UNIVERSIDAD ESTATAL A DISTANCIA
ESCUELA DE CIENCIAS EXACTAS Y NATURALES
PROGRAMA INFORMÁTICA ADMINISTRATIVA

GUÍA DE ESTUDIO DEL CURSO

Seguridad y Auditoría en las TICS

CÓDIGO 3070

Frank A. Mendoza Hernández

2008

Producción académica:
Fiorella Monge Lezcano

Encargada de cátedra y
especialista de contenidos:
Karol Castro Chaves

Revisión filológica:
Fiorella Monge Lezcano

TABLA DE CONTENIDO

PRESENTACIÓN

Esta guía de estudio está diseñada con la finalidad de orientarlo a través del cuatrimestre. Le indica claramente los temas y los capítulos del libro de texto así como la secuencia.

El objetivo de este curso es proporcionar una introducción a los fundamentos teóricos, prácticos y especializados que deben aplicarse para realizar con éxito una auditoría de sistemas computacionales.

No hay empresa o institución que no utilice hoy los sistemas computacionales para introducir datos, procesar esos datos, obtener resultados para la toma de decisiones, llevar el control de la empresa y almacenar dicha información para futuras operaciones.

Al igual que ha crecido la dependencia de los sistemas computacionales han crecido también los riesgos que pueden dañar esa información sea de manera accidental, por catástrofes naturales o por personas que traten simplemente de curiosear la información o de manera deliberada o hurtar esa información provocando pérdidas económicas a la empresa.

De allí que sea de suma importancia que la empresa esté preparada para este tipo de ataques tanto internos como externos y se creen los mecanismos necesarios para la prevención de cualquier posible daño a los datos.

Las empresas deben tener personal capacitado sea interna o externamente para ayudar a prevenir cualquier tipo de riesgo.

Esta guía incluye diez capítulos que resumen los puntos más importantes que deben tomarse en cuenta para prevenir los riesgos. Sin embargo, para fines de evaluación, esta guía sustituye al libro de texto. Es responsabilidad del estudiante estudiar a fondo los diferentes tópicos y aclarar dudas o inquietudes en las tutorías presenciales que brinda este curso.

Los temas son de gran importancia para la formación académica del estudiante. El orden en que se presentan estos temas está de acuerdo con su nivel de dificultad. Por lo tanto, el estudiante debe seguir al detalle esta guía para lograr un buen entendimiento de la materia.

Los temas de estudio son los siguientes:

- Conceptos generales.
- Normas ético-morales que regulan la actuación del auditor.
- Control interno informático.
- Metodología para realizar auditorías de sistemas computacionales.
- Papeles de trabajo para la auditoría de sistemas computacionales.
- Informes de auditoría de sistemas computacionales.
- Instrumentos de recopilación de información aplicables en una auditoría de sistemas computacionales.
- Técnicas de evaluación aplicables en una auditoría de sistemas computacionales.
- Técnicas especiales de auditoría de sistemas computacionales.
- Propuesta de puntos que se deben evaluar en una auditoría de sistemas computacionales.

DESCRIPCIÓN DEL CURSO

OBJETIVO GENERAL

Introducir al estudiante en el ambiente de auditoría y seguridad en las Tecnologías de Información y Comunicaciones.

OBJETIVOS ESPECÍFICOS

Al finalizar este curso, usted deberá estar en capacidad de:

- ✓ Demostrar conocimientos básicos sobre los tipos de auditoría y las normas ético-morales que controlan la actuación del auditor.
- ✓ Dominar los conocimientos sobre los diferentes controles internos que se deben aplicar para una mayor seguridad en el área de informática.
- ✓ Analizar la metodología para la realización de auditorías de sistemas computacionales y los papeles de trabajo que se requieren para esta
- ✓ Demostrar conocimientos sobre la elaboración de informes de Auditoría de Sistemas Computacionales y los diferentes instrumentos necesarios para la recopilación de información.
- ✓ Dominar los diferentes aspectos que se consideran en las técnicas de evaluación y especiales de una auditoría, para una mayor seguridad en los sistemas computacionales.
- ✓ Dominar los conocimientos sobre las diferentes áreas que se deben evaluar en una Auditoría de Sistemas Computacionales para una mayor seguridad en el área informática

REQUISITOS DEL CURSO

Este curso está diseñado para una carga académica asignada de tres créditos. Es parte del plan de Bachillerato de la carrera de Informática Administrativa (código 30). En él se asume que usted ha aprobado, como mínimo, los cursos de Telemática y Redes I (883) y Telemática y Redes II (3076) o, en su defecto, que posee conocimientos básicos de dichas áreas. El no tener los conocimientos previos que le entregan los cursos antes mencionados, le dificultará enormemente el éxito en esta asignatura. Por lo tanto, piénselo antes de seguir adelante.

MATERIAL DE APOYO

La siguiente lista de materiales didácticos se brinda a los estudiantes el día que matricula el curso. Su objetivo es proporcionar al estudiante la ayuda necesaria para comprender los temas de estudio.

- Libro de texto: Muñoz R., Carlos. (2002). *Auditoría en Sistemas Computacionales*. Primera edición. Editorial Pearson Prentice Hall. México.
- Pacheco Urbina, Adela María. (2008). *Material Complementario para el curso de Seguridad y Auditoría en las TIC*. EUNED.

- Pacheco Urbina, Adela María. (2008). *Orientación para el curso Seguridad y Auditoría en las TIC*. EUNED.
- Esta guía de estudio que usted está leyendo.

Además, se brinda la siguiente lista de bibliografía de apoyo como material de consulta:

- Marcelo C., Julián. (2002). *Riesgo y Seguridad de los Sistemas Informáticos*. Editorial Universidad Politécnica de Valencia, España.
- Merike, Kaeo. (2002). *Diseño de seguridad en redes*. Editorial Pearson Educación. México.
- Piattini, Mario G. y del Peso N., Emilio. (2005). *Auditoría informática*. *Un enfoque práctico*. Segunda edición ampliada y revisada. Editorial Ra-Ma. España.
- Stallings, William. (2004). *Fundamentos de seguridad en redes. Aplicaciones y Estándares*. Segunda edición. Editorial Pearson Educación. Madrid.

DESGLOSE DE CAPÍTULOS

El curso Seguridad y Auditoría en las TICS consta de 10 capítulos principales: Para un adecuado aprovechamiento del curso, se escogió utilizar, como unidad didáctica, el libro de texto autodidáctico de Muñoz, que motiva al estudiante a continuar con el aprendizaje de los temas señalados.

En la siguiente tabla se detallan los temas principales, los subtemas correspondientes, el número del capítulo del libro y el número de páginas del libro donde podrán localizar cada uno de ellos:

TEMA	Capítulo del libro	Páginas
Conceptos generales	1	2-31
Normas ético-morales que regulan la actuación del auditor	3	51-94
Control Interno Informático	5	133-178
Metodología para realizar Auditorías de Sistemas Computacionales	6	179-242
Papeles de rebajo para la Auditoría de Sistemas Computacionales	7	243-269
Informes de Auditoría de Sistemas Computacionales	8	271-326
Instrumentos de recopilación de información en una Auditoria de Sistemas Computacionales	9	327-416
Técnicas de Evaluación aplicables en una Auditoria de Sistemas Computacionales	10	417-476
Técnicas especiales de Auditoría de Sistemas Computacionales	11	477-556
Propuesta de puntos que se deben evaluar en una Auditoría de Sistemas Computacionales	12	557-685

GUÍA DE LECTURAS

En cada tema de esta Guía de estudio, usted, encontrará una sección llamada *Guía de lecturas.* Esta tiene como finalidad indicarle las páginas respectivas que usted debe leer y estudiar de su libro de texto para cada capítulo y subcapítulo.

COMENTARIOS GENERALES

Los comentarios generales presentados para cada capítulo en esta Guía de estudio brindan aspectos importantes de este capítulo y su ubicación dentro de cada capítulo del libro de texto. Le servirán para sintetizar los conceptos transmitidos. De esta manera, usted podrá determinar si requiere repasar o aclarar alguno de los conceptos antes de desarrollar los ejercicios.

Capítulo 1

Conceptos generales

Sumario

Conceptos básicos sobre la auditoría.
Clasificación de los tipos de auditorías.
Objetivos generales de la auditoría.
Marco esquemático de la auditoría de sistemas computacionales.

Propósito del capítulo

El propósito de este capítulo consiste en mostrar al estudiante el ámbito de acción de los diferentes tipos de auditoría incluyendo las que se relacionan con las TICS, así como la presentación de conceptos básicos.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Conocer los antecedentes y los conceptos fundamentales de la materia de auditoría así como la clasificación y definiciones de los tipos de auditorías.

- Contextualizar los elementos que cimentan la existencia de la disciplina de auditoría, en general, para analizar los aspectos básicos de la auditoría de sistemas computacionales, que encontrará a lo largo de este libro.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
1.2 Conceptos básicos sobre la auditoría.	10
1.3 Clasificación de los tipos de auditorías.	12
1.3.1 Clasificación de la auditoría por su lugar de origen.	13
1.3.2 Clasificación de auditorías por su área de aplicación.	15
1.3.4 Auditoría en sistemas computacionales (Auditoría informática)	22
1.5 Marco esquemático de la auditoría de sistemas computacionales	30

COMENTARIOS GENERALES

El desarrollo normal de las actividades comerciales y financieras de las empresas requiere una constante vigilancia y evaluación; así mismo, las empresas necesitan una opinión, preferiblemente independiente, que les ayude a medir la eficiencia y eficacia en el cumplimiento de sus objetivos.

Por lo general, la evaluación consiste en una revisión metódica, periódica e intelectual de los registros, tareas y resultados de la empresa, con lo cual se busca medir y diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones. Eso es auditoría.

Conceptos básicos sobre la auditoría

Los campos de aplicación de la auditoría han evolucionado mucho, desde su uso en los aspectos netamente contables, hasta su uso en áreas y disciplinas de carácter especial, como la ingeniería, la medicina y los sistemas computacionales.

Evidentemente, junto con ese progreso, también se ha registrado el desarrollo de las técnicas, métodos, procedimientos y herramientas de cada uno de estos tipos de auditorías, así como un enfoque cada vez más característico y especializado hacia el uso de técnicas más apegadas al área que se va a evaluar.

En forma general, la definición que se propone para la auditoría es la siguiente:

Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.

(Para ahondar más en este tema, refiérase a las páginas de la 10 a la 11 del libro de texto).

Clasificación de la auditoría por su lugar de origen

Auditoría externa

Es la revisión independiente que realiza un profesional de la auditoría, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de las actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como de la razonabilidad en la emisión de sus resultados financieros.

La relación de trabajo del auditor es ajena a la institución donde se aplicará la auditoría y esto le permite emitir un dictamen libre e independiente.

Auditoría interna

Es la revisión que realiza un profesional de la auditoría, cuya relación de trabajo es directa y subordinada a la institución donde se aplicará con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funcionales que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de sus resultados financieros.

El objetivo final es contar con un dictamen interno sobre las actividades de toda la empresa, que permita diagnosticar la actuación administrativa, operacional y funcional de empleados y funcionarios de las áreas que se auditan.

Clasificación de auditorias por su área de aplicación

Auditoria financiera (contable)

Es la revisión sistemática, explorativa y crítica que realiza un profesional de la contabilidad a los libros y documentos contables, a los controles y registros de las operaciones financieras y a la emisión de los estados financieros de una empresa, con el fin de evaluar y opinar sobre la razonabilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros obtenidos durante un periodo específico o un ejercicio fiscal.

El propósito final es emitir un dictamen contable sobre la correcta presentación de los resultados financieros a los accionistas, clientes, autoridades fiscales y terceros interesados, en relación con las utilidades, pago de impuestos y situación financiera y económica de la institución.

Auditoría administrativa

Es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, en cuanto a organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones.

Su propósito es evaluar tanto el desempeño administrativo de las áreas de la empresa, como la planeación y control de los procedimientos de operación, y los métodos y técnicas de trabajo establecidos en la institución, incluyendo la observancia de las normas, políticas y reglamentos que regulan el uso de todos sus recursos.

Auditoría operacional

Es la revisión exhaustiva, sistemática y específica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones, cualesquiera que éstas sean, tanto en el establecimiento y cumplimiento de los métodos, técnicas y procedimientos de trabajo necesarios para el desarrollo de sus operaciones, en coordinación con los recursos disponibles, como en las normas, políticas, lineamientos y capacitación que regulan el buen funcionamiento de la empresa.

Auditoría integral

Es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluar, de manera integral, el correcto desarrollo de las funciones en todas sus áreas administrativas, cualesquiera que éstas sean, así como de evaluar sus resultados conjuntos y relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objetivo institucional.

Dicha revisión se lleva a cabo también a las normas, políticas y lineamientos sobre el uso de todos los recursos de la empresa.

Auditoría gubernamental

Es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental, cualquiera que sea la naturaleza de las dependencias y entidades de la Administración Pública Federal.

Esta revisión se ejecuta con el fin de evaluar el correcto desarrollo de las funciones de todas las áreas y unidades administrativas de dichas entidades, así como los métodos y procedimientos que regulan las actividades necesarias para cumplir con los objetivos gubernamentales, estatales o municipales.

También, se desarrolla en la aplicación y cumplimiento de presupuestos públicos, programas, normas, políticas y lineamientos, que regulan la participación de los recursos de la entidad en la prestación de servicios a la sociedad.

Auditoría informática

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, *software* e información utilizados en una empresa, sean

individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes.

Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.

El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

(Para ahondar más en este tema, refiérase a las páginas de la 13 a la 22 del libro de texto).

Marco esquemático de la auditoría de sistemas Hardware

Evaluación a:

Hardware.
- Plataforma de *hardware*.
- Tarjeta madre.
- Procesadores.
- Dispositivos periféricos.
- Arquitectura del sistema.
- Instalaciones eléctricas, de datos y de telecomunicaciones.
- Innovaciones tecnológicas de hardware y periféricos.

Software
- Plataforma del *software*.
- Sistema operativo.
- Lenguajes y programas de desarrollo.
- Programas, paqueterías de aplicación bases de datos.
- Utilerías, bibliotecas y aplicaciones.
- Software de telecomunicación.
- Juegos y otros tipos de *software*.

Gestión informática
- Actividad administrativa del área de sistemas.
- Operación del sistema de cómputo.
- Planeación y control de actividades.
- Presupuestos y gastos de los recursos informáticos.
- Gestión de la actividad informática.

- Capacitación y desarrollo del personal informático.
- Administración de estándares de operación, programación y desarrollo.

Información
- Administración, seguridad y control de la información.
- Salvaguarda, protección y custodia de la información.
- Cumplimiento de las características de la información.

Diseño de sistemas
- Metodologías de desarrollo de sistemas.
- Estándares de programación y desarrollo.
- Documentación de sistemas.

Bases de datos
- Administración de bases de datos.
- Diseño de bases de datos.
- Metodología para el diseño y programación de bases de datos.
- Seguridad, salvaguarda y protección de las bases de datos.

Seguridad
- Seguridad del área de sistema.
- Seguridad física.
- Seguridad lógica.
- Seguridad de las instalaciones eléctricas, de datos y de telecomunicaciones.
- Seguridad de la información, redes y bases de datos.
- Administración y control de las bases de datos.
- Seguridad del personal informático.

Redes de cómputo
- Plataformas y configuración de las redes.
- Protocolos de comunicaciones.
- Sistemas operativos y *software*.
- Administración de las redes de cómputo.
- Administración de la seguridad de las redes.
- Administración de las bases de datos de las redes.

Especialidades
- *Outsourcing*.
- *Helpdesk*.
- Ergonomía en sistemas computacionales.
- ISO-9000.
- Internet/Intranet.
- Sistemas multimedia.

(Para ahondar más en este tema, refiérase a las páginas de la 30 a la 31 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- ¿Se puede decir que existe alguna diferencia sustancial en cuanto a procedimientos de lo que se conoce como Auditoría Integral y una Auditoría Gubernamental?

2- Compare lo que se conoce como Auditoría al sistema de cómputo y una auditoría alrededor de la computadora.

Capítulo 3

Normas ético-morales que regulan la actuación del auditor

Sumario

Marco conceptual de la ética.
Principios de axiología y valores éticos.
Criterios y responsabilidades del auditor.

Propósito del capítulo

El propósito de este capítulo consiste en ofrecer tanto al estudiante como al profesional las reglas básicas de conducta con que debe conducirse un auditor tanto dentro como fuera de su recinto de trabajo.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Presentar los conceptos fundamentales de conducta que ayudan a identificar la correcta actuación profesional, laboral, social y personal de un auditor tomando en cuenta las principales directrices ético-morales, profesionales, sociales y personales que regulan su accionar ante las empresas, sus colegas de profesión y ante él mismo como especialista en la materia.

- Identificar los criterios y obligaciones fundamentales que debe cumplir el auditor en el campo ético, moral y profesional.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
3.1 Marco conceptual de la ética	52
3.1.1 Conceptos básicos relacionados con la ética	53
3.2 Principios de axiología y valores éticos	66
3.2.2 Principios y valores del auditor	69
3.3 Criterios y responsabilidades del auditor	73
3.3.2 Criterios y responsabilidades del auditor en el aspecto profesional-personal	76
3.3.3 Criterios y responsabilidades del auditor en el aspecto estrictamente laboral	79
3.3.4 Criterios y responsabilidades del auditor en el aspecto de elementos de juicio	82
3.3.5 Criterios y responsabilidades del auditor en su respuesta ante las autoridades, leyes, normas y reglamentos	83

COMENTARIOS GENERALES

Es muy grande la responsabilidad que tiene el auditor ante la sociedad, sus colegas de profesión y las empresas, porque el hecho de permitirle que revise profesionalmente documentos, información, activos y operaciones de la empresa, representa la confianza que se le otorga como profesional especializado en la materia; más aún, cuando se acepta su opinión en el dictamen que emite, se da por sentada su calidad moral, profesional y ética.

Por eso, la sociedad, los funcionarios y empleados de las empresas casi siempre están convencidos de que la actuación de un auditor siempre está respaldada por una gran experiencia, sólidos conocimientos en auditoría y en la utilización de las herramientas de evaluación, que corresponden a su área de revisión.

Relativo a la ética o moral, o que está de acuerdo con sus principios o su exigencia. Parte de la filosofía que estudia los fundamentos y las normas de la conducta humana. Dos son las corrientes principales: la que relaciona la ética con la naturaleza misma del hombre, la que no ve en las normas de conducta sociales más que unos convenios sociales reguladores lo que considera bueno o malo, conveniente o nocivo.

Lo mismo ocurre con la actuación del profesional dedicado a la auditoría, porque éste debe conducirse de acuerdo con las normas de conducta social, moral, religiosa, jurídica y profesional, las cuales regularán su actuación como profesional de la auditoría ante la sociedad, autoridades, empresas y empleados de estas últimas.

(Para ahondar más en este tema, refiérase a las páginas de la 52 a la 65 del libro de texto).

La axiología es la ciencia que trata de los valores de carácter moral que pretenden normar la conducta de los individuos ante la sociedad. Es evidente que el auditor, como parte de una sociedad, debe considerar y acatar los valores ético-morales regulados mediante esta ciencia. Por ello, es necesario profundizar un poco sobre estos valores antes de proponer las normas éticas que regularán la actuación del auditor de sistemas computacionales.

Se dice de quien actúa con veracidad, sinceridad, franqueza, honradez e imparcialidad en el cumplimiento de cualquier encomienda, actividad o trabajo.

Integridad

La persona que posee esta cualidad es de principios sólidos y fundamentales y actúa en forma honorable, recta, valerosa y se apega a sus convicciones, cualesquiera que éstas sean y las hace respetar. Lo mismo sucede con el cumplimiento de los compromisos, trabajo y actividades que se le encomiendan.

Cumplimiento

Se dice que una persona es cumplida y digna de confianza cuando cumple escrupulosamente sus promesas, sus compromisos y respeta la esencia y letra de los convenios que contrae.

Lealtad

En el caso del auditor, se considera que es la fidelidad que guarda con sus auditados al no utilizar ni revelar información que obtiene en forma confidencial de la empresa que audita.

Imparcialidad

Es cuando una persona, en este caso el auditor, busca actuar de manera equitativa en el cumplimiento de su trabajo o de cualquier acción que emprende al tratar de ser siempre justo, honesto y razonable en los juicios que emite y evitar tomar partido hacia algún lado en cualquier auditoría.

Además, como profesional de la auditoría, siempre debe estar dispuesto a reconocer errores y a cambiar de posición, creencia y acciones cuando sea necesario y debe procurar actuar siempre con un amplio compromiso de justicia, equidad, tolerancia y trato igual con los funcionarios y empleados que audite.

Respeto a los demás

En la cualidad que caracteriza a quien demuestra consideración y estima por la dignidad, la intimidad y el derecho de autodeterminación de la gente al actuar

siempre de manera cortés, expedita y decente y al proporcionarles lo que necesitan para la mejor toma de decisiones sin avergonzarlos ni degradarlos.

Ciudadano responsable

Se dice de la persona, en este caso del auditor, está dispuesta a respetar y hacer cumplir las leyes, normas y reglamentos del país al aceptar la responsabilidad y solidaridad tanto en los derechos como en las obligaciones, que le imponen la sociedad, las empresas y sus conciudadanos.

Ver por los demás

Cuando una persona es atenta y amable en su trato cuando es compartida, generosa y, además, tiene un amplio sentido de ayuda hacia sus semejantes.

Búsqueda de la excelencia

Es evidente que las personas de éxito así como los auditores profesionales destacados son aquellos que buscan la excelencia (que sobresalen en mérito y bondad) como parte fundamental de su ser al cumplir indefectiblemente con la responsabilidad personal y profesional que requiere esta importante actividad.

Responsabilidad

Se entiende como responsabilidad al hecho de aceptar el compromiso que implica la toma de decisiones y las consecuencias previstas por las acciones y omisiones en el cumplimiento del trabajo, de las actividades cotidianas y del desempeño profesional.

Confiabilidad

Esta es una de las cualidades más buscadas en el profesional que se dedica a la auditoría, porque se asume que su actuación está apegada a las normas y criterios que regulan esta profesión.

Veracidad

En el caso del auditor, se refiere a la utilización de las herramientas, métodos y procedimientos de auditoría con los cuales puede obtener datos fidedignos, apegados a los sucesos verdaderos y con resultados reales, que le permiten hacer juicios fidedignos y confiables.

(Para ahondar más en este tema, refiérase a las páginas de la 66 a la 73 del libro de texto).

Estos criterios son presentados con el propósito de señalar al auditor el rumbo ético y moral que deberá seguir para cumplir y hacer respetar dichos criterios y responsabilidades y para que norme su actuación profesional ante las empresas, la sociedad y sus colegas. Debe esmerarse en el buen cumplimiento de esta actividad; no sólo cuando le sea encomendada una auditoría, sino también en su desempeño personal.

Tener la suficiente independencia mental y profesional para ejercer la profesión de auditor.

Contar con la calificación, habilidad, aptitud y experiencia profesional en auditoría.

Manejar adecuadamente las relaciones personales, profesionales y laborales entre él y el auditado.

Utilizar la misma metodología y procedimientos de evaluación establecidos por los responsables de la gestión de la auditoría.

No modificar, ocultar o destruir evidencias en la evaluación.

Ser discreto, confiable y profesional con la información y los resultados de la evaluación.

Actuar con equidad, imparcialidad, razonabilidad y profesionalismo.

Emitir dictámenes profesionales, independientes y razonables.

Cumplir con los planes, programas, contratos y presupuestos acordados.

Aplicar los métodos, técnicas y procedimientos de evaluación debidamente avalados.

Revisar y profundizar sobre los puntos relevantes de las áreas que serán auditadas.

Elaborar las evaluaciones, dictámenes e informes conforme a las normas y lineamientos que regulan el desarrollo de las auditorías.

Acatar las normas disciplinarias y de conducta de la empresa de auditoría externa así como las de la empresa auditada.

Capacitar al personal subalterno.

Verificar la autenticidad de hechos, fenómenos y evidencias encontradas.

Apegarse a las normas y lineamientos básicos de auditoría emitidos por asociaciones y colegios de profesionales, así como a los de la propia empresa que se esté auditando.

Aplicar de manera uniforme los métodos, técnicas, procedimientos, herramientas y criterios de evaluación.

Evaluar en forma independiente, libre de influencias, presiones y prejuicios.

La responsabilidad del auditor va más allá de emitir un dictamen, porque el resultado de éste también puede llegar a otros interesados, aparte de la empresa, quienes pueden utilizarlo para efectuar acciones de carácter laboral e incluso acciones de tipo legal y/o penal.

Por esta razón, el dictamen del auditor debe estar bien fundamentado, apoyado en evidencias y plasmado con la mayor veracidad, debe contener la valoración de todo lo contemplado durante la revisión y debe estar totalmente apoyado en técnicas, métodos y procedimientos reconocidos para hacer una auditoría. Esto es lo que le dará vigencia y confiabilidad al trabajo del auditor.

Además de lo anterior, la actuación de este profesional puede tener resultados marginales en caso de que encontrara delitos, faltas e infracciones en perjuicio de la empresa y sus empleados, de las leyes, las normas y los reglamentos vigentes, los cuales tendría que denunciar con fundamentos.

Igual pudiera darse el caso de que los resultados de su actuación como auditor tuvieran que ser verificados y rectificados como parte de alguna acción de carácter legal.

También, puede darse el caso de que el propio auditor incurra en un trabajo no honesto, poco profesional y sin la integridad que se requiere en este tipo de trabajos. En este caso, el auditor sería el responsable de cometer esos delitos y su actuación profesional y laboral tendría que ser evaluada.

Por estas razones, cobran vigencia los criterios y obligaciones que a continuación se analizan:

- ✓ CIVILES por delitos e infracciones debidos a negligencia, impericia, abuso de confianza o dolo, tanto en los resultados encontrados como en la realización de la auditoría misma.

- ✓ FISCALES por los delitos e infracciones de carácter fiscal que se descubran o realicen.

- ✓ PENALES por delitos de fraude, robo, abuso de confianza, encubrimiento, revelación del secreto y responsabilidad profesionales por parte del auditado y del propio auditor.

- ✓ JUDICIALES por los resultados de la auditoría y por la actuación del auditor.

- ✓ LABORALES por las faltas detectadas al reglamento interno de la institución así como a la Ley Federal del Trabajo.

(Para ahondar más en este tema, refiérase a las páginas de la 73 a la 87 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- ¿Con qué propósito se presentan al auditor los criterios y responsabilidades como complemento a los principios éticos y morales que todo auditor debe cumplir?

2- ¿Cuánta importancia tienen para el auditor los principios de equidad, imparcialidad, razonabilidad y profesionalismo?

3- El trabajo del auditor puede verse influenciado o recibir presiones externas. ¿Qué opina al respecto?

Capítulo 5

Control interno informático

Sumario

Controles internos para la organización del área de informática.
Controles internos para el análisis, desarrollo e implementación de sistemas.
Controles internos para la operación del sistema.
Controles internos para los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados.
Controles internos para la seguridad del área de sistemas.

Propósito del capítulo

El propósito de este capítulo es presentar tanto al estudiante como al profesional de auditoría el origen y los responsables de establecer el control interno en las TICS.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Estudiar los conceptos y las características fundamentales del control interno en los sistemas computacionales a fin de identificar sus principales aplicaciones en la auditoría de sistemas para entender cómo se pueden satisfacer, con eficiencia y eficacia, las necesidades de evaluación, razonabilidad y oportunidad en la protección y seguridad de los bienes, de la información y del personal del área de sistemas de una institución.
- Analizar el desarrollo de las actividades, operaciones y resultados en el procesamiento de la información de las áreas de sistemas de una institución.
- Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de una empresa.
- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en una empresa.
- Implementar métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales para satisfacer los requerimientos de sistemas en una empresa.
- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de una empresa.
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en una empresa.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

COMENTARIOS GENERALES

Controles internos para la organización del área de informática

Dirección

La dirección es uno de los subelementos básicos del control interno en cualquier empresa, porque ésta es la función primordial de la entidad o persona

que tiene la misión de dirigir las actividades en la institución o en un área específica así como la de coordinar el uso de los recursos disponibles en el área para cumplir el objetivo institucional.

Los recursos de informática son muy especializados y frecuentemente muy costosos, pero son de suma importancia en las áreas de sistemas; por lo tanto, es necesario aprovecharlos de la mejor manera posible, lo cual solo se puede lograr mediante el establecimiento de la dirección como elemento del control interno. Con ello, se contribuye a la adecuada coordinación del uso y aprovechamiento de los recursos computacionales.

La coordinación de recursos

Como parte fundamental de la dirección del área de sistemas, se tienen que asignar y distribuir de manera correcta los recursos informáticos disponibles en la empresa con el fin de que dichos recursos sean más equitativos y productivos.

La supervisión de actividades

Es la vigilancia que realiza quien dirige el área de sistemas sobre la realización adecuada de las funciones y actividades que se tienen encomendadas en esta área al supervisar el trabajo que se realiza con los recursos informáticos de la empresa.

La delegación de autoridad y responsabilidad

Su finalidad es obligar al personal del área, de acuerdo con la delegación de autoridad y responsabilidad, a cumplir con las tareas, funciones y operaciones que tienen encomendadas.

La asignación de actividades

Este subelemento se aplica cuando la dirección instituye una definición clara y concreta de todas las funciones, tareas y operaciones de cada puesto con el fin de cumplir de manera adecuada con los objetivos del área de sistemas.

La distribución de recursos

Es la asignación que se hace de los recursos informáticos disponibles en el área de sistemas con el propósito de que los empleados de esta área cumplan eficientemente con las actividades y tareas que tienen encomendadas.

División de trabajo

A continuación se presentan las funciones básicas de cualquier centro de cómputo:

Dirección general del área de informática

Esta es la entidad encargada de integrar, coordinar y supervisar el buen desarrollo de las funciones y actividades de los demás recursos del área. También, es la entidad encargada de planear, organizar, dirigir y controlar los objetivos, programas y presupuestos de los recursos asignados del área de informática.

Área de análisis y diseño

Es la unidad de trabajo encargada de estudiar las necesidades de procesamiento e información de la empresa, así como de proponer mejoras y cambios en el desarrollo de nuevos sistemas por medio de las metodologías de análisis y diseño de éstos.

Área de programación

Sus integrantes son los responsables de realizar todas las actividades y operaciones que se requieren para codificar adecuadamente los programas a fin de lograr el buen funcionamiento del área de cómputo en la empresa.

Área de sistemas de redes

Es el área que está destinada a la administración y control de los sistemas de redes algunas de sus funciones son la configuración, manejo y mantenimiento de dichos sistemas a fin de satisfacer las necesidades de cómputo de la empresa.

Área de operación

Es el área encargada de realizar la operación, procesamiento y uso de los sistemas computacionales así como de la asignación de sus recursos íntegros para servicio de los usuarios y de las áreas de la empresa.

Área de telecomunicación

Es la unidad administrativa responsable de todos los servicios de comunicación interna o externa del sistema.

Área de administración

Es la unidad que se encarga de brindar todo el apoyo de tipo administrativo que se requiere en el centro de cómputo a fin de que pueda realizar con eficiencia y eficacia todas sus funciones.

Asignación de responsabilidad y autoridad

Este subelemento nos a ayuda a garantizar la eficiencia y eficacia del control interno en las unidades de sistemas, porque complementa la división del trabajo y delimita claramente la autoridad y la responsabilidad que tendrá cada integrante de esas áreas. Con ello, se asegura el mejor desarrollo de las

actividades, funciones y tareas y, consecuentemente, la realización del procesamiento de información en la empresa será más eficaz.

Establecimiento de estándares y métodos

En cualquier área de sistemas es de suma importancia estandarizar el desarrollo de todas las actividades y funciones a fin de que éstas se realicen de manera uniforme según las necesidades concretas de las unidades de informática que integran la empresa. En esta estandarización se deben respetar la división del trabajo y la asignación de actividades específicas.

La estandarización constituye un aspecto básico que se debe incluir para el establecimiento del control interno informático en cualquier empresa.

El siguiente aspecto es Perfiles de puestos:

Perfiles de puestos

Otro aspecto fundamental para la adopción de este elemento del control interno informático consiste en identificar y establecer requisitos, habilidades, experiencia y conocimientos específicos que necesita tener el personal, que ocupa un puesto en el área de sistemas.

Es trascendental destacar la importancia del uso del perfil de puestos para la selección adecuada del personal, que ocupará los puestos dentro del área de sistemas debido a que en este documento se establecerán en forma precisa y correcta las características, conocimientos y habilidades que deberán tener quienes ocupen dichos puestos.

(Para conocer ahondar más en el tema refiérase a las páginas de la 137 a la 145 del libro de texto).

Controles internos para el análisis, desarrollo e implementación de sistemas.

Para entender este elemento del control interno informático, es vital que primero presentemos las principales fases de lo que se puede entender como análisis y diseño de sistemas:

1. Análisis del sistema actual.
2. Diseño conceptual.
3. Diseño detallado.
4. Programación.
5. Pruebas y correcciones.
6. Documentación del sistema.
7. Capacitación de usuarios.
8. Implementación del sistema.
9. Liberación del sistema.
10. Mantenimiento.

El uso de esta metodología, la cual sólo presentamos en sus principales fases, requiere un seguimiento paso a paso y un uso casi irrestricto de todas sus fases y de cada una de las etapas que las integran. Con la aplicación de esta metodología para el desarrollo de un proyecto, se puede garantizar el análisis, el desarrollo y la implementación correctos de cualquier sistema.

A continuación se proponen los siguientes subelementos para el cumplimiento de este elemento del control interno en el área de sistemas:

Estandarización de metodologías para el desarrollo de proyectos

1. Asegurar que el beneficio del sistema sea óptimo.
2. Elaborar estudios de factibilidad del sistema.
3. Garantizar la eficiencia y eficacia en el análisis y diseño del sistema.
4. Vigilar la efectividad y eficacia en la implementación y el mantenimiento del sistema.
5. Lograr un uso eficiente del sistema por medio de su documentación.

La aplicación de una metodología estandarizada para el desarrollo de un proyecto informático garantiza la uniformidad en la aplicación de cualquier sistema y contribuye en gran medida a la máxima eficiencia en el uso de los recursos informáticos del área de sistemas; por esta razón, resulta necesario estandarizar el desarrollo de los proyectos de sistemas en una empresa.

Precisamente, se busca implementar este subelemento del control interno para el área de sistemas, cuyo objetivo será estandarizar su desarrollo.

Es indispensable contar con un elemento de control que regule el desarrollo correcto de un proyecto, porque este control es el sustento indispensable para estandarizar la realización de cualquier proyecto informático. Así, se contribuye a la máxima eficiencia en la realización de dicho proyecto.

Para conocer los principales puntos, que se deberán analizar durante una auditoría de sistemas, en cuanto al desarrollo de proyectos informáticos, a continuación se presentan las estandarizaciones básicas que se deben analizar durante cualquier revisión.

Estandarización de métodos para el diseño de sistemas.
Lineamientos en la realización de sistemas.
Uniformidad de funciones para desarrollar sistemas.
Políticas para el desarrollo de sistemas.
Normas para regular el desarrollo de proyectos.
Asegurar que el beneficio del sistema sea óptimo.

Al implementar un nuevo sistema se busca optimizar el desarrollo de las actividades que normalmente se llevan a cabo en la empresa o en cualquiera de sus áreas. Con ello, se pretenden mejorar las operaciones normales de

cómputo que se realizan en la empresa a fin de incrementar la eficiencia de sus sistemas actuales.

De hecho, el objetivo final, que se espera en las empresas con la implantación de un sistema informático, se puede circunscribir a dos aspectos concreto: Beneficios tangibles y beneficios intangibles.

Beneficios tangibles

Con el establecimiento de los sistemas en la empresa se pretende lograr mejoras sustanciales, realmente palpables, por parte de quienes utilizan dichos sistemas, lo cual exige que puedan ser cuantificados resultados.

Beneficios intangibles

Los beneficios que se espera obtener de los sistemas de cómputo son intangibles, porque sus resultados no pueden ser contados ni físicamente palpables; sin embargo, existen formas de cuantificación. De esta forma, la mayoría de los sistemas computacionales tienen ciertos valores cualitativos y es difícil otorgarles un valor cuantitativo.

Un aspecto específico de aplicación de este subelemento consiste en que, para el análisis y diseño del nuevo sistema, se tienen que establecer todos los beneficios que se obtendrían con el desarrollo de un sistema al enfocarlos desde múltiples puntos de vista.

Algunos de los beneficios son los siguientes:

1. El nivel informático, porque con la instalación de un nuevo proyecto se pretende mejorar los sistemas informáticos de la empresa.
2. El económico, debido a que los sistemas tienen un valor económico y con su desarrollo se pretende economizar el servicio informático de las empresas.
3. El social, porque congrega gente alrededor de los sistemas que se implementan en las empresas. Esta gente se interrelaciona con sus congéneres al crear vínculos sociales con ellos y con la ayuda de los sistemas.
4. El de los servicios, porque el propósito final de un sistema computacionales proporcionar servicios sistematizados a las áreas de una empresa.
5. El administrativo, porque ayuda al mejor manejo de la gestión informática de las empresas.
6. El operacional, porque con su adopción ayuda a la regulación y mejor realización de todas las operaciones del sistema computacional de la empresa.

Elaborar estudios de factibilidad del sistema

Todo proyecto de informática se evalúa desde dos criterios específicos: la viabilidad y la factibilidad. En estos dos factores se deben considerar por separado los puntos de vista operativo, económico, técnico y administrativo para poder valorar la optimización del nuevo sistema.

El resultado final de estas valoraciones será la certificación y confianza de que el proyecto será aplicable a las necesidades de la empresa para así poder satisfacer sus requerimientos de control interno de informática.

Debemos entender que un nuevo proyecto sólo se justifica si con él se busca satisfacer la eficiencia y eficacia de las actividades de la empresa, lo cual se logra por medio de la adopción de una metodología estándar en la realización de los sistemas para garantizar un buen resultado final con su implementación.

Entonces, resulta necesario contar con varias herramientas, técnicas, métodos y elementos que permitan uniformar los procedimientos, estándares, normas y lineamientos requeridos para desarrollar eficientemente estas actividades:

La adopción y seguimiento de una metodología institucional.

Adoptar una adecuada planeación, programación y presupuestación para el desarrollo del sistema.

Contar con la participación activa de los usuarios finales o solicitantes del nuevo sistema para garantizar su buen desarrollo.

Contar con personal que tenga la disposición, experiencia, capacitación y conocimientos para el desarrollo de sistemas.

Utilizar los requerimientos técnicos necesarios para el desarrollo del sistema, como son el *hardware*, *software* y personal informático.

Diseñar y aplicar las pruebas previas a la implementación del sistema.

Supervisar permanentemente el avance de actividades del proyecto.

No basta con elaborar el sistema, también se debe implementar totalmente para liberar el cargo del propio usuario y proporcionar un mantenimiento permanente que garantice su efectividad. Sólo mediante la adopción de este subelemento del control interno se pueden asegurar tanto la eficacia como la eficiencia de los sistemas computacionales de la institución.

Conviene señalar que es de suma importancia que, antes o durante la implementación del sistema, se proporcione la capacitación a sus usuarios finales debido a que sólo así se pueden garantizar la eficiencia y eficacia en la implementación del proyecto.

También, se debe contar con la completa documentación de respaldo y apoyo que sirva de consulta a los usuarios para el buen uso del sistema.

Otra garantía del buen funcionamiento del sistema es el establecimiento del control interno informático en relación con la documentación de dicho sistema a fin de que sirva de ayuda al usuario y al propio desarrollador del proyecto, lo cual contribuirá a su mejor operación y a su posterior modificación.

Algunos de los principales documentos del sistema son los siguientes:

Manuales e instructivos del usuario.
Manual e instructivo de operación del sistema.
Manual técnico del sistema.
Manual para el seguimiento del desarrollo del proyecto del sistema.
Manual e instructivo de mantenimiento del sistema.

Otros manuales e instructivos del sistema

(Para ahondar más del tema, refiérase a las páginas de la 145 a la 157 del libro de texto).

Controles internos para la operación del sistema

Resulta conveniente contar con un elemento de control interno que evalúe la adecuada operación de los sistemas. En este caso, será la adopción de un elemento que se encargue de vigilar y verificar la eficiencia y eficacia en la operación de dichos sistemas.

Para entender el papel que juega este elemento en el desarrollo de las actividades del centro de cómputo, podemos señalar que su existencia ayuda a garantizar el cumplimiento de los objetivos básicos del control interno.

Para prevenir y, en su caso, corregir los posibles errores de operación, ya sean involuntarios o premeditados, lo mejor es implementar mecanismos de control que permitan verificar la exactitud, suficiencia y calidad de los datos que serán procesados al vigilar el adecuado cumplimiento de la captura, el procesamiento y la emisión de resultados.

Cabe resaltar la utilidad de la aplicación de este elemento del control interno informático para las operaciones de los sistemas, porque requieren una permanente actualización debido a las siguientes razones:

- ✓ Constantes cambios en las características y modalidades del funcionamiento de los centros de cómputo, de sus sistemas y de las bases de datos.
- ✓ Creciente modificación en los sistemas de red y multiusuarios, la adopción de nuevas técnicas de configuración, *software* y otras formas de comunicación entre los sistemas y componentes.

- ✓ Niveles de acceso al sistema por parte del administrador, operadores y usuarios, según su nivel de participación a fin de satisfacer las necesidades del procesamiento de datos.
- ✓ Actualización en la programación de sistemas de aplicación, que permitan el buen funcionamiento de los sistemas computacionales de la empresa.
- ✓ Los programas de supervisión de los sistemas operativos con los cuales se pueden realizar supervisiones de manera rutinaria a los archivos de datos e, incluso, un monitoreo de las operaciones del sistema y la emisión de los resultados de dicho monitoreo, tipo auditoría del sistema, los cuales permiten evaluar su funcionamiento.
- ✓ Vigilar y delimitar los accesos y usos de programas y archivos con información privilegiada y otras formas específicas de procesamiento de información, entre otras muchas operaciones.

Otro aspecto de suma importancia para un adecuado control interno es vigilar la manipulación de la información que será procesada en el sistema, así como establecer las medidas necesarias para controlar su acceso y niveles de uso, para así prevenir un uso inadecuado de los sistemas, ya sea para beneficio de terceros, para realizar algún boicot en la institución, propiciar errores durante el proceso de datos o cualquier otro aspecto que sea ajeno de la operación normal de la empresa.

Es evidente que un centro de cómputo debe contar con las normas, programas y medidas de seguridad que le garanticen la buena operación y la adecuada custodia de sus bienes, programas e información. Esto se logra a través de planes y programas de seguridad de carácter físico (*hardware*, instalaciones y equipos periféricos asociados) y los de carácter lógico (sistemas operativos, lenguajes, programas e información).

Para entender la importancia de este elemento, recordemos algunos de los principales atributos de la información, como la confiabilidad, la oportunidad, la veracidad y la suficiencia. Estos son los elementos básicos que se utilizan para establecer un control interno adecuado en un centro de información debido a que con su adopción y uso permanente, como norma de trabajo, contribuyen a la cabal comprensión del objetivo fundamental del área de sistemas para la empresa en cuanto a la captura y procesamiento de datos, emisión de resultados y custodia de la información.

(Para ahondar más en el tema, refiérase a las páginas de la 157 a la 160 del libro de texto).

Controles internos para los procedimientos de entrada de datos, procesamiento de información y emisión de resultados

El control interno informático constituye el aspecto más importante para la adopción de estos controles en el área de sistematización, por lo que ~~es que~~ son de gran ayuda para la confiabilidad que brindan en el procesamiento de información.

Cuando entendamos que un sistema de información es un procedimiento simple de entrada, proceso y salida, en donde un dato de entrada se transforma en información útil de salida mediante algún procesamiento anterior, entenderemos también que el control interno informático es útil para verificar que este procedimiento se desarrolle correctamente.

Para una mejor comprensión de este punto, señalaremos que dicho proceso está compuesto de tres fases fundamentales:

1. La entrada de datos al sistema.
2. El procesamiento de datos por medio de un sistema de procesamiento interno (caja negra).
3. La emisión de resultados útiles para la toma de decisiones.

Estas fases son las que dan vigilancia a cualquier sistema. Utilizando como referencia lo anterior, a continuación analizaremos los siguientes subelementos del control interno:

- ✓ Verificar la existencia y funcionamiento de los procedimientos de captura de datos.
- ✓ Comprobar que todos los datos sean debidamente procesados.
- ✓ Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
- ✓ Comprobar la suficiencia en la emisión de información.

(Para ahondar más en el tema, refiérase a las páginas de la 160 a la 164 del libro de texto).

Controles internos para la seguridad del área de sistemas

Se refiere a lo relacionado con la seguridad y salvaguarda de los bienes tangibles de los sistemas computacionales de la empresa, la seguridad, la prevención de riesgos y protección de los recursos físicos informáticos de la empresa.

Seguridad lógica

Lo constituye lo relativo a la seguridad de los bienes intangibles de los centros informáticos, las medidas de seguridad, protección y forma de acceso a los archivos e información.

Seguridad de las bases de datos

Es la protección específica de la información que se maneja en las áreas de sistemas de la empresa, ya sea a través de las medidas de seguridad y control que limiten el acceso y uso de esa información o mediante sus respaldos periódicos con el fin de mantener su confidencialidad y prevenir las alteraciones, los descuidos, los robos y otros actos delictivos que afecten su manejo.

Seguridad en la operación

Alude a la seguridad en la operación de los sistemas computacionales en cuanto a su acceso y aprovechamiento por parte del personal informático y de los usuarios, al acceso a la información y base de datos, a la forma de archivar y utilizar la información y los programas institucionales, a la forma de proteger la operación de los equipos, los archivos y programas, así como las instalaciones, mobiliario, entre otros aspectos.

Seguridad del personal de informática

Se refiere a la seguridad y protección de los operadores, analistas, programadores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los beneficiarios de la información.

Seguridad de las telecomunicaciones

Es todo lo relacionado con la seguridad y protección de los niveles de acceso, privilegios, recepción y envío de información por medio del sistema de cómputo, protocolos, *software*, equipos e instalaciones que permiten la comunicación y transmisión de la información en la empresa.

Seguridad en las redes

Se relaciona con la seguridad y el control de contingencias para la protección adecuada de los sistemas de redes de cómputo en cuanto a la salvaguarda de información y datos de las redes, la seguridad en el acceso a los sistemas computacionales a la información y a los programas del sistema.

Prevención de contingencias y riesgos

Son todas las acciones tendientes a prevenir y controlar los riesgos y posibles contingencias que se presenten en las áreas de sistematización, las cuales prevendrán desde accidentes en los equipos, en la información y en los programas hasta la instalación de extintores, rutas de evacuación, resguardos y medidas preventivas de riesgos internos y externos, así como la elaboración de programas preventivos y simulaciones para prevenir contingencias y riesgos informáticos.

Con el establecimiento de los siguientes subelementos del control interno informático se busca determinar las bases fundamentales sobre las que se establecerán los requerimientos para manejar la seguridad de los sistemas de información.

Identificar aquellos elementos que pueden influir en la seguridad de sus instalaciones, de sus programas y de la información que se maneja en ellos y del personal que los opera, ayudará a identificar las eventualidades que pueden llegar a presentar en dicha área.

Control de accesos físicos del personal al área de cómputo

Es el establecimiento de las medidas tendientes a controlar el acceso de las personas que tengan que entrar la centro de cómputo.

Control de accesos al sistema, a las bases de datos, a los programas y a la información

Es el control que se establece en el sistema en forma administrativa por medio de procedimientos, claves y niveles de acceso, que permiten el uso del sistema, de sus archivos y de su información a los usuarios y al personal autorizado.

Uso de niveles de privilegio para acceso, palabras clave y control de usuarios

Se manejan, mediante un *software* especial las limitaciones y los privilegios de los usuarios en el uso del sistema, ya sea al no permitir el acceso a ciertos archivos y programas o con el uso de contraseñas con las cuales se pueda ingresar al sistema.

Monitoreo de accesos de usuarios, información y programas

Es el monitoreo que realiza el administrador del sistema con el propósito de verificar el uso del sistema, del *software*, de los archivos y de la información que está permitida al usuario.

Existencia de manuales e instructivos, así como difusión y vigilancia del cumplimiento de los reglamentos del sistema

Es el seguimiento de los diferentes manuales e instructivos a fin de controlar el uso de los sistemas, programas y archivos, así como el cumplimiento del reglamento de uso del centro de sistematización por parte de su personal y de sus usuarios.

Identificación de los riesgos y amenazas para el sistema, con el fin de adoptar las medidas preventivas necesarias

Es la identificación de los posibles riesgos y contingencias que se pueden presentar en el área de sistematización. Estas contingencias pueden tener un origen humano o un origen natural.

Elaboración de planes de contingencia, simulacros y bitácoras de seguimiento

Es el control de las contingencias y riesgos que se pueden presentar en el área de sistemas; estas contingencias se pueden evitar, controlar o remediar a través de planes y programas preventivos específicos, en los cuales se presenten las actividades a realizar antes, durante y después de alguna contingencia.

Controles para la seguridad física del área de sistemas

Es la sistematización para la protección y custodia de los equipos de cómputo, periféricos, mobiliario y equipo asignado a esa área, así como la protección y seguridad del personal, de los usuarios y demás personal involucrado en el centro de cómputo:

Inventario del *hardware*, mobiliario y equipo

Resguardo del equipo de cómputo.
Bitácoras de mantenimientos y correcciones.
Controles de acceso del personal al área de sistemas.
Control del mantenimiento a instalaciones y construcciones.
Seguros y fianzas para el personal, equipos y sistemas
Contratos de actualización, asesoría y mantenimiento del *hardware*.

Controles para la seguridad lógica de los sistemas

Control para el acceso al sistema, a los programas y a la información.
Establecimiento de niveles de acceso.
Dígitos verificadores y cifras de control.
Palabras clave de acceso.
Controles para el seguimiento de las secuencias y rutinas lógicas del sistema.

Controles para la seguridad de las bases de datos

Es el bien que más se debe proteger. El control interno informático ayuda a proteger las bases de datos de la empresa, por medio de controles especiales y medidas preventivas y correctivas. Con las restricciones de acceso al sistema se pueden evitar posibles alteraciones, uso fraudulento, piratería destrucción y sabotaje de la información de la empresa.

Los siguientes son algunos de los controles que se pueden establecer para la seguridad de las bases de datos de la empresa:

Programas de protección para impedir el uso inadecuado y la alteración de datos de uso exclusivo.
Respaldos periódicos de información.
Planes y programas para prevenir contingencias y recuperar información.
Control de accesos a las bases de datos.
Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos.

Controles para la seguridad en la operación de los sistemas computacionales

Es necesario establecer controles y medidas preventivas para evitar accidentes, actos dolorosos premeditados o negligencias que repercutan en la operación y funcionamiento del sistema o en la emisión de resultados del procesamiento de la información.

Los siguientes aspectos deben ser tomados en cuenta para la seguridad en la operación del sistema:

Controles para los procedimientos de operación.
Controles para el procesamiento de información.
Controles para la emisión de resultados.
Controles específicos para la operación de la computadora
Controles para el almacenamiento de información.
Controles para el mantenimiento del sistema.

Controles para la seguridad del personal de informática

El activo más valioso de las empresas es el personal que labora en ellas, debido a que es el que realiza todas las funciones y actividades desde la dirección hasta la operación de sus áreas y equipos.

Es indispensable el establecimiento de los controles internos informáticos en los centros de cómputo a fin de ayudar a proteger y salvaguardar la seguridad de este valioso activo del área de sistematización y de la empresa. Entre los principales subelementos de control que se pueden adoptar para salvaguardar la seguridad del personal de estas áreas se encuentran las siguientes:

Controles administrativos de personal.
Seguros y fianzas para el personal de sistemas.
Planes y programas de capacitación.

Controles para la seguridad en la telecomunicación de datos

Es necesario implementar controles internos informáticos en las áreas de sistematización para asegurar el buen funcionamiento de los sistemas de transmisión de datos de la empresa, es decir, desde el establecimiento de protocolos de comunicación, contraseñas y medios controlados de transmisión hasta la adopción de medidas de verificación de transmisión de la información, las cuales pueden ser dígitos verificadores, dígitos de paridad, protocolos de acceso a frecuencias y otras especificaciones concretas del área de transmisión de datos.

Controles para la seguridad en sistemas de redes y multiusuarios

El establecimiento de estos controles para la seguridad en sistemas de redes y sistemas multiusuarios de una empresa es de vital importancia, porque se deben establecer medidas específicas para la protección, resguardo y uso de programas, archivos e información y de sus demás características.

(Para ampliar más la información del tema, refiérase a las páginas de la 164 a la 178 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- ¿Por qué considera que la división del trabajo es un elemento de control interno? Relacione este concepto con el concepto de burocracia en la función pública.

2- ¿Por qué es importante, bajo el tema el control interno, la estandarización?

3- ¿Por qué considera que la prevención de riesgos y contingencias es importante a la hora de elaborar el control interno?

4- Se habla de múltiples riesgos y controles para minimizar estos riesgos. ¿Por qué considera, usted, que se debe aplicar un especial cuidado en los sistemas de redes y multiusuario?

Capítulo 6

Metodología para realizar auditorías de sistemas computacionales

Sumario

Marco conceptual de la metodología para realizar auditorías de sistemas computacionales.
Metodología para realizar auditorías de sistemas computacionales.
Primera etapa. Planeación de la auditoría de sistemas computacionales.
Segunda etapa. Ejecución de la auditoría de sistemas computacionales.
Tercera etapa. Dictamen de la auditoría de sistemas computacionales.

Propósito del capítulo

El propósito de este capítulo es presentar las diferentes metodologías que se pueden emplear a la hora de realizar una auditoría en los sistemas computacionales.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Proponer una metodología específica aplicable a la realización de cualquier tipo de auditoría en el campo de los sistemas computacionales.

- Planear, seleccionar las herramientas, desarrollar y presentar los resultados de las auditorías con base en las necesidades concretas de revisión en el ambiente de sistemas.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
6.1 Marco conceptual de la metodología para realizar auditorías de sistemas computacionales	182
6.2 Metodología para realizar auditorías de sistemas computacionales	185
6.3 Primera etapa: Planeación de la auditoría de sistemas computacionales	186
6.4 Según etapa: Ejecución de la auditoría de sistemas computacionales	235
6.5 Tercera etapa: Dictamen de la auditoría de sistemas computacionales	237
6.5.1 Analizar la información y elaborar un informe de situaciones	238
6.5.2 Elaborar el dictamen final	239
6.5.3 Presentar el informe de auditoría	241

COMENTARIOS GENERALES

Llevar a cabo una auditoría de sistemas computacionales requiere una serie ordenada de acciones y procedimientos específicos, los cuales deberán ser diseñados previamente de manera secuencial, cronológica y ordenada, de acuerdo a las etapas, eventos y actividades que se requieran para su ejecución, que serán establecidos conforme a las necesidades especiales de la institución. Además, estos procedimientos se deben adaptar de acuerdo con el tipo de auditoría de sistemas por realizar y con estricto apego a las necesidades, técnicas y métodos de evaluación del área de sistematización.

Con base en lo anterior, podemos entender la necesidad de establecer una metodología específica de revisión, la cual nos permitirá diseñar correctamente los pasos por seguir en la evaluación de las áreas de sistemas y actividades elegidas a fin de que el seguimiento, desarrollo y aplicación de las etapas eventos propuestos para esa auditoría sean más sencillos.

Dicha metodología también nos servirá para establecer las técnicas, métodos y procedimientos adaptables a las características especiales de la auditoría del área específica de sistemas a evaluar, incluyendo los recursos humanos, técnicos y materiales necesarios para dicha revisión.

Metodología para realizar auditorías de sistemas computacionales

Las principales etapas que nos servirán de guía para la realización de una evaluación dentro del ambiente de sistemas computacionales son los siguientes:

Primera etapa. Planeación de la auditoría de sistemas computacionales

El primer paso para realizar una auditoría en sistemas computacionales es definir las actividades necesarias para su ejecución, lo cual se logrará mediante

una adecuada planeación; es decir, se deben identificar las razones por las que se realizará la auditoría y la determinación del objetivo, así como el diseño de los métodos, las técnicas y los procedimientos necesarios para desarrollarla y para preparar los documentos que servirán de apoyo para su ejecución y culminar con la elaboración documental de los planes, los programas y los presupuestos para dicha auditoría:

P.1 Identificar el origen de la auditoría.
P.2 Realizar una visita preliminar al área que será evaluada.
P.3 Establecer los objetivos de la auditoría.
P.4 Determinar los puntos que serán evaluados en la auditoría.
P.5 Elaborar planes, programas y presupuestos para realizar la auditoría.
P.6 Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.
P.7 Asignar los recursos y sistemas computacionales para la auditoría.

Segunda etapa. Ejecución de la auditoría de sistemas computacionales

El siguiente paso, después de la planeación de la auditoría, es su ejecución, la cual estará determinada por las características concretas, los puntos y los requerimientos que se estimaron en la etapa de la planeación.

Concretamente, tenemos los siguientes conceptos:

- Realizar las acciones programadas para la auditoría.
- Aplicar los instrumentos y herramientas para la auditoría.
- Identificar y elaborar los documentos de desviaciones.
- Elaborar el dictamen preliminar y presentarlo a discusión.
- Integrar el legajo de papeles de trabajo de la auditoría.

Tercera etapa. Dictamen de la auditoría de sistemas computacionales

El último paso de la metodología, que hemos estudiado, es emitir el dictamen, el cual es el resultado final de la auditoría de sistemas computacionales. Para ello, presentamos los siguientes puntos:

D.1 Analizar la información y elaborar un informe de situaciones detectadas

D.1.1 Analizar los papeles de trabajo.
D.1.2 Señalar las situaciones encontradas.
D.1.3 Comentar las situaciones encontradas con el personal de las áreas afectadas.
D.1.4 Realizar las modificaciones necesarias.
D.1.5 Elaborar un documento de situaciones relevantes.

D.2 Elaborar el dictamen final

D.2.1 Analizar la información y elaborar un documento de desviaciones.
D.2.2 Elaborar el informe y el dictamen formales.
D.2.3 Comentar el informe y el dictamen con los directivos del área.
D.2.4 Realizar las modificaciones necesarias.

D.3 Presentar el informe de auditoría

D.3.1 Elaboración del dictamen formal.
D.3.2 Integración del informe de auditoría.
D.3.3 Presentación del informe de auditoría.
D.3.4 Integración de los papeles de trabajo.

(Para ahondar más en el tema, refiérase a las páginas de la 179 a la 242 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- ¿Por qué una auditoría debe planearse y qué se entiende por metodología?

2- Cuando se habla de identificar los diferentes orígenes que pueden dar lugar a una auditoría uno de los más curiosos o poco comunes es cuando los mismos empleados la solicitan. Explique.

3- En la informática hay una frase muy popular que dice “si basura entra, basura sale”. ¿Como relacionaría esta frase respecto a los riesgos operativos (lógicos)? ¿Cree, usted, que aunque no entre basura aún así salga basura? Explique.

4- Cuando se planea una auditoría, debe contar con una serie de recursos para permitir que se lleve adecuadamente y sin ningún contratiempo que pudiera contrariar los objetivos. ¿Cuáles son estos recursos?

Capítulo 7

Papeles de trabajo para la auditoría de sistemas computacionales

Sumario

Contenido del legajo de papeles de trabajo.
Claves del auditor para marcar papeles de trabajo.
Cuadros, estadísticas y documentos concentradores de información.
Diagrama de sistemas.

Propósito del capítulo

El propósito de este capítulo se centra en que el auditor informático conozca la importancia de documentar todas observaciones, que realice en el transcurso de la auditoría, como forma de respaldar su trabajo.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Identificar el apoyo documental que requiere el auditor al realizar cualquier auditoría de sistemas computacionales a fin de contar con el soporte que le permita avalar y testimoniar la aplicación de técnicas, métodos y procedimientos de auditoría.

- Respaldar el trabajo de la auditoría para satisfacer las necesidades específicas de soporte documental para la auditoría de sistemas.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

COMENTARIOS GENERALES

Una de las características fundamentales de la auditoría de sistemas computacionales y, en general, de cualquier tipo de auditoría es el registro eficiente de la información que el auditor recolecta durante su evaluación. Esa información le sirve para sostener las opiniones que emite en el informe de la auditoría.

Para ello, tiene que recopilar los datos obtenidos durante la auditoría y registrarlos formalmente en documentos. Estos documentos pueden ser manuscritos, manuales, instructivos, gráficas, resultados de procesamientos, concentrados de bases de datos en disquetes, respaldos (*backups*) o cualquier otro medio escrito o electromagnético en los cuales recopilará los hechos, pruebas, tabulaciones, interpretaciones, así como el análisis de los datos obtenidos. Con todo lo anterior, el auditor tendrá un apoyo para confirmar los hechos y validar la información, que utilizará como base para elaborar el informe de auditoría.

El soporte fundamental, aparentemente simple, para la auditoría, es el registro de la información recopilada en los llamados papeles de trabajo (para el caso de auditoría de sistemas computacionales pueden ser documentos, gráficas y

medios electromagnéticos), en los cuales se anotan los hechos, los acontecimientos y los fenómenos observados durante la revisión; asimismo, estos papeles de trabajo se utilizan para transcribir y concentrar los resultados de entrevistas, cuestionarios, pruebas, encuestas, investigaciones, observaciones y opiniones del personal auditado.

En una auditoría de sistemas computacionales, los papeles de trabajo representan el sustento para registrar los datos e información que se recolectan durante la evaluación; sin embargo, por la especialidad de medios que se utilizan para el registro de la información de las áreas de cómputo, la recopilación de datos se puede realizar en documentos o en medios electromagnéticos de captura y resguardo de datos.

Para que los papeles de trabajo o medios de captura se puedan admitir como soporte documental de una auditoría de sistemas y se utilicen como fundamento en los resultados y las opiniones que presenta el auditor, es necesario que tanto en su diseño como en su uso reúnan ciertos requisitos y formalidades, que serán determinados previamente por la empresa encargada de realizar la auditoría o por el auditor responsable.

Contenido del legajo de papeles

El legajo de papeles de trabajo, por su naturaleza y contenido, es el aspecto fundamental para elaborar el dictamen de la auditoría y su uso es confidencial y exclusivo del auditor de sistemas debido a que éste integra en estos papeles de trabajo los documentos reservados y de uso exclusivo de la empresa, que recopila durante su revisión y los complementa con los registros, en papel o en medios electromagnéticos, que obtiene como evidencias formales de alguna desviación en el área de sistemas auditada.

A continuación presentaremos una propuesta para integrar estos papeles:

- ✓ Hoja de identificación.
- ✓ Índice de contenido de los papeles de trabajo.
- ✓ Dictamen preliminar (borrador).
- ✓ Resumen de desviaciones detectadas (las más importantes).
- ✓ Situaciones encontradas (situaciones, causas y soluciones).
- ✓ Programa de trabajo de auditoría.
- ✓ Guía de auditoria.
- ✓ Inventario de *software*.
- ✓ Inventario de *hardware*.
- ✓ Inventario de consumibles.
- ✓ Manual de organización.
- ✓ Descripción de puestos.
- ✓ Reportes de pruebas y resultados.
- ✓ Respaldos (*backups*) de datos, disquetes y programas de aplicación de auditoría.
- ✓ Respaldos (*backups*) de las bases de datos y de los sistemas.
- ✓ Guías de claves para el señalamiento de los papeles de trabajo.
- ✓ Cuadros y estadísticas concentradores de información.

- ✓ Anexos de recopilación de información
- ✓ Diagramas de flujo, de programación y de desarrollo de sistemas.
- ✓ Testimoniales, actas y documentos legales de comprobación y confirmación.
- ✓ Análisis y estadísticas de resultados, datos y pruebas de comportamiento del sistema.
- ✓ Otros documentos de apoyo para el auditor.

Hoja de identificación

Esta es la parte frontal del legajo de papeles de trabajo de la auditoría de sistemas computacionales y es el primer documento formal que se identifica en dicho legajo. Esta portada (figura 7.2) debe contener, como mínimo, los siguientes datos:

Nombre de la empresa responsable de llevar a cabo la auditoría de sistemas.
Identificación del legajo de papeles de trabajo.
Nombre de la empresa o área de sistemas auditada.
Periodo en que se realizó la auditoría.
Puesto y cargo del responsable de realizar la auditoría.
Fecha de emisión del dictamen final.

Índice del contenido de los papeles de trabajo

En esta parte se elabora la descripción detallada y se pagina el contenido total de los papeles de trabajo con el propósito de identificar rápidamente la página en donde se encuentra cada una de las partes que integran este legajo de papeles.

Dictamen preliminar (borrador)

El auditor utiliza esta sección para conservar, como papeles de trabajo, el resultado del dictamen preliminar que presentó a discusión con los involucrados en la evaluación a fin de procesar el análisis y la consulta posteriores de todos los aspectos que presentó en forma de borrador.

Resumen de desviaciones detectadas (las más importantes)

El auditor elaborará el informe final con base en el análisis de estas desviaciones relevantes y lo presentará como informe final y dictamen de auditoría de sistemas computacionales.

Situaciones encontradas (situaciones, causas y soluciones)

En esta parte de los papeles de trabajo se presentan los manuscritos y en ocasiones los borradores mecanografiados de todas las situaciones detectadas durante la auditoría según el formato que se propone en el capítulo siguiente y separar, en situaciones encontradas, las causas que las originan y

las posibles soluciones. También se anota al responsable de solucionarlas y las fechas de solución para cada causa o situación reportada.

Programa de trabajo de auditoría

Es el documento formal (por escrito) de los planes, programas y presupuestos hechos para el control y desarrollo de la auditoría. Este documento se elabora en un formato especial o en una gráfica en la cual se anotan las etapas y actividades para la evaluación, así como los tiempos para llevarla a cabo. También, se anotan los recursos disponibles para realizar todas esas actividades.

Estos aspectos se deben señalar en forma cronológica, secuencial y correctamente coordinada. Los principales conceptos que el auditor debe incluir como parte del programa son los siguientes:

Primera etapa. Planeación de la auditoría de sistemas computacionales.

Segunda etapa. Ejecución de la auditoría de sistemas computacionales.

Tercera etapa. Dictamen de la auditoría de sistemas computacionales.

Guía de auditoria

En este documento se indica cada de los puntos que deberá evaluar el auditor, así como la forma de evaluarlos y la descripción de las técnicas, métodos y herramientas que deberá utilizar en dicha evaluación, que deben ser diseñados previamente de acuerdo con el tipo de auditoría y la especialidad informática que se tenga que evaluar en el centro de cómputo de la empresa (vea la figura 7.5).

Inventarios

Una de las principales herramientas que utiliza el auditor de sistemas son los inventarios, los cuales le sirven para contar los elementos que existen en el área que evaluará, según los equipos, artículos o partes del sistema que se traten.

A continuación presentaremos los principales inventarios para el área de sistemas:

- Inventario de *software*.
- Inventario de *hardware*.
- Inventario de bases de datos e información de la empresa.
- Inventario de proyectos y desarrollos computacionales.
- Inventario de puestos de trabajo en el área de sistemas.
- Inventario de reportes de pruebas y resultados.
- Inventario de mobiliario y equipos.
- Inventario de instalaciones de voz, datos y energía.
- Inventario de instalaciones de redes.

- Inventario de manuales e instructivos.
- Inventario de respaldos, disquetes, cintas y sistemas de resguardo de información.
- Inventario de consumibles.

Respaldo de datos (*BACKUPS*), información y programas de aplicación de auditoría

Los sistemas computacionales tienen características específicas en cuanto a la forma de captura, almacenamiento y emisión de información; por esta razón, encontramos que el respaldo de documentos es importante en una auditoría de sistemas computacionales.

En este tipo de auditorías los llamados papeles de trabajo adquieren un matiz muy especial debido a la forma en que se archiva la información en ellos; así encontramos que debemos documentar datos que muchas veces no están archivados en papel sino en sistemas computacionales; por lo tanto, debemos saber cómo capturar, extraer y archivar esa información en algún medio electromagnético de captura y lectura de información.

Otros documentos que debe contener el legajo de papeles de trabajo de la auditoría

Debemos señalar que el responsable de la auditoría de sistemas es quien debe definir el contenido y la forma de guardar los papeles de trabajo, y debe hacerlo de acuerdo con las necesidades específicas de evaluación, siguiendo, de preferencia, la forma acostumbrada de captura y almacenamiento de la información recabada en la empresa o área auditada.

A continuación, presentamos algunos otros documentos que debe contener el citado legajo.

Estadísticas y cuadros concentradores de información

Anexos de recopilación de información

Testimoniales, actas y documentos legales de comprobación y confirmación.

Análisis estadístico de resultados, datos y pruebas de comportamiento del sistema.

Otros documentos especializados de una auditoría de sistemas

En el legado de papeles de trabajo también se debe anexar la información (en papel o electrónicamente) relacionada con los reportes, análisis y resultados de pruebas, configuraciones y exámenes especializados del sistema computacional, de las instalaciones o de cualquier otro aspecto relacionado con el área de sistemas. También, se debe anexar lo relacionado con el procesamiento de información o con cualquier otra actividad informática.

(Para ahondar más en el tema, refiérase a las páginas de la 246 a la 263 del libro de texto).

Claves del auditor para marcar papeles de trabajo

Son las marcas de carácter informal que utiliza exclusivamente el auditor o el grupo de auditores que realizan la auditoría con el fin de facilitar la uniformidad de los papeles de trabajo y para identificarlos mejor. El auditor en jefe puede imponer el uso de estos símbolos o pueden ser utilizados por acuerdo del grupo, aunque también puede suceder que no sean utilizados en una auditoría.

Cuando alguien del grupo de auditores se encuentra algún documento con estas marcas, sabe que éste ya ha sido revisado o que tiene una característica especial en la cual se tiene que advertir alguna observación de acuerdo con el significado de los símbolos.

(Para ahondar más en el tema, refiérase a las páginas de la 263 a la 265 del libro de texto).

Cuadros, estadísticas y documentos concentradores de información

En esta parte se presentan todos los documentos del legajo de papeles de trabajo que servirán de soporte para presentar la información recopilada durante la auditoría y que es conveniente destacar por su importancia, por su nivel de información y para comprobar las desviaciones plasmadas en las situaciones detectadas y en las situaciones importantes.

Algunos documentos que pueden ser considerados dentro de este rubro son los siguientes:

Cuadro de concentración estadística.
Cuadro de comparación de información.
Gráficas de cualquier tipo.

(Para ahondar más en el tema, refiérase a las páginas de la 265 a la 267 del libro de texto).

Diagramas de sistemas

En el ambiente de sistemas, este diagrama es la representación gráfica de un procedimiento de sistematización, el cual está representado por líneas de flujo y símbolos que representan algún tipo de actividad, de documento o de una decisión. Esta simbología se acuerda previamente para que quienes la vean la interpreten de la misma manera.

Diagrama de flujo

En este tipo de diagramas se señalan los procedimientos por medio de símbolos adoptados para ejemplificar el flujo que siguen los datos.

Diccionario de datos

Este es otro de los documentos importantes para el auditor, porque le ayuda a identificar el contenido y la composición de las bases de datos, su forma, el tamaño de los archivos, el número de dígitos por cada registro que ingresa a la computadora y demás características que componen una base de datos.

Modelos

Estos documentos son importantes en la evaluación de los sistemas computacionales, porque ayudan al auditor a representar la realidad de lo que evaluará.

El modelo representa la abstracción gráfica de la realidad que el analista o programador conceptualiza para plasmarla en un documento.

De hecho, en estricto sentido, todas las gráficas y los diagramas de flujo, aquí mostrados, son modelos que representan la realidad.

(Para ahondar más en el tema, refiérase a las páginas de la 267 a la 269 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- Con el tema de papeles de trabajo, ¿puede conservarse la información en medio magnético un papel de trabajo?

2- ¿Qué se entiende por claves del auditor para marcar papeles de trabajo?

Capítulo 8

Informes de auditoría de sistemas computacionales

Sumario

Procedimiento para elaborar el informe de auditoría de sistemas computacionales.
Características del informe de auditoría de sistemas computacionales.
Estructura del informe de auditoría de sistemas computacionales.
Formatos para el informe de auditoría de sistemas computacionales.

Propósito del capítulo

El propósito de este capítulo consiste en que, tanto el auditor como el estudiante, conozcan la importancia del informe de auditoría y su adecuada presentación.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Redactar, en forma profesional, los informes de auditoría de sistemas computacionales a fin de expresar su opinión y los resultados de una revisión de manera correcta.

- Identificar las características básicas de fondo y forma del informe, el procedimiento fundamental para elaborarlo, la estructura que deberá tener su presentación, así como los formatos que se utilizan para una óptima presentación de las desviaciones encontradas.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

COMENTARIOS GENERALES

El informe es el documento más importante de la auditoría de sistemas computacionales debido que, a través de éste, se presentan los resultados obtenidos durante la evaluación.

En él se plasman, por escrito, las observaciones y el dictamen que emite el auditor, quien de acuerdo con su experiencia, conocimientos e información recopilada, evalúa el comportamiento del sistema, la actuación y el cumplimiento de su gestión informática, la realización correcta de sus objetivos, el cumplimiento de sus funciones, actividades y operaciones o cualquier otro aspecto de sistemas computacionales.

Procedimiento para elaborar el informe de auditoría de sistemas computacionales

En el informe de auditoría, también llamado dictamen, se reportan las situaciones encontradas durante la evaluación. También, se deben incluir las causas que originan esas situaciones y las posibles sugerencias para solucionar los problemas encontrados.

El procedimiento para elaborar dicho informe se compone de los siguientes pasos:

Aplicar instrumentos de recopilación

Con la aplicación de estos instrumentos, el auditor detecta las posibles desviaciones a la actividad que está evaluando y, de acuerdo con sus conocimientos y experiencia, las analiza y las registra.

Registrar en el formato de situaciones encontradas las desviaciones halladas durante la revisión

El auditor identifica aquellas posibles desviaciones que encontró durante su evaluación y elabora un análisis comparativo de la operación normal contra la esperada. Una vez hecho este análisis, entonces puede definir aquellas situaciones que considera como desviaciones y las reporta como situaciones encontradas en su evaluación.

Comentar las situaciones encontradas con los auditados

Es indispensable que cada una de estas desviaciones sean discutidas con los empleados, funcionarios o usuarios que fueron auditados, porque, de alguna manera, éstos son los responsables de que se presenten dichas situaciones (o cuando menos están involucrados en ellas). El propósito de informarles consiste en que ratifiquen o rectifiquen el origen de tales desviaciones.

Encontrar, conjuntamente con los auditados, las causas de las desviaciones y sus posibles soluciones

El verdadero trabajo del auditor consiste en reportar las desviaciones que encontró durante su evaluación, encontrar las causas que las originaron y acordar las posibles soluciones conjuntamente con el auditado. Así, se entiende y debe entenderse la función de la auditoría de sistemas.

Cuando se produce esta realimentación con el personal auditado se puede seleccionar a los posibles responsables del arreglo y la fecha compromiso en que se puede llegar a solucionar cada una de las desviaciones presentadas.

Analizar, depurar y corregir las desviaciones encontradas

Una vez que se comentaron las desviaciones con los auditados y se obtuvieron sus causas y posibles soluciones, el responsable de la auditoría de sistemas será el encargado de analizar las desviaciones al vigilar que cada una esté perfectamente plasmada y correctamente redactada en el formato de situaciones encontradas.

Jerarquizar las desviaciones encontradas y concentrar las más importantes en el formato de situaciones relevantes

Una vez que el responsable de la auditoría de sistemas haya supervisado que el informe de desviaciones encontradas esté correctamente elaborado, debe analizar todas las desviaciones reportadas, a fin de escoger las que considere más importantes para reportarlas en el formato de situaciones relevantes; el propósito es enfatizar lo que considera como lo más importante de la evaluación practicada, a fin de que los directivos conozcan los aspectos más relevantes.

Comentar las situaciones relevantes con los directivos del área de sistemas y confirmar las causas y soluciones

Por lo general, esta reunión es de carácter formal y en ella se reportan todas y cada una de las situaciones consideradas como relevantes, aunque se pueden presentar las llamadas situaciones encontradas.

En esta reunión se presentan los resultados de la auditoría de sistemas computacionales y el informe a los directivos del área auditada se debe emitir en forma abierta y, preferentemente, en presencia de todo el personal auditado.

Concentrar, depurar y elaborar el informe final de auditoría y el dictamen del auditor

Debido a que el informe es para el área directiva de la empresa, no debe exceder de dos a tres hojas. En este informe el auditor sólo debe señalar lo más relevante de la evaluación incluyendo su opinión. El informe final debe ser sencillo, claro y comprensible para ellos. Debe evitarse el uso de términos demasiado técnicos y desconocidos para personas ajenas a la informática. Sólo se deben destacar los aspectos más importantes del área desde el punto de vista de los directivos y no del personal que maneja los sistemas.

Presentar el informe y dictamen final a los directivos de la empresa

Este ya es el informe final de la auditoría practicada y, por lo tanto, no se debe admitir ningún comentario adicional que pudiera modificar lo ahí presentado, porque es el producto final de la auditoría y, por lo tanto, no cabe ninguna alteración. De hacerlo, sería tanto como crear expectativas de duda sobre la veracidad y confiabilidad de su contenido.

Por lo general, a esta presentación, solamente asisten el cuerpo directivo de la empresa auditada y el cuerpo ejecutivo de la empresa encargada de realizar la auditoría, aunque nada impide que estén presentes tanto el personal del área de sistemas auditada como los auditores participantes.

(Para ahondar más en el tema, refiérase a las páginas de la 273 a la 280 del libro de texto).

Características del informe de auditoría de sistemas computacionales

Características fundamentales

Características de fondo

Se refieren al cuidado que debe tener el auditor de sistemas al revisar que el contenido total del dictamen de auditoría sea acorde con lo que realmente tiene que señalar acerca de la revisión efectuada al referirse exclusivamente al contenido del informe.

Características de forma

Alude a la manera en que el auditor debe presentar el informe en cuanto al estilo de redacción, el contenido en partes, apartados, apéndices, tipo y tamaño de las hojas y el tipo de letra.

Características de la presentación del informe

Otras de las características más importantes de un informe de auditoría de sistemas computacionales son los atributos que deben tener la redacción y la presentación del informe. Para lograr mejores resultados en la elaboración del citado informe, el auditor debe tener en cuenta las características que proponemos a continuación:

Claridad	Exactitud
Confiabilidad	Imparcialidad
Propiedad	Objetividad
Concisión	Congruencia
Sencillez	Familiaridad
Acertividad	Veracidad
Ilación	Efectividad
Tono y fuerza	Positividad
Oportunidad	Sintaxis
Precisión	

Características importantes para el lector del informe de auditoría

Además de las anteriores características, el informe de auditoría se debe elaborar conservando los siguientes aspectos fundamentales de fondo y forma:

- Que el informe tenga familiaridad.
- Que el contenido del informe sea coloquial.
- Que el contenido del informe sea variado.
- Que se entregue y comente oportunamente.
- Que su lectura sea sencilla.
- Que su contenido esté fundamentado.
- Que su redacción sea clara.
- Que la información contenida sea contundente.
- Que esté redactado en un estilo impersonal.
- Que su contenido esté sintetizado.
- Que su contenido sea ameno y entendible.
- Que sea enfático en las situaciones reportadas.

(Para ahondar más en el tema, refiérase a las páginas de la 280 a la 305 del libro de texto).

Estructura del informe de auditoría de sistemas computacionales

Existen distintas formas de presentar el informe de auditoría de sistemas computacionales de acuerdo con las preferencias de la empresa o del auditor que realiza la auditoría. A continuación, proponemos un modelo para presentarlo.

Oficio de presentación

Es la primera parte del informe de auditoría y se trata de un documento de carácter oficial que sirve como presentación del informe. Debe contener, como mínimo, los siguientes aspectos (vea la figura 8.3).

Logotipo de identificación.
Nombre de la empresa (o área interna de auditoría).
Fecha de emisión del informe.
Identificación de la empresa o área auditada.
Ejecutivo receptor del informe.
Periodo de la evaluación.
Contenido (o cuerpo del oficio).
Responsable de emitir el dictamen.
Firma del responsable.
Introducción del informe de auditoría de sistemas computacionales.

Es la parte del informe donde el responsable de la auditoría presenta formalmente su trabajo. En este apartado se manifiesta el objetivo de la auditoría, las razones que motivaron a llevarla a cabo y, si es el caso, los fundamentos que apoyen su realización.

La introducción es frecuentemente la invitación a seguir leyendo el resto del informe.

Dictamen de la auditoría de sistemas computacionales

Tal vez ésta sea la parte más importante de una auditoría de sistemas computacionales y, en muchas ocasiones, lo que más esperan los directivos de la empresa o del área auditada, debido a que es una opinión profesional respecto al comportamiento de los sistemas.

Otros aspectos que deben incluirse en el informe de auditoría son los siguientes:

Situaciones relevantes

Estos son los documentos oficiales donde el responsable de la auditoría reporta las desviaciones que, según su criterio, son las más importantes encontradas durante el desarrollo de la auditoría.

Situaciones encontradas

Se enumeran todas las desviaciones encontradas durante la evaluación.

Anexos

Son documentos de gráficas, cuadros, declaraciones o cualquier otro formato que servirá de soporte para las desviaciones reportadas en el informe final.

Confirmaciones en papeles de trabajo

Estos documentos no se adjuntan al informe; pero, deben conservarse cuando se presenta el informe, en caso de duda en relación con algún asunto en particular.

(Para ahondar más en el tema, refiérase a las páginas de la 305 a la 317 del libro de texto).

Formatos para el informe de auditoría de sistemas computacionales

Formato de situaciones encontradas

Este documento, que es uno de los documentos más importantes para el desarrollo de cualquier auditoría de sistemas, constituye un formato especial para la recopilación de situaciones o desviaciones encontradas, el cual está formado por una serie de hojas (formatos individuales) en las cuales el auditor anota en manuscrito o tipografía todas las desviaciones que encuentra durante su evaluación.

A continuación, veremos un formato de presentación para las situaciones encontradas (ver la figura 8.5).

Identificación (en la parte superior izquierda del formato)
Área auditada (en la parte central del formato)

Fecha de evaluación (en la parte superior derecha)
Número de referencia (columna o)
Situaciones encontradas (columna 1)
Causas de la situación (columna 2)
Soluciones propuestas (columna 3)
Fecha de compromiso para la solución (columna 4)
Responsable de la solución (columna 5)
Elaboró la hoja de situaciones, nombre y firma (parte inferior izquierda)
Formato de situaciones relevantes

Este documento es una réplica simplificada del formato anterior, sólo que en éste únicamente se anotan las situaciones consideradas como relevantes, resultado del análisis al documento anterior, es decir, sólo se incluyen aquellas observaciones que a juicio del auditor o del responsable de la auditoría son realmente importantes para el desarrollo de las actividades del área de sistemas evaluada.

A continuación, presentamos una propuesta del formato de situaciones relevantes, el cual servirá de base para las siguientes aplicaciones de auditoría de sistemas (vea la figura 8.6).

Identificación (en la parte superior izquierda del formato).
Área auditada (en la parte central del formato).
Fecha de evaluación (en la parte superior derecha).
Número de referencia (columna 0).
Situaciones relevantes (columna 1).
Causas de la desviación (columna 2).
Soluciones propuestas (columna 3).

(Para ahondar más en el tema, refiérase a las páginas de la 317 a la 325 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- El informe de auditoría es el clímax. A partir de un estudio realizado, explique la importancia de presentar adecuadamente un informe.

2- ¿Qué debemos entender por el término “oportunidad” en la presentación de un informe de auditoría?

3- En el informe de auditoría hay dos conceptos, entre otros, que deben ser tomados en cuenta por el auditor: la imparcialidad y la objetividad. Explíquelos y relaciónelos con el tema de la ética, que se estudió en el capítulo 3.

Capítulo 9

Instrumentos de recopilación de información aplicables en una auditoría de sistemas computacionales

Sumario

Entrevistas
Cuestionarios
Encuestas
Observación
Inventarios
Muestreo
Experimentación

Propósito del capítulo

El propósito de este capítulo consiste en que el auditor conozca acerca de las diferentes herramientas con que puede contar para la recopilación de datos e información.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Identificar los principales instrumentos, técnicas, herramientas y métodos utilizados en la recopilación de información útil y pertinente para realizar una auditoría de sistemas fundamentados en las herramientas y métodos tradicionales de recopilación de información de las auditorías tradicionales en el análisis y diseño de sistemas y las ciencias sociales.

- Conocer la forma de aplicación y funcionamiento de los principales instrumentos, técnicas, herramientas y métodos en las auditorías de sistemas computacionales para adaptarlos a las necesidades específicas del ambiente de sistemas que se requiere auditar.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
9.1 Entrevistas	329
9.2 Cuestionarios	339
9.3 Encuestas	347
9.4 Observación	359
9.5 Inventarios	367
9.6 Muestreo	387
9.7 Experimentación	409

COMENTARIOS GENERALES

El auditor debe aprovechar las técnicas, los procedimientos y las herramientas tradicionales de auditoría aplicables en el área de sistemas computacionales.

El propósito consiste en que las diseñe y las utilice para evaluar en forma correcta el funcionamiento de dicha área, de la operación del propio sistema o de su gestión informática; por lo tanto, se beneficiará debido a la ya probada eficiencia y eficacia en otros tipos de auditorías, en las cuales se han conseguido los resultados esperados.

Entrevistas

Una de las técnicas más utilizada por los auditores es la entrevista, porque se obtiene información sobre lo que auditará.

La entrevista podría entenderse como la recopilación de información que se realiza en forma directa, cara a cara y a través de algún medio de captura de datos, es decir, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que audite.

Ciclo de la entrevista de auditoría

Es conveniente señalar que, para realizar una entrevista adecuada, es indispensable entender y seguir un procedimiento bien estructurado. La eficacia de una adecuada aplicación de esta técnica, en las auditorías tradicionales y en las ciencias sociales, ha sido plenamente comprobada.

El siguiente procedimiento es indispensable para realizar una entrevista oportuna:

- Inicio.
- Apertura.
- Clima o clímax.
- Cierre.

(Para ahondar más en el tema, refiérase a las páginas de la 329 a la 339 del libro de texto).

Cuestionarios

Es la recopilación de datos mediante preguntas impresas en cédulas o fichas, en las que el encuestado responde de acuerdo con su criterio; de esta manera, el auditor obtiene información útil que puede concentrar, clasificar e interpretar por medio de su tabulación y análisis, para evaluar lo que está auditando y emitir una opinión sobre el aspecto investigado.

El cuestionario tiene la gran ventaja de que puede recopilar una gran cantidad de información debido a que contiene preguntas sencillas cuyas respuestas no implican ninguna dificultad; además, como en otros métodos, su aplicación es de carácter impersonal y libre de influencias y compromisos para el entrevistado.

Ventajas

Entre las ventajas tenemos las siguientes:

- Facilitan la recopilación de información y no se necesitan muchas explicaciones ni una gran preparación para aplicarlos.
- Permiten la rápida tabulación e interpretación de los datos al proporcionarles la confiabilidad requerida.
- Evitan la dispersión de la información requerida al concentrarse en preguntas de elección forzosa.
- Por su diseño, los cuestionarios son rápidos de aplicar y ayudan a captar mucha información en poco tiempo.
- En el ambiente de sistemas es fácil capturar, concentrar y obtener información útil a partir de las respuestas, mediante el uso de la computadora. Incluso, se pueden proyectar los datos y construir gráficas.
- Impersonalidad en la aportación de respuestas; por lo tanto, en una auditoria ayudan a obtener información útil y confiable, si se plantean en forma adecuada las preguntas.

Desventajas

Entre las desventajas, tenemos las siguientes:

- Falta de profundidad en las respuestas y no se puede ir más allá del cuestionario.
- Se necesita una elección pertinente del universo y de las muestras utilizadas.
- Pueden provocar la obtención de datos equivocados si se formulan deficientemente las preguntas, si se distorsionan o si se utilizan términos ilegibles, poco usados o estereotipados.

- La interpretación y el análisis de los datos pueden ser simples si el cuestionario no está bien estructurado o no incluye todos los puntos requeridos.
- Limitan la participación del auditado, porque éste puede evadir preguntas importantes o se puede escudar en el anonimato que proporcionan los cuestionarios.
- Impersonalidad en la participación del personal auditado, por lo que la aportación de la información útil para la auditoría es limitada.
- Denotan la falta de experiencia y pocos conocimientos del auditor que las aplica, si no plantea ni estructura correctamente las preguntas, lo cual puede provocar que su trabajo sea rechazado.

(Para ahondar más en el tema, refiérase a las páginas de la 339 a la 347 del libro de texto).

Encuestas

Es la recopilación de datos concretos sobre un tema específico mediante el uso de cuestionarios o entrevistas diseñados con preguntas precisas para obtener las opiniones de los encuestados, las cuales permiten, después de elaborar una rápida tabulación, análisis e interpretación de esa información, conocer su punto de vista y actitud hacia un tópico específico.

Con la aplicación de encuestas en las auditorías de sistemas se busca que la forma de recopilar las opiniones sea ágil, sencilla y poco complicada para los encuestados; esto se logra mediante preguntas claras, sencillas y de fácil entendimiento, a fin de que las respuestas de los encuestados sean concretas y enfocadas hacia el tema de estudio.

(Para ahondar más en el tema, refiérase a las páginas de la 347 a la 359 del libro de texto).

Observación

La acción de observar es el hecho de examinar, analizar, advertir o estudiar algo. En este caso, cuando el auditor de sistemas aplica esta técnica, observa lo relacionado con los sistemas de una empresa con el propósito de percibir, examinar o analizar lo relacionado con los eventos que se presentan en el desarrollo de las actividades de un sistema, de un centro de sistematización, de la operación de la computadora o el desempeño de cualquiera de las actividades que le permitirán evaluar el cumplimiento de las operaciones del sistema.

(Para ahondar más en el tema, refiérase a las páginas de la 359 a la 367 del libro de texto).

Inventarios

Con la aplicación de esta herramienta de la auditoría tradicional, el auditor de sistemas también puede examinar las existencias de los elementos disponibles para el funcionamiento del área de informática o del propio sistema.

Para ello, contabiliza los equipos componentes de los sistemas de cómputo, la información y datos de la empresa, los programas, periféricos, consumibles, documentos, recursos informáticos y los demás aspectos cuya existencia real se quiere conocer, a fin de comparar dicha existencia (cantidad) con registros formales de la existencia que debería haber.

En la auditoría de sistemas, este método de recopilación de información ayuda enormemente a realizar una evaluación adecuada de la gestión administrativa del área de sistemas, así como del aprovechamiento, custodia y control de los bienes informáticos que hay en dicha área.

A continuación presentamos los principales tipos de inventarios aplicables en el ambiente de sistemas computacionales:

- Inventario del *software*.
- Inventario del *hardware*.
- Inventario de consumibles.
- Inventario de documentos.
- Inventario de inmuebles, instalaciones, mobiliario y equipos de sistemas.
- Inventario del personal informático.
- Inventario de bases de datos e información institucional.

(Para ahondar más en el tema, refiérase a las páginas de la 367 a la 387 del libro de texto).

Muestreo

Una de las técnicas que más aporta a la auditoría de sistemas computacionales es el muestreo, porque una aplicación correcta de los métodos y los procedimientos estadísticos ayuda bastantea seleccionar una parte representativa del universo que se tiene que revisar.

El propósito es obtener la misma información o parecida a la que se obtendría al revisar todo ese universo. De esta manera, el auditor puede determinar el comportamiento global de todo el universo y con ello puede contar con los elementos de juicio necesarios para emitir un dictamen apegado a la veracidad de los hechos auditados.

Esta herramienta es fundamental en la auditoría de sistemas debido a que el auditor apoya en los propios sistemas computacionales para diseñar la muestra, seleccionar la probabilidad de la captura de datos y después procesar

esa información para elaborar los cuadros y gráficas representativos de los resultados.

Otro aspecto fundamental del muestreo es que mediante programas especiales de cómputo también se pueden hacer simulaciones y proyecciones que son de gran utilidad en una auditoría de sistemas, aunque el muestreo sea matemático, estadístico o por computadora.

(Para ahondar más en el tema, refiérase a las páginas de la 387 a la 409 del libro de texto).

Experimentación

Es la observación de un fenómeno en estudio, a la que se le adaptan o modifican sus variables conforme a un plan predeterminado con el propósito de analizar sus posibles cambios de conducta como respuesta a las modificaciones que sufre dentro de su propio ambiente o en un ambiente ajeno. Todo ello, con el fin de estudiar su comportamiento bajo diversas circunstancias y sacar conclusiones.

En la experimentación, quien desarrolla la auditoría puede participar o no activamente en la observación del fenómeno en estudio y, conforme a un plan preconcebido (el programa de auditoría), puede hacer deliberadamente los cambios necesarios con los cuales modifica, sistemáticamente, el comportamiento del fenómeno en estudio.

Luego, el auditor observa las alteraciones que se presentan con esas modificaciones, las valora cuantitativa y cualitativamente y analiza las repercusiones que se presentan durante la experimentación a fin de ampliar su conocimiento sobre el fenómeno en estudio para poder emitir un juicio adecuado respecto a su comportamiento.

(Para ahondar más en el tema, refiérase a las páginas de la 409 a la 416 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- Una de las técnicas más populares para la recopilación de datos son los cuestionarios. Mencione tras ventajas y tres desventajas de la utilización de esta técnica.

2- ¿En qué circunstancias se debe aplicar la técnica de recopilación de datos cuando se trata de los inventarios?

3- ¿Cuándo debe aplicar la técnica del muestreo?

Capítulo 10

Técnicas de evaluación aplicables en una auditoría de sistemas computacionales

Sumario

Examen
Inspección
Confirmación
Comparación
Revisión documental
Acta testimonial
Matriz de evaluación
Matriz DOFA

Propósito del capítulo

El propósito de este capítulo consiste en que el auditor de sistemas conozca las diferentes técnicas, herramientas, procedimientos y métodos, para ser aplicados, cuando realice la auditoría.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Reconocer las principales técnicas de evaluación aplicables en una auditoría tradicional.

- Identificar los elementos fundamentales para realizar su auditoría de sistemas, así como todos los procedimientos, herramientas, técnicas y métodos que se pueden aplicar en la evaluación de los sistemas computacionales, de las áreas de sistemas, de las actividades, funciones y demás operaciones relacionadas con dichos sistemas.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
10.1 El examen	418
10.1.1 Examen del comportamiento del sistema	420
10.2 La inspección	425
10.3 Confirmación	427
10.4 Comparación	428
10.5 Revisión documental	430
10.6 Acta testimonial	435
10.7 Matriz de evaluación	446
10.8 Matriz DOFA	454

COMENTARIOS GENERALES

Como profesional especializado en el ramo, el auditor de sistemas computacionales utiliza una serie de técnicas específicas que le ayudan a examinar y evaluar correctamente los diferentes aspectos del ambiente de sistemas en el que realizará su trabajo.

A continuación, presentamos las técnicas, los métodos y los procedimientos o herramientas que analizaremos:

- El examen.
- La inspección.
- La confirmación.
- La comparación.
- La revisión documental.
- El acta testimonial.
- La matriz de evaluación.
- La matriz DOFA.

Examen

Consiste en analizar y poner a prueba la calidad y el cumplimiento de las funciones, las actividades y las operaciones que se realizan cotidianamente en una empresa y se aplica en un área o actividad específica o en una unidad administrativa completa.

El examen también se utiliza para evaluar los registros, planes, presupuestos, programas, controles y todos los demás aspectos que afectan la administración y control de una empresa o de las áreas que la integran.

El auditor aplica esta herramienta con el propósito de investigar algún hecho comprobar, alguna cosa, verificar la forma de realizar un proceso, evaluar la aplicación de las técnicas, los métodos y los procedimientos de trabajo,

verificar el resultado de una transacción, comprobar la operación correcta de un sistema computacional y para evaluar muchos otros aspectos.

Las principales aplicaciones de los exámenes en una auditoría de sistemas computacionales son las siguientes:

Examen del comportamiento del sistema

Esta aplicación se refiere a las pruebas que aplica el auditor e, incluso, el propio desarrollador de un sistema con el propósito de saber cómo se comporta el sistema en los distintos ambientes en donde se realiza su operación normal.

Examen de los resultados del sistema

Es la aplicación de las pruebas necesarias al ciclo normal de captura, procesamiento y emisión de la información procesada en el sistema computacional de la empresa por medio de exámenes específicos del comportamiento, velocidad, exactitud y demás características del procesamiento de los datos.

Pruebas de implantación

Son las comprobaciones previas a la implantación de un sistema computacional con el fin de verificar si el diseño del nuevo sistema corresponde al comportamiento real de dicho sistema.

Pruebas del sistema

Es la sucesión de pruebas, exámenes y comprobaciones de la actividad del sistema computacional en cuanto a la confiabilidad de su operación, el procesamiento de información, el funcionamiento de sus periféricos y equipos asociados, su arquitectura, el funcionamiento de sus procesadores, la velocidad de éstos, el trabajo de las memorias, la lectura y grabación correctas de información en los dispositivos externos y las demás pruebas que se realizan al sistema, con el propósito de conocer y evaluar su funcionamiento.

Pruebas de los programas de aplicación

Se conocen como pruebas de escritorio. Son las experimentaciones del diseño de un nuevo proyecto de sistemas a través de pruebas que se realizan de manera manual, mecánica o electromecánica (o también por medio de algún modelo) al comparar, uno por uno, todos los pasos que supuestamente seguirían las rutinas de procesamiento de información del nuevo sistema con el propósito de localizar las posibles deficiencias del nuevo proyecto.

Pruebas del sistema operativo

Son las rutinas de verificación y comprobación instaladas dentro del propio sistema computacional, las cuales se activan cuando inicia el sistema operativo.

El propósito de estas pruebas es verificar el funcionamiento del procesador, de sus componentes, las memorias, los sistemas de operación y procesamiento, los buses de conexión (conexiones del sistema) y funcionamiento de los periféricos, comunicaciones y demás partes que hacen funcionar el sistema.

Pruebas de encendido del sistema

Son las verificaciones y comprobaciones que el sistema, al encender, realiza de sus componentes, periféricos y programas de operación y procesamiento. Estas revisiones también se realizan por medio de rutinas y procedimientos de verificación internos diseñados por los fabricantes del sistema.

Exámenes de las instalaciones del centro de cómputo

Es la verificación y evaluación del funcionamiento de las instalaciones de un centro de cómputo, de sus comunicaciones, sus sistemas eléctricos, sus conexiones entre componentes, sus sistemas de aire acondicionado, las medidas de prevención para evitar y combatir incendios, inundaciones y demás riesgos internos o externos, así como de los sistemas de seguridad y planes de contingencias y, en sí, de todos los aspectos que repercuten en el funcionamiento del área de sistemas de la empresa.

(Para ahondar más en el tema, refiérase a las páginas de la 418 a la 425 del libro de texto).

Inspección

En la auditoría de sistemas computacionales, la técnica de inspección está relacionada con la aplicación de los exámenes para evaluar el funcionamiento de dichos sistemas en cuanto a eficiencia y eficacia en relación con la operación y el procesamiento de datos.

Lo mismo ocurre para la gestión administrativa de un centro de cómputo, en donde se efectúa una inspección detallada con el propósito de evaluar el cumplimiento de sus funciones, actividades, estructura organizacional y demás aspectos administrativos.

La inspección se realiza a cualquiera de las actividades, operaciones y componentes que rodean los sistemas. Con esta técnica se puede evaluar, verificar y juzgar el funcionamiento de los sistemas computacionales de la empresa así como la realización adecuada de todas sus actividades.

(Para ahondar más en el tema, refiérase a las páginas de la 425 a la 427 del libro de texto).

Confirmación

Uno de los aspectos fundamentales para la credibilidad de una auditoría es la confirmación de los hechos y la certificación de los datos obtenidos durante la

revisión, porque el resultado final de una auditoría es la emisión de un dictamen en el que auditor vierte sus opiniones; pero, para que el dictamen sea plenamente aceptado, es necesario garantizar la veracidad y confiabilidad de los datos veraces y confiables y que las técnicas y métodos utilizados para la auditoría se consoliden como los adecuados.

Un auditor jamás puede fundamentar sus opiniones en suposiciones y conjeturas falsas ni emitir juicios basados en datos que no sean verídicos o que no estén certificados plenamente o en datos obtenidos con técnicas y herramientas de auditoría, que no garanticen la comprobación de la información recabada.

(Para ahondar más en el tema, refiérase a las páginas de la 427 a la 428 del libro de texto).

Comparación

Otra de las técnicas utilizadas en el desarrollo de cualquier auditoría es la comparación de los datos obtenidos de un área o de toda la empresa. Se debe cotejar esa información contra datos similares o iguales de un área o empresa con características semejantes. Con la comparación de la información se pueden encontrar similitudes y diferencias entre ambas áreas o empresas, con lo cual se pueden conjeturar y deducir las desviaciones encontradas.

La utilidad de esta herramienta radica en que evalúa datos similares o iguales entre dos entidades (la analizada y una similar); así, se obtiene información relevante para la evaluación de la entidad evaluada, porque se compara la forma en que debería funcionar y la forma en que está funcionando en relación con la otra entidad.

(Para ahondar más en el tema, refiérase a las páginas de la 427 a la 430 del libro de texto).

Revisión documental

Una de las herramientas tradicionales y quizá, de las más utilizadas en cualquier auditoría, es la revisión de los documentos que avalan los registros de operaciones y actividades de una empresa, principalmente en aquellos casos donde la evaluación está enfocada a los aspectos financieros, el registro de los activos de la empresa y a cualquier otro aspecto contable y administrativo.

Esta técnica se aplica al verificar el registro correcto de datos en documentos formales de la empresa y, con mucha frecuencia, en la emisión de sus resultados financieros.

(Para ahondar más en el tema, refiérase a las páginas de la 430 a la 435 del libro de texto).

Acta testimonial

El acta testimonial es un documento de carácter formal que, por su representatividad, importancia y posibles alcances de carácter legal y jurídico, constituye uno de los documentos vitales para cualquier auditoría.

Este documento no sólo sirve de testimonio para comprobar, corroborar, ratificar o evidenciar cualquier evento que ocurra durante la revisión, sino que es tal su alcance que se puede convertir en un documento de carácter legal, probatorio de alguna anomalía de tipo jurídico, penal o de cualquier otro aspecto legal. Por esta razón, resulta fundamental que el auditor sepa elaborarla correctamente.

La utilidad de esta herramienta radica en que con su uso se pueden evidenciar pruebas fehacientes, circunstanciales, probatorias y, en algunos casos, jurídicas para comprobar desviaciones en el área auditada.

Incluso, se pueden utilizar para comprobar manejos dolosos, desviaciones de recursos o cualquier otro tipo de indecencias que el auditor descubra durante su evaluación y que, al plasmarlas en actas testimoniales, fundamenten posibles acciones posteriores a la evaluación o durante la misma evaluación.

(Para ahondar más en el tema, refiérase a las páginas de la 435 a la 446 del libro de texto).

Matriz de evaluación

La matriz de evaluación es uno de los documentos de recopilación más versátiles y de mayor utilidad para el auditor de sistemas computacionales debido a que, por medio de este documento, es posible recopilar una gran cantidad de información relacionada con la actividad, operación o función que se realiza en estas áreas informáticas así como apreciar anticipadamente el cumplimiento de dichas actividades.

Esta herramienta consiste en una matriz de seis columnas, de las cuales la primera corresponde a la descripción del aspecto que será evaluado y las otras cinco a un criterio de calificación descendente (o ascendente) en las que se anotan los criterios de evaluación para acceder a esa calificación.

(Para ahondar más en el tema, refiérase a las páginas de la 446 a la 454 del libro de texto).

Matriz DOFA (FODA)

Este es un método moderno de análisis y diagnóstico administrativo de gran utilidad para la evaluación de un centro de cómputo debido a que no sólo permite recopilar información más versátil, sino que admite evaluar el desempeño de los sistemas computacionales; asimismo, por medio de este documento se puede tener una apreciación preliminar sobre las fortalezas y

debilidades del propio centro de información de la empresa y se pueden analizar sus posibles amenazas y áreas de oportunidad.

Con dicho análisis, el auditor evalúa el cumplimiento de la misión y objetivo general del área de sistemas computacionales de la empresa.

(Para ahondar más en el tema, refiérase a las páginas de la 454 a la 475 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- Una de las herramientas de evaluación que utiliza el auditor en el área de sistemas es el examen. ¿A qué se refiere cuando se dice que el auditor debe efectuar pruebas de implantación? ¿Cómo se aplican?

2- ¿Qué debe incluir una evaluación de las instalaciones de un centro de cómputo?

3- ¿Qué es el acta testimonial?

Capítulo 11

Técnicas especiales de auditoría de sistemas computacionales

Sumario

Guías de evaluación
Ponderación
Modelos de simulación
Evaluación
Diagrama del círculo de evaluación
Lista de verificación
Análisis de la diagramación de sistemas
Diagrama de seguimiento de una auditoría de sistemas computacionales
Programas para revisión por computadora

Propósito del capítulo

El propósito de este capítulo consiste en brindar tanto al auditor como al estudiante una serie de técnicas especiales, que complementen las vistas en el capítulo anterior, que le serán de gran utilidad de acuerdo con el tipo de auditoría que realice.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Dar a conocer las técnicas, métodos y herramientas especiales que pueden ser aplicables en la auditoría de sistemas computacionales.

- Reconocer la forma de aplicación y el funcionamiento en la evaluación de los aspectos técnico-computacionales de las empresas y, al contar con ese conocimiento, aplicar dichas herramientas para cualquier otra necesidad específica de auditoría de sistemas.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
11.1 Guías de evaluación	478
11.2 Ponderación	487
11.3 Modelos de simulación	494
11.3.1 Simulación a través de modelos de metodología de sistemas	497
11.3.2 Simulación a través de diagramas de flujo de sistemas	501
11.3.3 Simulación a través del diseño de circuitos lógicos	502
11.4 Evaluación	505
11.4.1 Evaluación de la gestión administrativa del área de sistemas	508
11.4.2 Evaluación del equipo de cómputo	510
11.4.3 Evaluación integral de sistemas	517
11.4.4 Evaluaciones con el apoyo de la computadora	519
11.4.5 Evaluaciones sin el uso de la computadora	521
11.4.6 Evaluaciones de los controles en sistemas computacionales	521
11.4.7 Evaluaciones de otros aspectos de sistemas computacionales	523
11.4.8 Importancia de las evaluaciones de sistemas computacionales	530
11.5 Diagrama del círculo de evaluación	531
11.6 Lista de verificación (lista de chequeo)	535
11.7 Análisis de la diagramación de sistemas	537
11.7.1 Modelos de sistemas	538
11.7.2 Diccionario de datos	539
11.7.3 Diagrama Nassi-Schneiderman	540
11.8 Diagrama de seguimiento de una auditoría de sistemas computacionales	549
11.9 Programas para revisión por computadora	553
11.9.1 Programas de revisión elaborados por desarrolladores	554

COMENTARIOS GENERALES

En la auditoria de sistemas computacionales se utilizan múltiples herramientas y técnicas tradicionales de la auditoría que permiten hacer una eficiente revisión al funcionamiento de los sistemas de cómputo, a su gestión informática y a los diferentes aspectos del ambiente de sistemas.

Sin embargo, como profesional especializado en la evaluación de los sistemas de cómputo, el auditor de sistemas también debe conocer y utilizar otras herramientas, técnicas y procedimientos específicos del área de informática, los cuales le ayudan a examinar y evaluar con mayor eficiencia los aspectos propios de la actividad computacional.

Guías de evaluación

Las guías de auditoría son las herramientas más utilizadas y, quizá, las más importantes en cualquier auditoría de sistemas computacionales. Estas guías son un documento formal que indica el procedimiento de evaluación que debe

seguir el auditor; asimismo, en este instrumento, se indican todos los puntos, aspectos concretos y áreas que deben ser revisados, así como las técnicas, herramientas y procedimientos que deben ser utilizados en la auditoría de sistemas computacionales.

Para cualquier auditor, con experiencia o sin ella, la guía de evaluación es un documento que le permitirá realizar, en forma eficiente y efectiva, su reconocimiento de auditoría para cualquier aspecto relacionado con los sistemas computacionales, porque en esta guía se le indica todo el procedimiento que debe seguir, los puntos que debe evaluar y las herramientas que debe utilizar para su revisión, que incluya la manera de aplicarlas.

(Para ahondar más en el tema, refiérase a las páginas de la 478 a la 487 del libro de texto).

Ponderación

La ponderación es una técnica especial de evaluación mediante la cual se procura darle un peso específico a cada una de las partes que serán evaluadas. Su objetivo es tratar de compensar el valor que les asignamos a las actividades o tópicos que tienen poca importancia en la evaluación en relación con los que tienen mayor peso e importancia.

Esta técnica de evaluación permite equilibrar las posibles descompensaciones que existen entre las áreas o sistemas computacionales que tienen mayor peso e importancia y las áreas o sistemas que tienen poco peso e importancia en la evaluación. Lo que se busca con la ponderación es que todas las áreas tengan un valor similar y respetar, en cada caso, el peso e importancia representativos que tienen para el sistema computacional o para todo el centro de cómputo.

(Para ahondar más en el tema, refiérase a las páginas de la 487 a la 494 del libro de texto).

Modelos de simulación

Esta herramienta es una de las más utilizadas para el análisis y diseño de sistemas. También, puede ser de mucha utilidad para la auditoría de sistemas computacionales, porque mediante el uso del modelo, conceptual o físico.

Se simula el comportamiento de un sistema computacional de un programa, de una base de datos, de una operación, de una actividad o de cualquier tarea de sistemas que tenga que ser revisada, con el propósito de investigar cuál es, fue o será el comportamiento del fenómeno de sistemas en estudio, bajo ciertas condiciones y características concretas en las que se presentan todas las simulaciones necesarias que se asemejen al medio ambiente real en donde actúa dicho fenómeno para valorar su auténtico aprovechamiento, sus eficiencias y deficiencias de funcionamiento y sus principales problemas, entre otros.

El uso de esta técnica de simulación es indispensable para el trabajo de los desarrolladores de nuevos sistemas, porque permite elaborar un ambiente análogo al del nuevo sistema con el fin de estudia su posible comportamiento. Una vez estudiado el posible comportamiento del sistema, se pueden obtener conclusiones para corregir sus fallas de funcionamiento, así como sus principales problemas antes de implantar dicho sistema.

Con el uso de modelos concretos o de pruebas de simulación también se pueden evaluar la integridad, seguridad y confiabilidad de la información contenida en las bases de datos originales, así como verificar la existencia de redundancias, alteraciones y comportamientos irregulares de la información contenida en esas bases de datos.

Además, se puede simular, por medio de modificaciones controladas en el prototipo del sistema original, el acceso al sistema, la protección, el ingreso a las bases de datos e, incluso, el comportamiento de los usuarios del sistema o el manejo de los datos.

La utilidad de la simulación radica en que se pueden confeccionar pruebas controladas o libres que permiten realizar una buena evaluación al sistema sin necesidad de alterar el funcionamiento del sistema original. En este tipo de observación, se pueden aplicar las pruebas en sistemas paralelos: uno es el propio sistema con datos reales o ficticios y el otro es un modelo semejante al sistema que será evaluado.

Algunos de estos modelos de simulación son los siguientes:

Simulación a través de modelos de metodología de sistemas.
Simulación a través de diagramas de flujo de sistemas.
Simulación a través del diseño de circuitos lógicos.
Simulación a través de otros documentos gráficos.

(Para ahondar más en el tema, refiérase a las páginas de la 494 a la 505 del libro de texto).

Evaluación

La evaluación es una de las técnicas más comunes en cualquier tipo de auditoría y es considerada como la herramienta típica para auditar cualquier actividad, porque permite determinar, mediante pruebas concretas, si lo cuantificado (o cualificado) es lo que se esperaba obtener de lo que se está evaluando.

Así, se determina si se está cumpliendo con la actividad revisada conforme a lo que se esperaba de ella.

En esta técnica se aplica el principio fundamental del control: establecer parámetros de medición, recopilación de información y comparación de lo realmente alcanzado con lo planeado y con el resultado obtenido se realimentan los resultados de esta evaluación.

En ambos casos, evaluación de carácter cuantitativo o cualitativo, el resultado será determinado por la posible diferencia que se encuentre entre el valor esperado y el valor obtenido mediante las pruebas de auditoría que se hayan utilizado.

Después se continúa con la realimentación a través de la elaboración y presentación del informe para su valoración y solución.

A continuación, presentaremos los principales tipos de auditoría en donde se aplica la evaluación:

Evaluación de la gestión administrativa del área de sistemas.
Evaluación del equipo de cómputo.
Evaluación integral de sistemas.
Evaluaciones con el apoyo de la computadora.
Evaluaciones sin el uso de la computadora.
Evaluaciones de los controles en sistemas computacionales.
Evaluaciones de otros aspectos de sistemas computacionales.
Evaluación de los sistemas de redes.
Evaluación del servicio *OUTSOURCING*
Evaluación de la función ergonómica de los sistemas.
Evaluación de la calidad ISO-9000 aplicable a los sistemas.
Evaluación de los proveedores y distribuidores de sistemas.

(Para ahondar más en el tema, refiérase a las páginas de la 505 a la 531 del libro de texto).

Diagrama del círculo de evaluación

Con esta herramienta de apoyo para la evaluación de los sistemas computacionales se puede valorar, visualmente, el comportamiento de los aspectos de los sistemas que están siendo auditados, así como su cumplimiento y limitaciones (ver figura 11.7).

A continuación, se indican algunos ejemplos de aspectos comunes que pueden ser evaluados mediante esta herramienta:

Para evaluar la seguridad en el área de sistemas computacionales (en este caso siete sectores):

- Seguridad en el acceso físico al área de sistemas.
- Seguridad en el acceso y uso de las bases de datos.
- Seguridad en el mantenimiento y resguardo de las bases de datos e información.
- Seguridad del personal informático.
- Seguridad de las instalaciones del área de sistemas.
- Plan contra contingencias del área de sistemas.
- Seguridad lógica del sistema.

Para la evaluación administrativa del área de sistemas (en este caso 11 sectores):

- Evaluación de la misión, visión y objetivos del área de sistemas.
- Evaluación de las estrategias, planes y programas del área de sistemas.
- Evaluación de la estructura de organización del área de sistemas, en lo relacionado con las funciones, actividades y tareas, líneas de autoridad y responsabilidad.
- Perfil de puestos del área de sistemas.
- Documentación de sistemas.
- Seguridad y protección de los activos informáticos.
- Instalaciones del área de sistemas.
- Capacitación y promoción del personal del área de sistemas computacionales.
- Desarrollo de proyectos informáticos.
- Estandarización de metodologías, programas, equipos y sistemas
- Mobiliario, equipos y componentes del sistema.

Para la evaluación de los sistemas computacionales (en este caso 8 sectores):

- Diseño lógico del sistema computacional.
- Diseño físico del sistema computacional.
- Controles de acceso y salida de datos.
- Controles de procesamiento de información.
- Controles de almacenamiento de datos.
- Controles de seguridad.
- Controles para la operación del sistema.
- Aspectos técnicos del sistema.

(Para ahondar más en el tema, refiérase a las páginas de la 531 a la 535 del libro de texto).

Lista de verificación (o lista de chequeo)

Este es uno de los métodos de recopilación y evaluación de auditoría más sencillos, cómodos y fáciles de utilizar debido a la simplicidad de su elaboración, la comodidad en su aplicación y por la facilidad para encontrar desviaciones, lo cual la hace una de las herramientas más confiables y utilizables para cualquier revisión de sistemas computacionales; asimismo, se aplica tanto para el área de sistemas, para la gestión administrativa o cualquier otra función informática.

Esta herramienta consiste en la elaboración de una lista ordenada, en la cual se anotan todos los aspectos que se tienen que revisar del funcionamiento de un sistema, de sus componentes, del desarrollo de una actividad, del cumplimiento de una operación o de cualquier otro aspecto relacionado con la evaluación del área de sistemas. Esta lista se complementa con una o varias columnas en las que se califica el cumplimiento del aspecto evaluado.

(Para ahondar más en el tema, refiérase a las páginas de la 535 a la 537 del libro de texto).

Análisis de la diagramación de sistemas

Esta es una de las principales herramientas de apoyo para el análisis y diseño de los sistemas computacionales y es de las que más utilizan los desarrolladores de sistemas debido a que, por medio de estos diagramas el analista, se pueden representar los flujos de información, actividades, operaciones, procesos y los demás aspectos que intervendrán en el desarrollo de los propios sistemas; además, por medio de los diagramas, el programador puede visualizar el panorama específico del sistema para elaborar de manera más precisa la codificación de instrucciones del programa.

El auditor de sistemas computacionales también puede evaluar el desarrollo correcto los proyectos de sistemas que se realizan en la empresa, porque le permite considerar si el flujo de información es acorde con las necesidades del programa y si las operaciones y actividades que se realizan satisfacen los requerimientos.

El uso de esta herramienta de análisis y diseño de sistemas puede ser de gran ayuda para auditar el desarrollo de proyectos informáticos de la empresa, las acciones de cómputo que se satisfacen con dichos proyectos y la forma en que los usuarios operan el sistema.

Modelos de sistemas

Los modelos de sistemas se utilizan para tratar de interpretar una realidad acerca de las necesidades informáticas del usuario al identificar el comportamiento que tendrá el sistema a través de sus distintos procesos, actividades y componentes, que el auditor puede evaluar de manera gráfica y sencilla (ver figura 11.9).

Diccionario de datos

El diccionario de datos se aplica principalmente en el desarrollo de las bases de datos de un sistema para determinar cada uno de los campos de datos, el tipo, tamaño y descripción de los datos que contendrán dichas bases de datos, (ver figura 11.10).

Diagrama Nassi-Schneiderman

Al igual que los diagramas de sistemas anteriores, los desarrolladores de sistemas computacionales también utilizan este diagrama gráfico para el análisis y diseño del *software* estructurado de un nuevo sistema. En este diagrama gráfico se definen, lo más objetiva y claramente posible, procesos, decisiones e iteraciones del sistema a fin de señalar gráficamente todas las acciones que seguirá el programa para su funcionamiento adecuado (ver la figura 11.11).

(Para ahondar más en el tema, refiérase a las páginas de la 537 a la 548 del libro de texto).

Diagrama de seguimiento de una auditoría de sistemas computacionales

El uso de esta técnica, también conocida como mapa conceptual de evaluación, es utilidad en una auditoría de sistemas computacionales, porque permite elaborar un mapa conceptual de todos los aspectos de los sistemas en evaluación.

Al utilizar esta técnica, se le proporciona un seguimiento concreto de todas y cada una de las partes que componen el sistema, lo cual permite que el auditor tenga un panorama completo del sistema a fin de evaluar integralmente todos sus aspectos. Los diagramas de seguimiento se usan tanto para la gestión informática, para la seguridad del sistema, los componentes del sistema o cualquier otro aspecto informático en evaluación.

Esta herramienta informática se aplica mediante un diagrama descriptivo del sistema, de tipo secuencial descendente, con sangrías significativas de izquierda a derecha, la cuales señalan cada una de las partes que integran el aspecto de sistemas auditado, de tal manera que el auditor pueda identificarlas.

Con ello, logra un panorama general de lo que está auditando y puede señalar las principales observaciones que encuentra, así como las partes que se ven afectadas por esas desviaciones. Si esta herramienta se aplica correctamente, evidenciará los aspectos de sistemas involucrados así como sus posibles desviaciones.

(Para ahondar más en el tema, refiérase a las páginas de la 549 a la 553 del libro de texto).

Programas para revisión por computadora

Esta técnica es de las más utilizadas en cualquier auditoría de sistemas computacionales debido a que permite revisar, desde la misma computadora y mediante un programa específico, el funcionamiento del sistema, de una base de datos, de un programa especial o de alguna aplicación de interés, ya sean sus procesamientos, su funcionamiento interno, el aprovechamiento de las aplicaciones informáticas, el consumo de recursos, los resultados del procesamiento de información o el comportamiento específico de alguna actividad administrativa, entre otros aspectos.

Esta herramienta tiene dos vertientes importantes; por un lado, el uso de programas específicos, previamente diseñados por desarrolladores de sistemas con el propósito de evaluar aspectos específicos de sistemas de contabilidad, nóminas o cualquier otro aspecto especial de la gestión administrativa de la empresa o de los propios sistemas computacionales.

Por otro lado, el diseño de programas concretos que el auditor desarrolla le permiten evaluar aspectos concretos que desea auditar, los cuales pueden ser

desde aspectos netamente de sistemas, casos concretos de gestión informática, el funcionamiento interno del sistema, su arquitectura o su procesamiento de datos. Algunas veces hasta la revisión interna del sistema, en cuanto al *hardware*, *software*, componentes, instalaciones y aspectos técnicos del sistema.

(Para ahondar más en el tema, refiérase a las páginas de la 553 a la 555 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- Explique en qué consiste la técnica de auditoría de sistemas denominada simulación.

2- ¿Por qué la auditoría de sistemas computacionales debe incluir entre sus objetivos de auditoria a los proveedores y distribuidores de sistemas?

3- ¿En qué consiste la técnica de auditoría llamada lista de verificación o lista de chequeo?

4- Dentro de los programas para la revisión por computadora hay unos que son elaborados por el mismo auditor. En otras palabras, ¿debe el auditor de sistemas ser un experto desarrollador de programas? Explique.

Capítulo 12

Propuesta de puntos que se deben evaluar en una auditoría de sistemas computacionales

Sumario

Auditoría con la computadora
Auditoría sin la computadora
Auditoría a la gestión informática del área de sistemas
Auditoría al sistema computacional
Auditoría alrededor de la computadora
Auditoría de la seguridad de los sistemas computacionales
Auditoría a los sistemas de redes
Auditoría *outsourcing* en los sistemas computacionales
Auditoría ISO-9000 a los sistemas computacionales
Auditoría ergonómica de los centros de cómputo
Auditoría integral a los centros de cómputo

Propósito del capítulo

El propósito de este capítulo consiste en que el auditor conozca acerca de las herramientas con que puede contar de acuerdo con el tipo de auditoría que vaya a realizar.

Objetivos de aprendizaje

Al finalizar el estudio de este tema, usted, deberá estar en la capacidad de:

- Identificar los diferentes tipos de auditoría de sistemas computacionales.
- Reconocer los puntos específicos que el auditor debe considerar para aplicarlos de acuerdo con la actividad de sistemas que tenga que auditar.

Guía de lecturas

Para lograr los objetivos descritos anteriormente, es importante que usted realice las siguientes lecturas:

Subtema	Página
12.1 Auditoría con la computadora	559
12.2 Auditoría sin la computadora	569
12.3 Auditoría a la gestión informática del área de sistemas	578
12.4 Auditoría al sistema computacional	584
12.4.1 Auditoría al sistema computacional según las características de su *hardware*	586
12.4.2 Auditoría al sistema computacional según las características de su *software*	588
12.4.3 Auditoría al diseño lógico del sistema	591
12.4.4 Auditoría al diseño físico del sistema	591
12.4.5 Auditoría a la administración y control de accesos y salidas de datos	593
12.4.6 Auditoría a la administración y control del procesamiento de datos	593
12.4.7 Auditoría a los controles de almacenamiento	594
12.4.8 Auditoría a los controles de seguridad del sistema computacional	595
12.4.9 Auditoría a los controles adicionales para la operación del sistema	596
12.4.10 Auditoría a la administración del área de sistemas computacionales	596
12.4.11 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría de sistemas computacionales	597
12.5 Auditoría alrededor de la computadora	600
12.6 Auditoría de la seguridad de los sistemas computacionales	610
12.7 Auditoría a los sistemas de redes	621
12.7.1 Evaluación del diseño, instalación y aprovechamiento de la red de cómputo	623
12.7.2 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría a los sistemas de redes	637
12.8 Auditoría *outsourcing* en los sistemas computacionales	641
12.8.1 Auditoría a los sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de los servicios *outsourcing*	645
12.8.2 Evaluación de la forma en que la empresa contratante recibe el servicio *outsourcing*	649
12.8.3 Evaluación del servicio *HelpDesk* (ayuda en línea) de la empresa	652
12.8.4 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría *outsourcing* en los sistemas computacionales	655
12.9 Auditoría ISO-9000 a los sistemas computacionales	660
12.9.1 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría ISO-9000 a los sistemas computacionales	665
12.10 Auditoría ergonómica de los centros de cómputo	668
12.10.1 Auditoría de las repercusiones de los sistemas computacionales en la salud visual del usuario	670
12.10.2 Evaluación de las repercusiones en la salud de la espalda, columna vertebral, tórax, cuello, nuca, piernas y pies a causa de la posición que adoptan los usuarios	671
12.10.3 Evaluación de las repercusiones musculares-esqueléticas de manos, muñecas, dedos y brazos del usuario	673
12.11 Auditoría integral a los centros de cómputo	677

COMENTARIOS GENERALES

En los siguientes capítulos también señalamos los principales elementos de sistemas que se deben tomar en cuenta en cada uno de los tipos de auditoría ahí propuestos.

A continuación, se analizará la manera de aplicar cada uno de los tipos de auditoría sugeridos a fin de que el lector conozca los puntos que debe considerar al planear su auditoría de sistemas computacionales de acuerdo con las necesidades específicas de evaluación de sistemas de la empresa que audite.

Auditoría con la computadora

Podemos definir este tipo de auditoría de la siguiente manera:

Es la auditoría que se realiza con el apoyo de los equipos de cómputo y sus programas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas pero sí susceptibles de ser automatizadas; dicha auditoría se realiza también a las actividades del propio centro de sistemas y a sus componentes.

La principal característica de este tipo de auditoría es que, sea en un caso o en otro, o en ambos, se aprovecha la computadora y sus programas para la evaluación de las actividades que se revisarán, de acuerdo con las necesidades concretas del auditor al utilizar, en cada caso, las herramientas especiales del sistema y las tradiciones de la propia auditoría.

Este tipo de revisiones de auditoría se puede clasificar de acuerdo con las siguientes aplicaciones específicas:

- Uso de la computadora y aplicaciones exclusivamente en auditorías de los sistemas computacionales de la empresa.
- Uso de la computadora y aplicaciones exclusivamente en auditorías de las demás áreas de la empresa.
- Auditorías con la computadora y aplicaciones, en combinación con las herramientas tradicionales, para evaluar los sistemas computacionales.

(Para ahondar más en el tema, refiérase a las páginas de la 559 a la 569 del libro de texto).

Auditoria sin la computadora

Podemos definir este tipo de auditoría de la siguiente manera:

Es la auditoría cuyos métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional del comportamiento y validez de las transacciones económicas, administrativas y operacionales de un área de secciones económicas, administrativas y operacionales de un área de cómputo y, en sí, de todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos. Dicha evaluación se realiza sin el uso de los sistemas computacionales.

Se evalúa tanto a la estructura de organización, funciones y actividades de funcionarios y personal de un centro de cómputo, así como a los perfiles de sus puestos, a los reportes, informes y bitácoras de los sistemas a la existencia y aplicación de planes, programas y presupuestos en dicho centro, así como del uso y aprovechamiento de los recursos informáticos para la realización de actividades, operaciones y tareas.

Asimismo, es la evaluación de los sistemas de seguridad y prevención de contingencias, de la adquisición y uso del *hardware*, *software* y personal informático y, en sí, de todo lo relacionado con el centro de cómputo, pero sin el uso directo de los sistemas computacionales.

A continuación, presentamos algunas gestiones concretas de carácter administrativo que pueden ser evaluadas en forma tradicional:

- Auditoría a la actividad administrativa del centro de cómputo.
- Auditoría a la gestión financiera del centro de cómputo.
- Auditoría a la operación de los sistemas.
- Auditoría al desarrollo de los proyectos de sistemas computacionales.
- Auditoría a las técnicas y sistemas de procesamiento.
- Auditoría a los sistemas de seguridad y prevención de contingencias.
- Auditoría a los consumibles para el funcionamiento de los sistemas.
- Auditoría del uso y acceso a los sistemas y programas computacionales.

(Para ahondar más en el tema, refiérase a las páginas de la 569 a la 578 del libro de texto).

Auditoria a la gestión informática del área de sistemas

Podemos definir este tipo de auditoría de la siguiente manera:

Es la auditoría cuya aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo, que se realizan dentro de un centro de cómputo tales como la planeación, organización, dirección y control de dicho centro.

Esta auditoría también se realiza con el fin de verificar el cumplimiento de las funciones y actividades asignadas a los funcionarios, empleados y usuarios de las áreas de sistematización, así también para revisar y evaluar las operaciones del sistema. El uso y la protección de los sistemas de procesamiento, de los programas y de la información.

Se aplica también para verificar el desarrollo correcto, instalación, mantenimiento y explotación de los sistemas computacionales, así como de sus equipos e instalaciones con el propósito de dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de una empresa y del propio centro informático.

Esta auditoría bien puede ser realizada por un auditor de sistemas computacionales, administrativo u operacional, siempre y cuando contemple en su revisión, entre otras cosas, los siguientes aspectos:

- Auditoría a la planeación estratégica en la empresa y el área de sistemas.
- Auditoría a la estructura de organización del área de sistemas.
- Auditoría al cumplimiento de las funciones, tareas y operaciones de la actividad informática en la empresa y el área de sistemas.
- Auditoría a la dirección del área de sistemas.
- Auditoría a la administración del factor humano en el área de sistemas.
- Auditoría a la administración de los recursos informáticos no humanos del área de sistemas.
- Auditoría a los controles informáticos del área de sistemas.
- Evaluación de la existencia, establecimiento y uso de los estándares de sistemas.
- Auditoría a la documentación de los sistemas en el área de informática y a la documentación de las demás áreas de la empresa que cuenten con servicios informáticos.

(Para ahondar más en el tema, refiérase a las páginas de la 578 a la 584 del libro de texto).

Auditoria al Sistema Computacional

Podemos definir este tipo de auditoría de la siguiente manera:

Es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de cómputo, así como de su *hardware*, *softwar*e y periféricos asociados.

Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o externas, así como al diseño, desarrollo y uso del *software* de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo, o paquetería de aplicación institucional que se utiliza en la empresa donde se

encuentra el equipo de cómputo que será evaluado. Se incluye también la operación del sistema.

En relación con lo anterior, a continuación presentamos algunas de las consideraciones que se deben tomar en cuenta sobre los sistemas computacionales:

- El tipo de procesador del sistema computacional, así como su velocidad, capacidad, memoria y demás características con los cuales opera el sistema de cómputo.
- Los fabricantes del *hardware*, *software* y periféricos del sistema computacional.
- Las características y especificaciones del diseño del sistema computacional.
- Las plataformas, ambientes, el tamaño y configuración del sistema computacional.
- Los sistemas operativos, lenguajes, programas de desarrollo y aplicación, utilerías y demás software del sistema computacional.
- La forma de administrar el sistema y sus componentes asociados.
- El sistema de administración de bases de datos e información manejado.
- La arquitectura del sistema, sus periféricos, equipos asociados y demás componentes.
- Las aplicaciones concretas para las que está destinado el sistema computacional.

A continuación, presentamos algunos aspectos que se deben evaluar en este tipo de auditorías:

Auditoría al sistema computacional según las características de su *hardware*
Auditoría al sistema computacional según las características de su *software*
Auditoría al diseño lógico del sistema
Auditoría al diseño físico del sistema
Auditoría a la administración y control de accesos y salidas de datos
Auditoría a la administración y control del procesamiento de datos
Auditoría a los controles de almacenamiento
Auditoría a los controles de seguridad del sistema computacional
Auditoría a los controles adicionales para la operación del sistema
Auditoría a la administración del área de sistemas computacionales
Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría de sistemas computacionales

(Para ahondar más en el tema, refiérase a las páginas de la 584 a la 600 del libro de texto).

Auditoria alrededor de la computadora

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión específica que se realiza a todo lo que está alrededor de un equipo de cómputo, como son sus sistemas, actividades y funcionamiento, evalúa los métodos y procedimientos de acceso y procesamiento de datos, la emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del centro de cómputo, los aspectos operacionales y financieros, la gestión administrativa de accesos al sistema, la atención a usuarios y al desarrollo de nuevos sistemas, las comunicaciones internas y externas y, en sí, todos aquellos aspectos que contribuyen al buen funcionamiento de un área de sistematización.

A continuación presentamos algunos aspectos del entorno de la computadora que deben ser evaluados:

- El diseño físico del área de sistemas y de las áreas de la empresa que cuenten con sistemas computacionales.
- El análisis y aprobación de las propuestas para la adquisición del software, hardware, periféricos, equipos adicionales, bienes muebles, consumibles y materiales diversos que permiten el funcionamiento del sistema.
- El ambiente de trabajo en el que se realiza la función informática de la empresa.
- La gestión administrativa de la función informática de la empresa.
- El diseño de proyectos de nuevos sistemas computacionales en el área de sistemas.
- El diseño de formatos, formas y métodos para la recopilación de información que será procesada en el sistema.
- La administración y control de los sistemas de seguridad y salvaguarda de los activos informáticos, la información, el personal y los usuarios del sistema.
- La administración y control de accesos a las instalaciones del área de cómputo, a los sistemas, a la información y los bienes informáticos del área.
- Todos aquellos aspectos especiales que intervienen de alguna manera en el aprovechamiento y explotación del sistema computacional y en la gestión administrativa del centro de cómputo con la condición indiscutible de no interferir directamente en el uso del equipo de cómputo.

A continuación presentamos los aspectos generales que intervienen en una auditoría alrededor de la computadora, porque esta auditoría se debe realizar de acuerdo con las características, las necesidades y las repercusiones de la administración del área de sistemas de cada empresa o del propio equipo procesador:

Auditoría a la administración del software de la empresa.

Auditoría a la configuración física del área de sistemas de la empresa

Auditoría a los métodos de acceso, seguridad y salvaguarda de los activos informáticos del área de sistemas

Auditoría a la administración del área de sistemas.

Auditoría a los aspectos técnicos del sistema.

Auditoría a la administración del sistema.

(Para ahondar más en el tema, refiérase a las páginas 600 a la 610 del libro de texto).

Auditoria de la seguridad de los sistemas computacionales

Podemos definir este tipo de auditoría de la siguiente manera:

Consiste en la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema computacional, de sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales de las bases de datos, redes, sistemas, instalaciones y usuarios.

Es también la revisión de los planes contra contingencias y medidas de protección para la información, los usuarios y los propios sistemas computacionales y, en sí, la evaluación de todos aquellos aspectos que contribuyen a la protección y salvaguarda del buen funcionamiento del área de sistematización, sistemas de redes o computadoras personales. Se incluye la prevención y erradicación de los virus informáticos.

Los principales aspectos que se deben considerar en la auditoría de la seguridad de los sistemas computacionales, los presentaremos de manera general, porque su real aplicación se implementa de acuerdo con las características y las necesidades de la administración de la seguridad, protección y salvaguarda de los bienes informáticos o del sistema computacional del área de cómputo de cada empresa:

- Auditoría de la seguridad en las condiciones e instalaciones físicas del área de sistemas.
- Protección contra riesgos y contingencias de origen natural relacionadas con el ambiente de trabajo.
- Protección contra riesgos y contingencias relacionados con el medio ambiente de trabajo en las áreas de sistemas de la empresa.
- Protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos y desastres naturales incontrolables.
- Protección contra riesgos y contingencias derivados del suministro de la energía eléctrica.

- Protección y seguridad de los espacios físicos de las instalaciones de cómputo.
- El análisis a los planes de contingencias informáticas.
- Auditoría de la seguridad y protección en el diseño de las instalaciones del área de sistemas de la empresa o empresas de cómputo.
- Auditoría de la seguridad en los sistemas computacionales.
- Auditoría de la seguridad del *hardware*.
- Auditoría de la seguridad del *software*.
- Auditoría de la seguridad en los sistemas computacionales.
- Auditoría para verificar la captura, procesamiento de datos y emisión de resultados.
- Auditoría de la prevención de actos premeditados que afecten el funcionamiento de los sistemas computacionales.
- Protección contra los actos ilegales en contra de los sistemas, activos informáticos e información.
- Protección contra el mal uso de la información.
- Protección contra la piratería y robo de información.
- Protección para el almacenamiento de la información.
- Protección contra actos no intencionales.
- Protección contra virus informático.
- Protección y seguridad para el desarrollo de programas y proyectos de sistemas.
- Protección y seguridad para los accesos al sistema computacional y a la información.
- Protección y seguridad del hardware, componentes del sistema, periféricos y equipos asociados.
- Mantenimiento preventivo y correctivo a la CPU.
- Mantenimiento preventivo y correctivo al sistema.
- Mantenimiento preventivo y correctivo a los periféricos.
- Mantenimiento preventivo y correctivo al equipo adicional.
- Resultados de auditorías de sistemas.
- Prevención de huelgas.
- Prevención ante cambios sociales, económicos, legales, entre otros.
- Prevención ante cambios tecnológicos.

(Para ahondar más en el tema, refiérase a las páginas de la 610 a la 621 del libro de texto).

Auditoria a los Sistemas de Redes

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos privilegios, administración, funcionamiento y aprovechamiento.

Constituye también la revisión del *software* institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos e instalaciones de un sistema de red.

Para analizar el impacto de las redes en las empresas, se examinarán las siguientes orientaciones que permitirán evaluar los principales aspectos que impactan el funcionamiento de los sistemas de red de área local, metropolitana y amplia, así como de Internet:

- Los objetivos de una red de cómputo.
- Las características de la red de cómputo.
- Los componentes físicos de una red de cómputo.
- La conectividad y comunicaciones de una red de cómputo.
- Los servicios que proporciona una red de cómputo.
- Los sistemas operativos, lenguajes, programas, paqueterías, utilerías y bibliotecas de la red de cómputo.
- Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.
- Los protocolos de comunicación interna de la red.
- La administración de una red de cómputo.
- La seguridad de las redes de cómputo.

Evaluación del diseño, instalación y aprovechamiento de la red de cómputo

En esta parte de la auditoría **se estudian las** razones por las que fue necesario implantar una red de cómputo en la empresa al investigar el análisis de las necesidades del proyecto, el diseño de la red y su configuración lógica y física, su implementación y aprovechamiento.

El auditor de sistemas debe analizar, mediante el uso de las herramientas señaladas en los capítulos anteriores, los aspectos relacionados con los sistemas de red, que se presentan a continuación:

- Evaluación del análisis de una red de cómputo.
- Evaluación de la existencia y uso de metodologías, normas, estándares y políticas para el análisis y diseño de redes de cómputo.
- Análisis de la definición de la problemática y solución para instalar redes de cómputo en la empresa.
- Análisis del cumplimiento de los objetivos fundamentales de la organización para instalar una red de cómputo.
- Análisis de la delimitación de los proyectos de red, a fin de evaluar la manera en que se cumple.
- Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de una red de cómputo en la empresa.
- Evaluación del diseño e implementación de la red según el ámbito de cobertura.

Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría a los sistemas de redes

En esta auditoria se evalúan los aspectos específicos de la red de cómputo, considerando las características de la red, su tamaño y cobertura,

configuraciones física y lógica, topologías, protocolos de comunicación y aspectos técnicos de su composición.

También, se evalúa la forma en que se aprovechan los recursos informáticos de la organización, la información y todo lo relacionado con la función informática en la institución con el objeto de validar la administración adecuada de la red, su funcionamiento correcto y el aprovechamiento de las actividades informáticas de la empresa.

(Para ahondar más en el tema, refiérase a las páginas de la 621 a la 641 del libro de texto).

Auditoria *Outsourcing* en los Sistemas Computacionales

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, sistemática y especializada para evaluar la calidad, eficiencia y oportunidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra con el fin de verificar la confiabilidad, oportunidad, suficiencia y asesoría por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades que tienen encomendados los prestadores de servicios, usuarios y el personal, en general. Dicha revisión se realiza también en los equipos y sistemas.

Con la auditoría *outsourcing* en los sistemas computacionales se busca evaluar la eficiencia y eficacia de los servicios que se proporcionan a las organizaciones al enfocarlos desde dos puntos de vista: por un lado, aquel en el cual se auditan las actividades, funciones y operaciones del prestador de servicios en cuanto a la administración de sus recursos informáticos, la confiabilidad, la oportunidad y la eficiencia con las que trata la información de las organizaciones, los resultados que obtienen del procesamiento de datos y la eficiencia y eficacia de sus servicios.

Por otro lado, aquel en donde se evalúa la forma en que se desarrolla la actividad de *outsourcing* en la empresa que lo proporciona, analizar calidad, rapidez, oportunidad, confiabilidad, eficacia y eficiencia con las que trabaja para suministrar de una manera adecuada la actividad informática a la institución contratante.

En ambos casos, el auditor de sistemas deberá realizar dicha auditoría con base en los siguientes aspectos:

- La infraestructura informática para la prestación de los servicios *outsourcing*.
- La administración adecuada y el control en la prestación del servicio de *outsourcing* informático.
- La eficiencia y eficacia de los sistemas de comunicación entre prestador y contratante de los servicios informáticos.

- La confiabilidad, veracidad, integridad, oportunidad, suficiencia y calidad con las que se procesa la información de la empresa que contrata los servicios.
- La configuración, composición e integración de los sistemas computacionales para evaluar la capacidad y suficiencia del prestador de los servicios de cómputo.
- El mantenimiento preventivo y correctivo de los servicios de cómputo tanto del prestador como del que los contrata.

Auditoría a los sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de los servicios *outsourcing*

En esta auditoría se evalúa la eficiencia y la eficacia con las que el prestador de servicios proporciona los servicios informáticos a la organización que lo contrató.

Para realizar esta evaluación se debe tomar en cuenta estos criterios: si el servicio se proporciona a través de sistemas de redes o si los servicios se aprestan con sistemas individuales.

En el caso de ambas posibilidades, se sugiere aplicar la auditoría que corresponda al tipo de prestación de servicios junto con los aspectos que complementan la auditoría *outsourcing*, los cuales se mencionan a continuación:

- Evaluación de la prestación de los servicios *outsourcing* informáticos.
- Evaluación de las estructuras de organización del área de sistemas del prestador de servicios y de la empresa receptora del servicio *outsourcing* informático.
- Evaluación de la administración de las funciones, actividades, tareas y operaciones del prestador del servicio para cumplir con la actividad *outsourcing* informática de la empresa contratante.
- Evaluación de la administración de los recursos informáticos no humanos del área de sistemas.
- Evaluación de los controles informáticos del área de sistemas dedicada a la prestación/recepción del servicio *outsourcing* informático.

Evaluación de la forma en que la empresa contratante recibe el servicio *outsourcing*

Con la realización de esta auditoría se busca evaluar la calidad, suficiencia, eficiencia y eficacia de la recepción de servicios *outsourcing* informáticos en la empresa, encausando la revisión hacia el análisis de los sistemas computacionales con los cuales se proporciona el servicio a los usuarios de la empresa así como la forma en que se lleva a cabo esta actividad.

Es recomendable aplicar la auditoría que corresponda a cualquiera de los dos tipos de recepción de servicios que tratamos anteriormente, junto con los aspectos que complementan la auditoría *outsourcing*, que presentamos a continuación:

- Inventarios de la prestación de servicios *outsourcing* informáticos.
- Evaluación de la recepción de los servicios *outsourcing* informáticos.
- Evaluación de las estructuras de organización del área de sistemas del prestador de servicios *outsourcing* informáticos, así como de las de la empresa que contrata dichos servicios.
- Evaluación de la administración de las funciones, actividades, tareas y operaciones del prestador del servicio para cumplir con la actividad *outsourcing* informática de la empresa contratante.
- Evaluación de la administración de los recursos informáticos no humanos del área de sistemas.
- Auditoría de los controles informáticos del área de sistemas dedicada a la prestación/recepción del servicio *outsourcing* informático.

Evaluación del servicio *HelpDesk* (ayuda en línea) de la empresa

El servicio *HelpDesk* funciona para ayudar a resolver, dentro de la misma empresa, los problemas que se les presentan a los usuarios en el manejo de sus sistemas computacionales. Con esta ayuda se abarcan todos los problemas que ocurren durante la actividad informática.

La función del auditor es, precisamente, evaluar todos los aspectos relativos a la calidad, rapidez y confiabilidad con la que se proporciona este servicio a los usuarios.

- Evaluación del soporte técnico, de asistencia y capacitación a los usuarios, así como del mantenimiento de los sistemas y detección de incidencias de problemáticas para la solución a los reportes de los usuarios.
- Evaluación de las actividades técnicas para proporcionar asistencia y mantenimiento a los sistemas computacionales.

Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría *outsourcing* en los sistemas computacionales

Como hemos señalado, en esta auditoría *outsourcing* en los sistemas computacionales se busca evaluar la eficiencia y eficacia con las que la empresa prestadora de estos servicios proporciona dichos servicios a la empresa que los contrata al enfocarlos a la administración de la actividad de *outsourcing*, analizar calidad, rapidez, oportunidad, confiabilidad, eficacia y eficiencia con las que trabaja para administrar la actividad informática y la información de la institución contratante, recursos informáticos, manejo, confiabilidad, oportunidad, calidad, el tratamiento de la información y los resultados.

(Para ahondar más en el tema, refiérase a las páginas de la 641 a la 660 del libro de texto).

Auditoria ISO-9000 a los sistemas computacionales

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, sistemática y especializada que realizan, únicamente, los auditores especializados y certificados en las normas y procedimientos ISO-9000 al aplicar, en forma exclusiva, los lineamientos, procedimientos e instrumentos establecidos por esta asociación.

El propósito fundamental de esta revisión consiste en evaluar, dictaminar y certificar que la calidad de los sistemas computacionales de una empresa se apegue a los requerimientos del ISO-9000.

Por lo general, esta auditoría ISO-9000 es de carácter externo y tiene que ser practicada por algún despacho reconocido y autorizado para otorgar la certificación ISO-9001, ISO-9004 o la más reciente, que es la ISO-14000, aplicables según los criterios de certificación a los sistemas de cómputo.

Los fundamentos de la calidad ISO-9000 se pueden resumir en tres acciones fundamentales:

- Documentar lo que se elabore.
- Desarrollar lo que se está documentando.
- Revisar lo que se elabora con lo documentado.

Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría ISO-9000 a los sistemas computacionales

Esta auditoria incluye aspectos específicos que **la diferencian de** las demás auditorías de sistemas, debido a que cuenta con características peculiares de aplicación. Todas ellas enfocadas a la certificación ISO-9000, porque las personas que aplican la auditoría de certificación de calidad ya tienen definidas las herramientas, técnicas y procedimientos especiales, que utilizan sin ninguna variación, porque están normados para la certificación de calidad.

(Para ahondar más en el tema, refiérase a las páginas de la 660 a la 668 del libro de texto).

Auditoria Ergonómica de los Centros de Cómputo

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión técnica, específica y especializada que se realiza para evaluar la calidad, eficiencia y utilidad del entorno, hombre, máquina y ambiente, que rodean el uso de los sistemas computacionales en una empresa.

Esta revisión se realiza también con el propósito de evaluar la adquisición y el uso correctos del mobiliario, equipo y sistemas a fin de proporcionar el bienestar, confort y la comodidad que requieren los usuarios de los sistemas computacionales de la empresa, así como para evaluar la detección de los

posibles problemas y sus repercusiones y la determinación de las soluciones relacionadas con la salud física y el bienestar de los usuarios de los sistemas de la empresa.

Auditoría de las repercusiones de los sistemas computacionales en la salud visual del usuario.

Evaluación de las repercusiones en la salud de la espalda, columna vertebral, tórax, cuello, nuca, piernas y pies a causa de la posición que adoptan los usuarios.

Evaluación de las repercusiones musculares-esqueléticas de manos, muñecas, dedos y brazos del usuario.

(Para ahondar más en el tema, refiérase a las páginas de la 668 a la 677 del libro de texto).

Auditoria integral a los centros de cómputo

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, sistemática y global de todas las actividades y operaciones de un centro de sistematización, que realiza un equipo multidisciplinario de auditores a fin de evaluar, en forma integral, el uso adecuado de sus sistemas computacionales, periféricos y equipos de apoyo para el procesamiento de información de la empresa, así como el desarrollo correcto de las funciones de sus áreas, personal y usuarios.

Además, incluye la revisión de la administración del sistema, del manejo y control de los sistemas operativos, lenguajes, programas y paqueterías de aplicación, así como de la administración y control de proyectos, de la adquisición del *hardware* y *software* institucionales, de la integración y uso adecuado de sus recursos informáticos y de la existencia y cumplimiento de las normas, políticas, estándares y procedimientos que regulan el uso del sistema y la actuación del personal y usuarios del centro de cómputo.

Tipos de auditoría integral de sistemas

Aunque no existe ninguna clasificación formal de este tipo de auditorías, a continuación presentamos dos formas para realizar una auditoría integral de sistemas; por un lado, la auditoría externa y por otro lado la auditoría interna:

- Auditoria externa de sistemas.
- Auditoria interna de sistemas.

Auditoría externa de sistemas computacionales

La auditoria externa de sistemas computacionales es aquella que realiza un auditor o un grupo de auditores que son ajenos a la operación normal de la organización en donde se revisa el sistema.

La principal característica de esta auditoría consiste en que los profesionales participen en estos trabajos con absoluta libertad en la aplicación de sus métodos, técnicas y procedimientos de evaluación, sin que ningún funcionario o empleado del centro de cómputo de la empresa interfiera en su trabajo. Por lo tanto, su dictamen es de carácter independiente.

Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría integral a los centros de cómputo

Esta auditoría concentra todos los tipos anteriores sólo que, aquí, se enfoca en una revisión global del lugar donde se supone se concentran todas las actividades informáticas de una empresa.

Se pretende que esta auditoría abarque todos los aspectos de sistemas, en una forma profunda, completa y amplia, a fin de evaluar en forma integral todos los aspectos que intervienen en el ámbito de sistemas. Así, la auditoría integral siempre se realizará de acuerdo con el alcance e intención que se le quiera dar a la evaluación, así como con la disponibilidad de recursos y tiempo para realizarla.

La auditoria integral a los centros de cómputo tiene aspectos específicos, que vislumbran cada una sea en forma diferente de la otra. Se encuentran notables diferencias entre una auditoría practicada a una empresa con un pequeño centro de cómputo y a otra cuyo centro sea de mayor envergadura.

Ambas auditorías son de carácter integral y similares en algunos alcances, intenciones e, incluso, en los puntos que abarquen; no obstante, las herramientas, los procedimientos, las técnicas y los métodos de evaluación son totalmente diferentes.

(Para ahondar más en el tema, refiérase a las páginas de la 677 a la 685 del libro de texto).

PREGUNTAS PARA AUTOEVALUACIÓN

1- Una de las tareas de la auditoría de sistemas es realizar evaluaciones a la gestión informática del área de sistemas, ¿qué aspectos principales debe incluir este tipo de revisión? Mencione, al menos, cuatro de ellos.

2- ¿Cuáles son los aspectos más relevantes que deben evaluarse en una auditoría al sistema de redes de una empresa?

3- Hay dos tipos de servicios que se dan a la empresa que deben ser evaluados por el auditor de sistemas, los servicios *outsourcing* y el servicio *Help Desk*. ¿Qué aspectos se incluyen para cada uno de estos servicios?

REFERENCIAS BIBLIOGRÁFICAS

Marcelo C., Julián. (2002). *Riesgo y Seguridad de los Sistemas Informáticos*. Editorial Universidad Politécnica de Valencia: España.

Merike, Kaeo. (2002). *Diseño de seguridad en redes*. Editorial Pearson Educación: México.

Muñoz Razo, Carlos. (2002). *Auditoría en Sistemas Computacionales*. Primera edición. Editorial Pearson Prentice Hall: México.

Pacheco Urbina, Adela María. (2008). *Material Complementario para el curso de Seguridad y Auditoría en las TIC*. EUNED: San José, C.R.

_____. (2008). *Orientación para el curso Seguridad y Auditoría en las TIC*. EUNED: San José, C.R.

Piattini, Mario G. y del Peso N., Emilio. (2005). *Auditoría informática*. *Un enfoque práctico*. Segunda edición ampliada y revisada. Editorial Ra-Ma: España.

Stallings, William. (2004). *Fundamentos de seguridad en redes. Aplicaciones y estándares*. Segunda edición. Editorial Pearson Educación: Madrid, Esp.

RESPUESTAS A LAS PREGUNTAS DE AUTOEVALUACIÓN

Capítulo 1

1- Una diferencia, pero que no es fondo o sustancial, es el hecho de que en la segunda se realiza para entidades meramente gubernamentales. Por lo demás, podremos decir que no hay gran diferencia entre ellas pues, en ambas, se realiza una auditoría general de todos los procesos.

Una situación que sí puede marcar diferencia es el hecho de que en el caso de la auditoría, debe realizarse tomando en cuenta todas aquellas entidades gubernamentales que generan disposiciones para las entidades públicas como el caso, en nuestro país, de la Contraloría General de la República, Procuraduría General y la SUGEF, entre otras.

No obstante, la junta directiva de una empresa no gubernamental gira directrices por seguir en diferentes campos y está interesada de que éstos se cumplan.

2- La primera es la auditoría técnica y especializada se enfoca, únicamente, a la evaluación del funcionamiento y usos correctos del equipo de cómputo, su hardware, software y periféricos asociados.

Esta auditoría se realiza a la composición y arquitectura de las partes físicas y demás componentes de hardware incluyendo equipos asociados, instalaciones, comunicaciones internas y externas, así como el diseño y uso del software de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo y paquetería.

La segunda consiste en una revisión específica que se realiza a lo que está alrededor de un equipo de cómputo como son sus sistemas, actividades y funcionamiento mediante una evaluación de sus métodos y procedimientos de acceso y procesamiento de datos, la emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del propio equipo del centro de cómputo, entre otros.

Capítulo 3

1- Con el propósito de señalar al auditor el rumbe ético y moral que deberá seguir para cumplir y hacer respectar dichos criterios y responsabilidades y para que se norme su actuación profesional ante las empresas, la sociedad y sus colegas. Así, deberá esmerarse en el buen cumplimiento de esta actividad; no sólo cuando le sea encomendada una auditoría, sino también en su desempeño personal.

2- La equidad es una virtud que trata de igualar la justicia, ponderación y emisión de juicios. La imparcialidad es el tratar de evitar la preferencia injusta sobre algo y la razonabilidad es la capacidad del individuo para

discurrir y emitir un juicio. En el caso del auditor está comprometido a actuar de manera ecuánime (igualdad de ánimo), imparcial (sin cargo hacia algún lado) y razonada (fundada en el razonamiento).

El auditor no puede realizar una revisión si carece de alguna de estas virtudes, porque en la aplicación correcta de cada una de ellas es en donde se fundamenta su actuación profesional.

3- El trabajo del auditor sólo es válido y confiable si emite un dictamen confiable y veraz, el cual sea resultado de una avaluación profesional, libre de cualquier influencia y presión tanto de carácter interno (de la empresa, área o personal auditado) como externo (de autoridades, terceros o de sus jefes). De esta forma, cuando emita un dictamen, su juicio debe ser absolutamente independiente.

Capítulo 5

1- La división del trabajo, desde el punto de vista laboral, se efectúa con el propósito de buscar una mayor eficiencia y eficacia en las labores. Por lo tanto, se crea una especialización que beneficia a la empresa.

Desde el punto de vista del control interno la división del trabajo se realiza para evitar que un mismo funcionario u operario realice tareas incompatibles; por ejemplo, generación y aprobación de cheques.

Desde el punto de vista de la burocracia, justamente este el propósito, evitar tareas incompatibles en la función pública. El problema consiste en que la función pública la han desmeritado los mismos funcionarios debido a que no hay supervisión en cuanto a la eficiencia con que deben realizarse los trámites.

Al haber división de trabajo, tanto en lo privado como en lo público, para que haya un fraude deben ponerse de acuerdo, al menos, dos personas que, aunque se da, es más difícil. Si un trámite lleva el concurso de dos o más personas, sin llegar al abuso en cuanto a división de tareas, el riesgo de un fraude informático o de otra índole se minimiza.

2- En cualquier área de sistemas es de suma importancia estandarizar el desarrollo de todas las actividades y funciones a fin de que éstas se realicen de manera uniforme conforme a las necesidades concretas de las unidades de informática que integran la empresa.

En esta estandarización se deben respetar la división del trabajo, la asignación de actividades específicas. Este es un aspecto básico que se debe considerar para el establecimiento del control interno informático en cualquier empresa.

3- Porque la prevención son todas aquellas acciones tendientes a prevenir y controlar los riesgos y las posibles contingencias que se presenten en las áreas de sistematización, las cuales van desde prevenir accidentes en los equipos, en la información y en los programas.

En otras, palabras, no hay que esperar que un riesgo o contingencia se materialice para actuar sino que la administración debe ir uno o dos pasos adelante para evitar que éstos se presenten.

4- Precisamente, los sistemas monousuarios son mucho más fáciles de controlar pues se sabe con certeza quién es el usuario y se puede llevar una bitácora respecto al uso del sistema.

Pero, en un sistema multiusuario y de redes la afluencia de usuarios es mucho mayor. Hay muchas aplicaciones puestas a disposición de las personas para su uso y ante tanta variedad se hace más difícil controlar lo que cada persona realiza. De allí, la importancia de mantener un especial cuidado en los sistemas multiusuario y en los niveles de acceso de cada uno de ellos.

Capítulo 6

1- Desarrollar una auditoría de sistemas computacionales requiere una serie ordenada de acciones y procedimientos específicos, los cuales deberán ser diseñados previamente de manera secuencial, cronológica y ordenada, de acuerdo con las etapas, los eventos y las actividades que se requieran para su ejecución, que serán establecidos conforme a las necesidades especiales de la institución.

Además, estos procedimientos se deben adaptar de acuerdo con el tipo de auditoría de sistemas que se vaya a realizar y con estricto apego a las necesidades, técnicas y métodos de evaluación del área de sistematización.

Con base en lo anterior, podemos entender la necesidad de establecer una metodología específica de revisión, la cual nos permitirá diseñar correctamente los pasos por seguir en la evaluación de las áreas de sistemas y actividades elegidas a fin de que el seguimiento desarrollo y la aplicación de las etapas y eventos propuestos para esa auditoría sean más sencillos.

Dicha metodología, también, nos servirá para establecer las técnicas, los métodos y los procedimientos adaptables a las características especiales de la auditoría del área específica de sistemas por evaluar incluyendo los recursos humanos, las técnicos y los materiales necesarios para dicha revisión.

2- Es inusual, porque, generalmente, las auditorías se solicitan por los niveles más altos. Es posible que para autorizar la realización de esta evaluación, tiene que ser analizada por los mandos medios o superiores de la empresa y si existe algún motivo real y válido que justifique su ejecución, entonces se desarrollará. De todas maneras, es importante averiguar los verdaderos motivos de esta solicitud.

3- Los riesgos lógicos en los sistemas son frecuentes. Nadie garantiza que el desarrollador haya tomado en cuenta todos los aspectos de seguridad y restricción para que los sistemas funcionen adecuadamente. Tampoco se

puede garantizar que a la hora de realizar las pruebas antes de poner el sistema en producción, se hayan abarcado todas las posibles situaciones y que las restricciones de entrada de datos filtren cualquier dato erróneo.

Si entra un dato no correcto, se espera que el resultado no sea el correcto. Pero, aún entrando un dato correcto, no siempre es posible garantizar en un cien por ciento que la salida esté correcta.

Únicamente, con la ejecución del programa se podrán ir corrigiendo aquellos factores que pudieran haberse quedado por fuera en la etapa de pruebas. Ocurre, con frecuencia, que los programas no están preparados para recibir datos que hayan sido cambiados por nuevas políticas de la compañía.

4- El equipo humano, es decir, funcionarios especializados en el área y con vasta experiencia y en cantidad adecuada. Además, son fundamentales los recursos informáticos y tecnológicos de acuerdo con el tipo de trabajo que se realice, accesos a los sistemas de cómputos, a los datos, a los programas, uso de paquetes especializados para extracción y análisis de datos, entre otros.

También, recursos materiales tales como papelería y, en caso de ser auditoría externa, con mobiliario adecuado y con seguridad donde se puedan salvaguardar los registros y papelería que serviría como evidencia. Otros recursos son viáticos, transporte, tiempo y otros.

Capítulo 7

1- En este tipo de auditorías, los llamados papeles de trabajo adquieren un matiz especial debido a la forma en que se archiva la información en ellos; así encontramos que debemos documentar datos que muchas veces no están archivados en papel sino en sistemas computacionales; por lo tanto, debemos saber cómo capturar, extraer y archivar esa información en algún medio electromagnético de captura y lectura de información.

2- Son las marcas de carácter informal que utiliza, exclusivamente, el auditor o el grupo de auditores que realizan la auditoría con el fin de facilitar la uniformidad de los papeles de trabajo y para identificarlos mejor. El auditor en jefe puede imponer el uso de estos símbolos o pueden ser utilizados por acuerdo del grupo, aunque puede suceder que no sean utilizados en una auditoría.

Cuando alguien del grupo de auditores se encuentra algún documento con estas marcas, sabe que éste ya ha sido revisado o que tiene una característica especial en la cual se tiene que advertir alguna observación de acuerdo con el significado de los símbolos.

Capítulo 8

1- El informe es el documento más importante de la auditoría de sistemas computacionales debido que, a través de éste, se presentan los resultados de la evaluación.

   En él se plasman, por escrito, las observaciones y el dictamen que emite el auditor quien, de acuerdo con su experiencia, conocimientos e información recopilada, evalúa el comportamiento del sistema, la actuación y el cumplimiento de su gestión informática, la realización correcta de sus objetivos, el cumplimiento de sus funciones, actividades y operaciones o cualquier otro aspecto de sistemas computacionales.

   De este informe se emanan, generalmente, una serie de observaciones y recomendaciones, que deberán ser puestas por la administración para el mejor funcionamiento del área y para minimizar los riesgos.

2- La oportunidad consiste precisamente en presentar a tiempo las desviaciones que fueron observadas, a fin de corregirlas de inmediato y de tomar las medidas necesarias para su solución.

   La esencia de la auditoría de sistemas es reportar lo que se observa durante una evaluación a fin de que los directivos sepan cómo está funcionando la operación de los sistemas y cómo se están utilizando los recursos asignados a esa área.

   Pero dicho informe deber ser hecho a tiempo y formalmente de tal manera que, al conocer las desviaciones observadas por el auditor, los directivos puedan tomar las medias pertinentes y evitar que se presenten a futuro.

3. La imparcialidad es uno de los requisitos más importantes que se le exigen al auditor. Incluye conceptos como integridad y profesionalismo en la elaboración de un informe anotando las observancias y cómo las encontró durante su evaluación, es decir, que reporte con ecuanimidad la situaciones que informa, que no tome partido ni para perjudicar enfatizando la gravedad de las desviaciones ni para solapar ni minimizar los errores encontrados durante su evaluación.

   La objetividad es el entendimiento de las cosas, ideas y valores por sí mismos y no por lo que se piensa, razona o interpreta. En el caso del informe de auditoría de sistemas es la descripción apegada a la realidad. En este caso, de lo que se comprueba por medio de la evaluación con el propósito de redactar las observaciones tal y como se presentan, se describen los resultados de la auditoría lo más naturalmente posible.

   La aplicación de estos dos elementos manifiestan la honestidad del auditor en cuando a las razones por las cuales realizó la auditoría. Si el auditor ha sido influenciado y prejuiciado, por terceras personas o por diferencias personales con el auditado, es posible que pierda la objetividad y la imparcialidad, en cuyo caso está atenta contra la ética y la moral.

Capítulo 9

1- **Ventajas**

- Facilitan la recopilación de información y no se necesitan muchas explicaciones ni una gran preparación para aplicarlos.

- Por su diseño, los cuestionarios son rápidos de aplicar y ayudan a captar mucha información en poco tiempo.

- Confieren un carácter de impersonalidad con la aportación de respuestas; por la tanto, en una auditoría ayudan a obtener información útil y confiable, si se plantean bien las preguntas.

Desventajas

- Falta de profundidad en las respuestas y no se puede trascender más allá del cuestionario.

- Limitan la participación del auditado, porque éste puede evadir preguntas clave o se puede escudar en el anonimato de los cuestionarios.

- La participación del personal auditado es impersonal, por lo que el aporte de la información útil para la auditoría se limita.

2- En la auditoría de sistemas, el método de recopilación de información facilita una evaluación adecuada de la gestión administrativa del área de sistemas, así como el aprovechamiento, la custodia y el control de los bienes informáticos en dicha área. Con este método, se pretende conocer la totalidad de los bienes informáticos en materia de software, hardware, documentación, personal y datos.

3- La aplicación correcta de los métodos y los procedimientos estadísticos ayuda a seleccionar una parte representativa del universo que se tiene que revisar. El propósito es obtener la misma información o parecida a la que se obtendría al revisar todo el universo.

De esta manera, el auditor puede apreciar el comportamiento global de todo el universo y con ellos puede contar con los elementos de juicio necesarios para emitir un dictamen apegado a la veracidad de los hechos auditados.

Capítulo 10

1- Son las comprobaciones previas a la implantación de un sistema computacional con el fin de verificar si el diseño del nuevo sistema corresponde al comportamiento real de dicho sistema. Estas comprobaciones se realizan a través del procesamiento de datos (supuestos y verdaderos) comparando los resultados que ofrecen las pruebas del nuevo sistema con los resultados reales que se obtuvieron por cualquier otro medio.

2- El funcionamiento de las instalaciones de un centro de cómputo, de sus comunicaciones, sus sistemas eléctricos, sus conexiones entre componentes, sus sistemas de aire acondicionado, las medidas de prevención para evitar y combatir incendios, inundaciones y demás riesgos internos o externos, así como de los sistemas de seguridad y planes de contingencias y, en sí, de todos los aspectos que repercuten en el funcionamiento del área de sistemas de la empresa.

3- Es un documento de carácter formal, que por su representatividad, importancia y posibles alcances legales y jurídicos, es uno de los documentos vitales para cualquier auditoría. Este documento no sólo sirve de testimonio para comprobar, corroborar, ratificar o evidenciar cualquier evento que ocurra durante la revisión, sino que es tal su alcance que se puede convertir en un documento legal, probatorio de alguna anomalía de tipo jurídico, penal o de cualquier otro aspecto legal.

Capítulo 11

1- Esta herramienta es una de las más utilizadas para el análisis y diseño de sistemas. También puede ser de utilidad para la auditoría de sistemas computacionales, porque mediante el uso de un modelo, conceptual o físico se simula el comportamiento de un sistema computacional, de un programa, de una base de datos, de una operación, de una actividad o de cualquier tarea de sistemas que tenga que ser revisada con el propósito de investigar cuál es, fue o será el comportamiento del fenómeno de sistemas en estudio bajo ciertas condiciones y características concretas en las que se presentan todas las simulaciones necesarias que se asemejen al ambiente real en donde actúa dicho fenómeno para valorar su auténtico aprovechamiento, sus eficiencias y deficiencias de funcionamiento y sus principales problemas, entre otros.

2- Los permanentes cambios tecnológicos exigen evaluar constantemente las adquisiciones de nuevos sistemas no sólo en cuanto al software, sino en lo relativo al hardware, los equipos periféricos y todos los componentes de sistemas de una empresa. Incluso, en la capacitación de los usuarios, se deben verificar que los cambios de la tecnología computacional sean conforme a las necesidades reales de las áreas de las empresas.

   Por eso, el auditor de sistemas computacionales debe evaluar los aspectos relacionados con la adquisición de nuevos productos informáticos, así como a los proveedores y distribuidores que los proporcionan a fin de garantizar las adquisiciones más adecuadas al menor costo y con la más alta calidad y servicio para las necesidades de cómputo de la empresa.

3- Consiste en la elaboración de una lista ordenada en la cual se anotan todos los aspectos que se tienen que revisar del funcionamiento de un sistema, sus componentes, del desarrollo de una actividad, del cumplimiento de una operación o de cualquier otro aspecto relacionado con la evaluación del área de sistemas. Esta lista se complementa con una o varias columnas en las que se califica el cumplimiento del aspecto evaluado.

4- El auditor identifica los aspectos de los sistemas de la gestión administrativa o de las bases de datos que debe revisar en el área de sistemas y establece, en forma anticipada, uno a uno los asuntos concretos que revisará mediante el apoyo de un sistema computacional. Posteriormente, debe desarrollar una aplicación que cumpla con el objetivo establecido.

Es frecuente que el auditor de sistemas desconozca el uso del lenguaje o programas de desarrollo, que se utilizan en el sistema computacional de la empresa, por lo que tendrá que recurrir a los servicios de un programador de acuerdo con las características y estándares de programación, seguirá las instrucciones determinadas por el auditor y el diseño del programa del auditor.

Así, realizará la codificación de instrucciones, elaborará las pruebas correspondientes y liberará el programa de cómputo para que el auditor lo aplique en su revisión.

Sería ideal que el mismo auditor sea quien desarrolle su propia aplicación, pero según las circunstancias mencionadas anteriormente, no es un requisito indispensable para usar esta técnica si puede recurrir a los servicios de un programador de sistemas.

Capítulo 12

1-

- Auditoría a la planeación estratégica en la empresa y el área de sistemas.
- Auditoría a la estructura de organización del área de sistemas.
- Auditoría al cumplimiento de las funciones, tareas y operaciones de la actividad informática en la empresa y el área de sistemas.
- Auditoría a la administración del factor humano en el área de sistemas.

2- Los objetivos de una red de cómputo.
- Las características de la red de cómputo.
- Los componentes físicos de una red de cómputo.
- La conectividad y las comunicaciones de una red de cómputo.
- Los servicios que proporciona una red de cómputo.
- Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.
- Los protocolos de comunicación interna de la red.
- La administración de una red de cómputo.
- La seguridad de las redes de cómputo.

3- La auditoría a los servicios *outsourcing* es aquella en el cual se auditan las actividades, las funciones y las operaciones del prestador de servicios en cuanto a la administración de sus recurso informáticos, la confiabilidad, la oportunidad y la eficiencia con las que trata la información de las

organizaciones, los resultados del procesamiento de datos y la eficiencia y eficacia de los servicios.

Respecto al servicio, el auditor debe evaluar todos los aspectos relativos a la calidad, la rapidez y la confiabilidad con que se proporciona este servicio a los usuarios, evaluación del soporte técnico, la asistencia y capacitación a los usuarios, así como el mantenimiento de los sistemas y detección de incidencias de problemáticas para la solución a los reportes de los usuarios.