.

Acceso controlado o restringido

Se refiere a la seguridad física, tanto del efectivo, inventarios, activo fijo, documentos, libros, reportes, formas, archivos de la computadora en medios magnéticos, etc.

El objetivo del control de acceso restringido es delimitar la responsabilidad de la guarda, custodia y utilización de los bienes muebles e inmuebles, así como específicamente de *software* y de *hardware* con el objeto de evitar mal uso de los mismos y de la información que de ella emana. Para ello se tiene que contar con bitácoras de acceso a bienes informáticos y normativa interna que permita su mejor control.

Finalmente, las medidas físicas de seguridad deben también proteger los archivos y registros contra deterioro, destrucción o pérdida.

Supervisión

Probablemente es la disciplina más importante sobre los controles básicos, ya que aumenta la confianza en la información. La supervisión del sistema y de quienes lo operan, tiene un efecto obvio en la exactitud y en la confiabilidad.

a. Controles integrados o verificación interna por supervisión

Por ejemplo, quien autoriza un pago debe cerciorarse de que los documentos estén firmados o inicializados por el personal apropiado en sus diferentes procesos o el pago no podrá hacerse.

b. Supervisión administrativa

Los responsables de la administración de la función de informática deben normar el uso de los mismos con el objeto de evitar subutilización de recursos o mal uso de ellos.

Sin una supervisión adecuada se corre el riesgo de que aún los mejores sistemas y control se vuelvan erráticos y no confiables en poco tiempo, ya que con la presión normal del trabajo tienden a distorsionarse las rutinas y el personal busca formas más fáciles de hacer su tarea.

La falta de supervisión puede detectarse, aún en sistemas bien diseñados, por problemas en las cuentas, como un desusado número de errores y excepciones,

retraso en el trabajo, cuellos de botella en los registros, y el abandono de procedimientos prescritos.

c. Algunos indicadores de error.

- Voluminosos listados de transacciones rechazadas por la computadora (listados de validación) y el análisis de las causas de error (estadísticas por tipo de error y frecuencia).
- Análisis financiero:
- Razones financieras.
- Variaciones.
- Porcientos integrales.

d. Pista de auditoría

Son todos aquellos elementos que permiten reconstruir los eventos ocurridos, es decir, los hechos. Y mantiene la cronología de los eventos acerca del origen de la transacción y su futuro proceso, así como la cronología de los eventos desde que los datos son validados hasta que son corregidos (cuando hay errores) y se consideran aceptables para continuar en el proceso.

4.5. Auditoría de seguridad

La seguridad en informática no sólo abarca el aspecto físico, es decir, de acceso a donde se tiene el equipo de cómputo; sino se extiende al *software* y a las telecomunicaciones, ya que se han tenido que implementar dispositivos adicionales para dar seguridad a la información contenida en los sistemas de cada institución.

Por lo tanto, se tendrá que tomar en cuenta la seguridad física y lógica de los sistemas informáticos.

Seguridad física

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 y/o divulgación de información confidencial.
- Alteración de equipos sensible.
- Cambio sin 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 las cintas o discos magnéticos.
- Bóvedas de respaldos.
- Oficina de control de entradas y salidas.
- Clóset de comunicaciones.
- Microcomputadoras y terminales remotas.
- Área de programación.

La revisión abarca principalmente 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.
- 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.
    - 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 de los equipos.

Control de acceso

- Control de puertas. El acceso sólo 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 a seleccionar; es decir, hasta cuantas veces se aceptará que el sistema niegue el acceso a una persona autorizada o lo permita a una que no lo está.
- 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 al crecimiento institucional.
- Sencillez en su operación desde su instalación hasta su puesta en marcha.

- Cantidad y frecuencia de acceso de acuerdo al 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.

Auditoría a la seguridad lógica

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

- Determinar si 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 interfaz entre el usuario de un sistema y el computador mismo. Su propósito primario es establecer la identificación y la autenticación del que pretende ser usuario del sistema, para lo cual se necesitará 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 al nivel jerárquico y funciones del personal. Protegiendo la instalación de:

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

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

- Equipos.
- Programas.
- Comunicaciones.
- Datos.
- Facilidades.

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

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

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.

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

- Información memorizada, "*passwords*" o 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.

El sistema de control de accesos mediante *passwords* debe establecer perfiles de usuarios que incluyan los siguientes datos.

- Nombre del usuario.
- Identificador del usuario “USER ID”.
- Área a que pertenece.
- Privilegios dentro del sistema.
- Vigencia de acceso al sistema.

El archivo en donde reciben los *passwords* deber ser protegidos con su respectiva contraseña.

Cobra una gran importancia el concienciar al personal para que no rebele los *passwords*, enfatizando lo que éstos representan en la reducción de riesgo de transferencia, modificación, perdida o divulgación, accidental o intencional de información confidencial.

Normalmente, los sistemas computarizados para seguridad proporcionan una bitácora de las actividades efectuadas en el proceso electrónico de datos. Constituyendo pistas de auditoría que pueden analizarse periódicamente y tomar decisiones; en esta bitácora deben quedar registrados todos los accesos ocurridos y los intentos de acceso no autorizados a fin de que se puedan tomar las medidas

pertinentes cuando el número de incidencias es relevante: en qué terminal ocurre, a qué hora, cuántas veces, qué persona la utiliza, etc.

Los datos que pueden ser útiles como pistas de auditoría son:

- Identificación del usuario.
- Información dada para autentificación.
- Recursos requeridos.
- Acciones privilegiadas (derechos) requeridas.
- Identificación del dispositivo (terminal).
- Hora de inicio y terminación del acceso.
- Número de intentos de acceso.
- Recursos proporcionados o negados.
- Acciones privilegiadas (derechos) otorgadas o negadas.

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.

Existen básicamente tres métodos para transformación de información:

Sustitución. Mediante este método se conserva la posición original de los caracteres del mensaje y se esconde su identidad, pues los remplaza por otros caracteres de acuerdo a una tabla de códigos equivalentes, ya sean numéricos o alfabéticos.

Transposición o permutación. Consiste en cambiar el orden de los caracteres del mensaje original.

Híbrido. Este método combina las características de los métodos de sustitución y de transposición.

Con el objeto de estandarizar la forma de encriptar, se diseñó un algoritmo llamado “des” (*data encryption standard*) basado en la técnica de sustitución o transposición de datos; el cual fue adoptado por la “nbs” (*national bureau of standards*) de los Estados Unidos de Norteamérica.

La seguridad no puede depender de un sólo elemento como lo es un algoritmo de encripción. Pues la persona que quisiera acceder información confidencial protegida, lo único que tendría que hacer es enfocar sus esfuerzos a descubrir los detalles de dicho algoritmo. Por esto, se requiere de un segundo elemento llamado “llave de encripción”, que es un número generado en forma aleatoria con el objeto de mantener su confidencialidad.

El concepto de encripción por *hardware* se aplica cuando se utiliza un dispositivo eléctrico denominado encriptor para transportar datos que viajan a través de un medio de comunicación. Se dice que la encripción es vía *software*, cuando se utilizan una serie de programas para transformar los datos, independientemente de que éstos se encuentren almacenados o viajando a través de cables, líneas telefónicas, etc.

Aspectos importantes para evitar cambios no autorizados a los programas y datos.

- Segregación de funciones.
  - Diferentes personas.
  - Diferentes bibliotecas y directorios en disco (para producción desarrollada).
- Adecuado sistema de medios de identificación, por ejemplo, palabras claves (*passwords*) definición de autorizaciones, frecuencia de cambios estructurales, etc.

- Supervisión.

Plan de contingencias

Ha existido mucha dificultad para la plantación y prevención de desastres durante los últimos años. Un buen punto de inicio fue el reconocimiento del poder de las comunicaciones (teléfono, fax MODEM, etc.) y cómo afectó a los centros de cómputo el temblor de septiembre de 1985 en México, D.F. El impacto mayor no es en muchas veces el desastre mismo, sino las acciones que se tomen en el momento del desastre.

Los desastres pueden ser naturales, humanos y materiales. Normalmente se piensa en los fenómenos naturales, pero no en lo de todos los días. Roedores, fugas de agua, etc. Y eso muchas veces es lo primero a controlar. Otro ejemplo es el que cualquiera puede llegar a las instalaciones, a recursos vitales como las comunicaciones.

Se entiende como:

- Desastre: accidente, tragedia, emergencia.

- Recuperación: sanar, reponer, ganar de nuevo.

Se puede definir un plan de recuperación como la habilidad de una organización para continuar sus operaciones diarias, a pesar de que ocurra un desastre, por medio de una serie de acciones coordinadas y planeadas con el conocimiento y el apoyo gerencial. El gerente de informática debe ser el líder del plan. Pero debe involucrarse seriamente el director de finanzas.

Para que un plan de recuperación ante contingencias funcione, deben ser del conocimiento y reconocimiento de todos los involucrados. Para obtener un mayor convencimiento se puede recurrir a fuentes externas. Es una póliza de seguro diferente.

En general, los planes de contingencia pueden definirse como un elemento de control interno que es establecido para asegurar la disponibilidad de datos valiosos y los recursos del computador en el caso de un evento que ocasione la interrupción de operaciones.

Un buen plan de contingencia y recuperación detalla los procedimientos para emigrar a una situación de emergencia en el menor tiempo posible y con el menor grado de riesgo, así como regresar a la operación normal de la misma forma.

La preparación de los planes de contingencia no es una tarea simple y realizable por un solo individuo. Es una actividad compleja y multifacética que requiere la involucración de toda una organización. Por lo que resulta necesaria la creación de un comité que administre todo lo relacionado con el plan de contingencias: recursos humanos y financieros; aunque el desarrollo del plan requiere de la cooperación de todas las áreas de la institución, una persona debe tener la responsabilidad de coordinar, complementar y dar mantenimiento al plan. A esta persona se le conoce como líder del proyecto.

Una parte del proceso de planeación para los casos de contingencia es la determinación de los desastres potenciales de la organización. Diferenciándose un desastre de una falla operativa. La clave para la determinación efectiva de los planes de contingencia es el entendimiento de los requerimientos de procesamiento y sus prioridades.

A continuación, se indican algunos puntos a considerar dentro de un plan de contingencia:

- Tener un mejor entendimiento de la entidad.
- Ver las cosas no con una perspectiva simplemente tecnológica, sino de protección y seguridad. Muchos problemas se van generando paulatinamente y en un momento se convierten en desastre, porque pasan inadvertidos diariamente.

- Imposición de sanciones (penalizaciones y multas) por violaciones o infracciones a las reglas de seguridad por empleados irresponsables o descuidados. Por ejemplo, en el caso de cortes de cables.

- Deberá realizarse un inventario que incluya todos los sistemas y recursos de cómputo disponibles; así como una lista de las personas que operan dichos recursos; también, el inventario deberá incluir el mobiliario y las condiciones físicas del lugar, como son: aire acondicionado, puertas, cerraduras, etc.

- Analizar todos los conflictos legales y laborales considerados como potenciales en caso de desastre, con empleados accionistas, clientes, proveedores, etc.

- Cuidar la coordinación cuando se comparte el inmueble con otras instituciones. Fincando responsabilidad compartida, también es el caso de construcciones y remodelaciones vecinas.

- Auxiliarse de documentos modelos y preparar un plan preliminar, en términos de negocios.

- Incluir procedimientos detallados iniciales de avisos y acciones. Lo más importante es proteger la vida humana. Las telecomunicaciones en muchos casos son críticas en caso de desastres. El seguir las instrucciones ordenadamente puede evitar que un desastre se convierta en una catástrofe. Puede darse el caso de tener la necesidad de reemplazar trabajadores valiosos que renuncian como resultado de tener sentimientos de inseguridad o percibir un alto riesgo para sus vidas.

- Lista de personas que deben arrancar el plan contra desastres, que deben ser informadas de manera inmediata y de los coordinadores responsables de la centralización y diseminación de la información durante la emergencia.

- Clasificar los recursos informáticos de acuerdo a su importancia.

- Requerimientos de personal para recuperación.

- Procedimientos de seguridad que deberán tenerse en cuenta al trasladar los recursos informáticos.

Direcciones y teléfonos de:

  - Centro alterno de proceso de datos.
  - Proveedores.
  - Clientes.

- Doctores.
- Policía.
- Servicios de emergencia, bomberos, hospitales, etc.
- Agencias de personal para nuevas contrataciones
- Personal activo.

- Rutas de transportación primaria y alterna en el caso de que resulte necesario enviar empleados a su domicilio.
- Procedimiento en caso de amenaza de bombas.
- Procedimientos para activar el equipo de soporte.
- Mecanismo de notificación y control de actividades.
- Operaciones a procesar en el centro de apoyo o facilidades alternas.
- Prioridades de operación de sistemas.
- Planes de evacuación y planes alternos en caso de fuego, bomba o explosión.
- Procedimientos para solicitar asistencia de la policía y los bomberos.
- Procedimiento para recuperación, conmutación telefónica y restauración de los servicios del centro de procesos de datos.
- Reporte y evaluación de riesgos existentes.
- Copia de contratos y seguros de mantenimiento y respaldos.
- Mecanismos de respaldo existentes. Guardar la versión “abuelo” de los archivos en medios magnéticos en un lugar seguro y fuera de la zona en que se ubique el centro de proceso de datos.
- Convenios con otras instalaciones para formalizar soporte de equipo en caso de catástrofes.
- Existencia del manual de contingencias en el lugar en que se encuentre la bóveda de respaldos.
- Los procedimientos deben funcionar siempre, por lo que es importante efectuar una revisión periódica de ellos y actualizar los ejemplares que se

tengan del manual por el comité de contingencias cada vez que ocurran cambios en:

- Personal.
- Equipo o instalación propia y/o soporte.
- Teléfonos.
- Usuarios.
- Contratos de mantenimiento y respaldo.

RESUMEN

Como se puede ver en este capítulo, las variantes para realizar una auditoría en informática son muchas, y depende de las necesidades de cada institución las que se puedan aplicar; son sólo enunciativas, más no limitativas.
Aquí sólo se mencionaron las siguientes:

Auditoría de sistemas.
Auditoría de datos.
Auditoría del equipo de cómputo.
Auditoría de procesos.
Auditoría de seguridad.

Estos tipos de auditoría tienen su importancia en función de la necesidad del auditado. En el primer tipo de auditoría se observa la auditoría a la metodología de sistemas; en la segunda, a la integridad de datos de entrada, proceso, salida, etc. A los equipos de cómputo, desde su adquisición hasta su puesta en marcha y las características de las mismas. En los procesos, la secuencia de pasos para llevar a cabo la auditoría; y, por último, la importancia de la seguridad y confiabilidad de la guarda y custodia tanto de *software* como de *hardware*, que lleva a plantear el alcance de contar con un plan de contingencias.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

Autor	Capítulo	Páginas
Carlos Muñoz Razo.	6. “Metodologías para Realizar Auditorías de Sistemas Computacionales”	179-237
José de Jesús Aguirre Bautista	4. “Auditoría de Sistemas”	1-26

Bibliografía Básica

Piattini, Mario y Emilio Del Peso (2001). *Auditoría informática, un enfoque práctico* (2ª. Ed.). España: Alfa-Omega.

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

Bibliografía Complementaria

Solís Montes, Gustavo Adolfo (2002). *Reingeniería de la auditoría en informática*. México: Trillas.

Weber, Ron (1998). *EDP Auditing: Conceptual Foundations and Practice*. Ed. McGraw Hill.

Sitios de Internet

Sitio	Descripción
fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf	Auditoría de sistemas.
http://fcaenlinea1.unam.mx/informatica/file.php/67/unidad04/index.html	Auditoría de sistemas.

UNIDAD 5

Planeación de la auditoría informática

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno tendrá los conocimientos adecuados para diseñar, evaluar y determinar el costo de realizar la auditoría informática.

TEMARIO DETALLADO

(12 horas)

5. Planeación de la Auditoría Informática
5.1. Planeación
5.2. Revisión preliminar
5.3. Diagnóstico de la información
5.4. Definición de pruebas de controles
5.5. Definición de pruebas sustantivas
5.6. Evaluación de los sistemas de acuerdo al riesgo
5.6.1 Investigación preliminar
5.7. Definición de equipo de auditoría

INTRODUCCIÓN

Es importante señalar que esta etapa va a dar la oportunidad de concretar la auditoría y el alcance y los objetivos de la misma; se analizarán los recursos a utilizar, tanto humanos, financieros y tecnológicos. Primero es establecer el tipo de auditoría que se va a realizar, el manejo de la información; es decir, contar con los elementos que deberán ser útiles para que la institución auditada contemple la oportunidad de que la auditoría va a auxiliar a minimizar el riesgo de una probable interrupción en las operaciones normales informáticas de cada área y, por consiguiente, de toda la institución.

5.1. Planeación

Dentro de esta etapa, se debe considerar la determinación del tipo de auditoría en informática que se desea realizar; para ello, se tienen que establecer, entre otros aspectos, los objetivos, metas, políticas, reglamentos, procedimientos, planes y programas; además de la elección de los cursos de acción para lograrlos con base en la investigación y elaboración de programas de trabajo que incluya. Asimismo, la creación y función del comité u órgano interno de cómputo, que debe ser el encargado de administrar los bienes informáticos, independientemente de la parte operativa de los recursos informáticos.

Para poder realizar la planeación, lo más cercana a la realidad, se tienen que considerar, entre otros aspectos, los que se mencionan a continuación:

Solicitar:

- Manual de organización, donde se identificó:
    - ❖ Funciones, personal y equipo del área.
    - ❖ Objetivos del área.
    - ❖ Objetivos particulares de cada departamento.
    - ❖ Políticas del área.
    - ❖ Procedimientos del área.
    - ❖ Programas.

En esta fase vamos a revisar ¿qué es lo que se va a realizar? e incluye establecer:

- Misión.
- Visión.
- Objetivos.
- Políticas.
- Estrategias.
- Procedimientos.
- Planes.
- Programas.
- Etc.

En esta fase, debemos reconocer los avances tecnológicos, los cambios organizacionales, situación política, económica y legal de la empresa que se quiera auditar.

Lo ideal sería establecer un comité de planeación informática o comité de cómputo que evalúe los planes y establezca prioridades de ejecución, en el cual el auditor informático tiene la participación con voz; pero sin voto en la toma de decisiones.

Cuando un auditor realiza esta fase, debe tener los conocimientos técnicos suficientes, que le permitan evaluar y opinar sobre las acciones que se llevarán a cabo en la empresa en materia de informática.

Ahora bien, cuando el proceso de planeación de auditoría está considerando los aspectos antes mencionados, es poco probable que existan desviaciones en tiempo, personal y costo; sin embargo, cuando no se tiene un proceso de planeación estructurado, la función de la planeación en la auditoría en informática actúa por reacción, improvisando sobre la marcha y esto compromete los resultados y, en

consecuencia, los objetivos iniciales de la auditoría se distorsionan, lo que conlleva al incremento de costos que los entes auditados difícilmente querrán absorber.
Es importante señalar que la planeación es tan sólo una herramienta que ayuda a lograr los objetivos de la auditoría en informática y trata de tener un cronograma de funciones y actividades que puedan controlar sistemáticamente el flujo de la auditoría en informática. Es decir, se trata de que lleven un orden en sus funciones y actividades; además, como valor agregado, está el tratar de disminuir riesgos y otorgar una seguridad razonable de que lo que están haciendo se hace bajo una óptica de beneficio y un margen de error estrecho. Esto, sin descuidar que demasiada planeación es tan mala como la ausencia de ésta.

Un plan debe contener, entre otras, las siguientes características:

- Adaptable.
- Comprensible.
- Medible.
- Cuantificable.

Además, debemos considerar el establecimiento de indicadores en la planeación de la función de informática, como pueden ser las siguientes:

- Excesiva o escasa utilización del equipo de cómputo.
- Excesiva o escasa carga de trabajo y pago de tiempo extra.
- Obsolescencia en recursos informáticos.
- Demora en la solución de requerimientos del usuario.
- Verificación de causas y efectos de estas circunstancias.

Por consiguiente, la etapa de planeación, debe realizarse de forma específica dependiendo el tipo de auditoría en informática por efectuarse.

5.2. Revisión preliminar

Aquí se procederá a conocer la empresa y, de ser posible, se validará la problemática que fue expuesta por el cliente; si es que ella ocurrió. Después de esta fase, se estará en posibilidades de hacer una mejor estimación del tiempo y de los honorarios, si es que no lo pudo hacer en la fase de planeación.

PLANEACIÓN

Dentro de esta fase se debe:

Solicitar:

- Manual de organización, donde se identificó:

    - Funciones, personal y equipo del área.
    - Objetivos del área.
    - Objetivos particulares de cada departamento.
    - Políticas del área.
    - Procedimientos del área.
    - Programas.

ORGANIZACIÓN

En esta fase, se deberá considerar el establecimiento de la estructura necesaria, para la optimización de los recursos a través de la determinación de jerarquías y agrupación de actividades con el fin de realizar y simplificar las funciones del área.

Solicitar:

- Organigrama general y particular del área de cómputo.

Dentro de esta fase, además se verifica la función a través de la cual el encargado de la administración de la función informática elige y se allega de los recursos humanos necesarios para cumplir con los objetivos previamente establecidos.

Solicitar:

- Planes y programas de trabajo respecto a:

    - Reclutamiento.
    - Selección.
    - Inducción.
    - Capacitación.
    - Desarrollo.

DIRECCIÓN

En esta fase, se consideró si existe supervisión y coordinación de las actividades desarrolladas por el personal del área de cómputo.

Solicitar.

- Documentos que establezcan:
  - Frecuencia con que se realiza.
  - Quién es el responsable de realizarla.
  - Formas en que se realiza.

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.

5.3. Diagnóstico de la información

El diagnóstico tiene por objetivo proporcionar una panorámica de cómo la institución auditada percibe y practica la administración de los recursos informáticos.

Identificar áreas u operaciones con problemas para adoptar acciones preventivas, es una de las primeras labores del auditor en informática, debido a que la contratación de los servicios de auditoría en informática se puede dar porque el cliente o institución ya conozca la problemática, o porque el auditor en informática le deba realizar un diagnóstico y éste le detecte la misma problemática u otra no contemplada por el cliente.

Asimismo, un buen diagnóstico permitirá la determinación de los recursos necesarios para llevar a cabo la auditoría. Aunado a lo anterior, la comunicación a las partes involucradas en la auditoría.

En la actualidad, lo difícil no es obtener información, sino que existe demasiada y es precisamente la labor del auditor saber discriminar cuál es importante y necesaria para su labor y cuál se puede suprimir.

Por lo que se hace necesario no solicitar información de forma arbitraria, sino de forma consensuada; es decir, que debemos planear qué información es suficiente y cuál es competente, entendiendo que suficiente se refiere a la cantidad de información y la competente a la calidad de esa información.

Es importante señalar que la obtención de la información debe ser veraz, confiable y oportuna, de tal manera que la misma cumpla las características de oportunidad y necesidad; es adecuado señalar que, de la información emanada de la institución, y que solicita el auditor, se están tomando decisiones importantes y que el análisis adecuado de la misma contribuirá al cumplimiento de los objetivos de la institución auditada.

De todas las áreas funcionales de la institución, se obtiene información como resultado de sus procesos operativos, por lo tanto, se debe conocer qué tipo de información resulta del uso de las TI y cuál su utilidad, si el resultado del trabajo es finalmente un informe o información y no es necesaria para la toma de decisiones habrá que replantear ese proceso de información.

Asimismo, hay que percibir que debe existir retroalimentación para saber que la información obtenida por los auditores es necesaria para la adecuada toma de decisiones.

Con todos los elementos planteados, tenemos que preguntar a la institución cómo han llegado hasta esta situación, en donde se requiere una auditoría, y, posteriormente, el auditor evaluará las circunstancias que llevaron a la problemática existente en la institución.

5.4. Definición de pruebas de controles

Es importante reconocer que en esta etapa se va a poner en evidencia el talento del auditor, debido a que las pruebas tendrán características específicas para obtener resultados de alguna de las funciones de informática.

Definición

En este contexto, se refiere a los procedimientos que tienden a disminuir los riesgos; es decir, la posibilidad de que existan errores en la información, o bien, ineficiencia operativa.

Tipos de control

Preventivos: Se anticipan a la presencia del error, es decir, lo previenen.

Detectivos: Identifican la presencia de un error y avisan mediante una señal sonora o simplemente visible en la pantalla del monitor de la computadora o en un reporte.

Correctivos: Presentan las medidas establecidas para corregir los errores detectados por los del tipo anterior.

Objetivos básicos del control

Para poder evaluar un sistema, básicamente el auditor debe tomar en cuenta aspectos que garanticen la viabilidad y funcionamiento del sistema en operación; para ello, debe verificar y validar los siguientes elementos:

A. Integridad: Registro inicial, suministro, alimentación, actualización, datos generados por la computadora.
B. Precisión: Registro inicial, alimentación, actualización, datos generados por la computadora.
C. Autorización. Adecuada al puesto.
D. Continuidad: Total, exacta e importante.
E. Oportunidad. Para comprobar su efectividad.
F. Beneficio. Porcentaje de utilización y servicio.

Básicamente, nuestro objetivo será dar una opinión sobre la confiabilidad de la información que se procesa electrónicamente, tomando en consideración lo siguiente con respecto a los controles.

- Si no disminuye el riesgo, es procedimiento operativo.
- Si se disminuye el riesgo, es procedimiento de control.

A. Integridad

Este objetivo persigue que todas las operaciones:

- Se registren íntegramente.
- Se suministren al sistema.
- Actualicen los diferentes archivos manejados en la aplicación.
- Se consideren en los procedimientos de cálculo, totalización, etc.

Es importante considerar la retroalimentación de errores, omisiones y correcciones para cada fase.

B. Precisión

Este objetivo persigue que los datos importantes de cada operación o actividad sean correctos:

- Inicialmente: manualmente, automáticamente.
- Cuando han alimentado a la computadora.
- Al actualizar los diferentes archivos manejados en la aplicación.
- Al considerarse por los procedimientos de cálculo, totalización, categorización.

C. Autorización

El control primario de una operación dada, es el acto de su autorización, la que consiste en que alguien, comparándola con los planes, condiciones, limitaciones o conocimiento general de lo que constituye una operación correcta, decide si es o no válida; el acto debe ser ejecutado por una persona reconocida en el sistema establecido como quien tiene la facultad y el nivel jerárquico para hacerlo.

D. Continuidad

Este objetivo persigue que las operaciones / actividades, permanezcan completas y exactas en el tiempo.

E. Oportunidad

Este objetivo persigue que el registro de las operaciones / actividades y la información que se produce sea oportuna en su registro y en la emisión de reportes para la toma de decisiones.

F. Beneficio

Este objetivo persigue que la información que se produce sea útil para la toma de decisiones.

Prinicipales técnicas de control

Chequeo de secuencia numérica

El mejor medio para asegurarse de que al procesar las operaciones no se escape alguna de ellas, es numerarlas para, después de procesadas, compararlas (se enumeran previamente los documentos/ operaciones).

- Chequeo de uno por uno, reportes de cómputo contra documentos fuente.
- Comparación contra datos pre-registrados.

El documento de una operación puede anexarse a otro como evidencia y validez, por ejemplo, la factura del proveedor, que puede acompañarse con informes de recepción y la orden de compra.

Algunos datos pueden compararse con estándares predeterminados o listas de normas establecidas.

- Comparación de totales de control.
- De documentos.
- De renglones.
- De importes.
- De cualquier campo numérico (número de cuenta, folio, número de parte, utilidades, etc.).
- Dígito verificador.

El totalizar ciertos números claves antes y después de procesar todo un grupo de operaciones, es una forma tradicional de asegurarse de que todas se han procesado. Por supuesto, subsiste la posibilidad de errores compensados, pero esta posibilidad es una posibilidad remota.

Algunas medidas de control, consisten en comparar una cifra con otra que se ha determinado independientemente, lo que con frecuencia requiere también una conciliación.

Conciliaciones bancarias. Consisten en la conciliación de la suma de los saldos detallados del auxiliar, con el saldo global de la cuenta de control (de mayor); los recuentos físicos de caja (arqueos), de valores, de inventarios o de otros activos; así como la confirmación directa de saldos de deudores y de acreedores.

El cálculo del dígito verificador involucra la multiplicación de cada uno de los dígitos del código original por cierto factor de ponderación, la suma de estos resultados y luego la división de esta suma por un número que representa el valor del módulo. Finalmente, se resta el valor del módulo del residuo de la división anterior. El analista de sistemas, elige la ponderación y el módulo a utilizar.

Por ejemplo, cuando el número de cuenta de un estudiante de la UNAM o el RFC que contiene la homoclave de la persona o institución dada de alta (ya que se puede

repetir el nombre y apellidos de la persona e inclusive la fecha de nacimiento) ésta es la herramienta utilizada.

Se toma un número al azar para ponderar. (Código Original).

700534

Opcionalmente, si así lo consideras, puedes darle vuelta a la numeración, como se puede hacer en una dirección de INTERNET.

435007

Y los vamos a multiplicar por cualquier factor o serie de números.
Por ejemplo: la serie de 2, 3, 4, 5, 6, y 7.

Entonces quedaría de la siguiente forma.

4 X 2= 8
3 X 3= 9
5 X 4= 20
0 X 5= 0
0 X 6= 0
7 X 7= 49

A continuación, se debe realizar la suma para obtener el resultado:

8+9+20+0+0+49= 86.

Como es en la mayoría de los casos un Estándar, se utiliza el dígito 11.

Entonces el 86 se divide entre 11 y se obtiene: 86/11= 7

Entonces se continúa utilizando el digito 11 y el resultado anterior se le resta a este dígito.

11-7=4
Por lo tanto, el dígito verificador es el 4.

Si fuera el caso que el resultado está entre el 1 y el 9 ese es el dígito verificador; si da como resultado 11 esto es igual a 0 y 10 es igual a K.

Los tipos de errores que puede detectar son:

- Sustitución de dígitos.
- Transposición de dígitos.

El enfoque de dígito verificador es útil cuando los códigos originales son de 5 o más cifras.

Verificación de razonabilidad.

- rangos, por ejemplo, tabuladores de sueldos.
- constantes, por ejemplo femenino/masculino, sí / no, etc.

- Verificación del formato, sintaxis (naturales: campos numéricos, alfabéticos, alfanuméricos y longitud de campos).

- Chequeo de generaciones de archivos (abuelo, padre, hijo).

- Reproceso selectivo de partidas.

El mismo que ejecuta una operación puede checarla, pero se asegurará más el control y la verificación interna si lo hace otra persona / programa de cómputo.

- Control de pendientes

Otra verificación bastante común de que todo se registra, consiste en listar las operaciones o conservar un expediente con copia de los documentos que las originan y tachar de las listas o retirar de los expedientes las operaciones que se van procesando. Sin embargo, estos archivos o expedientes de asuntos no terminados o pendientes, requieren para su funcionamiento efectivo y para que constituyan una medida de control, ser revisados periódicamente para tomar las medidas procedentes y no dejar en ellos asuntos pendientes por demasiado tiempo.

- Lista de recordatorio

Ejemplos típicos de estas listas, son los archivos de facturas o cuentas por pagar por fecha de vencimiento o los calendarios de obligaciones fiscales.

Disciplinas sobre los controles básicos

A tres actividades de control se les ha dado la categoría de “disciplinas”, incluyendo los controles básicos y sus resultados. La disciplina es importante porque ofrece una razonable seguridad de que las operaciones básicas y de control funcionan o se ejercen tal como fueron diseñadas.

Las disciplinas sobre los controles básicos son aquellos aspectos de un sistema que aumentan la confianza de que los controles básicos operan adecuadamente.

Las disciplinas sobre los controles, además, incrementan la seguridad de que los errores se detectan oportunamente.

Las disciplinas sobre los controles básicos son:

- Segregación de funciones.
- Adecuada custodia de activos; es decir, acceso controlado o restringido.
- Supervisión.

Segregación de labores / funciones.

En un ambiente de P.E.D.[2] es importante considerar la segregación de funciones del personal que labora en el área de informática.

En la segregación de labores, el trabajo de una persona actúa como medida disciplinaria o de verificación de otra. El acceso controlado o restringido, es una disciplina necesaria, para prevenir actividades no autorizadas de cualquier índole, desde la pérdida o mal uso de los activos, hasta la pérdida o mal uso del libro mayor.

La separación de una actividad de otra tiene varios propósitos: aparte de los objetivos de control, facilita la especialización de labores y del personal que las ejecuta.

No obstante, debe medirse el costo relativo en cada caso: normalmente, sólo se obtiene eficiencia con la segregación de labores cuando el volumen de operaciones justifica la especialización.

Lo que se quiere establecer es la supervisión de actividades a través de operaciones simultáneas que requieren y se entrelazan una con la otra.

[2] Procesamiento Electrónico de Datos.

La correcta distribución de labores a través de niveles jerárquicos diferentes que intervienen desde el inicio hasta el fin de una actividad, disminuye el grado de ocurrencia de un riesgo; es decir, para cometer un acto indebido forzosamente tiene que haber involucramiento de más de una persona en tal operación.

Acceso controlado o restringido

Se refiere a la seguridad física, tanto del efectivo, inventarios, activo fijo, documentos, libros, reportes, formas, archivos del computador en medios magnéticos, etc.

Es muy común pensar en la restricción del acceso con relación a activos disponibles como dinero, valores y algunas veces inventarios y otros activos que pueden ser fácilmente vendibles o de uso personal. Sin embargo, debe aplicarse también a los libros y registros contables y a los medios con que pueden alterarse, como serían las formas en blanco de pólizas, cheques, placa autográfica de cheques, archivos, sala de computación, archivos de cintas de computador o cualquier otro elemento del sistema. Los sistemas y las normas de disciplina deben procurar limitar el acceso, a estos medios, al personal competente y responsable.

Finalmente, las medidas físicas de seguridad deben también proteger los archivos y registros contra deterioro, destrucción o pérdida.

Supervisión

Probablemente es la disciplina más importante sobre los controles básicos, ya que aumenta la confianza en la información.

La supervisión del sistema y de quienes lo operan, tiene un efecto obvio en la exactitud y en la confiabilidad.

1. Controles integrados o verificación interna por supervisión

Por ejemplo, quien autoriza un pago debe cerciorarse de que los documentos estén firmados o iniciados por el personal apropiado en sus diferentes procesos y el pago no podrá hacerse (excepto por descuido) sin esa autorización.

2. Controles superimpuestos o supervisión administrativa

Los supervisores o administradores normalmente deben asegurarse de que el personal atienda adecuadamente sus funciones.

Sin una supervisión adecuada, se corre el riesgo de que aún los mejores sistemas y control se vuelvan erráticos y no confiables en poco tiempo; ya que con la presión normal del trabajo, tienden a distorsionarse las rutinas y el personal busca formas más fáciles para hacer su tarea.

La falta de supervisión puede detectarse, aún en sistemas bien diseñados, por problemas en las cuentas, como un desusado número de errores y excepciones, retraso en el trabajo, cuellos de botella en los registros, y el abandono de procedimientos prescritos.

ALGUNOS INDICADORES DE ERROR

- Voluminosos listados de transacciones rechazadas por el computador (listados de validación) y el análisis de las causas de error (estadísticas por tipo de error y frecuencia).
- Análisis financiero.
- Razones Financieras.
- Variaciones.
- Porcentajes Integrales.

PISTA DE AUDITORÍA

Definición- Son todos aquellos elementos que permiten reconstruir los eventos ocurridos, es decir, los hechos.

- Controles y pistas de auditoría que garanticen un resultado confiable.
- Alcance, naturaleza y control interno.
- Todas las técnicas de control.

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 normativa 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. [3]

Esta división es según el IMCP.

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,

[3] Instituto Mexicano de Contadores Públicos. (2013). *Normas y procedimientos de auditoría y Normas para atestiguar y otros servicios relacionados versión estudiantil*. (3ª ed.) México: IMCP.

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.

Entonces, cuando se lleva a cabo este tipo de trabajo, se debe tener en cuenta que la revisión debe consistir en realizar pruebas que coadyuven a la atención e interpretación de cómo la administración procura los controles en materia de informática y cómo se tienen constituidos, así como su grado de cumplimiento y eficacia.

5.5. Definición de pruebas sustantivas

Las pruebas sustantivas de acuerdo al libro de *Normas de Auditoría*, el IMCP las define como sigue:

> Consisten en comprobaciones diseñadas para obtener la evidencia de la validez y propiedad de las transacciones y saldos que componen los estados financieros. Estas incluyen comprobaciones de detalles, como las aplicaciones de muestreo, y procedimientos de revisión analítica, cálculo, investigación, etc. El auditor diseña dichas pruebas para detectar errores o fraudes en los saldos de las cuentas de los estados financieros.

> Las pruebas sustantivas son definidas como pruebas de detalles y procedimientos analíticos ejecutados para detectar posibles violaciones, errores u omisiones en las transacciones. [4]

Si bien esta definición se basa específicamente en transacciones financieras, con respecto al ámbito de la auditoría en informática su significado es más amplio, debido a la división y los diferentes tipos de auditoría.

Pasos a seguir para la aplicación de las pruebas sustantivas:

- Definir los objetivos:

Este paso consiste en la determinación del objetivo de la prueba, el alcance de la prueba y la prospectiva de los resultados esperados, para posteriormente compararlo contra los resultados obtenidos.

- Preparar los datos de prueba

Para este efecto, se tiene que contar con el análisis de la información previa y la realización de cédulas de prueba, ya sea de sistemas, procedimientos y/o de operaciones que se vayan a llevar a cabo con base en lo que se debe realizar y lo que realmente se obtiene del producto a probar.

- Calcular los resultados previstos para el procesamiento

[4] Instituto Mexicano de Contadores Públicos. (2013). *Normas y procedimientos de auditoría y Normas para atestiguar y otros servicios relacionados versión estudiantil*. (3ª ed.) México: IMCP.

Al analizar los resultados esperados, debemos realizarlos bajo un ambiente controlado que permita asegurar que el resultado es confiable y se efectuó en una circunstancia específica.

- Procesamiento de los datos de prueba.

Cuando se lleva a cabo la prueba, se busca que los datos introducidos sean reales y que se trabaje con una pista de auditoría (ésta consiste en una réplica del sistema o proceso a auditar) que permita obtener resultados confiables y veraces.

- Comparación de los resultados de las pruebas realizadas contra los producidos por el procesamiento real

Los resultados obtenidos, se deben comparar contra los esperados, y se deben analizar si es que hubo variaciones, de existir éstas debe analizar las causas que originaron esta variación y, si es necesario, repetir la prueba en circunstancias controladas que permitan un resultado óptimo de las pruebas.

- Resolver las excepciones.

Este paso consiste en proponer nuevas guías de acción que permitan conocer los distintos escenarios en que se realiza una prueba, ya sea con ambiente controlado o no, y el origen de las variaciones; pero, sobre todo, dar una solución a las posibles variaciones.

5.6. Evaluación de los sistemas de acuerdo al riesgo

La importancia de conocer los riesgos inherentes de una institución, es porque, derivado de ello, se puede realizar una buena planeación y una excelente evaluación de riesgos de detección y riesgo de control; para conocer mejor los riesgos se mencionan a continuación sólo algunos conceptos de ello:

- Es una condición o evento incierto que, en caso de ocurrir, tiene un efecto negativo en los objetivos de un proyecto (Gray and Larson, 2009: 38).
- Es un conjunto de circunstancias que afectan negativamente el logro de los objetivos de una organización (Griffths, 2009: 589).
- Es la combinación de la probabilidad de que ocurra un evento y la magnitud de sus consecuencias (Organización Internacional de Estándares, ISO).

Para evaluar los sistemas con base en el riesgo, se debe tomar en cuenta qué es riesgo y qué no es riesgo:

Lo que **sí es riesgo**.

- *Software* y/o *hardware* desarrollados o adquiridos que incumplen con los estándares de calidad.
- Proveedores seleccionados sin ser los más adecuados.
- Usuarios conectados y desconectados ilícitamente a la red y sus aplicaciones.
- Información privilegiada filtrada ilegalmente a proveedores de recursos informáticos.
- Proveedores y funcionarios coludidos en la asignación de contratos de *software*, *hardware* y telecomunicaciones.

- ❖ Informes anuales elaborados con información sesgada o incompleta para la correcta toma de decisiones.
- ❖ Bases de licitaciones para servicios informáticos elaboradas de forma incompleta o incorrecta.
- ❖ Sistemas informáticos necesarios no desarrollados por el departamento de TI.
- ❖ Personal para desarrollo de sistemas contratado en exceso sin funciones sustanciales.

- ➢ Ejemplos **INCORRECTOS** de la redacción de un riesgo:

  - o Impunidad de los funcionarios responsables de la administración de los recursos informáticos.

    - ▪ NO ES RIESGO, sino el resultado de una inacción.

  - o Corrupción en el otorgamiento o adjudicación de recursos informáticos.

    - ▪ NO ES RIESGO, sino una dimensión y una causa subyacente de riesgo.

  - o No cumplir con los objetivos de los programas informáticos.

    - ▪ NO ES RIESGO, sino una consecuencia genérica del riesgo.

  - o Inadecuada aplicación de la normativa, ya sea interna o externa, por desconocimiento o interpretación indebida.

    - ▪ NO ES RIESGO, sino un factor de riesgo.

(Un factor de riesgo es una circunstancia asociada con el incremento en la probabilidad de que se materialice un riesgo.)

Algunos ejemplos de factores de riesgo:

- Excesivas adjudicaciones directas o invitaciones a tres personas cuando la normativa interna o externa marca restricciones para ello.
- Insuficiente personal capacitado para supervisar y administrar los recursos informáticos.
- Personal carente de conocimiento técnico especializado en materia informática.
- Lagunas en la normatividad del o los procedimientos de usos eficiente de los recursos informáticos.
- Bases para adjudicación de recursos informáticos sesgadas o dirigidas a proveedores específicos.
- Sistemas de información obsoletos, en desuso o de difícil aplicación.
- Incentivos insuficientes para el personal que administra los recursos informáticos.
- Deficiencias en el diseño conceptual y operativo del o los programas informáticos, ya sea en su administración o en su aplicación.
- Sistema informático deficiente a las necesidades de la institución auditada.

- Plan de desarrollo informático institucional no apegado a las necesidades de la Institución.

- Supervisión deficiente por parte del personal de mandos superiores.

Ahora bien, como auditores, podemos contar con el riesgo de que, en un momento dado, una situación importante o relevante no haya sido observada y por consecuencia se puede presentar un riesgo en la apreciación del trabajo e informe final; sin embargo, es importante señalar que tal situación debe formar parte de los riesgos inherentes a la auditoría.

5.6.1 Investigación preliminar

Dentro de este tema se determinará con base en el alcance de la auditoría la información que se va a solicitar a la institución o cliente, que permitirá desarrollar el trabajo del auditor, dependiendo de cuál tipo de auditoría se realizará.

Aunado a lo anterior, se presenta a continuación alguna información a desarrollar o a solicitar a la institución.

ENFOQUE DE AUDITORÍA

Antecedentes

- Configuración del *hardware.*
- *Software* disponible.
- Organigramas de las áreas usuarias y de informática.
- Normativa interna y externa.

CONOCIMIENTO DEL AMBIENTE

Algunas de las herramientas a utilizar para documentar el conocimiento y evaluación de los controles en los sistemas de información computarizados, tanto en lo que se refiere a los procedimientos manuales como automatizados, son:

- Los flujogramas panorámicos. Se debe conocer la simbología de

diagramación. (Se sugiere documentar separadamente el conocimiento de los procedimientos manuales y computarizados).

- La descripción narrativa complementaria de controles de manuales y computarizados.
- El diseño de los principales archivos de datos.
- La matriz de control.

FUENTES DE INFORMACIÓN

- Análisis de documentación actualizada (manuales de procedimientos y de sistemas).

- Entrevistas de personal que conoce las diferentes partes del sistema (usuarios, mesa de control y líder en desarrollo y mantenimiento de sistemas).

FACTORES DE INFORMACIÓN.

- Análisis de documentación actualizada (manuales de procedimientos de sistemas).
- Entrevistas de personal que conoce las diferentes partes del sistema (usuarios, mesa de control y, líder en desarrollo y mantenimiento de sistemas).

FACTORES QUE AFECTAN LA ENTREVISTA.

- Elección del personal adecuado para entrevistar.
- Familiarización con el sistema, documentos y reportes.
- Explicación de los objetivos e indicación de la duración aproximada de la entrevista al entrevistado, así como la razón de haberle elegido para

entrevistarlo. El uso del tiempo del auditor y del auditado es un factor muy importante a controlar.

- Haga del conocimiento del entrevistado lo que hará con la información y asegure confidencialidad.
- Comenzar con preguntas y comentarios generales no comprometedores y después equilibrar la cantidad y orden de preguntas abiertas, cerradas y de sondeo, evitando preguntas tendenciosas. Mencione el grado de detalle que desea obtener en las respuestas y haga énfasis en los procedimientos de control.
- Manejo adecuado del comportamiento verbal y no verbal (corporal / actitudes).
- Contacto visual: Mirar al inicio de un tema / pregunta al interlocutor, durante el desarrollo mirar alrededor y al concluirlo mirar nuevamente al interlocutor. Una mirada persistente incomoda.
- Movimiento de las manos: El estrechar firmemente la mano ayuda a establecer credibilidad y confianza. Las manos colocadas sobre la frente o cara son señal de que se intenta ocultar la verdad o revelar más de lo debido. Los dedos en contacto yema con yema denotan confianza en sí mismo.
- Vestimenta apropiada en apego a las normas de la cultura organizacional.
  - Control de reacciones emotivas.
- Gesticulación apropiada: Entusiasmo, interés, etc.
- Voz: No demasiado elevada ni baja de volumen. Claridad al hablar, sin prisa.
- Parafrasear en aspectos complejos o dudosos: Repetir en palabras propias.

DIAGRAMAS DE FLUJO

Un diagrama de flujo sirve principalmente para facilitar la comprensión, evaluación y comunicación de los procedimientos, mediante la expresión de los mismos en forma gráfica, concisa y completa.

El diagrama de flujo permite al auditor identificar aspectos de control, fortalezas y debilidades, en los sistemas de información y destacarlos. Para su aplicación se requiere tiempo y uso frecuente como herramientas de trabajo.

Ventajas.

a) Requieren menos tiempo que las descripciones narrativas.
b) Representan más fácilmente el flujo de las operaciones.
c) Reducen el riesgo de malas interpretaciones por el estilo de redacción y la capacidad de síntesis.
d) Son más fáciles de actualizar, principalmente cuando se elaboran con herramientas para PC.

Para obtener los beneficios de la elaboración de diagramas de flujo se deberán mostrar:

- Los procedimientos / actividades en secuencia y en líneas de flujo, paso por paso desde su iniciación hasta su término. Especialmente las actividades de control: los que disminuyen riesgos, como son las autorizaciones, la conciliación de cifras control, etc. Los procedimientos manuales y los computarizados.

Deben destacarse las diferencias en las actividades de control en operaciones del mismo tipo, cuando éstas son procesadas en diferentes localidades o por diferentes personas.

Cada actividad debe ser numerada secuencialmente.

- La documentación / informes generados en las diferentes secciones, departamentos, áreas de la empresa (obteniendo) fotocopia de las hojas que sean diferentes.
- Todas las copias de los documentos y su flujo correspondiente.

  N= Foliada
  0= Original
  1= Copia número 1
  2= Copia número 2
  3= Copia número 3
  Azul= Copia azul
  Rosa= Copia rosa
  Etc.

- Los archivos de documentos / transacciones significativas en medios manuales:

  N= Numérico.
  A= Alfabético.
  C= Por fecha o cronológico.

Las letras se pueden indicar en minúsculas cuando los archivos son temporales y en mayúsculas cuando son permanentes.

- El nombre del puesto y, cuando sea significativo, el nombre de las personas

que ejecutan el procedimiento.

Algunos otros criterios recomendables al preparar los diagramas de flujo son:

- En la preparación de los diagramas deben usarse símbolos, cuyo significado más común se muestra al final de este documento.
- De preferencia se deben elaborar utilizando paquetes para diagramación en PC, o bien, utilizando plantillas de diagramación y a lápiz.

- Se debe considerar la claridad, buena organización y simplicidad en la presentación. Evitar gráficas excesivamente complejas.

La experiencia dicta que un diagrama debe ser reorganizado a medida que se cuente con más información.

Primero se puede preparar un diagrama de flujo panorámico y, adicionalmente diagramas de flujo de cada operación / procedimiento por separado.

Deberá conocerse y documentarse el flujo de una operación o procedimiento a la vez, para llegar a una conclusión lógica (segregación).

El grado de subdivisión en un diagrama (S) depende de la diferenciación de las funciones que se realizan o controlan.

La bifurcación se puede manejar por medio del uso de conectores de hoja o página, minimizando la referenciación.

- Se puede incluir una breve descripción por separado y con referencias cruzadas al diagrama de las actividades complejas y de control, mostrando aspectos como son:

- Límites de autoridad.
- División de labores.
- Evidencia del ejercicio de controles.
- Naturaleza del proceso.
- Se deben titular cada diagrama y numerar cada una de las hojas.
- Se debe explicar cada una de las abreviaturas y marcas empleadas.
- Proporciona un mejor entendimiento los diagramas de forma “horizontal”, para ser leído de izquierda a derecha a lo ancho de la hoja, anotando la explicación en la última columna de la derecha.
- Se recomienda la utilización de formatos estándar.
- Se debe verificar el entendimiento de los procedimientos con los responsables, obteniendo aprobación.
- Se debe mantener un ejemplar de cada versión de los procedimientos; es decir, conservar los anteriores cuando se actualicen como registro permanente.

La información necesaria para la preparación / actualización de los diagramas de flujo, se obtiene por medio de entrevistas al personal operativo y de niveles de mando, así como mediante el análisis de los manuales de procedimientos. A continuación, se proporciona una guía para la obtención de la información:

- Identifique a la persona adecuado para la entrevista.
- Elabore previamente un cuestionario básico.
- Esté alerta a actividades / operaciones poco frecuentes pero que pudieran ser claves.
- Analice los efectos del exceso de actividad / detalle, ausencias o cambios de rutina.
- Considere las consecuencias de la demasiada simplificación.

- Pregunte al personal entrevistado:

    - Los procedimientos / actividades que realiza.
    - Los registros que mantiene bajo su control.
    - Los documentos que prepara y procesa.
    - De quién recibe documentos, cuáles y de qué manera.
    - A quién envía los documentos, cuáles y de qué manera.
    - Qué métodos utiliza para detectar errores, de qué naturaleza han sido y con qué frecuencia aproximada. Cuál y cuando fue el último error detectado.
    - Qué hace para corregir errores descubiertos.

En las auditorías recurrentes o de seguimiento también deben tomarse en cuenta los siguientes aspectos:

- Las recomendaciones de auditorías anteriores, cuándo se adoptaron y cuáles fueron sus efectos.
- Las recomendaciones no adoptadas y su justificación.
- Los cambios a los procedimientos, por ejemplo, la automatización de labores.
- Cambios en la situación o estrategias generales de la empresa. Hechos relevantes en la organización.

ELEMENTOS DE LOS FLUJOGRAMAS DE LOS PROCEDIMIENTOS MANUALES

- Departamentos o áreas involucradas.
- Documentos fuente.
- Reportes / Informes elaborados manualmente.
- Procedimientos de control.

Nota: Es conveniente solicitar copia de los documentos fuente (llenados) y de una hoja de los reportes preparados manualmente. También se recomienda mencionar el volumen promedio de operaciones e impacto monetario en sistemas financieros importantes.

ELEMENTOS DE LOS FLUJOGRAMAS DE LOS PROCEDIMIENTOS COMPUTARIZADOS

- Archivos maestros (Diseño de registros y periodicidad de respaldo y medio de almacenamiento).
- Principales archivos de transacciones (diseño de registros y periodicidad de respaldo y medio de almacenamiento).
- Documentos fuente (nombre y procedencia).
- Reportes generados con el computador (nombre y distribución)
- Breve descripción de los procedimientos de:

    - Validación.
    - Cálculo (Incluye totalización y categorización).
    - Actualización.

EVALUACIÓN DE CONTROLES

Matrices de control / Cuestionario de control interno.

Las matrices de control son una nueva clase de herramientas para evaluar los riesgos en los sistemas de información computarizados y el grado de cobertura de los objetivos de control.

Ventajas sobre los cuestionarios de control interno:

- Son más flexibles.

- Presentan más claramente el panorama de control en el sistema.

Se deben preparar matrices de control para evaluar por separado la etapa de entrada, la de proceso y la de salida de datos.

REGISTRO DE DEBILIDADES DE CONTROL (RDC)

El propósito del RDC es encontrar en un sólo documento:

- La descripción de todas las debilidades importantes.
- Las repercusiones de la debilidad.
- Las alternativas de solución sugeridas.
- El resultado de la discusión de dichas debilidades y nombre y puesto del responsable.

Cada debilidad incluida en el RDC debe ser referenciada a la matriz de control / cuestionario de control interno, o al resultado de las pruebas de cumplimiento, en el caso de excepciones no aclaradas.

PROGRAMA DE PRUEBAS DE CUMPLIMIENTO

Se deben probar los controles referenciados en la matriz de control (es decir, aquellos que en apariencia existen) y cuantificar el posible efecto de las debilidades.

COLUMNAS DEL PROGRAMA DE PRUEBAS DE CUMPLIMIENTO

- Descripción de la prueba.
- Alcance.
- Referencia a papeles de trabajo (índice de cédulas analíticas).
- Control de excepciones:

- Totales.
- Aclaradas.
- No aclaradas.

CONSIDERACIONES PARA DECIDIR REALIZAR PRUEBAS CON LA COMPUTADORA

- Alcance.
- Carencia de información en papel.
- Búsqueda de excepciones.
- Establecimiento del margen de tolerancia de error.
- Control del número de casos a imprimir.
- Cuantificación del efecto total (en importe y cantidad de casos).
- Porcentaje total de desviación (en importe y cantidad de casos).
- Oportunidad de las pruebas de acuerdo a la frecuencia de respaldos de archivos en medios legibles por el computador.
- Personal de auditoria capacitado.
- Disponibilidad de tiempo máquina.

EJEMPLOS DE PRUEBAS CON LA COMPUTADORA

Facturas / Cuentas por cobrar.

- Estratificación de cartera.
- Confirmación de saldos.
- Cobros posteriores.
- Comparación de catálogos de clientes de dos periodos (altas, bajas y cambios).
- Saldos contrarios.
- Saldos superiores al límite de crédito.

- Antigüedad de saldos.
- Sumarización de ventas por mes.
- Verificación de listas de precios.
- Cálculos de las facturas.

Inventarios.

- Estratificación del inventario.
- Saldos contrarios.
- Lento movimiento.
- Artículos con existencia y sin costo unitario.
- Costos fuera de mercado.
- Valuación de inventarios.

Nóminas:

- Empleados fuera de tabulador.
- Comparación de catálogos de empleados de dos periodos (altas, bajas y cambios).
- Recálculo de la nómina.
- Empleados con recepciones netas abajo del mínimo.

Cómo se puede apreciar en el tema desarrollado, sólo se presentan algunos aspectos importantes a considerar en el desarrollo de la auditoría, referente a la etapa de investigación preliminar.

5.8. Definición de equipo de auditoría

En esta etapa, se debe
definir el personal y los perfiles del mismo que son considerados los más aptos para cumplir el objetivo de la auditoría.

Cuando se establece un equipo de trabajo se tienen que tomar en cuenta los siguientes aspectos:

Los integrantes del equipo deben saber que la suma de las partes, nos da como resultado un todo; esto es, que cada integrante, tiene la misma importancia en el desarrollo de las actividades, ninguno cuenta con situación privilegiada ni alguien en el equipo representa más ni otros menos.

La información que maneja cada integrante debe ser del conocimiento de los demás, ya que entre más informado esté el equipo, menor el riesgo de que se les pase alguna situación importante durante la auditoría.

Un equipo tiene que pasar de ser un grupo a un equipo y esto se logra a través de la confianza.

Por lo tanto, lo que se busca al establecer equipos de trabajo es que compartan conocimientos, habilidades y experiencias complementarias y que, comprometidos con un propósito común, se establecen metas realistas, retadoras y una manera eficiente de alcanzarlas también compartidas, asegurando resultados oportunos,

previsibles y de calidad, por los cuales los miembros se hacen mutuamente responsables.

Para realizar una auditoría de forma clara, se debe establecer un programa de trabajo claro que presente las actividades a desarrollar por cada uno de los integrantes del equipo y el tiempo para cada actividad, por lo que los auditores deben entender lo siguiente:

- 🕮 Cada integrante del equipo desarrolla tareas diferentes que, al sumarlas, producen un trabajo completo.

- 🕮 Se requiere, como en cualquiera actividad, que la autoridad se delegue y la responsabilidad se comparta.

- 🕮 Todas las actividades deben desarrollarse a través de una planeación.

Cada actividad debe contar con un objetivo específico de realización.

No se trata solamente de objetivos operativos; sino también de valores de comportamientos.

Habiendo integrado ya su competencia técnica y su capacidad de escucharse mutuamente, los miembros de un equipo se centran en la elaboración de esta visión compartida y el reajuste continuo del papel de cada uno y del equipo a esta propia visión, constantemente reactualizada en función de la evolución de la realidad que se tiene alrededor.

El desarrollo de la auditoría en informática 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 auditada.

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 auditor y cómo se evaluará su desempeño.

RESUMEN

La fase de planeación de auditoría es muy importante ya que en ella se determinará el alcance y objetivo de la auditoría, como auditores planearemos qué es lo que vamos a realizar, el personal a utilizar, el tiempo y el costo-beneficio para realizar la auditoría, ya que se deben tomar en cuenta para la planeación que ésta sea medible, comprensible, medible y cuantificable.

En la revisión preliminar, se procederá a conocer la empresa y de ser posible, se validará la problemática que fue expuesta por el cliente, si es que esto ocurrió. Después de esta fase se estará en posibilidades de hacer una mejor estimación del tiempo y de los honorarios, si es que no lo pudo hacer en la fase de planeación.

El diagnóstico de la información auxilia a identificar áreas u operaciones con problemas para adoptar acciones preventivas; es una de las primeras labores del auditor en informática, debido a que la contratación de los servicios de auditoría en informática se puede dar porque el cliente o institución ya conozca la problemática, o porque el auditor en informática le deba realizar un diagnóstico y éste le detecte la misma problemática u otra no contemplada por el cliente.

La etapa de definición de pruebas de controles y sustantivas son importantes, ya que se entra de lleno a la auditoría en la etapa de ejecución; asimismo, es imperativo reconocer que en esta etapa se va a poner en evidencia el talento del auditor, debido a que las pruebas tendrán características específicas para obtener resultados de alguna de las funciones de informática.

La auditoría basada en riesgos nos auxilia para reconocer la importancia de los riesgos inherentes de una institución, porque, derivado de ello, se puede realizar

una buena planeación y una excelente evaluación de riesgos de detección y riesgo de control; para conocer mejor los riesgos se mencionan a continuación sólo algunos conceptos de ello:

La investigación preliminar auxiliará para establecer el alcance de la auditoría con base en la información que se va a solicitar a la institución o cliente, que permitirá desarrollar el trabajo del auditor, dependiendo cuál tipo de auditoría se lleve a cabo.

Para definir el equipo de auditoría, se debe contar con la capacidad para determinar el personal y los perfiles del mismo que son considerados los más aptos para cumplir el objetivo de la auditoría.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

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

Gray, C.F., & Larson, E.W. (2009). *Administración de proyectos* (4ª Ed.). México: McGraw-Hill.

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

Piattini, Mario y Emilio del Peso (2001). *Auditoría informática, un enfoque práctico* (2ª. Ed.). España: Alfa-Omega.

Griffiths, A. (1999).”Organizational Interventions: facing the limits of the natural science paradigm”. *Scandinavian Journal of Work,* Environment and Health, 25, 589-59.

Bibliografía Complementaria

Solís Montes, Gustavo Adolfo (2002). *Reingeniería de la auditoría en informática.* México: Trillas.

Weber, Ron (1998). *EDP Auditing: Conceptual Foundations and Practice*. México: McGraw-Hill.

Sitios de Internet

Sitio	Descripción
http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf	AUDITORÍA DE SISTEMAS
http://fcaenlinea1.unam.mx/informatica/file.php/67/unidad04/index.html	AUDITORÍA DE SISTEMAS

Licenciatura: Informática

UNIDAD 6

Evaluación de los recursos informáticos

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno identificará las áreas de la organización en las que se puede aplicar la auditoría informática utilizando las metodologías vistas anteriormente.

TEMARIO DETALLADO

(14 horas)

6. Evaluación de los recursos informáticos

- 6.1. Evaluación del personal involucrado
- 6.2. Entrevistas con el personal involucrado
- 6.3. Recopilación de la información organizacional
- 6.4. Características de la información
- 6.5. Desarrollo de pruebas de controles
- 6.6. Documentación de pruebas
- 6.7. Marcas de auditoría
- 6.8. Estándares de documentación
- 6.9. Interpretación de la información
- 6.10. Comparación con las mejores prácticas

6.11. COBIT

6.12. ITIL

6.13. ISO

INTRODUCCIÓN

Es importante conocer los elementos básicos para poder desarrollar mejor el trabajo de auditoría, por ello el conocimiento y habilidades del personal involucrado y las actividades a desarrollar por cada persona es importante para realizar un excelente trabajo.

Por ello, la importancia de conocer las capacidades del personal que administra los recursos informáticos nos lleva a desarrollar herramientas que nos permitan obtener un escenario que presente la realidad de la institución a auditar.

Para finalmente establecer los modelos de informe y control que tendremos que plasmar y utilizar en el desarrollo de la auditoría, ya que ello permitirá exponer las fortalezas y debilidades de la institución y con el informe presentado establecer nuevos controles y auxiliar en la adecuada toma de decisiones.

6.1. Evaluación del personal involucrado

El propósito de la revisión de la auditoría en informática es 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.

Queda entonces la evaluación del personal que ejerce la administración de los recursos informáticos, esta parte es difícil, ya que, si bien existen pruebas psicológicas para realizar la contratación del personal, también es importante realizar pruebas de conocimiento y confianza, debido a la importancia y confidencialidad del manejo de los recursos informáticos, así como su guarda y custodia.

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.

El quehacer cotidiano de la auditoría en informática ha arrojado resultados poco halagadores ya que la experiencia de la mayoría de las instituciones, sean privadas o gubernamentales, indica que los beneficios obtenidos del proceso de desarrollo de los sistemas de información, que incluye *software*, *hardware* y *humanware,* son deficientes.

A continuación, se presentan algunos ejemplos:

- 🕮 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.

Todos estos enunciados son causa de la deficiencia en el personal involucrado en el manejo de los recursos.

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.
- Que el personal que administra los recursos informáticos cumpla con su cometido de forma eficiente.
- Que el personal sea capacitado constantemente.

Es recomendable que dentro de la institución exista un comité de auditoría en informática, cuya figura establezca los lineamientos para la utilización y designación de los recursos informáticos, así como la evaluación de los recursos humanos que desarrollan la actividad de la administración de los recursos informáticos.

El auditor no participa directamente en la evaluación del personal adscrito al área de informática, ya que la auditoría en informática no evalúa al personal; sino el resultado del trabajo de ellos; 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, por lo tanto, no puede emitir una opinión sobre el desempeño del personal a menos que se esté realizando una auditoría al desempeño exclusivo para el personal de informática.

Ahora bien, es recomendable que se establezcan indicadores para evaluar el desempeño de cada integrante con base en la eficiencia en el cumplimiento de las metas y objetivos, por área y en general.

Si es el caso, se verifica la función a través de la cual el encargado de la administración de la función informática elige y se allega de los recursos humanos necesarios para cumplir con los objetivos establecidos.

SOLICITAR

- Planes y programas de trabajo respecto a:

    - Reclutamiento.
    - Selección.
    - Inducción.
    - Capacitación.
    - Desarrollo.

En esta etapa, vamos a evaluar sólo el procedimiento y perfiles de puesto.

6.2. Entrevistas con el personal involucrado

Normalmente, para este tipo de procesos, se establece una serie de herramientas; entre ellas se encuentra la entrevista, el cuestionario, las declaraciones, etc. El auditor debe conocer el objetivo de la auditoría para saber cuál de aquéllas o cuál combinación de las mismas utilizará.

El auditor comienza a continuación las relaciones personales con el auditado. Lo puede hacer de varias formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad, esto se puede realizar nombrando un enlace que atienda los requerimientos de la auditoría, o solicitarlo con cada responsable de área con el objeto de analizar la información que se obtiene del área auditada.

2. A través de entrevistas, ya sean formales o informales, en las que no se sigue un plan predeterminado, dado que las preguntas ocurren conforme se desarrolle la misma o conforme a lo que el entrevistado plantee; tampoco existe un método estricto de sometimiento a un cuestionario más rígido.

La entrevista es una de las actividades personales más importantes del auditor; en ella, 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, de conocimiento, de la concepción que tiene el auditado dentro del entorno institucional; es lo que hace un auditor, interroga y obtiene información que auxilie en el desarrollo de su trabajo. 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, ya que el auditado normalmente se encuentra a la defensiva, como si el auditor quisiera obtener una confesión, pero en realidad lo que busca el auditor es que el auditado conteste sencillamente una serie de preguntas variadas, también sencillas.

Sin embargo, esta sencillez es sólo aparente, tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

6.3. Recopilación de la información organizacional

Es importante utilizar las herramientas que están al alcance del auditor para poder obtener la información necesaria que permita tener una perspectiva.

Para ello, debemos elaborar un programa que contenga los requerimientos de información de forma cronológica, con fechas de entrega por parte de la Institución, ya que esto permitirá discriminar la información útil y la inútil.

Es importante que el auditor esté consciente de que la información solicitada puede variar si nos encontramos con la siguiente problemática:

- 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 las que efectúan cambios injustificados.

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.

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.

Análisis

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

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.).

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.

Investigación

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

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).

Observación

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

Cálculo

Es la verificación de las correcciones aritméticas de aquellas cuentas u operaciones que se determinan fundamentalmente por cálculos sobre bases precisas.

Esta fase principalmente no auxiliará a reconocer las herramientas y técnicas utilizadas para la obtención de información veraz, confiable y oportuna.

6.4. Características de la información

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.

Por ejemplo, dependiendo del tipo de auditoría, las características de la información a solicitar son diferentes, he aquí algunos de ellos:

AUDITORÍA A COMPUTADORAS AUTÓNOMAS (ACA)

Este tipo de auditoría se efectúa en aquellas computadoras que, debido al grado de importancia de la información que allí se maneja, no es conveniente que estén en red.

Podremos definir este tipo de auditorías como el análisis y evaluación de la información contenida en un equipo independiente, con el fin de validar la importancia de la misma y justificar su uso de esta forma.

Se compone de las siguientes fases:

- Desarrollo.
- Controles en ambiente de computadoras autónomas.
- Controles generales.

A continuación, se desarrolla cada fase:

DESARROLLO

Básicamente, para este tipo de auditorías, analizamos y validamos el porqué existe equipo que no está en red.

El auditor deberá analizar la importancia y conveniencia de que ciertos equipos se encuentren aislados y si se justifica.

El auditor verificará:

- Concentración de funciones.

- Habilidad del manejo de una computadora.
- Reportes que emite.
- Documentación.
- Limpiado de archivos.
- Pérdida de confidencialidad.
- Acceso no autorizado.
- Mantenimiento inoportuno o deficiente.
- Ausencia de respaldos.
- Programas no utilizados.
- Programas no autorizados.
- Programas “piratas”.
- Antigüedad de archivos.
- Información sin identificación.
- Discos sin etiqueta.

6.5. Desarrollo de pruebas de controles

Continuando con el ejemplo anterior, el desarrollo de pruebas de controles establecido para este tipo de auditorías sería el que se menciona a continuación:

CONTROLES EN UN AMBIENTE DE AUDITORÍA DE COMPUTADORAS AUTÓNOMAS

Elementalmente, el enfoque de auditoría está basado en la identificación de los riesgos por la carencia o incumplimiento de los procedimientos de control.

Debemos analizar los inventarios de *software* y *hardware* de la empresa auditada, revisando como mínimo lo siguiente:

- Marca y configuración del equipo.
- *Software* utilizado.
- Sistema operativo.
- Paquetería.
- Ubicación de los equipos.
- Nombre del responsable.
- Número de inventario.
- Antivirus.
- Licencias.
- Fecha de adquisición.
- Importe del equipo.

- Nombre del proveedor.
- Garantía.
- Contrato de mantenimiento.

Para continuar con los ejemplos del desarrollo de pruebas de controles, se les presenta otro ejemplo de tipos de auditoría, ésta se llama auditoría de gestión de informática o de controles generales.

CONTROLES GENERALES

En esta fase, se realizará una revisión de aspectos frecuentes, que se toman en cuenta al empezar el uso de las computadoras, así como sus controles mínimos para justificar la independencia del equipo de cómputo.

- Configuración de los sistemas a utilizar.
- Seguridad de programas.
- Seguridad de archivo.
- Operación del equipo.
- Aquí, básicamente, el auditor debe realizar un cuestionario de control interno.
- Controles sobre operación del equipo.
- Seguridad física.
  (Mobiliario, ubicación, reguladores de voltaje, extinguidores, fundas, limpieza, etc.).
- Políticas de controles sobre la prohibición de fumar, comer, ingerir líquidos cerca de los equipos.
- Control de accesorios y papelería.
- Contratos de mantenimiento.
- Plan de contingencias.
- Controles sobre seguridad de programas.
- Establecimientos para evitar cambios no autorizados.

- Estándares y custodia de la documentación, por ejemplo, los manuales.
- Políticas para el uso y manejo del equipo.
- Procedimiento y periodicidad de respaldos.
- Medidas de seguridad física sobre los respaldos.

A la conclusión de este tipo de auditoría, estaremos en posibilidad de justificar, o no, la independencia y necesidad de contar con equipos independientes no conectados a la red de la institución, debido a la sensibilidad e importancia de la información que manejan estos equipos y los controles para su uso.

6.6. Documentación de pruebas

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.

Debido a que lo único constante en sistemas es el cambio, en esta etapa se analiza y evalúa cómo ha sido el mantenimiento de sistemas para proteger a la instalación de cambios incorrectos, no autorizados o decisiones equivocadas.

“El primer cambio surge el día en que se instala el sistema”.

El mantenimiento de sistemas se origina por los siguientes factores:

- 🕮 Cambios en la normativa interna y externa de la entidad.
- 🕮 Desarrollo tecnológico.
- 🕮 Comportamiento del entorno, competencia.
- 🕮 Costos excesivos.

Normalmente los cambios obligatorios se efectúan con menos controles, por la presión implícita, mientras que los cambios por mejoras (refinamiento, creatividad, ventajas tecnológicas) se atienden más controladamente.

Al auditor le preocupa que haya un sistema para administrar los cambios, por ejemplo, hacer los cambios por grupos o lotes pertenecientes a un mismo módulo/programa. La documentación de los cambios debiera mostrar:

- 🕮 Control numérico.
- 🕮 Fecha de implantación.
- 🕮 Persona solicitante.
- 🕮 Persona que efectuó el cambio.
- 🕮 Justificación.
- 🕮 Descripción narrativa.
- 🕮 Documentación de las pruebas.
- 🕮 Autorización formal.

Todo cambio debiera originar la actualización de la documentación correspondiente.

La conciencia de la calidad, seguridad y control, debe iniciarse en las áreas de desarrollo, contemplando un balance adecuado con la productividad de los sistemas.

Área de Control / Planeación de Sistemas.

Los objetivos de control del proceso de planeación de sistemas son asegurar que:

1.- Los proyectos de desarrollo de sistemas de información se planeen con la suficiente anticipación.

2.-Las necesidades y objetivos sean definidos adecuadamente.

3.-Se evalúen adecuada y suficientemente las desventajas, los aspectos económicos, técnicos, humanos, políticos y de operación.

4.-Los sistemas sean planeados de acuerdo a estándares.

“Si no se puede planear, tampoco se podrá hacer”.

Área de Control / Diseño de Sistemas.

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

1.- Los programas son construidos de acuerdo con las especificaciones aprobadas por el usuario en la etapa de diseño del sistema.

2.- Los programas son desarrollados con base en especificaciones detalladas por programa.

3.- Los sistemas son verdaderamente probados / documentados.

4.-Los usuarios son adecuadamente entrenados.

5.- El sistema está de acuerdo a estándares.

La participación del autor de sistemas de información en el proceso de desarrollo se basa en la siguiente afirmación:

“La detección y corrección de controles inadecuados o incompletos durante la fase de diseño ahorrará tiempo y dinero cuando el sistema está operando”.

A continuación, se presenta un ejemplo referente al Programa de Pruebas de Nóminas.

Número de Prueba	Descripción	Resultados Esperados	Observaciones
1	Evalúe los controles existentes sobre los pagos de sueldos a trabajadores en sucursales u otras localidades donde la compañía tiene operaciones, así como en la casa matriz.	Verificar si el proceso de la nómina es centralizado o descentralizado, analizando los controles establecidos por los usuarios para el envío proceso y pago de la nómina.	

2	Antes de iniciar el programa de prueba al sistema de nóminas, estudie y evalúe el control interno alrededor del sistema y asegúrese de entender la mecánica de operación al sistema de nómina.	Identificar el flujo de operaciones en el área (entradas-proceso-salida) su integración en el sistema, y aquellos controles supletorios que en su conjunto soporten un adecuado nivel de confiabilidad sobre los productos obtenidos por el sistema.	
3	Identifique los procedimientos utilizados por los usuarios, para el control de cifras iniciales previas al del proceso de nómina.	El usuario debe mantener controles necesarios para asegurar que las entradas aprobadas son procesadas por el sistema, tales como: ❖ Cifras control por lote. ❖ Control numérico de los movimientos. ❖ Fecha de preparación. ❖ Recuento de documentos. ❖ Formatos preestablecidos. ❖ Registro de movimientos.	

Responsable de las pruebas. JJAB	Fecha de las pruebas. 19/03/2XXX…	Avalo resultados de las pruebas. PRC

Elaboración propia.

Con el cuadro anterior se presenta sólo una parte o ejemplo de cómo se elaboran las pruebas dependiendo del tipo de auditoría; en este caso es con base en la auditoría de *un sistema de información en operación*.

6.7. Marcas de auditoría

La utilización de las marcas de auditoría en la elaboración de cédulas de trabajo es esencial, ya que es la evidencia que deja el auditor sobre el desarrollo de su trabajo y la documentación fuente que haya consultado para plasmarlo en su cédula.

Básicamente, se puede definir a las marcas de auditoría como la representación simbólica del trabajo que se ha realizado y de lo observado sobre el desarrollo del mismo.

No existe una estandarización sobre la utilización de los símbolos que se realizan en las marcas de auditoría, ya que cada auditor puede diseñar las que mejor le convengan, lo que sí importa es dejar un listado de qué significa cada marca utilizada en auditoría, a través de un índice de marcas.

Por ejemplo, al efectuar una revisión sobre el *hardware* de la institución auditada, para conocer si existen resguardos, si coincide el número de inventario, si el lugar asignado es el correcto, éstos deben ser cotejadas con el listado proporcionado por el área de tecnologías o el responsable del activo fijo de la institución, para saber si es correcta la información y, al realizar la inspección física, demostrar que el listado es correcto, sino fuere así se anotarán las diferencias encontradas.

En lugar de escribir todas estas características y revisiones en el caso del *hardware,* se realiza a través de marcas de auditoría que elabora el auditor y que son validadas posteriormente por el supervisor para que quede constancia del trabajo realizado en la cédula correspondiente, en donde se detalla el procedimiento realizado.

Normalmente, al inicio del legajo de auditoría, se presenta el catálogo de marcas.

Ejemplos de marcas de auditoría:

Simbología o Marca	Significado
✓	Verificado vs. Documento original o comprobatoria.
⃠	Pendiente de revisión.
✖	Datos Incorrectos
☑	Verificado físicamente.
☒	Sumas incorrectas
⓪	Cifra no considerada en el total

Como se puede observar, lo que se busca en la utilización de las marcas de auditoría es facilitar el trabajo del auditor.

6.8. Estándares de documentación

La homogeneidad de la documentación busca uniformidad en el resultado del trabajo del auditor, para que las personas usuarias de la información puedan utilizarlas en la adecuada toma de decisiones.

Gracias al avance de las tecnologías de la información, la documentación utilizada para la realización de las auditorías no varía de una auditoría a otra, ni la información solicitada es la misma para cada tipo de auditoría en informática.

Un elemento que ha propiciado reducir los errores de interpretación de la información en materia de auditoría en informática es la estandarización en la documentación utilizada por el auditor y por solicitar a la institución, esta estandarización ha permitido obtener mejores resultados, y que en ausencia del auditor se interprete de forma homogénea.

Como se ha mencionado durante el desarrollo de esta unidad, para estandarizar documentos y procedimientos, es importante la utilización de algunas herramientas para ello, como son las técnicas de auditoría.

6.9. Interpretación de la información

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.

La evaluación de los sistemas no se refiere únicamente a la metodología para el 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, el costo-beneficio o la 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.

6.10. Comparación con las mejores prácticas

Como se ha mencionado en capítulos anteriores, el nacimiento de nuevos estilos e informes de control interno ha llegado hasta la auditoría en informática con base en la ética con que debe realizarse el trabajo de auditor en informática. En México se sigue el *Código de mejores prácticas corporativas* del Consejo Coordinador Empresarial, que en su mayoría adopta la esencia del control interno; en esencia, todos los informes pretenden promover la creación e importancia de la existencia de un gobierno corporativo, que auxilia a obtener la excelencia y transparencia en las instituciones, los valores éticos en las prácticas profesionales, las responsabilidades en el conjunto de las personas encargadas de la administración y uso de la información.

Es necesario recordar lo que se dijo en la unidad 2:

Tener toda la información no sirve, si no lo aprovechamos para que los demás sepan qué es lo que se pretende alcanzar con esa información, y lejos de pensar que el que tiene la información tiene el poder, debemos pensar que quien comparte la información y sabe qué espera de las personas, esa persona en realidad tiene el poder, el secreto es compartir. Ese compartimiento de información, conlleva un grado de compromiso y responsabilidad, además de solidaridad en la toma de decisiones.

6.11. COBIT

COBIT es una herramienta de gobierno de TI que ayuda al entendimiento y a la administración de los riesgos, así como de los beneficios asociados con la información y sus tecnologías relacionadas.

A continuación, se presenta un extracto del Modelo COBIT. El documento completo se puede localizar en **http://www.isaca.org/cobit/pages/default.aspx**

ISACA propone la metodología COBIT. Está dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un

conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Los usuarios del COBIT son:

- La gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

- Los usuarios finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

- Los auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

Se definen como la estructura de relaciones y procesos que dirigen y controlan la organización en orden de conseguir sus objetivos institucionales añadiendo valor, balanceando riesgos contra beneficios.

El marco referencial conceptual puede ser enfocado desde tres puntos estratégicos:

1. Requerimientos de información.

2. Recursos de IT.

3. Procesos de IT.

COMPONENTES

Los *objetivos de control* están dirigidos a la administración y al *staff* de TI, a las funciones de control y auditoría y, lo más importante, a los propietarios de los

procesos del negocio. Los objetivos de control proporcionan un trabajo, que es un *documento* de escritorio para esos individuos. Se identifican definiciones precisas y claras para un mínimo conjunto de controles con el fin de asegurar la efectividad, eficiencia y economía de la utilización de los recursos. Objetivos de control detallados son identificados para cada proceso, como los controles mínimos necesarios. Esos controles serán analizados por los profesionales de control para verificar su suficiencia.

Los objetivos de control permiten el traslado de los conceptos presentados en el marco de referencia hacia controles específicos aplicables a cada proceso de TI.

- Recursos.
- Efectividad.
- Eficiencia.
- Integridad.
- Disponibilidad.
- Cumplimiento.
- Confidencialidad.
- Confiabilidad.
- Gente.
- Aplicaciones.
- Tecnología.
- Instalaciones.
- Datos.

Las *Directrices Gerenciales* de COBIT son genéricas y son acciones orientadas al propósito de responder los siguientes tipos de preguntas gerenciales: ¿Qué tan lejos debemos ir y se justifica el costo respecto al beneficio obtenido? ¿Cuáles son los indicadores de buen desempeño? ¿Cuáles son los factores críticos de éxito?

¿Cuáles son los riesgos de no lograr nuestros objetivos? ¿Qué hacen otros? ¿Cómo nos podemos medir y comparar?

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios; se extrajeron siete categorías distintas, ciertamente superpuestas. A continuación, se muestran las definiciones utilizadas por COBIT y son:

A. Efectividad

Se refiere a que la información relevante sea pertinente para el proceso del negocio, que su entrega sea oportuna, correcta, consistente y de manera utilizable.

B. Eficiencia

Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

C. Confidencialidad

Se refiere a la protección de información sensible contra divulgación no autorizada.

D. Integridad

Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

E. Disponibilidad

Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

F. Cumplimiento

Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

Confiabilidad de la información

Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los recursos de TI identificados en COBIT pueden explicarse/definirse como se muestra a continuación:

1. Datos

Son objetos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

2. Sistemas de Aplicación

Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

3. Tecnología

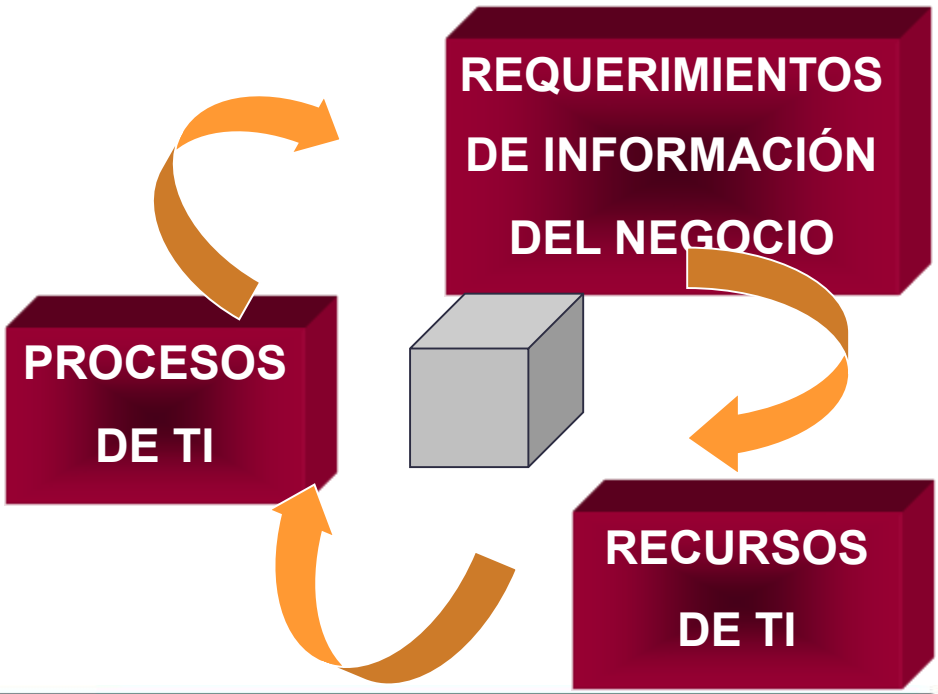
La tecnología cubre *hardware*, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

4. Instalaciones

Recursos para alojar y dar soporte a los sistemas de información.

5. Personal

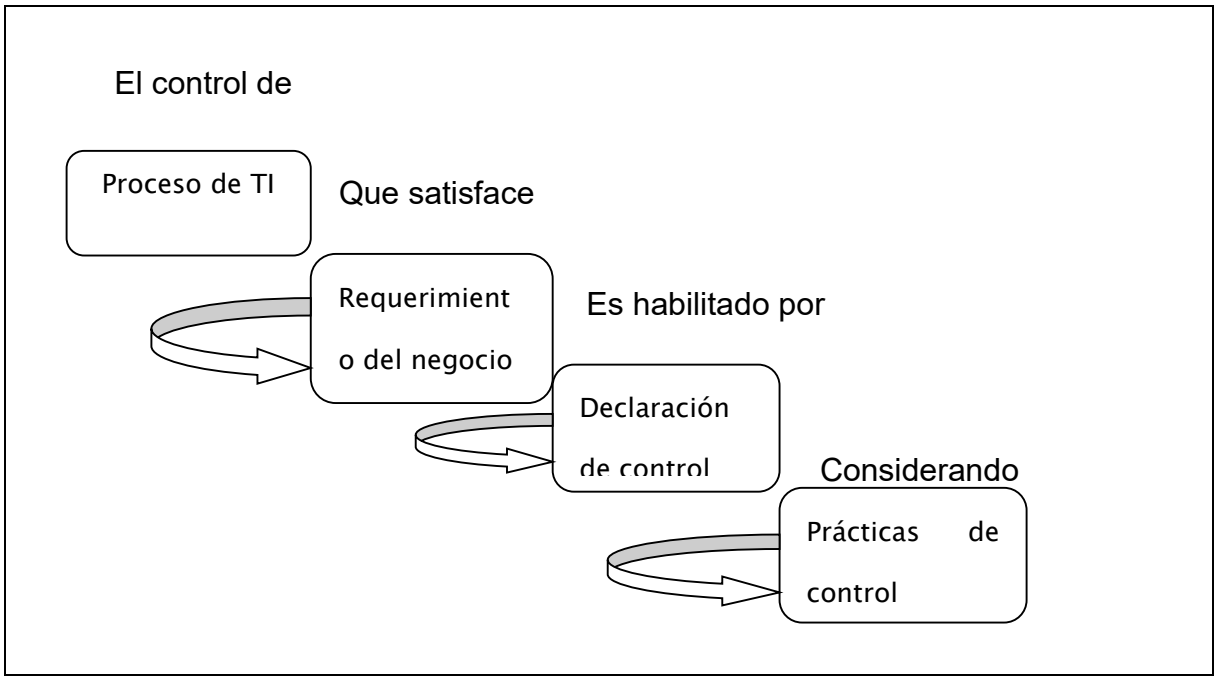
Habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorizar servicios y sistemas de información.



CUADRO 1. Propuesta de ISACA. Esquematización de los principios del COBIT. Elaboración propia.

A continuación, presentaremos un cuadro sobre control del proceso de tecnologías de información.

Cuadro 2. Cuadro de control de proceso TI[5]



Elaboración propia.

Definición de un plan Estratégico de Tecnología de Información que satisface los requerimientos del negocio de lograr un balance óptimo entre las oportunidades de

[5] Comité Directivo de COBIT y el IT Governance Institute ®

tecnología de información y los requerimientos del negocio para TI, así como para asegurar sus logros futuros, lo que se hace posible a través de:

Un proceso de planeación estratégica emprendido en intervalos regulares, dando lugar a planes a largo plazo.

Los planes a largo plazo, deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, considerando lo siguiente:

- Estrategia del negocio de la empresa.
- Definición de cómo TI soporta los objetivos de negocio.
- Inventario de soluciones tecnológicas e infraestructura actual.
- Monitorización del mercado de tecnología.
- Estudios de factibilidad oportunos y chequeos con la realidad.
- Análisis de los sistemas existentes.
- Posición de la empresa sobre riesgos, en el proceso de compra (*time-on-market*), calidad.
- Necesidades de la administración en el proceso de compra, soportado en revisión crítica.

La organización actual de las instituciones está consciente de que la inversión en tecnologías de la información representa una necesidad presente en todas las operaciones fundamentales para obtener información veraz, confiable y oportuna, que nos auxilie en una adecuada toma de decisiones, con el objeto de dar cumplimiento en tiempo y forma a los objetivos y metas institucionales; dicha información es uno de sus activos principales, si no es que el más importante, operativamente hablando, por lo tanto, deben estar sometidas a las normas y estándares de control de la organización y las particulares propias de la función relacionada con las tecnologías. Para esto, la empresa debe estar sensibilizada y

convencida de que las TI son parte integral de la misma y no una mera función técnica que esté de moda.
Estas tecnologías deben proporcionar a las empresas grandes ventajas en el incremento de su productividad, reducción de costos, apoyo a la estrategia competitiva, la medición del desempeño empresarial y a los procesos de negocio, constituyéndose, luego del recurso humano, en las herramientas más poderosas para apoyar a las organizaciones en el cumplimiento de su misión.

La meta consiste en que las nuevas tecnologías contribuyan, de manera efectiva, al crecimiento de la institución. Para ello, es necesario que la estrategia informática se encuentre en el centro de la estrategia corporativa; manejar los gastos en informática como inversiones; dar a los servicios de información el status de servicios de negocio, considerando a los múltiples clientes o partes interesadas; y hacer todo el esfuerzo posible por capitalizar la especialización tecnológica que la empresa posea.

La conceptuación del control se aleja de la antigua perspectiva, en la que se veía el control como un elemento inmerso en las actividades de una entidad o como una carga inevitable, impuesta por los organismos reguladores o por los dictados de burócratas excesivamente celosos.

Los controles impuestos por la auditoría deben ser incorporados a toda la infraestructura de una entidad, no deben ser añadidos, de manera que no deben entorpecer, sino favorecer la consecución de los objetivos de la entidad.

Cada día el auditor enfrenta el desafío de actualizar sus competencias tecnológicas, a fin de poder proveer el soporte que las nuevas tecnologías requieren. Aun cuando la empresa pueda tener una visión innovadora o conservadora, en términos de tecnología, se ha demostrado que el involucrarse temprano en nuevos proyectos de planificación estratégica suele ser un área de alto retorno de la inversión.

El rol del auditor es clave para construir un *gobierno en tecnología de información* maduro, alineado con los objetivos del negocio y que soporte las necesidades de la empresa y de todas las partes interesadas.

Los cambios en la tecnología influyen en qué auditar y en cómo auditar, por lo que, inevitablemente, la auditoría ha cambiado de manera drástica en los últimos años con el gran impacto que han generado las técnicas informáticas en la forma de procesarla.

Los procesos de negocios, que se llevan a cabo dentro de las unidades de una organización, se coordinan en función de los procesos de gestión básicos de planificación, ejecución y supervisión. El control que provee la auditoría es parte de dichos procesos y está integrado en ellos, permitiendo su funcionamiento adecuado y supervisando su comportamiento y aplicabilidad en cada momento, con lo que constituye una herramienta útil para la gestión, pero no un sustituto de ésta.

Y en efecto, el COBIT sobre la base de cuatro dominios que comprenden el universo que hace al ámbito informático, logra establecer un marco conceptual de procesos a efectuar y objetivos de control de alto nivel a cumplir para cada uno de los dominios, integrando toda la estructura de forma precisa y eficaz.

A su vez, los procesos y objetivos de control los vincula con los criterios de información y los recursos de la tecnología informática, logrando asociar y procurando proveer los medios (por medio de actividades y tareas) para la adecuada interacción de los protagonistas esenciales de las organizaciones, como los gerentes de sistemas y usuarios, responsables, especialistas, auditores, la alta gerencia, etc.

Para concluir, el COBIT es un producto de excelencia para aplicar al entorno informático, no sólo porque su marco comprende de forma extensiva e intensiva el ámbito informático, sino por la permanente preocupación de actualizar sus alcances conforme se vaya dando la evolución de la tecnología informática.

6.12. ITIL

A continuación se presenta un breve extracto de lo que significa el Modelo ITIL en la auditoría en informática.[6]

¿Qué es ITIL?

Desarrollada a finales de los ‘80, la biblioteca de infraestructura de TI (ITIL) se ha convertido en el estándar mundial en la gerencia de servicio, el marco ha probado ser útil para las organizaciones de todos los sectores a través de su adopción por muchas compañías, como base para la dirección del servicio de consulta, educación y soporte de herramientas de *software*. Actualmente, ITIL es conocido y utilizado por todo el mundo.

Siendo una base para mejorar los procesos de administración de las tecnologías de la información, ITIL describe los contornos de organizar la administración del servicio. Los modelos o diseños indican los objetivos, las actividades generales,

[6] Para conocer más de este modelo puedes consultar la siguiente página: http://www.itil.org/en/vomkennen/itil/ueberblick/index.php Fecha de consulta: 3/09/2014

entradas y productos de varios procesos, que puede ser constituido dentro de organizaciones de TI. Donde básicamente lo que se requiere es conocer los servicios importantes e imprescindibles que se deben de desarrollar en la administración de las TIC. La implementación del ITIL, no es una receta de cocina, pues si bien existen estándares, éstos deben de aplicarse de forma individual para cada institución. En vez de eso, se concentra en las mejores prácticas que pueden ser utilizadas de diferentes maneras de acuerdo con las necesidades.
Se debe de realizar un diagnóstico de los procedimiento y procesos actuales para compararlos y valorar su grado de efectividad de una manera objetiva dentro de la institución con el objeto de conocer mejor el estado en que éstos operan, teniendo en cuenta que se le dará mayor énfasis a aquellos procesos que presenten deficiencias marcadas que puedan mejorar con el establecimiento de ITIL.

Esta aportación adicional debe aspirar a identificar esos aspectos que están funcionando bien; por lo tanto, determina cuál es la mejor práctica actualmente usada y debe ser conservada.

Este diagnóstico debe contener, entre otras cosas, lo siguiente:

- Valoración inmediata de los procesos actuales y los resultados presentados a la administración para valorar de manera objetiva la eficiencia de los procesos de la administración del servicio.

- Identificar restricciones tanto económicas como de factor humano, así como de procedimientos y áreas de oportunidad detectables.

- Derivado de lo anterior, el resultado con base en la experiencia y diagnóstico deber servir para proporcionar consejos de cómo administrar más efectivamente los procedimientos de las TIC.

- Proporcionar consejos de cómo rediseñar o mejorar los procesos de administración de servicios de las TIC.

Algunos ejemplos de tópicos generales que deben ser dirigidos por las preguntas en el chequeo de salud incluyen:

- Actividades por cada proceso.
- La organización a través de tareas y responsabilidades.
- Líneas de comunicación entre procesos.
- El control de conjuntos de la administración del servicio.
- Una descripción de la infraestructura de TI.
- Control sobre cambios para la infraestructura de TI.
- El nivel de satisfacción del cliente con el servicio de TI.

Algunas mejoras requieren mayores cambios para los procesos actuales, dentro de la organización y teniendo un tiempo considerado antes de ser implementado.

6.13. ISO

A continuación se presenta un breve extracto de lo que significa el Modelo ISO en la auditoría en informática.[7]

[7] Para conocer más de este modelo puedes consultar la siguiente página: http://www.hipertexto.info/documentos/norm_document.htm#iso **Fecha de consulta: 3/09/2014**

La ISO (*International Standarization Organization*), con sede en Ginebra, es el principal organismo que promueve la normalización en el mundo. Se trata, en realidad, de una federación de organismos, ya que cuenta con numerosas delegaciones nacionales, que, a su vez, actúan como oficinas delegadas de normalización en cada país. Así encontramos a AENOR en España, AFNOR en Francia, DIN en Alemania, etc. donde cada una de estas oficinas cuenta con comités técnicos que desarrollan las normas en sus respectivos países. Por ejemplo, AENOR (Asociación Española de Normalización y Certificación) publica las normas UNE, Una Norma Española, que se corresponden con las de la ISO. El Comité Técnico de Normalización y Documentación número 50 de AENOR en España (CTN/50) es el encargado de actualizar y redactar las normas UNE sobre documentación:

Las normas no son más que un modelo constituido por reglas que tiene como fin definir las características técnicas que debe poseer un objeto o producto para que exista compatibilidad y puedan usarse a nivel internacional. Esto abarca, por ejemplo, desde la especificación de un modelo o tipo de enchufe en un aparato eléctrico, hasta la forma de elaborar una referencia bibliográfica. La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir mayor eficacia y efectividad y para que los objetos o usos sean compatibles a nivel internacional.

En realidad, las normas ISO tienen un valor meramente indicativo, aunque su uso crece y se extiende día a día. Sus ámbitos de aplicación son muy variados, destacando de manera notable en el campo de la información científica y técnica. En el campo de la documentación, las normas ISO han sido un referente indispensable para la normalización en la descripción, búsqueda y recuperación del documento. Entre las normas ISO referidas al campo de la documentación destacan: Normas ISO referentes a los Números Normalizados para libros, publicaciones seriadas, programas de ordenador,

informes técnicos, música, obras audiovisuales... (ISBN, ISSN, ISRC, ISRN, ISMN, ISAN, etc.), Norma ISO 690:1987, para referencias bibliográficas, e ISO 690-2, para referencias bibliográficas de documentos electrónicos, ISO 5963/85 sobre metodología de indización, ISO 5127-3ª/81 sobre identificación y análisis del contenido, ISO 15836:2003 sobre metadatos Dublin, Core, etc. En capítulo aparte se ofrece un extracto con las principales normas ISO referidas a documentación, publicación, edición, etc.

Fuente: http://www.hipertexto.info/documentos/norm_document.htm#iso
(Fecha de consulta: 3/09/2014)

Para realizar la auditoría de ISO, que se refiere en términos generales a calidad, se utiliza de igual forma la metodología tradicional que se ha observado en la auditoría: planeación, obtención de evidencia ejecución, ejecución, informe, etc., aunque el objetivo es diferente, ya que lo que se busca es estandarizar procesos, procedimientos, controles, etcétera.

El auditor, al realizar su revisión a través de esta norma, busca la satisfacción del usuario primario y usuario secundario de la información derivada de las TI; ya que si bien las ISO han sido un estándar en México, existen las Normas Oficiales Mexicanas o NOM, que muchas veces sobrepasan las exigencias de cualidades y calidades a las permitidas por estas Normas ISO, al realizar este tipo de auditorías se establecen indicadores de satisfacción del usuario que se miden en tiempo de respuesta, resoluciones de problema, etc., así como la utilidad en general de los recursos informáticos.

Para entender un poco mejor lo que es la calidad, me permito transcribir una entrevista que considero deja más en claro aspectos importantes de la calidad:[8]

-Maestro, ¿qué es la calidad?

> Estamos viviendo en una era de cambios profundos y acelerados, se respira una atmósfera de competitividad y esto en todos los campos. El mundo camina inexorablemente para la calidad pero, para entender mejor el concepto de calidad, debemos entender antes otro concepto paralelo a éste, que es el de *cantidad***.**
>
> ¿Qué es *cantidad*? Una de las definiciones del diccionario: "Porción grande o abundancia de algo".
>
> ***¿Cómo se relaciona con calidad?***
>
> Desde niños aprendimos a conjugar muy bien el verbo **TENER** y muy mal el verbo **SER**. Me explico: el pronombre interrogativo **CUÁNTO** está en la boca de todo continuamente:
> ¿Cuánto gana?, ¿Cuánto cuesta?, ¿Cuántos años tienes?, ¿Qué carro tienes? ¡Sí, porque dependiendo del carro que tienes es lo que tú vales! ¿Cuánto?, ¿Cuánto?, ¿Cuánto?
>
> Fuimos educados para ver el mundo **CUANTITATIVAMENTE** y nos garantizaban que si yo tuviese mucha **CANTIDAD**, yo tendría también mucha **CALIDAD**, y esto no es cierto. No estamos negando el valor de la

[8] Entrevista realizada al Maestro Guy Paulo Bisi Fochesato, funcionario de la Universidad de Sotavento, sobre "Calidad", en Coatzacoalcos Veracruz, por L.C y M. AUD. José de Jesús Aguirre Bautista.

CANTIDAD, lo que estamos diciendo es que existe una profunda dicotomía entre **CANTIDAD y CALIDAD**. Un joven hace un examen en la universidad, la pregunta de los papás: "¿Hijo, de cuánto ha sido tu promedio?" Ahora, si el conocimiento fue significativo, si realmente el joven aprendió algo, eso no interesa, eso no importa. Desgraciadamente, nuestras instituciones, de un modo general, son más **cuantitativas** que **cualitativas**, ésta es una triste realidad.

Por eso nuestra institución busca la certificación de la norma: NMX-CC-9001-IMNC-2000.

- **Enhorabuena, ¿pero cómo podemos saber qué es calidad y qué no lo es?**

Ni asesores, ni profesionales están de acuerdo en una definición universal. En un estudio, se preguntó a los administradores de 86 empresas de Estados Unidos que definieran *calidad*. Docenas de respuestas incluían: perfección, consistencia, eliminación de desperdicio, rapidez de entrega, agradar a los clientes, servicio total al cliente, proporcionar un proyecto bueno. Coca-Cola contestó: "Nuestro compromiso con la *calidad* es algo en lo que jamás perderemos el gusto, la calidad no es un destino, sino una forma de vida".

CALIDAD ES:	CALIDAD NO ES:
Una filosofía	Un arreglo rápido
Ajustarse a los estándares de perfección	Simplemente hacer bien las cosas
Previsión	Pura inspección
Seguir una guía específica	Una actitud conformista
Un proceso que dura toda la vida	Un programa de motivación
Compromiso	Coincidencia

Apoyo a los supervisores	Tomar resoluciones al azar
Una actitud positiva	Una mentalidad de perro guardián
Llegar a acuerdos	Hacer sus propias cosas
Voluntad de comunicación	Datos aislados
Comprensión de su propio proceso	Adivinanzas
Prever las posibilidades de error	Detección de errores hasta el final
Capacidad	Hacer siempre lo mismo

LO QUE ES CALIDAD Y LO QUE NO ES

Hoy es tal la amplitud del término *calidad* que se hace necesario acotarlo. La Organización Internacional de Estándares nos da una definición confiable: "CALIDAD es la totalidad de partes y características de un producto o servicio que influyen en la habilidad de satisfacer necesidades declaradas o implícitas"

-¿Qué deben hacer las universidades para preparar gente de CALIDAD?

Las universidades que no forman personas de CALIDAD no tienen justificación histórica para existir, porque, como diría Mario Haddad Slim, "serían esqueletos más o menos burocráticos lanzando al mercado casi en serie profesionistas más o menos mediocres o indiferentes, y eso sería inadmisible".
El éxito en los estudios no depende sólo de la inteligencia y del esfuerzo, sino también de la eficacia de los métodos y las técnicas de estudios que se utilicen; el alumno que las ignora difícilmente obtendrá buenos resultados.

-Para concluir, ¿cuál sería la labor de un maestro para transmitir o dejar la inquietud del término CALIDAD?

Sócrates una vez caminaba por las calles de Atenas, cuando se detuvo frente a unos albañiles. -¿Qué haces? -Preguntó a uno de ellos-, “trabajo, a cambio de un salario para poder comer”, “estoy labrando esta cantera”, -respondió el segundo. Al interpelar al tercero, éste contestó: “estoy levantando un templo”. Esta anécdota clásica señala la diferencia entre un obrero, un artesano y un artista. En todas las actividades hay niveles. El nuestro está en nuestra mente.

La educación es una obra de arte. En sentido amplio, los maestros son artistas.

RESUMEN

Al realizar las auditorías en informática, los elementos que se toman en cuenta para lograr una efectiva revisión, se encuentran en la capacidad del personal involucrado que cuente con entrenamiento técnico, conocimiento científico y experiencia profesional, para que pueda desarrollar bien una entrevista que se utiliza en auditoría y otras herramientas necesarias para obtener un diagnóstico real y fehaciente de la situación informática de la institución auditada.

Las características anteriores, permitirán que el auditor sea capaz de poder discriminar la información esencial y no esencial para el desarrollo de su auditoría, conocer qué características deben contener éstas y cuáles son necesarias para minimizar el riesgo en la auditoría.

La auditoría busca siempre mejorar procesos tratando de optimizar recursos informáticos que contengan mejores prácticas y que éstas se ejecuten lo mejor posible; derivado ello, se presentan los estándares internacionales relacionados para este efecto, como son COBIT, ITIL e ISO, que presentan la elaboración de desarrollo de documentación estandarizada para aplicar cuando se efectúe una auditoría en alguno de sus elementos.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

Autor	Capítulo	Páginas
Aguirre Bautista, José de Jesús	Apuntes de la asignatura de auditoría en informática. Capítulo VII	130-137
ITIL, IT Management Practices: *Information Technology Infrastructure Library*.	*Practices and guidelines developed by the Central Computer and telecommunications Agency* (CCTA), London, 1989.	1-84
ISO 9000-3: *International Organization for Standardization. Quality Management and Quality Assurance Standards - telecommunications*	Part 3: *Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software, Switzerland*, 1991.	1-54

Bibliografía Básica

Ayala Rodiles, Sara Isabel (1996). *Seminario de auditoría en informática* (apuntes) Patronato universitario (UNAM).

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

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: NBS Special Publication 500-153: National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, [1988].

Piattini, Mario y Emilio del Peso (2001). *Auditoría informática, un enfoque práctico*. Madrid: Alfa-Omega. 2ª. Ed.

Bibliografía Complementaria

ISO 9000-3. (1991). *International Organization for Standardization. Quality Management* and *Quality Assurance Standards - Part 3: Guidelines for the Application of ISO 9001 to the development, supply and maintenance of software.* Geneva Switzerland.

ITIL IT Management Practices (1989). *Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and* telecommunications *Agency (CCTA).* London.

Muñoz Razo, Carlos (2002). *Auditoría en sistemas computacionales*. México: Prentice Hall.

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

Hernández Hernández, Enrique (2002) *Auditoría en informática* 82ª. Ed.). México: CECSA.

Sitios de Internet

Sitio	Descripción
http://www.isaca.org/cobit/pages/default.aspx	Modelo de control COBIT.
http://www.cce.org.mx/sites/default/files/CodigoMejoresPracticas.pdf	Modelo del código de mejores prácticas corporativas.
http://www.hipertexto.info/documentos/norm_document.htm#iso	Normas ISO.
http://www.iso.org/iso/home/news_index/iso-in-action.htm	Normas ISO.
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Ac11146	INFOSEC Comité Consultivo para la Comisión Europea en Materia de Seguridad TI. (Advisory Committee for IT Security Matters to the European Commission).

Licenciatura: Informática

UNIDAD 7

Informe de auditoría

SUAyED UNAM
Sistema Universidad Abierta y Educación a Distancia

Plan 2012 2016 actualizado

OBJETIVO PARTICULAR

El alumno podrá entregar informes de auditoría con la profesionalidad requerida, cubriendo los requisitos que estos informes necesitan.

TEMARIO DETALLADO

(8 horas)

7. Informe de Auditoría

- 7.1. Características del informe
- 7.2. Estructura del informe
- 7.3. Formato para el informe
- 7.4. Evidencia

INTRODUCCIÓN

El informe de auditoría es la conclusión del trabajo del auditor, aquí la experiencia juega un papel importante, pues ella influye poderosamente en la forma de interpretar la información, ya que se ven reflejados los objetivos trazados al inicio de la auditoría, si éstos se cumplieron o se tuvieron que cambiar sobre la marcha. Es importante señalar que la estructura del informe se presenta por una razón que establece la consistencia del trabajo y las conclusiones del mismo, así como el establecimiento de sugerencias y acciones de mejora a desarrollar.

7.1. Características del informe

Informe de auditoría

Aun cuando las diversas organizaciones tengan definidos formatos de informes, es conveniente que éste se presente con los siguientes elementos, ya que esto facilitará la toma de decisiones por la dirección acerca de los puntos tratados en el mismo.

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.

Hay que recordar que el objetivo de un informe es generar acciones y que, por definición, un informe que no lo logre es un informe que no será útil a la institución auditada.

Finalmente, lo importante es que se presenta como una película completa del trabajo hecho, basado en hallazgos reales y soportables.

Los elementos son los siguientes:

- Hallazgo, muestra objetivamente, cuantitativa o cualitativamente, la situación o resultado irregular que se puso de manifiesto en la revisión.

- Como la auditoría está basada en riesgos, se tiene que señalar si éstos se generan por los hallazgos detectados y si es posible determinar su grado de realización o de exposición al riesgo.

- Es importante señalar el grado de impacto en la institución, sea cuantitativa o cualitativamente, tratándose de planes o funciones o procedimientos estratégicos.

- Causas que dieron lugar a lo anterior, menester ser extremadamente cuidadosos en estas percepciones, por el impacto que puede tener en la institución auditada.

- Alternativas de solución a la problemática planteada, aquí es claro que el auditor actuará como consultor en aquellos casos en que la situación se refiera a ausencia de políticas y procedimientos.

- Consecuencias por no realizar las sugerencias plasmadas en el informe.

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, aun si éstos han sido omitidos; el informe de auditoría sólo se hace responsable de lo presentado por la administración y lo observado por los auditores.

7.2. Estructura del informe

La estructura del informe, se refiere al acomodo y orden en que se debe de presentar un informe bien elaborado. Un informe que responda a esta estructura tendrá una mayor probabilidad de éxito.

Ejemplo de estructura A:

- Objetivo y alcance del trabajo.
- Fecha o periodo al cual se refiere la opinión del auditor.
- Limitaciones al alcance si es que las hubo y los riesgos inherentes a cualquier sistema auditado.
- Responsabilidad de la administración en cuanto a la definición y mantenimiento del sistema de control interno.
- Opinión.

Ejemplo de estructura B:

- Fecha de preparación.
- Responsabilidad asumida.
- Alcance del trabajo.
- Referencia a normativa consultada.

- 🕮 Periodo cubierto en la revisión.
- 🕮 Descripción de las debilidades de control y sugerencias, repercusión y alternativas de solución.
- 🕮 Nombre, puesto y firma de los auditores que participaron en la revisión.

Con los ejemplos anteriores, no importa cuál estructura se elija, lo importante es que el informe o dictamen presente las observaciones determinadas, en qué consistió el trabajo y qué se tiene que hacer para revertir una situación en donde existan debilidades de control.

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, va junto con las cuentas anuales del ejercicio.

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

- El título o identificación del tipo de auditoría a la que se hace referencia.
- A quién va dirigido.
- Introducción del trabajo ejecutado.
- El párrafo de "Alcance". Se refiere al objetivo y período de revisión de la auditoría y en qué consistió ésta.
- El párrafo de "Opinión". Se refiere a la situación real de la institución auditada, sobre si funciona bien en general o si existen aspectos a mejorar.
- El párrafo o párrafos de "Énfasis". Se refiere a un hallazgo considerado importante y que sobresale por encima de los demás determinados en la

auditoría; por ejemplo, si existió desviación de recursos informáticos durante el período de la revisión.

- El párrafo o párrafos de "Salvedades". Si es que se trata de este tipo de informe se refiere a que la mayoría de los aspectos importantes funcionan razonablemente, excepto por alguna situación importante que no desvirtúa la opinión del auditor.
- El párrafo sobre el "Informe de la Administración". Se refiere a la importancia de ver cómo ejerce la administración la alta dirección; es decir, se opina sobre controles y procedimientos para alcanzar los objetivos y metas institucionales.
- La firma del informe del auditor responsable de la auditoría.
- La fecha del informe.

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 normativa.

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 normativa 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 con que se verifica 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 los tres anteriores tipos de opinión.

7.3. Formato para el informe

El formato para elaborar el informe de auditoría debe establecer la forma y contenido del informe que debe emitir el auditor al término de su examen practicado de conformidad con la normativa aplicable para ello. Generalmente, el dictamen se dirigirá a los accionistas o a quien haya contratado los servicios del auditor.

El auditor debe mencionar en su informe la responsabilidad que asume respecto a los recursos informáticos auditados, indicando en los párrafos del alcance y la opinión, las fechas y periodos de los recursos informáticos por él examinados.

En el informe se deberá describir el alcance del trabajo efectuado mediante las afirmaciones siguientes:

- Que el trabajo fue realizado de acuerdo con las normas de auditoría en informática aplicable a la institución auditada o a las normas internas vigentes durante la realización de la auditoría.

- La auditoría fue planeada y realizada para obtener una seguridad razonable acerca de que la utilización y distribución de los recursos informáticos se encuentran libres de errores importantes, y que están preparados de acuerdo con la normativa aplicable a la institución.

- Que el examen se efectuó mediante pruebas selectivas.

- Que la auditoría proporcionó bases razonables para la opinión.

El informe deberá establecer claramente la opinión del auditor acerca de si los recursos informáticos presentan razonablemente, en todos los aspectos importantes, la situación de esos recursos con base en la normativa aplicable para ello.

Es importante señalar que se pueden presentar dos tipos de informe: El ejecutivo, que menciona sólo los aspectos más relevantes de la auditoría, como puede verse en el ejemplo que se presenta en el anexo 1, y otro informe en donde se indique más a detalle lo plasmado en el informe ejecutivo que incluye anexos necesarios para soportar la información contenida en el informe.

Véase: Anexo 1. Formato de informe.

7.4. Evidencia

La evidencia de auditoría representa el sustento principal de nuestra opinión, así como de las observaciones o hallazgos detectados por el auditor durante su revisión; de ahí la importancia que reviste la suficiencia, relevancia, pertinencia y competencia de la evidencia, así como la calidad, cantidad y claridad de la misma.

La evidencia es suficiente cuando por los resultados de la aplicación de una o varias pruebas, el auditor interno pueda adquirir certeza o seguridad razonable de que los hechos revelados se encuentran satisfactoriamente comprobados; es decir, la suficiencia se basa en hechos que se pueden cuantificar y que representan un razonable grado de confiabilidad.

Cuando la evidencia es competente, se refiere a que debe ser válida y confiable; es decir, este hecho se basa en aspectos cualitativos de la prueba, hecho o hallazgo.

La evidencia es relevante cuando denota un grado de importancia que lleva a demostrar su valía y que es un hecho de alto impacto durante la revisión.

La evidencia es pertinente cuando demuestra su grado de efectividad y apoya el hecho o hallazgo del auditor durante la revisión.

Derivado de la explicación anterior, se pueden mencionar varios tipos de evidencias; sin embargo, para obtener ésta nos auxiliamos de las técnicas de auditoría mencionadas en los capítulos anteriores. Por ejemplo:
Evidencia documental. Como su nombre lo indica, el documento obtenido es la evidencia de la prueba.

Evidencia electrónica. Se refiere a la obtención de información a través de las tecnologías de la información.

Y derivadas de estos tipos de evidencia se pueden desprender evidencias testimoniales, legales, etc.

RESUMEN

El informe de auditoría en informática es un informe crítico que se presenta derivado del trabajo realizado por el auditor con el fin de evaluar la eficacia y eficiencia de una empresa en lo que se refiere a los recursos informáticos, ya que este tipo de informe, presentado en las auditorías en informática, comienza con bases cualitativas, pero termina con bases cuantitativas que sirven de soporte a la toma de decisiones.

Asimismo, la evidencia de auditoría es la documentación obtenida en donde el auditor sustenta la opinión del trabajo realizado que se plasma en el informe.

BIBLIOGRAFÍA DE LA UNIDAD

SUGERIDA

Autor	Capítulo	Páginas
Instituto Mexicano de Contadores Públicos. (2013). *Normas de auditoría para atestiguar revisión y otros servicios relacionados* (3ª ed.) México: IMCP.	Norma Internacional de Auditoría 700 “Formación de la opinión y emisión del informe de auditoría sobre los estados financieros”.	971-1006
Instituto Mexicano de Contadores Públicos. (2013). *Normas de auditoría para atestiguar revisión y otros servicios relacionados* (3ª ed.) México: IMCP.	Norma Internacional de Auditoría 500 “Evidencia de auditoría”.	642-858

Bibliografía Básica

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

Piattini Velthuis, Mario G., Peso Navarro, Emilio del. (2001). *Auditoría Informática: un enfoque práctico*. Madrid: Ra-Ma.

Bibliografía Complementaria

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

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

Sitios de Internet

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.*

Plan 2012

2016

actualizado