REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD NACIONAL EXPERIMENTAL POLITÉCNICA
" ANTONIO JOSE DE SUCRE "
VICE-RECTORADO PUERTO ORDAZ
DIRECCIÓN DE INVESTIGACIÓN Y POSTGRADO
MAESTRÍA EN INGENIERÍA INDUSTRIAL
CURSO DE NIVELACIÓN: SISTEMAS DE INFORMACIÓN

AUDITORÍA DE SISTEMAS

Autores:
Ing. Henry López
Ing. Yusvelin Herrera
Ing. Milagro García

Facilitador: MSc. Ing. Iván Turmero

Puerto Ordaz, 10 de Junio del 2008

ÍNDICE

INTRODUCCIÓN 3
AUDITORIA 5
Evolución de la auditoria 5
Definición de auditoria 6
Objetivo de la auditoria 6
Finalidad de la auditoria 6
Clasificación de la auditoria 6
Auditoria externa 6
Auditoria interna 7
AUDITORIA ADMINISTRATIVA 7
Evolución de la auditoria administrativa 7
Objetivos de la auditoria administrativa 10
EL AUDITOR 10
Funciones generales del auditor: 11
AUDITORIA DE SISTEMAS 12
Objetivos generales de una auditoria de sistemas 12
Objetivos específicos de la auditoria de sistemas: 13
Fines de la auditoria de sistemas: 14
Tipos de auditoria 14
Justificativos para efectuar una auditoria de sistemas 15
Pasos a seguir para implementar auditoría en un sistema de información 15
Estándares de auditoria informática y de seguridad 16
Aspectos del medio ambiente informático que afectan el enfoque de la auditoria y sus procedimientos. 16
Requerimientos del auditor de sistemas 17
RIESGO INFORMÁTICO 17
Modelo de Riesgo 17
Tipología de Riesgos en Entornos Informáticos 17
CONTROLES INFORMÁTICOS 18
Clasificación general de los controles 18
Controles preventivos 18
Controles detectivos 18
Controles correctivos 18
Principales controles físicos y lógicos 19
Autenticidad 19
Exactitud 19

Totalidad 19
Redundancia 19
Privacidad 19
Existencia 20
Protección de Activos 20
Efectividad 20
Eficiencia 20
Controles automáticos o lógicos 20
Periodicidad de cambio de claves de acceso 20
Combinación de alfanuméricos en claves de acceso 21
Individuales 21
Confidenciales 21
No significativas 21
Verificación de datos de entrada 21
Conteo de registros 21
Totales de Control 21
Verificación de límites 21
Verificación de secuencias 22
Dígito autoerificador 22
Utilizar software de seguridad en los microcomputadores 22
Controles administrativos en un ambiente de procesamiento de datos 22
Controles de preinstalación 22
Controles de organización y planificación 23
Controles de sistema en desarrollo y producción 24
Controles de procesamiento 25
Controles de operación 26
Controles en el uso del microcomputador 27
Metodología de una auditoría de sistemas: 28
Normas generales para los sistemas de auditoría de la información. 29
Ejemplos en la aplicación de auditoria de sistema 32
Informativos sobre auditoria de sistemas 33
Las compañías españolas se preocupan por la auditoría de sistemas de información. 33
Servicios de auditoría de tecnologías de la información 35
Certificación oficial como Auditor de Sistemas de Información 35
La Auditoría Interna en CVG: 37
Normas Generales 37
CONCLUSIÓN 42
BIBLIOGRAFÍA 43

INTRODUCCIÓN

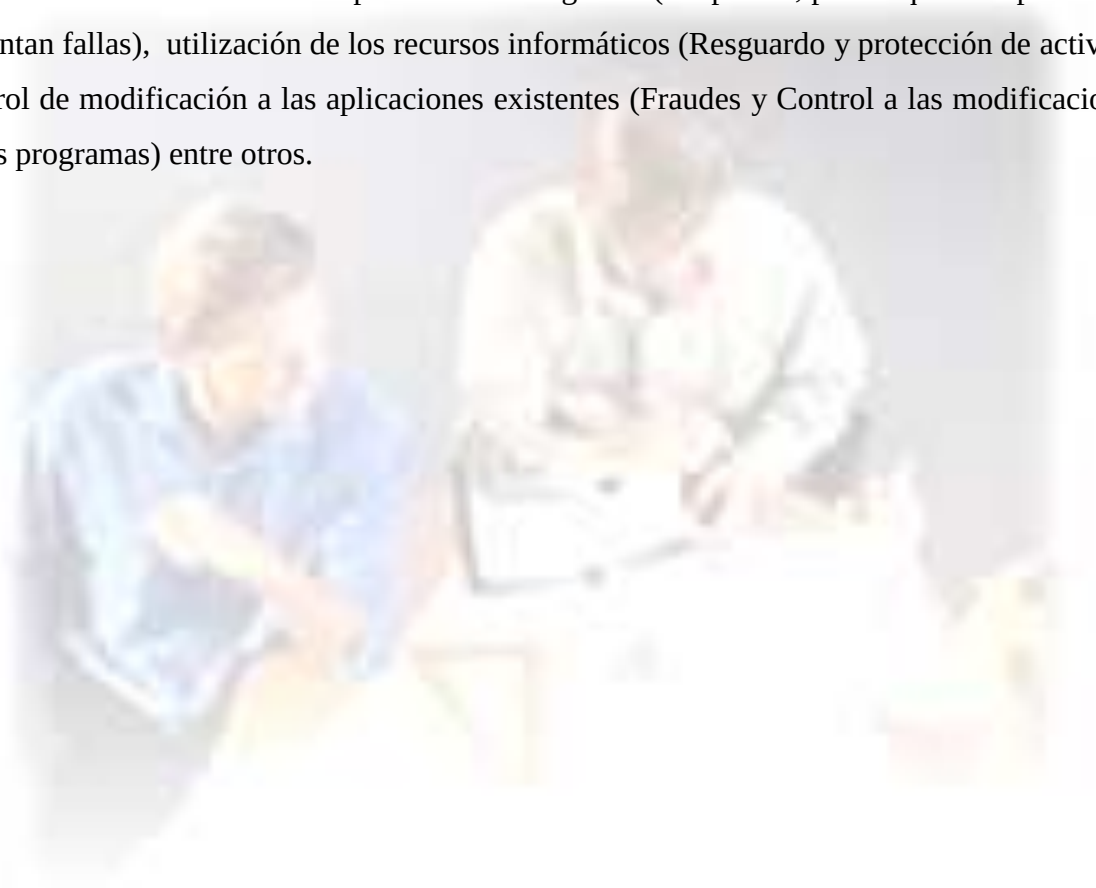
A finales del siglo XX, los Sistemas Informáticos se convirtieron en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial como son los sistemas de información de una empresa.

La evolución tecnológica hoy en día, está subsumida en la gestión integral de la empresa y por eso las normas y estándares propiamente informáticos deben estar presentes en ella. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la tecnología no gestiona propiamente la empresa, sino que ayuda a la toma de decisiones, pero no decide por sí misma, sin embargo, actúa como un apoyo dentro de la organización, debido a que a través de una auditoria se monitorea el cumplimiento de los procesos y por ende las normas y procedimientos, en los cuales se basa cada proceso, bien sea administrativo, financiero o de sistema. Permitiendo así cotejar una información veraz, pues esta basada en el resultado del cumplimiento de ciertas normas establecidas dentro de la empresa. Es por eso, que debido a su importancia en el funcionamiento correcto de los procesos dentro de una empresa, existe lo que conocemos hoy en día, como Auditoria de sistemas, basado en el uso de la tecnología informática, para hacer más efectiva y rápida la información.

Las empresas dependen, cada día más, de las computadoras en el logro de sus objetivos y estrategias de negocio. La competencia y el cambio siguen afectando a las empresas y aunque el uso de las Tecnologías de Información les provee competencia, su evolución obliga a su cambio constante para que las empresas mantengan la ventaja competitiva de los avances tecnológicos en el manejo del negocio.

Es por eso, que muchas empresas deben tener como prioridad la auditoría y seguridad informática. Por tratarse de "algo que no se ve a simple vista", las empresas hoy en día destinan presupuesto para mantener niveles mínimos de seguridad en sus instalaciones informáticas. Ya que es mejor invertir a tiempo que hacer "algo" sólo cuándo tienen el problema encima y se deben entregar resultados inmediatos; ya que de lo contrario, cuando se den cuenta que "algo" no funcionó o funcionó mal y no lo previnieron, se les viene encima muchos problemas. No se puede esperar actuar cuando se dan cuenta que alguien violó sus

instalaciones y con ello la confidencialidad de su información por no cumplir con los parámetros mínimos de seguridad e integridad. Debido a que no previnieron el hecho, que en ocasiones puede ser tan lamentable al resultar dañada su imagen y su información, ya que se verían afectadas en algunos de los puntos importantes como: Evaluación de controles, Cumplimiento de la metodología., Evaluación de la seguridad en el área informática, Evaluación de suficiencia en los planes de contingencia (Respaldos, prever qué va a pasar si se presentan fallas), utilización de los recursos informáticos (Resguardo y protección de activos), Control de modificación a las aplicaciones existentes (Fraudes y Control a las modificaciones de los programas) entre otros.



AUDITORIA

Evolución de la auditoria

La auditoria es una de las aplicaciones de los principios científicos de la contabilidad, basada en la verificación de los registros patrimoniales de las haciendas, para observar su exactitud; no obstante, este no es su único objetivo.

Su importancia es reconocida desde los tiempos más remotos, teniéndose conocimientos de su existencia ya en las lejanas épocas de la civilización sumeria.

Acreditase, todavía, que el termino auditor evidenciando el titulo del que practica esta técnica, apareció a finales del siglo XVIII, en Inglaterra durante el reinado de Eduardo I.

En diversos países de Europa, durante la edad media, muchas eran las asociaciones profesionales, que se encargaban de ejecuta funciones de auditorias, destacándose entre ellas los consejos Londineses (Inglaterra), en 1.310, el Colegio de Contadores, de Venecia (Italia), 1.581.

La revolución industrial llevada a cabo en la segunda mitad del siglo XVIII, imprimió nuevas direcciones a las técnicas contables, especialmente a la auditoria, pasando a atender las necesidades creadas por la aparición de las grandes empresas (donde la naturaleza es el servicio es prácticamente obligatorio).

Se preanuncio en 1.845 o sea, poco después de penetrar la contabilidad de los dominios científicos y ya el "Railway Companies Consolidation Act" obligada la verificación anual de los balances que debían hacer los auditores.

También en los Estados Unidos de Norteamérica, una importante asociación cuida las normas de auditoria, la cual publicó diversos reglamentos, de los cuales el primero que conocemos data de octubre de 1.939, en tanto otros consolidaron las diversas normas en diciembre de 1.939, marzo de 1.941, junio de 1942 y diciembre de 1.943.

El futuro de nuestro país se prevé para la profesión contable en el sector auditoria es realmente muy grande, razón por la cual deben crearse, en nuestro circulo de enseñanza cátedra para el estudio de la materia, incentivando el aprendizaje y asimismo organizarse cursos similares a los que en otros países se realizan.

Definición de auditoria

Holmes escribe la auditoria como:

"... El examen de las demostraciones y registros administrativos. El auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos."

Objetivo de la auditoria

El objetivo de la Auditoria consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades. Para ello la Auditoria les proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

Finalidad de la auditoria

Los fines de la auditoria son los aspectos bajo los cuales su objeto es observado. Podemos señalar los siguientes:

1. Indagaciones y determinaciones sobre el estado patrimonial.
2. Indagaciones y determinaciones sobre los estados financieros.
3. Indagaciones y determinaciones sobre el estado reditual.
4. Descubrir errores y fraudes.
5. Prevenir los errores y fraudes.
6. Estudios generales sobre casos especiales, tales como:
    a. Exámenes de aspectos fiscales y legales.
    b. Examen para compra de una empresa(cesión patrimonial).
    c. Examen para la determinación de bases de criterios de prorrateo, entre otros.

Clasificación de la auditoria

Auditoria externa

Es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un Contador Público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento.

Auditoria interna

Es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la misma. Estos informes son de circulación interna y no tienen trascendencia a los terceros pues no se producen bajo la figura de la Fe Publica.

AUDITORIA ADMINISTRATIVA

Evolución de la auditoria administrativa

Con el propósito de ubicar como se ha ido enriqueciendo a través del tiempo, es conveniente revisar las contribuciones de los autores que han incidido de manera más significativa a lo largo de la historia de la administración.

En el año de 1935, James O. McKinsey, en el seno de la American Economic Association sentó las bases para lo que él llamó "auditoria administrativa", la cual, en sus palabras, consistía en "una evaluación de una empresa en todos sus aspectos, a la luz de su ambiente presente y futuro probable."

Más adelante, en 1953, George R. Terry, en Principios de Administración, señala que "La confrontación periódica de la planeación, organización, ejecución y control administrativos de una compañía, con lo que podría llamar el prototipo de una operación de éxito, es el significado esencial de la auditoría administrativa."

Dos años después, en 1955, Harold Koontz y Ciryl O´Donnell, también en sus Principios de Administración, proponen a la auto-auditoría, como una técnica de control del desempeño total, la cual estaría destinada a "evaluar la posición de la empresa para determinar dónde se encuentra, hacia dónde va con los programas presentes, cuáles deberían ser sus objetivos y si se necesitan planes revisados para alcanzar estos objetivos."

El interés por esta técnica llevan en 1958 a Alfred Klein y Nathan Grabinsky a preparar El Análisis Factorial, obra en cual abordan el estudio de "las causas de una baja productividad para establecer las bases para mejorarla" a través de un método que identifica y cuantifica los factores y funciones que intervienen en la operación de una organización.

Transcurrido un año, en 1959, ocurren dos hechos relevantes que contribuyen a la evolución de la auditoría administrativa: 1) Víctor Lazzaro publica su libro de Sistemas y Procedimientos, en el cual presenta la contribución de William P. Leonard con el nombre de auditoría administrativa y, 2) The American Institute of Management, en el Manual of Excellence Managements integra un método para auditar empresas con y sin fines de lucro, tomando en cuenta su función, estructura, crecimiento, políticas financieras, eficiencia operativa y evaluación administrativa.

El atractivo por el tema se extiende al ámbito académico y, en 1960, Alfonso Mejía Fernández, de la Escuela Nacional de Comercio y Administración de la Universidad Nacional Autónoma de México, en su tesis profesional La Auditoria de las Funciones de la Gerencia de las Empresas, realiza un recuento de los aspectos estructurales y funcionales que el nivel gerencial de las empresas debe contemplar para aplicar una auditoria administrativa.

Para 1962, Roberto Macías Pineda, de la Escuela Superior de Comercio y Administración del Instituto Politécnico Nacional, dentro del programa de doctorado en ciencias administrativas, en la asignatura Teoría de la Administración, destina un espacio para presentar un trabajo de auditoría administrativa.

Por otra parte, en 1964, Manuel D´Azaola S., de la Escuela Nacional de Comercio y Administración de la Universidad Nacional Autónoma de México, en su tesis profesional La Revisión del Proceso Administrativo, considera la necesidad de que las empresas analicen su comportamiento a partir de la revisión de las funciones de dirección, financiamiento, personal, producción, ventas y distribución, así como registro contable y estadístico.

A finales de 1965, Edward F. Norbeck da a conocer su libro Auditoria Administrativa, en donde define el concepto, contenido e instrumentos para aplicar la auditoria. Asimismo, precisa las diferencias entre la auditoría administrativa y la auditoria financiera, y desarrolla los criterios para la integración del equipo de auditores en sus diferentes modalidades.

En 1966, José Antonio Fernández Arena, presenta la primera versión de su texto “La Auditoria Administrativa”, en la cual desarrolla un marco comparativo entre diferentes enfoques de la auditoría administrativa, presentando una propuesta a partir de su propia visión de la técnica.

Más adelante, en 1971, se generan dos nuevas contribuciones: Agustín Reyes Ponce, en Administración de Personal, dedica un apartado para tratar el tema, ofreciendo una visión

general de la auditoría administrativa, en tanto que William P. Leonard publica Auditoria Administrativa: Evaluación de los Métodos y Eficiencia Administrativos, en donde incorpora los conceptos fundamentales y programas para la ejecución de la auditoría administrativa.

Para 1977, se suman las aportaciones de dos autores en la materia. Patricia Diez de Bonilla en su Manual de Casos Prácticos sobre Auditoria Administrativa, propone aplicaciones viables de llevar a la práctica y, Jorge Álvarez Anguiano, en Apuntes de Auditoria Administrativa incluye un marco metodológico que permite entender la auditoría administrativa de manera por demás accesible.

En 1978, la Asociación Nacional de Licenciados en Administración, difunde el documento Auditoria Administrativa, el cual reúne las normas para su implementación en organizaciones públicas y privadas.

Poco después, en 1984, Robert J. Thierauf presenta Auditoria Administrativa con Cuestionarios de Trabajo, trabajo que introduce a la auditoria administrativa y a la forma de aplicarla sobre una base de preguntas para evaluar las áreas funcionales, ambiente de trabajo y sistemas de información.

En 1988, la oficina de la Contraloría General de los Estados Unidos de Norteamérica prepara las Normas de Auditoría Gubernamental, que son revisadas por la Contraloría Mayor de Hacienda (entidad de la Secretaría de Hacienda y Crédito Público), las cuales contienen los lineamientos generales para la ejecución de auditorias en las oficinas públicas.

Al iniciarse la década de los noventa, la Secretaría de la Contraloría General de la Federación se dio a la tarea de preparar y difundir normas, lineamientos, programas y marcos de actuación para las instituciones, trabajo que, en su situación actual, como Secretaría de Contraloría y Desarrollo Administrativo, continúa ampliando y enriqueciendo.

Según Williams P. Leonard la auditoria administrativa se define como:

"Un examen completo y constructivo de la estructura organizativa de la empresa, institución o departamento gubernamental; o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que de a sus recursos humanos y materiales".

Objetivos de la auditoria administrativa

Entre los objetivos prioritarios para instrumentarla de manera consistente tenemos los siguientes:

De control.- Destinados a orientar los esfuerzos en su aplicación y poder evaluar el comportamiento organizacional en relación con estándares preestablecidos.

De productividad.- Encauzan las acciones para optimizar el aprovechamiento de los recursos de acuerdo con la dinámica administrativa instituida por la organización.

De organización.- Determinan que su curso apoye la definición de la estructura, competencia, funciones y procesos a través del manejo efectivo de la delegación de autoridad y el trabajo en equipo.

De servicio.- Representan la manera en que se puede constatar que la organización está inmersa en un proceso que la vincula cuantitativa y cualitativamente con las expectativas y satisfacción de sus clientes.

De calidad.- Disponen que tienda a elevar los niveles de actuación de la organización en todos sus contenidos y ámbitos, para que produzca bienes y servicios altamente competitivos.

De cambio.- La transforman en un instrumento que hace más permeable y receptiva a la organización.

De aprendizaje.- Permiten que se transforme en un mecanismo de aprendizaje institucional para que la organización pueda asimilar sus experiencias y las capitalice para convertirlas en oportunidades de mejora.

De toma de decisiones.- Traducen su puesta en práctica y resultados en un sólido instrumento de soporte al proceso de gestión de la organización.

EL AUDITOR

Es aquella persona profesional, que se dedica a trabajos de auditoria habitualmente con libre ejercicio de una ocupación técnica.

Funciones generales del auditor:

Para ordenar e imprimir cohesión a su labor, el auditor cuenta con un una serie de funciones tendientes a estudiar, analizar y diagnosticar la estructura y funcionamiento general de una organización.

Las funciones tipo del auditor son:

- Estudiar la normatividad, misión, objetivos, políticas, estrategias, planes y programas de trabajo.
- Desarrollar el programa de trabajo de una auditoria.
- Definir los objetivos, alcance y metodología para instrumentar una auditoria.
- Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones y sistemas utilizados.
- Recabar y revisar estadísticas sobre volúmenes y cargas de trabajo.
- Diagnosticar sobre los métodos de operación y los sistemas de información.
- Detectar los hallazgos y evidencias e incorporarlos a los papeles de trabajo.
- Respetar las normas de actuación dictadas por los grupos de filiación, corporativos, sectoriales e instancias normativas y, en su caso, globalizadoras.
- Proponer los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización
- Analizar la estructura y funcionamiento de la organización en todos sus ámbitos y niveles
- Revisar el flujo de datos y formas.
- Considerar las variables ambientales y económicas que inciden en el funcionamiento de la organización.
- Analizar la distribución del espacio y el empleo de equipos de oficina.
- Evaluar los registros contables e información financiera.
- Mantener el nivel de actuación a través de una interacción y revisión continua de avances.
- Proponer los elementos de tecnología de punta requeridos para impulsar el cambio organizacional.
- Diseñar y preparar los reportes de avance e informes de una auditoria.

AUDITORIA DE SISTEMAS

La palabra auditoria viene del latín *auditorius* y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

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

La auditoria en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoria en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

Objetivos generales de una auditoria de sistemas

- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados por el PAD
- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones
- Apoyo de función informática a las metas y objetivos de la organización
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático

- Minimizar existencias de riesgos en el uso de Tecnología de información
- Decisiones de inversión y gastos innecesarios
- Capacitación y educación sobre controles en los Sistemas de Información

Objetivos específicos de la auditoria de sistemas:

1. Participación en el desarrollo de nuevos sistemas:
    a. Evaluación de controles
    b. Cumplimiento de la metodología.
2. Evaluación de la seguridad en el área informática.
3. Evaluación de suficiencia en los planes de contingencia.
    a. Respaldos, prever qué va a pasar si se presentan fallas.
4. Opinión de la utilización de los recursos informáticos.
    a. Resguardo y protección de activos.
5. Control de modificación a las aplicaciones existentes.
    a. Fraudes
    b. Control a las modificaciones de los programas.
6. Participación en la negociación de contratos con los proveedores.
7. Revisión de la utilización del sistema operativo y los programas
    a. Utilitarios.
    b. Control sobre la utilización de los sistemas operativos
    c. Programas utilitarios.
8. Auditoría de la base de datos.
    a. Estructura sobre la cual se desarrollan las aplicaciones.
9. Auditoría de la red de teleprocesos.
10. Desarrollo de software de auditoría.

Es el objetivo final de una auditoria de sistemas bien implementada, desarrollar software capaz de estar ejerciendo un control continuo de las operaciones del área de procesamiento de datos.

Fines de la auditoria de sistemas:

1. Fundamentar la opinión del auditor interno (externo) sobre la confiabilidad de los sistemas de información.
2. Expresar la opinión sobre la eficiencia de las operaciones en el área de TI.

Tipos de auditoria

La auditoria se clasifica en Auditoria Financiera y Operativa. Los servicios de auditoría pueden ser de distinta índole:

Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno

Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores

Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.

Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.

Auditoria de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.

Auditoria de código de aplicaciones. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de los softwares y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Justificativos para efectuar una auditoria de sistemas

- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos).
- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados con el computador.
- Falta de una planificación informática.
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano.
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.
- Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción.

Pasos a seguir para implementar auditoría en un sistema de información

Se requieren varios pasos para realizar una auditoria. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoria que consta de objetivos de control y procedimientos de auditoria que deben satisfacer esos objetivos. El proceso de

auditoria exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoria que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia de auditoria debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoria además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

Estándares de auditoria informática y de seguridad

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas practicas sugeridas. Existen estándares orientados a servir como base para auditorias de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoria apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoria y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

Aspectos del medio ambiente informático que afectan el enfoque de la auditoria y sus procedimientos.

- Complejidad de los sistemas.
- Uso de lenguajes.
- Metodologías, son parte de las personas y su experiencia.
- Centralización.
- Departamento de sistemas que coordina y centraliza todas las operaciones relaciones los usuarios son altamente dependientes del área de sistemas.
- Controles del computador.

Requerimientos del auditor de sistemas

1. Entendimiento global e integral del negocio, de sus puntos claves, áreas críticas, entorno económico, social y político.
2. Entendimiento del efecto de los sistemas en la organización.
3. Entendimiento de los objetivos de la auditoría.
4. Conocimiento de los recursos de computación de la empresa.
5. Conocimiento de los proyectos de sistemas.

RIESGO INFORMÁTICO

Podemos definir el riesgo informático como la probabilidad de que se dé un error, falle un proceso, o tenga lugar un hecho negativo para la empresa u organización, incluyendo la posibilidad de fraudes. El riesgo se puede evaluar mediante un modelo.

Modelo de Riesgo

Se puede establecer un modelo de riesgo informático como una función de los siguientes componentes:

- Activos
- Amenazas
- Impacto
- Vulnerabilidades

Estos componentes se pueden evaluar como factores del análisis del riesgo existente.

Tipología de Riesgos en Entornos Informáticos

Existen diferentes tipos de riesgos en entornos informáticos, los podríamos clasificar de la siguiente manera:

- Riesgos de fraude
- Riesgos de confidencialidad
- Riesgos de pérdida de imagen
- Riesgos de inexactitud de los datos

- Riesgos de integridad de la información
- Riesgos en la protección de activos
- Riesgos de incumplimiento de normas legales
- Riesgos en la eficiencia y eficacia de los procesos y
- Utilización de los recursos

Nos protegemos con dos elementos claves contra hechos fortuitos o potenciales que dañen a los sistemas de información y por consiguiente a la organización: los procedimientos de control y la auditoria.

CONTROLES INFORMÁTICOS

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Clasificación general de los controles

Controles preventivos

Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones; Sistemas de claves de acceso.

Controles detectivos

Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los mas importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Ejemplos: Archivos y procesos que sirvan como pistas de auditoría. Procedimientos de validación.

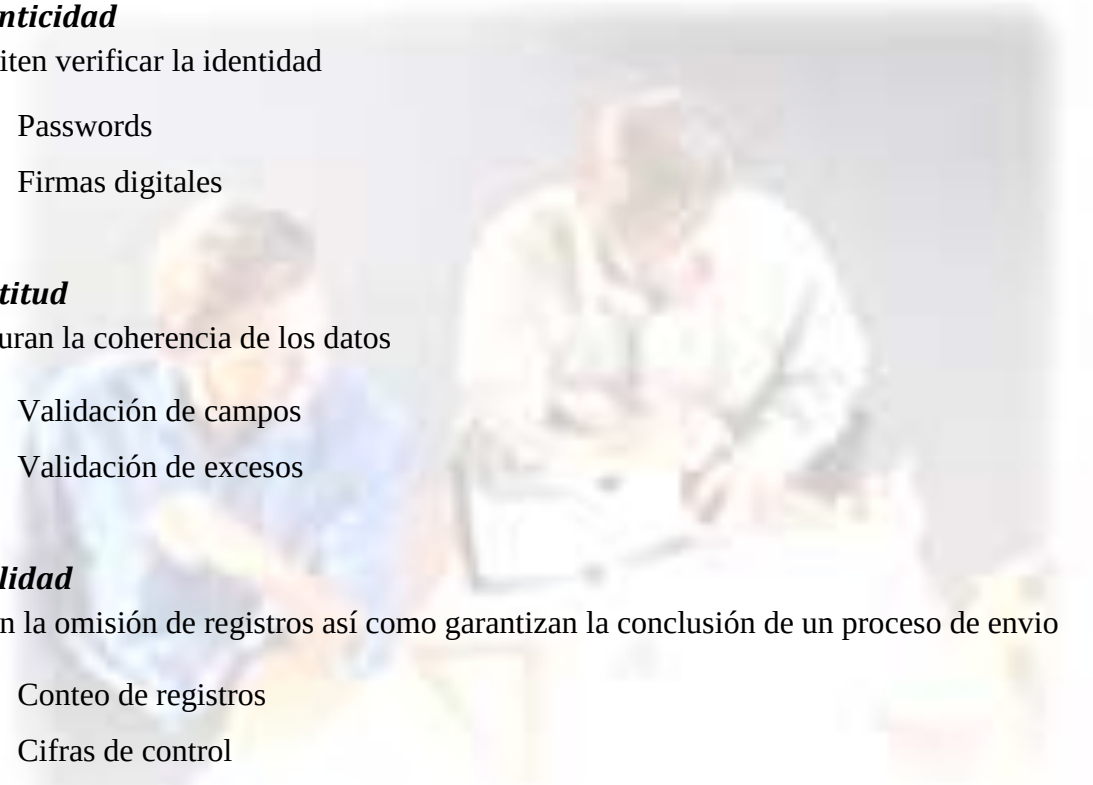
Controles correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los

controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Principales controles físicos y lógicos

Controles particulares tanto en la parte física como en la lógica se detallan a continuación:



Autenticidad

Permiten verificar la identidad

- Passwords
- Firmas digitales

Exactitud

Aseguran la coherencia de los datos

- Validación de campos
- Validación de excesos

Totalidad

Evitan la omisión de registros así como garantizan la conclusión de un proceso de envio

- Conteo de registros
- Cifras de control

Redundancia

Evitan la duplicidad de datos

- Cancelación de lotes
- Verificación de secuencias

Privacidad

Aseguran la protección de los datos

- Compactación
- Encriptación

Existencia
Aseguran la disponibilidad de los datos

- Bitácora de estados
- Mantenimiento de activos

Protección de Activos
Destrucción o corrupción de información o del hardware

- Extintores
- Passwords

Efectividad
Aseguran el logro de los objetivos

- Encuestas de satisfacción
- Medición de niveles de servicio

Eficiencia
Aseguran el uso óptimo de los recursos

- Programas monitores
- Análisis costo-beneficio

Controles automáticos o lógicos

Periodicidad de cambio de claves de acceso

Los cambios de las claves de acceso a los programas se deben realizar periódicamente. Normalmente los usuarios se acostumbran a conservar la misma clave que le asignaron inicialmente.

El no cambiar las claves periódicamente aumenta la posibilidad de que personas no autorizadas conozcan y utilicen claves de usuarios del sistema de computación.

Por lo tanto se recomienda cambiar claves por lo menos trimestralmente.

Combinación de alfanuméricos en claves de acceso

No es conveniente que la clave este compuesta por códigos de empleados, ya que una persona no autorizada a través de pruebas simples o de deducciones puede dar con dicha clave.

Para redefinir claves es necesario considerar los tipos de claves que existen:

Individuales

Pertenecen a un solo usuario, por tanto es individual y personal. Esta clave permite al momento de efectuar las transacciones registrar a los responsables de cualquier cambio.

Confidenciales

De forma confidencial los usuarios deberán ser instruidos formalmente respecto al uso de las claves.

No significativas

Las claves no deben corresponder a números secuenciales ni a nombres o fechas.

Verificación de datos de entrada

Incluir rutinas que verifiquen la compatibilidad de los datos mas no su exactitud o precisión; tal es el caso de la validación del tipo de datos que contienen los campos o verificar si se encuentran dentro de un rango.

Conteo de registros

Consiste en crear campos de memoria para ir acumulando cada registro que se ingresa y verificar con los totales ya registrados.

Totales de Control

Se realiza mediante la creación de totales de línea, columnas, cantidad de formularios, cifras de control, etc., y automáticamente verificar con un campo en el cual se van acumulando los registros, separando solo aquellos formularios o registros con diferencias.

Verificación de límites

Consiste en la verificación automática de tablas, códigos, límites mínimos y máximos o bajo determinadas condiciones dadas previamente.

Verificación de secuencias

En ciertos procesos los registros deben observar cierta secuencia numérica o alfabética, ascendente o descendente, esta verificación debe hacerse mediante rutinas independientes del programa en si.

Dígito autoerificador

Consiste en incluir un dígito adicional a una codificación, el mismo que es resultado de la aplicación de un algoritmo o formula, conocido como MODULOS, que detecta la corrección o no del código. Tal es el caso por ejemplo del decimo dígito de la cédula de identidad, calculado con el modulo 10 o el ultimo dígito del RUC calculado con el módulo 11.

Utilizar software de seguridad en los microcomputadores

El software de seguridad permite restringir el acceso al microcomputador, de tal modo que solo el personal autorizado pueda utilizarlo.

Adicionalmente, este software permite reforzar la segregación de funciones y la confidencialidad de la información mediante controles para que los usuarios puedan accesar solo a los programas y datos para los que están autorizados.

Programas de este tipo son: WachDog, Lattice, Secret Disk, entre otros.

Controles administrativos en un ambiente de procesamiento de datos

La máxima autoridad del Área de Informática de una empresa o institución debe implantar los siguientes controles que se agruparan de la siguiente forma:

1. Controles de Preinstalación
2. Controles de Organización y Planificación
3. Controles de Sistemas en Desarrollo y Producción
4. Controles de Procesamiento
5. Controles de Operación
6. Controles de uso de Microcomputadores

Controles de preinstalación

Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes.

Acciones a seguir del control preinstalación:

- Elaboración de un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio.
- Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación
- Elaborar un plan de instalación de equipo y software (fechas, actividades, responsables) el mismo que debe contar con la aprobación de los proveedores del equipo.
- Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales. Este proceso debe enmarcarse en normas y disposiciones legales.
- Efectuar las acciones necesarias para una mayor participación de proveedores.
- Asegurar respaldo de mantenimiento y asistencia técnica.

Controles de organización y planificación

Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades del área PAD, en labores tales como:

- Diseñar un sistema
- Elaborar los programas
- Operar el sistema
- Control de calidad

Se debe evitar que una misma persona tenga el control de toda una operación.

Es importante la utilización óptima de recursos en el PAD mediante la preparación de planes a ser evaluados continuamente.

Acciones a seguir en los controles de organización y planificación:

- La unidad informática debe estar al más alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.
- Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.

- Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.
- Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.
- El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
- Las actividades del PAD deben obedecer a planificaciones a corto, mediano y largo plazo sujetos a evaluación y ajustes periódicos "Plan Maestro de Informática".
- Debe existir una participación efectiva de directivos, usuarios y personal del PAD en la planificación y evaluación del cumplimiento del plan.
- Las instrucciones deben impartirse por escrito.

Controles de sistema en desarrollo y producción

Se debe justificar que los sistemas han sido la mejor opción para la empresa, bajo una relación costo-beneficio que proporcionen oportuna y efectiva información, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados.

Acciones a seguir en los controles de sistema en desarrollo y producción:

- Los usuarios deben participar en el diseño e implantación de los sistemas pues aportan conocimiento y experiencia de su área y esta actividad facilita el proceso de cambio.
- El personal de auditoría interna/control debe formar parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de control.
- El desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías estándares, procedimientos y en general a normatividad escrita y aprobada.
- Cada fase concluida debe ser aprobada documentadamente por los usuarios mediante actas u otros mecanismos a fin de evitar reclamos posteriores.
- Los programas antes de pasar a Producción deben ser probados con datos que agoten todas las excepciones posibles.
- Todos los sistemas deben estar debidamente documentados y actualizados. La documentación deberá contener:

    - Informe de factibilidad.
    - Diagrama de bloque.
    - Diagrama de lógica del programa.
    - Objetivos del programa.
    - Listado original del programa y versiones que incluyan los cambios efectuados con antecedentes de pedido y aprobación de modificaciones.
    - Formatos de salida.
    - Resultados de pruebas realizadas.
- Implantar procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.
- El sistema concluido será entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos.

Controles de procesamiento

Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información, lo que conlleva al establecimiento de una serie de seguridades para:

- Asegurar que todos los datos sean procesados.
- Garantizar la exactitud de los datos procesados.
- Garantizar que se grabe un archivo para uso de la gerencia y con fines de auditoría.
- Asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.

Acciones a seguir en los controles de procesamiento:

- Validación de datos de entrada previo procesamiento debe ser realizada en forma automática: clave, dígito autoverificador, totales de lotes, etc.
- Preparación de datos de entrada debe ser responsabilidad de usuarios y consecuentemente su corrección.
- Recepción de datos de entrada y distribución de información de salida debe obedecer a un horario elaborado en coordinación con el usuario, realizando un debido control de calidad.
- Adoptar acciones necesarias para correcciones de errores.

- Analizar conveniencia costo-beneficio de estandarización de formularios, fuente para agilitar la captura de datos y minimizar errores.
- Los procesos interactivos deben garantizar una adecuada interrelación entre usuario y sistema.
- Planificar el mantenimiento del hardware y software, tomando todas las seguridades para garantizar la integridad de la información y el buen servicio a usuarios.

Controles de operación

Abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento, la administración de la cintoteca y la operación de terminales y equipos de comunicación por parte de los usuarios de sistemas on-line.

Los controles tienen como fin:

- Prevenir o detectar errores accidentales que puedan ocurrir en el Centro de Cómputo durante un proceso.
- Evitar o detectar el manejo de datos con fines fraudulentos por parte de funcionarios del PAD.
- Garantizar la integridad de los recursos informáticos.
- Asegurar la utilización adecuada de equipos acorde a planes y objetivos.
- Recursos.
- Informáticos.

Acciones a seguir en los controles de operación:

- El acceso al centro de computo debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado
- Implantar claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado.
- Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y como responder ante esos eventos.
- Mantener un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.

- Los operadores del equipo central deben estar entrenados para recuperar o restaurar información en caso de destrucción de archivos.
- Los backups no deben ser menores de dos (padres e hijos) y deben guardarse en lugares seguros y adecuados, preferentemente en bóvedas de bancos.
- Se deben implantar calendarios de operación a fin de establecer prioridades de proceso.
- Todas las actividades del Centro de Computo deben normarse mediante manuales, instructivos, normas, reglamentos, etc.
- El proveedor de hardware y software deberá proporcionar lo siguiente:
    - Manual de operación de equipos.
    - Manual de lenguaje de programación.
    - Manual de utilitarios disponibles.
    - Manual de Sistemas operativos.
- Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras.
- Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía.
- Contratar pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación.

Controles en el uso del microcomputador

Es la tarea más difícil pues son equipos mas vulnerables, de fácil acceso, de fácil explotación pero los controles que se implanten ayudaran a garantizar la integridad y confidencialidad de la información.

Acciones a seguir en los controles en el uso del microcomputador:

- Adquisición de equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo.
- Vencida la garantía de mantenimiento del proveedor se debe contratar mantenimiento preventivo y correctivo.
- Establecer procedimientos para obtención de backups de paquetes y de archivos de datos.

- Revisión periódica y sorpresiva del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa.
- Mantener programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos.
- Propender a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y mantener actualizadas las versiones y la capacitación sobre modificaciones incluidas.
- Analizados los distintos tipos de controles que se aplican en la Auditoría de Sistemas efectuaremos a continuación el análisis de casos de situaciones hipotéticas planteadas como problemáticas en distintas empresas, con la finalidad de efectuar el análisis del caso e identificar las acciones que se deberían implementar.
- Análisis de Casos de Controles Administrativos.

Metodología de una auditoría de sistemas:

Existen algunas metodologías de Auditorías de Sistemas y todas dependen de lo que se pretenda revisar o analizar, pero como estándar analizaremos las cuatro fases básicas de un proceso de revisión:

- Estudio preliminar.
- Revisión y evaluación de controles y seguridades.
- Examen detallado de áreas criticas.
- Comunicación de resultados.

Estudio preliminar.- Incluye definir el grupo de trabajo, el programa de auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el control interno, solicitud de plan de actividades, Manuales de políticas, reglamentos, Entrevistas con los principales funcionarios del PAD.

Revisión y evaluación de controles y seguridades.- Consiste de la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de

aplicaciones de las áreas criticas, Revisión de procesos históricos (backups), Revisión de documentación y archivos, entre otras actividades.

Examen detallado de áreas criticas.-Con las fases anteriores el auditor descubre las áreas criticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance Recursos que usara, definirá la metodología de trabajo, la duración de la auditoría, Presentará el plan de trabajo y analizara detalladamente cada problema encontrado con todo lo anteriormente analizado en este folleto.

Comunicación de resultados.- Se elaborara el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentara esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la auditoria.

El informe debe contener lo siguiente:

- Motivos de la auditoria.
- Objetivos.
- Alcance.
- Estructura Orgánico-Funcional del área Informática.
- Configuración del Hardware y Software instalado.
- Control Interno.
- Resultados de la auditoria.
- Caso Práctico.

Normas generales para los sistemas de auditoría de la información.

> "Emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información".

010 Título de auditoría

010.010 Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

020 Independencia

020.010 Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

020.020 Relación organizativa

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

030 Ética y normas profesionales

030.010 Código de Ética Profesional

El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

030.020 Atención profesional correspondiente

En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

0**40 Idoneidad**

040.010 Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

040.020 Educación profesional continúa

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

050 Planificación

050.010 Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

060 Ejecución del trabajo de auditoría

060.010 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

060.020 Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

070 Informes

070.010 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

080 Actividades de seguimiento

080.010 Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Fecha de vigencia: 25 de julio de 1997

Ejemplos en la aplicación de auditoria de sistema

Situación 1

Al realizar una prueba de facturación los auditores observaron que los precios facturados en algunos casos no coincidían con los indicados en las listas de precios vigentes. Posteriormente se comprobó que ciertos cambios en las listas de precios no habían sido procesados, razón por la cual el archivo maestro de precios estaba desactualizado.

Alternativas de solución

- Uso de formularios prenumerados para modificaciones y controles programados diseñado para detectar alteraciones en la secuencia numérica de los mismos.
- Creación de totales de control por lotes de formularios de modificaciones y su posterior reconciliación con un listado de las modificaciones procesadas.
- Conciliación de totales de control de campos significativos con los acumulados por el computador.
- Generación y revisión de los listados de modificaciones procesadas por un delegado responsable.
- Revisión de listados periódicos del contenido del archivo maestro de precios.

Situación 2

El operador del turno de la noche, cuyos conocimientos de programación eran mayores de los que los demás suponían, modifico (por consola) al archivo maestro de remuneraciones a efectos de lograr que se abonara a una remuneración más elevada a un operario del área de producción con el cual estaba emparentado. El fraude fue descubierto accidentalmente varios meses después.

Alternativas de solución

- Preparación de totales de control del usuario y reconciliación con los acumulados del campo remuneraciones, por el computador.
- Aplicación de control de límites de razonabilidad.

Informativos sobre auditoria de sistemas

Las compañías españolas se preocupan por la auditoría de sistemas de información. Un tercio dispone de departamento dedicado, según datos de KPMG, IAI e ISACA:

La auditoría de sistemas de información evoluciona rápidamente como parte de los departamentos de auditoría interna de las organizaciones, ya que las firmas son cada vez más conscientes de la importancia que tiene realizar un adecuado control de los riesgos tecnológicos. Pero, aunque siete de cada diez grandes empresas españolas reconoce la importancia de esta función, un 67 % aún carece de un departamento específico para ejecutarla.

Éstas son las conclusiones a las que ha llegado el primer estudio sobre la Función de Auditoría Interna de Sistemas de Información en España, realizado por la firma de servicios profesionales KPMG, las Asociación de Auditores de Sistemas (Capítulo de Madrid de ISACA) y el Instituto de Auditores Internos de España (IAI) y cuyo objetivo es conocer la relevancia y el nivel de actividad que realiza la auditoría en nuestro país.

El informe, que se ha elaborado con las respuestas de directores de área de auditoría interna y directores financieros, pone de relieve una creciente tendencia a valorar la criticidad de auditar los sistemas de información. Un 73% de las empresas reconoce la importancia de este control,

aunque son muchas menos, un 33%, las que disponen de un área específica dentro de sus departamentos de auditoría. El resto externalizan esta función o no la realizan.

Donde está más establecida esta unidad es en el sector de la banca y seguros. El 43% de las empresas financieras consultadas cuenta con un departamento de auditoría interna de sistemas de información, algo que se explica por el alto grado de protección de los datos al que la ley obliga a estas empresas.

Energía e industria, con el 21 por ciento, y distribución y consumo, con el 15 siguen a finanzas en la implantación de esta función.

Esta situación coloca a España aún lejos de Europa y de EE.UU. en cuanto a implantación de esta herramienta de control interno de los riesgos tecnológicos, según los autores de este estudio. En Norteamérica cerca de un 60% de las empresas disponen de un área específica para llevarlo a cabo. Aún así KPMG se muestra optimista, dada la evolución ascendente que se está produciendo: "No es un problema, sino una oportunidad. Especialmente para numerosos profesionales especializados en sistemas de información que están esperando para colocarse en primera línea".

Estos profesionales también son centro de atención en este estudio, en el que se observa la gran movilidad que mantienen los auditores externos de sistemas de información en contraste con la baja rotación de los que trabajan en departamentos internos.

En cuanto a su formación, un 66% de las empresas consultadas coincide en señalar la necesidad de que los auditores internos de sistemas de la información posean conocimientos específicos, especialmente la certificación CISA.

El estudio revela que los departamentos de auditoría interna de las empresas españolas están realizando esfuerzos considerables para mejorar su funcionamiento, aplicando en sus prácticas habituales, metodologías estándar (CobIT), herramientas de interrogación de ficheros o de análisis de riesgo, entre otras. "Se observa que las empresas están dando pasos importantes encaminados a cubrir áreas como la seguridad informática, el control interno informático y el análisis de riesgos tecnológicos mediante la utilización de las herramientas adecuadas" concluye el análisis.

Servicios de auditoría de tecnologías de la información

La Auditoria de las Tecnologías de la Información y las Comunicaciones está adquiriendo cada vez una mayor importancia debido a la necesidad de garantizar la seguridad, continuidad y disponibilidad de las infraestructuras informáticas sobre las que se sustentan los procesos de negocio de toda empresa u organismo, necesitando adicionalmente que todos estos procesos se realicen de forma eficiente.

Por otro lado, los entornos legislativos actuales (LSSICE, LOPD) también hacen referencia a la obligatoriedad de acreditar el cumplimiento de sus normas mediante Auditorías de Sistemas de Información y como parte inherente de la Auditoría Financiera, se está requiriendo cada vez más que los Sistemas de Información sean, a su vez, auditados.

Es por ello que ofrecemos entre nuestros servicios la inscripción de los ficheros existentes en el Registro General de Protección de Datos, previo estudio, evaluación y clasificación del contenido y tipología de los mismos. Así mismo le ofrecemos nuestra ayuda para desarrollar el Plan de Seguridad requerido por la legislación vigente.

En TICS Consulting ofrecemos los servicios de Auditoría de Sistemas aplicando metodologías de auditoría tecnológicamente avanzada, metodologías estándar (CobiT, ITIL, etc.), herramientas de interrogación de ficheros y análisis de riesgos, etc. Todo ello siguiendo el Código de Ética Profesional de ISACA® establecido para dirigir la conducta personal y profesional de los miembros de la asociación y/o de aquellos que cuenten con cualquiera de las credenciales de certificación internacional.

Certificación oficial como Auditor de Sistemas de Información

La certificación internacional como Auditor de Sistemas de Información (*Certified Information Systems Auditor*™ - CISA) está reconocida a nivel mundial como uno de los estándares más prestigiosos en las áreas de auditoria, control, seguridad y

gobernabilidad de Sistemas de Información. Para obtenerla, hay que superar una prueba escrita que demuestre los conocimientos del candidato en las áreas de auditoria, control y seguridad de Sistemas de Información y justificar ante la Junta de Certificación un mínimo de cinco años de experiencia en tareas relacionadas con estas áreas.

Además de esto, para obtener la certificación hay que adherirse al Código de Ética Profesional de ISACA®, elaborar y cumplir un plan de educación continua (para garantizar que se está al tanto de las novedades tecnológicas en estas áreas) y cumplir con los Estándares de Auditoria de Sistemas de Información.

La certificación proporciona a los miembros de ISACA® acceso a una serie de foros y herramientas de colaboración e intercambio de experiencia con profesionales de la Auditoria a través de publicaciones, encuentros, jornadas de formación y herramientas a disposición de los miembros de la asociación, bien directamente desde su web o a través de los capítulos locales existentes en cada país.

Si lo desea puede ampliar esta información sobre los Servicios de Auditoría de Sistemas de Información que le ofrecemos en TICS Consulting.

La Auditoría Interna en CVG:

De acuerdo al Manual de Normas y Procedimientos de la Corporación Venezolana de Guayana se estableció un procedimiento para el proceso de auditoria interna, en el cual a continuación se detallan algunos aspectos importantes.

La Unidad de Auditoría Interna de la Corporación Venezolana de Guayana, en el ámbito de sus competencias es la que realiza Auditorías, inspecciones, fiscalizaciones, exámenes, estudios, análisis e investigaciones de todo tipo y de cualquier naturaleza en el ente sujeto a su control para verificar la legalidad, exactitud, sinceridad y corrección de sus operaciones, evaluar el cumplimiento y los resultados de los planes de su gestión, y las actuaciones que sean necesarias a fin de comprobar la ocurrencia de actos, hechos u omisiones contrarios a una disposición legal o sublegal, determinar el monto de los daños causados al patrimonio del ente sujeto a su control, si fuere el caso, además de la procedencia de acciones fiscales.

Los tipos de Auditorías que ejecuta el órgano de control interno son:

• **Auditoría de Gestión:** Examen a la gestión administrativa, los recursos empleados y las metas alcanzadas y cumplimiento de los objetivos planificados por el ente, así como la eficiencia, efectividad y economía de las operaciones.

• **Auditoría de Cumplimiento:** Verifica la normativa legal aplicable al área auditada y la comprobación y evaluación de los controles y procedimientos operativos del organismo.

• **Auditoría Financiera:** Verifica la razonabilidad de las cifras presentadas en los estados financieros, así como la situación económica del ente auditado.

• **Auditoría de Sistemas:** Revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, así como los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Normas Generales

- La Unidad de Auditoría Interna es la única unidad de la Corporación Venezolana de Guayana responsable de planificar, coordinar y programar la ejecución de Auditorías sobre éste instituto autónomo y sobre los entes bajo el control de ésta unidad, de

acuerdo a la Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal y la Ley Orgánica de Administración Financiera del Sector Público.

- Las unidades auditadas están en la obligación de permitir las visitas de inspección o fiscalización del órgano de control interno, así como a suministrar toda la información requerida a través de memorando, entrevistas o cuestionarios de control, pudiendo la Unidad de Auditoría participar como observador en aquellos actos que estime conveniente.
- La Unidad de Auditoría Interna deberá mantener reserva de la información que maneja con ocasión de sus actuaciones, así mismo de los documentos bajo investigación administrativa.
- Las solicitudes de información sobre las actividades realizadas por la Unidad de Auditoría Interna será autorizada por el Auditor Interno, quien determinara ello es procedente, así como la forma de entrega de lo requerido.
- Toda solicitud de auditoría por parte de las unidades sujetas al control de la Unidad de Auditoría Interna de la Corporación Venezolana de Guayana, no contenida en el Plan Anual, deberá estar debidamente justificada por el solicitante, a los fines de que el Auditor Interno evalué su ejecución su ejecución. La planificación del trabajo a realizar por la Unidad de Auditoría Interna debe obedecer a un Plan Anual de Auditoría, el cual contendrá:
    - Identificación de la Auditoría a practicar
    - Ente y/o unidad a auditar
    - Horas Hombres estimadas
- La Planificación de cada actuación de auditoría será suscrita por el Auditor Interno, y deberá abarcar desde el otorgamiento de la Credencial, hasta la remisión del Informe Definitivo (anexo n°1)

- La Credencial suscrita por el Auditor Interno donde identifica al funcionario actuante, le confiere autoridad suficiente a éste último para solicitar al auditado toda la información relativa a su examen que estime conveniente. (anexo n°2)
- La Unidad de Auditoría Interna producto de sus actuaciones, genera los informes siguientes: Preliminar, Definitivo y de Seguimiento, los cuales deberán:
    - Ser redactados de manera objetiva, persuasiva y constructiva y en forma clara, precisa y concreta.
    - Tener insertados los detalles necesarios, que contribuyan a evitar equívocos y ambiguedades.
    - Ser remitidos oportunamente a las autoridades a quienes corresponda y presentados ante el Comité de Auditoría Interna de la Corporación Venezolana de Guayana.
    - Realizarse siguiendo la estructura siguiente:
        - Identificación
        - Estructura del informe
        - Origen de la Auditoría
        - Alcance de la Auditoría
        - Objetivo
        - Metodología, procedimientos y técnicas utilizadas en la Auditoría.
        - Observaciones, conclusiones, anexos.
- El Informe Preliminar que realiza la Unidad de Auditoría es enviado al ente o unidad auditada, así como a las unidades relacionadas a los fines de permitir las aclaratorias sobre el contenido del mismo, con indicación de que las personas a asistir al análisis del informe deberán poseer suficiente competencia y capacidad para asumir los compromisos que se originen a los fines de garantizar su validez y cumplimiento.

- Las aclaratorias deben ser formuladas en reuniones de trabajo y realizarse en un lapso no mayor a quince (15) días hábiles a partir de la recepción del Informe Preliminar por parte del auditado. En la reunión de trabajo el auditado deberá consignar los soportes de las aclaratorias que manifieste el auditado. Si el auditado no asiste a la reunión, se dejarán firmes las observaciones, conclusiones y recomendaciones contenidas en el Informe Preliminar, el cual será denominado Informe Definitivo. El resultado de estas reuniones será asentado en una minuta que será elaborada y suscrita por los asistentes.
- El Informe Definitivo debe ser dirigido por el Auditor Interno a la máxima autoridad del organismo, a los fines de ser considerados y distribuidos a cada dependencia que tenga elación o responsabilidad con los resultados del examen realizado.

Toda actuación que genere un Plan de Acción Correctivo, será objeto de una actuación de seguimiento, a fin de verificar su cumplimiento.

Si en la actuación de seguimiento se determina que no se han realizado las acciones correctivas de acuerdo al Informe Definitivo y los acuerdos establecidos en el Plan de Acción Correctivo, se podrá otorgar una prórroga que se establecerá de común acuerdo entre las partes involucradas; si al realizarse el próximo seguimiento persiste el incumplimiento, se evaluará la remisión de la observación al Presidente de la Corporación para que instruya su cumplimiento. Agotadas estas dos alternativas, se deberá remitir a la Contraloría General de la República, la situación antes descrita.

Los Programas de Auditoría, se realizarán de acuerdo al Formato establecido en el anexo n°6 y bajo las siguientes condiciones:

a) Programa General :

• Será elaborado por el Supervisor inmediato del funcionario responsable de la Auditoría, y contará con el visto bueno del Auditor Interno y el Gerente de la Unidad. El Supervisor inmediato entregará el programa al funcionario al inicio de la evaluación en conjunto con la Credencial.

b) Programa Específicos:

• Será preparado por el funcionario responsable de la auditoría, en concordancia con el Programa de Auditoría General y aprobado por el Supervisor inmediato del funcionario responsable de la actuación.

Las Entrevistas y Cuestionarios de Control Interno que aplique el Auditor en el transcurso de la Auditoría, deben ser plasmados en los formatos que se muestran en el anexo n° 7.

En todo proceso de evaluación el Auditor debe solicitar por escrito a los entes involucrados las informaciones, con indicación expresa del lapso de tiempo otorgado para la recepción de la misma y la obligatoriedad de estar suscrita por el funcionario autorizado. Si vencido el lapso y no se ha recibido lo requerido, la solicitud deberá ser ratificada por el titular de Auditoría Interna, con indicación del nuevo lapso de espera, el cual no será mayor de tres (03) días hábiles, informándose al responsable sobre las sanciones a las que está sujeto al no suministrar lo solicitado.

Al concluir el trabajo de campo, se deberá elaborar el Acta de Conclusión de Audítoría anexo n° 8.

Los Papeles de Trabajo soporte del trabajo de auditoria deberán ser elaborados de acuerdo al anexo n° 9. Para más detalles se anexa en digital el manual de Normas y procedimientos de auditoría Interna.

CONCLUSIÓN

La Auditoría de las Tecnologías de la Información y las Comunicaciones adquiere cada vez mayor importancia, debido a la necesidad de garantizar la seguridad, continuidad y disponibilidad de las infraestructuras informáticas sobre las que se sustentan los procesos de negocio de toda Empresa u Organismo, necesitando adicionalmente que todos estos procesos se realicen de forma eficiente. Por otra parte los entornos legislativos actuales también hacen referencia a la obligatoriedad de acreditar el cumplimiento de sus normas mediante Auditorías de Sistemas de Información y como parte consustancial de la Auditoría Financiera, se está requiriendo cada vez más que los Sistemas de Información sean, a su vez, auditados.

Este escenario implica que la Auditoría de Sistemas de Información es una de las actividades presentes y futuras con mayor proyección para un amplio colectivo de sectores, ya que cada proyecto puede requerir intervenciones especializadas en temas concretos a auditar.

La auditoría en informática es muy importante dentro de una empresa, debido a que es parte de la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática debe comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

BIBLIOGRAFÍA

Willingham J.Carmichael DR.,(1982).”Auditoria .Concepto y metodos”. Mc Graw Hill.

Sánchez Fernández de Valderrama JL., (2004). “Teoría y práctica de la auditoría I. Concepto y metodología". Pirámide. 3edición.

http://www.monografias.com/trabajos14/auditoria/auditoria.shtml

http://www.monografias.com/trabajos16/auditoria-de-informacion/auditoria-de-informacion.shtml

http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml

http://html.rincondelvago.com/auditoria-de-los-sistemas-de-informacion.html

http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n

http://www.ticsconsulting.es/auditor.php

http://www.alipso.com/monografias/auditosis/

http://www.idg.es/computerworld/articulo.asp?id=176019