UNIVERSIDAD LATINA, S.C.

INCORPORADA A LA U.N.A.M.

CAMPUS CUERNAVACA 8344-48

FACULTAD DE INFORMÁTICA

“AUDITORIA INFORMATICA”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

P R E S E N T A:

JOSE MIGUEL ORGANISTA ALARCON

ASESOR: JOSE MATA DOMINGUEZ

CUERNAVACA, MOR. MARZO 2019

DEDICATORIA

A DIOS DUEÑO DE MI VIDA QUIEN MARCA LOS TIEMPOS DE MANERA PERFECTA; Y MANTUVO LA LUZ DE LA ESPERANZA EN MI.

A:

MI MADRE: MARIA DEL CARMEN

PARA VERME CRECER Y PODER LLEGAR DONDE ESTOY, GRACIAS POR EL PRIVILEGIO DE EXISTIR, SU AMOR, PACIENCIA, TOLERANCIA Y ENTREGA SON LOS ELEMENTOS QUE DIERON EXISTENCIA A MI VIDA.

AGRADECIMIENTOS

A:

A MIS TIOS CONCEPCION IRENE Y ROSENDO

DE MANERA ESPECIAL POR HABER SIDO LA MEDULA ESPINAL EN ESTE TRABAJO, QUE COMPARTIERON E IMPULSARONEN LA REALIZACION Y CULMINACION DE ESTE PROYECTO; GRACIAS POR SUS AFECTOS.

A:

Mis hermanos: Yuridia Del Carmen, Yiset Areli y Mario Armando:

POR HABERME REFLEJADO EN ELLOS Y SER EL MOTOR Y VISION DE ESTE DOCUMENTO QUE VEIA INALCANZABLE.

A:

MI ABUELITA Y TIA: MARIA DE LA LUZ Y MARGARITA

QUIENES CAMINARON JUNTO A MI Y ESE MANANTIAL DE CARIÑO Y ESPERANZA, SUS LAGRIMAS VALIERON LA PENA.

Índice

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 inmersa 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 está 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 tiene 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 vienen 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.

1. AUDITORIA

1.1. Evolución de la auditoria

En la Edad Media, la auditoría trataba de descubrir fraudes; este enfoque se mantiene hasta finales del siglo XIX.

Hasta la Revolución Industrial la economía se desarrollaba en base a una estructura de empresa familiar donde la propiedad y la dirección de sus negocios confluían en las mismas personas, que, por tanto, no sentían ninguna necesidad de la auditoría independiente ni tampoco se les imponía por normativa legal.
Con la aparición de las grandes sociedades, la propiedad y la administración quedó separada y surgió la necesidad, por parte de los accionistas y terceros, de conseguir una adecuada protección, a través de una auditoría independiente que garantizara toda la información económica y financiera que les facilitaban los directores y administradores de las empresas.
La razón de ser Gran Bretaña la cuna de la auditoría se explica por ser este país el pionero en la Revolución Industrial.

Estados Unidos, en la actualidad, está a la vanguardia del estudio e investigación de las técnicas de auditoría y de su desarrollo a nivel legislativo.
La crisis de Wall Street en 1929 y la creación de la Securities and Exchange Commission (SEC), órgano regulador y controlador de la Bolsa, han sido factores determinantes para conseguir las cotas de desarrollo que los profesionales de la auditoría han alcanzado en aquel país.

1.2. 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."

1.3. 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.

1.4. 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.

1.5. Clasificación de la auditoria

1.5.1. 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.

1.5.2. 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.

Los términos internos y externos son independientes al tipo de auditoría que se haga. Una auditoría operativa o una auditoría financiera puede ser interna o externa en función de la ubicación organizativa del responsable de la misma. Es necesario precisar esto porque suele identificarse erróneamente la auditoría interna con la auditoría contable o financiera.

2. AUDITORIA ADMINISTRATIVA

2.1. 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 auditoría 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.

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 auditorías 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"

2.2. Ubicación del desarrollo de la auditoria

La auditoría administrativa es y será siempre la herramienta más útil en la administración de una organización, ya que a través de ella se puede penetrar en lo más hondo de la empresa, para entender dónde está ubicada, cómo llegó hasta allí, de dónde partió y a dónde quiere llegar.

En este punto llegaremos a entender para exponer y entender qué es la auditoría administrativa, con el fin de que comprendas su significado, objetivos, alcance y campo de aplicación, para que así percibas la importancia de esta herramienta en el desarrollo y crecimiento de las empresas

En este punto el lector definirá el concepto de auditoría administrativa y evaluará su implicación en la organización.

¿Sabes cuál es la definición del autor Franklin para la auditoría administrativa?

Franklin recupera algunas definiciones propuestas por diversos autores, entre ellos encontramos una citada por Fernández, que dice que la auditoría administrativa es “la técnica que tiene el objeto de revisar, supervisar y evaluar la administración de una empresa” (Franklin, 2007: 8).

En la misma obra hallamos la definición propuesta por Macías Pineda: “La auditoría administrativa puede definirse como un examen completo y constructivo de la estructura organizativa de una empresa, institución o departamento gubernamental; o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales” (Frankin, 2007: 10).

Por su parte, Franklin define a la auditoría administrativa como: “Una revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y perfilar oportunidades de mejora para innovar, valorar y lograr una ventaja competitiva sustentable” (Frankin, 2007: 11).

2.3. Pasos del proceso administrativo

El proceso administrativo y sus componentes, planeación, organización, dirección y control, resultan de la mayor importancia para la empresa dentro del sistema de toma de decisiones.

- **La planeación**: es la primera ficha de este rompecabezas, dentro de ella se siguen los siguientes pasos: investigación del entorno e interna, planteamiento de estrategias, políticas y propósitos, así como de acciones a ejecutar en el corto, medio y largo plazo.
- **La organización:** la segunda ficha, es un conjunto de reglas, cargos, comportamientos que han de respetar todas las personas que se encuentran dentro de la empresa, la función principal de la organización es disponer y coordinar todos los recursos disponibles como son humanos, materiales y financieros.
- **La dirección** es la tercera ficha del rompecabezas, dentro de ella se encuentra la ejecución de los planes, la motivación, la comunicación y la supervisión para alcanzar las metas de la organización.
- **El control**: la ficha de cierre, es la función que se encarga de evaluar el desarrollo general de una empresa.

2.4. Objetivos de la auditoria administrativa

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

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

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

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

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

3. Génesis De La Migración

3.1. Objetivos

- Exponer la importancia del cambio y su relación con el proceso administrativo, desempeño laboral, proceso de implementación, y la auditoria en un proceso de cambio.

3.2. Proceso del Cambio

Los procesos de cambio implican "transiciones" para los colaboradores de la organización, si no se identifican las transiciones y no se diferencian, atienden y planean de manera paralela al proceso central de "cambio", los resultados no serán como se espera.

Estamos inmersos en un profundo cambio de todo tipo. Las empresas y organizaciones dependen de los órdenes económicos, industriales, y sociales en los que se encuentra inmersas porque, si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben adaptarse rápidamente a las nuevas circunstancias para sobrevivir. Una de las tendencias actuales más significativas es que se dirige desde una Sociedad Industrial hacia una llamada *Sociedad de información*.

Este cambio es muy rápido, está afectando al mundo entero, y su comprensión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los sistemas y tecnologías de información. Aunque los avances tecnológicos de los últimos veinte años han sido constantes y espectaculares, en los últimos cinco años se ha producido una verdadera revolución tecnológica de gran calidad e impacto para la propia industria informática, así como de consecuencias importantes para el resto de los sectores

Cada vez mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes. De igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información, son indispensables. La gerencia debe establecer un sistema de control interno adecuado. Tal sistema debe soportar debidamente los procesos del negocio.

La auditoría Informática plantea unos métodos y procedimientos de control de los sistemas de información que son válidos para cualquier tamaño de empresa.

La competencia global es una realidad. Las empresas y organizaciones se deben reestructurar hacia operaciones cada vez más competitivas y, como consecuencia, deben aprovechar los avances de las tecnologías de los sistemas de información para mejorar su situación competitiva.

3.3. Administración del cambio

La escala y alcance de los cambios que a menudo necesita RPE (reingeniería en los procesos de la empresa) significa que muchos de los retos existen, no tanto en la comprensión de los procesos y cómo pueden rediseñarse, sino más bien cómo poner en práctica el cambio necesario para lograr una mejoría potencial. Las empresas tienden a ser conservadoras y la resistencia al cambio tiene que convertirse en una colaboración activa.

El rediseño del proceso es la parte de más sencilla, en realidad, poner en práctica el nuevo diseño de proceso es donde fracasan la mayor parte de los proyectos. Obtener beneficios requiere de cambios y éstos pueden ser difíciles de lograr. El planteamiento o el marco de referencia para abordar un programa de RPE constan de cinco de fases clave[26]:

1. Crear el entorno

2. Analizar, diagnosticar y rediseñar los procesos.

3. Reestructurar la empresa

4. Hacer pruebas de piloto y poner en marcha el proceso.
5. Ejecutar la estrategia.

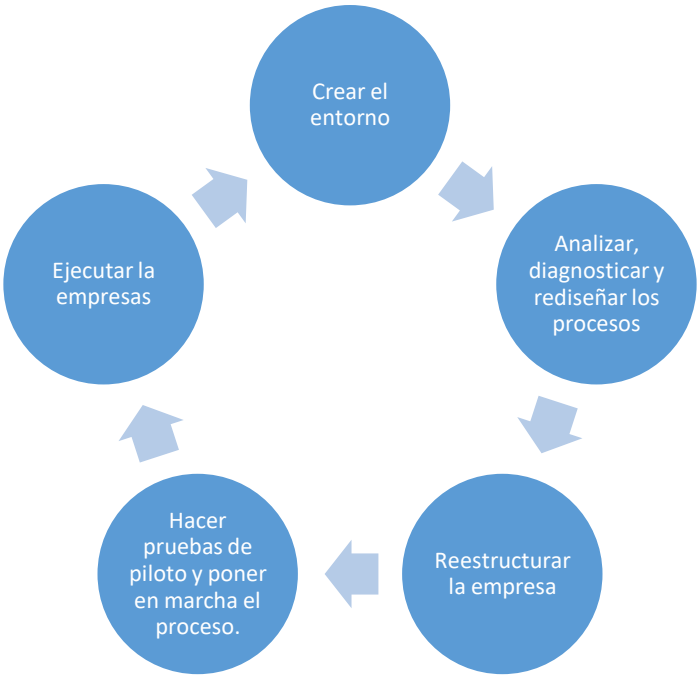
Cada uno de los anteriores puede subdividirse en más pasos, algunos de los cuales pueden ejecutarse en paralelo.

El nivel organizacional

El nivel de proceso
El nivel de puesto de trabajo / ejecución

Figura 7. Enfoque general de RPE.

Algunas de las fases de un cambio son:



Analizar, diagnosticar y rediseñar los proceso

Reestructurar la

Empresa

1. Sensibilizar sobre la importancia del cambio
2. Diseñar la secuencia del proceso de cambio

3. Implementar herramientas de orientación para enfrentar el proceso de cambio

4. Lograr el compromiso y aprobación de la dirección

5. Lograr el compromiso y aprobación de los empleados y colaboradores

6. Ejecutar y verificar el plan de cambio y del plan de transición

7. Adecuar y capacitar al personal para el cambio.

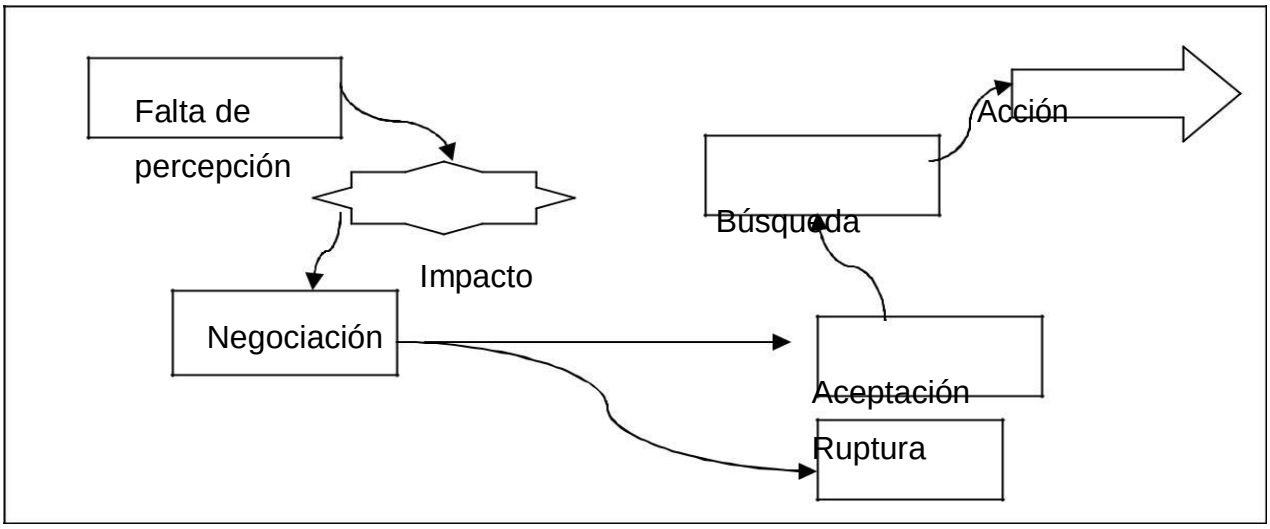
Para conseguir el compromiso de la dirección y del personal es fundamental

Comprender cómo se puede conseguir el cambio y elevar el rendimiento. Para esto se destacan tres niveles que deben enfrentarse en la iniciativa de mejora:

Poner en práctica el cambio en cada uno de estos niveles es difícil, aunque sea simplemente porque amenaza el status quo. Cuando entienda cómo administrar la empresa será necesario comprender la reacción de los individuos a los cambios propuestos.

Aunque cada una de las personas reaccionará en forma distinta hacia los cambios, existen algunas fases reconocibles por las que atraviesan las personas, como se ilustra en la siguiente figura[27]:

Figura 3. Reacciones Generales al cambio.



Un papel importante de la gerencia es que las personas pasen por estas etapas ya asegurarse que la resistencia al cambio no vence a la iniciativa. El grado de resistencia dependerá del tipo de cambio y de lo bien que se comprenda éste, sobre todo el grado de ruptura real o percibida. Existen tres condiciones que crean resistencia significativa al cambio:

Cuando las personas se sienten cómodas con el status quo. Cuando no comprenden el porqué es conveniente el cambio

Cuando tiene dudas respecto a la capacidad de la empresa para conseguir el cambio deseado.

Los trabajadores también podrían tener miedo que el rediseño que los amenaza minimice sus conocimientos.

3.4. Auditoría Informática

Desde el inicio de la humanidad las distintas culturas han dado una importancia enorme a los temas de contabilidad, y por lo tanto también han necesitado medios que permitieran verificar sus registros, es decir, de la auditoría. De hecho se piensa que la invención de la escritura surgió como respuesta a la necesidad de auditar. Flesher (1993); por lo que lo de auditor sería una de las profesiones más antiguas[28].

A partir de 1950, la informática se convierte en una herramienta muy importante las labores de auditoría financiera, ya que permite llevar a cabo de forma rápida y precisa, operaciones que manualmente consumirían demasiados recursos.

Sin embargo, al convertirse los sistemas informáticos de la empresa cada vez más dependientes de las computadoras, surge la necesidad de verificar que dichos sistemas funcionen correctamente (finales de los años sesenta).

Así surge la necesidad de una nueva especialidad dentro de la auditoría, cuyo objetivo es precisamente verificar el funcionamiento correcto, eficaz y eficiente de la informática, en definitiva, la auditoría informática.

Las empresas invierten enormes cantidades de dinero y tiempo en la creación de Sistemas de Información que les ofrezcan la mayor productividad y calidad posible por eso que los temas relativos a la auditoría informática cobran cada vez más relevancia tanto en el ámbito internacional como nacional.

Auditoría es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. Es decir es una función que se acomete a posteriori, en relación con actividades ya realizadas, sobre las que hay emitir opinión.

Se puede descomponer el concepto anterior en lo siguiente[29]:

1. Contenido	Una opinión
2. Condición	Profesional
3. Justificación	Sustentada en determinados procedimientos
3. Objeto	Una determinada información obtenida en cierto soporte
4. Finalidad	Determinar si presenta adecuadamente la realidad o está responde a las Expectativas que le son atribuidas, es decir, su fiabilidad.

Se tienen al día de hoy 4 diferentes clases de auditoría, para nuestro caso, solo nos vamos a apoyar en la auditoría Informática y Administrativa[30]:

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas Anuales	Presentan realidad
Informática	Opinión	Sistemas de Aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente según normas establecidas.
Gestión o de Administración	Opinión	Dirección	Eficacia, eficiencia, economicidad
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas.

3.5. Proceso de Consultaría

La consultaría consiste en dar asesoramiento o consejo sobre lo que se ha de hacer o cómo llevar a cabo adecuadamente una determinada actividad para obtener los fines deseados. Los elementos de la consultaría podrían resumirse en:

1. Contenido	Dar asesoramiento o consejo
2. Condición	De carácter especializado
3. Justificación	Sobre la base de un examen o análisis
4. objeto	La actividad o cuestión sometida a consideración
5. Finalidad	Establecer la manera de llevarla a cabo adecuadamente

Es una función a priori con el fin de determinar cómo llevar a cabo una función o actividad de forma que obtenga los resultados pretendidos. La auditoría verifica a posteriori si estas condiciones, una vez realizada esta función o actividad, se cumplen y los resultados pretendidos se obtienen realmente. Los tipos de consultaría o clase son los siguientes[32]:

Clase	Contenido	Objeto	Finalidad
Financiera	Asesoramiento	Planes de Cuentas. Procedimientos administrativos	Diseño e implementación
Informática	Asesoramiento	Aplicaciones. Planes de Contingencia.	Desarrollo. Diseño e implementación

Con lo anterior, se observa que la auditoría informática engloba el concepto de consultoría. Así la auditoría informática es una parte integrante de la auditoría, se estudia por separado para tratar problemas específicos y para aprovechar los recursos del personal. El cometido de la auditoría informática se puede dividir en:

- Un estudio del sistema y un análisis de los controles organizativos y operativos del departamento de informática.

- Una investigación y análisis de los sistemas de aplicación que se estén desarrollando o que ya estén implementados.

- La realización de auditorías de datos reales y de resultados de los sistemas que se estén utilizando.

- La realización de auditoría de eficiencia y eficacia.

La auditoría informática es la revisión de la propia informática y de su entorno y las actividades a que da lugar esta definición pueden ser:

- Análisis de riesgos y Planes de contingencia

- Desarrollo de aplicaciones y Asesoramiento en paquetes de seguridad

- Evaluación de la gestión de los recursos informáticos.

- Revisión de controles y cumplimiento de los mismos, así como de las normas legales aplicables.

- La auditoría informática es un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficiencia exigida en el marco de la organización correspondiente.

- De las definiciones anteriores se desprenden conceptos que abarca la auditoría y la consultoría. No son términos equivalentes y es preciso distinguirlos.

3.6. Auditoría Operativa Organizativa y administrativa

Auditoría Operativa como aquella que tiene como objeto el análisis y la mejora de cualquier componente de la organización a excepción de su sistema financiero y contable. Pero no toda la literatura organizativa ni todos lo auditores utilizan la misma terminología.

Por un lado, se encuentra la auditoría administrativa que se encarga de examinar y analizar los sistemas, los procedimientos, las estructuras, los recursos humanos, los recursos materiales y los programas de los diferentes complejos de organización. Es decir, el campo de actividad de esta auditoría incluye todas las funciones que integran la gestión a excepción de la financiera, para verificar su buen funcionamiento, proponer mejoras y mejorar sus comportamientos disfuncionales.

De esta forma, auditoría administrativa y auditoría operativa significan lo mismo. Igual ocurre con la auditoría organizativa aunque en ocasiones se imita su uso a las dimensiones de estructura y procesos.

3.7. Auditoría Operativa en el proceso de cambio

Las empresas y demás tipos de organizaciones se enfrentan a momentos de incertidumbre. Su entorno modifica sus necesidades y pautas de conducta de manera rápida y, en ocasiones, impredecible. La multiplicidad de organizaciones origina una intensa disputa por un mercado cada vez más saturado y exigente. Se encuentran bajo la presión de la competitividad donde la renovación es la clave no sólo del éxito sino también para la mera subsistencia.

El cambio organizativo ha dejado de ser fenómeno excepcional para convertirse en una compañía necesaria y continúa: las organizaciones deben cambiar constantemente. El problema, lógicamente no es cambiar sino en qué dirección orientar el cambio, qué elementos de la organización deben modificarse y cómo conseguir que empresarios, ejecutivos, empleados y consultores unifiquen esfuerzos en estos momentos de renovación.

Las organizaciones requieren perspectivas y herramientas que les permitan estar atentas a la evolución de su entorno y de las necesidades del mercado. Requieren técnicas de diagnóstico que identifiquen los elementos internos de la organización que no se comportan como debieran: técnicas que, a su vez, sugieran las pautas de renovación de estos elementos fallidos u obsoletos.

De esta manera, directivos y consultores necesitan unos métodos que posibiliten un mejor conocimiento de la organización y de su entorno, que ayuden a encontrar nuevos objetivos y diseños más eficaces y eficientes y, por último, requieren unas técnicas que consigan implementar estos anhelos de cambio.

Las áreas clave de una organización son dimensión política y estratégica que es el punto de encuentro entre el entorno y los objetivos estratégicos (qué hacemos), la dimensión organizativa y de pilotaje (cómo lo llevaremos a cabo), los recursos de la organización, es decir, los empresarios, ejecutivos y empleados (quienes lo llevarán a cabo y en qué condiciones) y el momento en que se encuentra la organización (dónde del ciclo de vida de la organización) ya que podemos estar enfrente de una organización incipiente, joven, madura o vieja. La respuesta a estas preguntas configura la estructura de la organización, que se denominan los niveles de análisis de una organización.

3.8. Desarrollo de la auditoría operativa

Tiene como objetivo presentar los mecanismos para elaborar un diagnóstico de los distintos niveles de la organización (cómo es) y una propuesta de mejora de

los mismos (hacia qué, cómo, con qué, con quienes y dónde). En primer lugar se abordan tres relevantes temas: los modelos de estudio aplicables a las organizaciones donde se explica que hay distintos tipos de organizaciones y cómo cada uno de ellos requiere un estilo de análisis distinto, así mismo es necesario identificar los límites de la auditoría operativa.

Otros de los asuntos propios de la auditoría operativa son los sistemas de capacitación y tratamiento de la información donde se presentan las técnicas de recogida de la información necesaria; el tratamiento de esta información y cómo se elabora un diagnóstico y unas propuestas de carácter organizativo, y el sistema de planificación de la auditoría operativa donde se precisan las etapas del proceso de auditoría, la planificación de este tipo de estudios, así como la memoria de las actividades de auditoría.

Así mismo se maneja un enfoque de productividad donde se muestran los estrechos lazos entre la competitividad y la auditoría operativa. Combinar la perspectiva teórica con la práctica pero reforzando la última, basado en la experiencia de consultores de organizaciones que pertenecen al sector público.

Esto no significa que se adopte una perspectiva distinta a la que requieren otros tipos de organizaciones, más bien al contrario, de la experiencia que se deriva de nuestro contacto con las organizaciones públicas, que suelen tener más problemas que las privadas, surge una orientación y unas herramientas más completas y sofisticadas que pueden ayudar a la compresión y tratamiento de los problemas de cualquier tipo de empresa y, en especial, de las empresas de servicios.

Los modernos directores deben complementar sus habilidades de dirección y de gestión con una cierta capacidad de auto análisis y mejora del área de la que son responsables. Para ser los catalizadores y conductores del cambio deben saber la manera de diagnosticar las dimensiones externas e internas de su organización y, de esta manera, atinar mejor con sus objetivos y con la forma y los medios para conseguirlos.

Como dice Townsend, los directivos competentes no necesitan consultores: Un auténtico directivo dedica parte de su tiempo a hablar con sus empleados y sabe lo que debe hacerse en un momento determinado o cómo averiguarlo.

Pero esta aseveración no significa que los consultores (en este caso auditores operativos) no sean en algunas ocasiones necesarios; pero sí que deberían limitar su colaboración a aquellos problemas y circunstancias que objetivamente rebasan el tiempo y los conocimientos organizativos de los directivos.

Son precisamente los consultores organizativos (los consultores del cambio) los segundos destinatarios y especialmente en ellos se centra el esquema propuesto.

El esquema está pensado para aquellas personas que deseen mejorar sus conocimientos sobre organizaciones, sean estudiantes u otras personas interesadas en el tema:

- Estrategia Metodológica

- Estrategia de RECURSOS HUMANOS

Uno de los aspectos que más suele criticarse de la gestión de los departamentos de recursos humanos es su pobre visión estratégica del negocio, su falta de participación en las decisiones y en la construcción de la visión orientadora de la organización.

Una buena administración de los Recursos Humanos puede ser la causa del éxito de una pequeña o mediana empresa. Una de las muchas funciones que tiene el área de recursos humanos es el manejar la nomina, la formación e ingeniería administrativa las cuales a su vez abarcan puntos estratégicos que son necesarios para que la empresa pueda lograr sus objetivos.

Nominas	Sueldos, salarios, Incentivos y Seguridad Social.
Formación	Capacitación Desarrollo y planeación de carreras
Ingeniería administrativa	Análisis de puestos, Valuación de puestos, evaluación del desempeño y estudios de trabajo
Relaciones laborales	Negociación colectiva, reclamaciones, administración del contrato colectivo

Estas cuatro funciones son fundamentales para que el personal pueda involucrase sin necesidad de otras técnicas represivas. Recordemos que por lo general el personal del área de sistemas esta contratado como personal de confianza razón por la cual solo es necesario manejar adecuadamente estos factores, por ejemplo el contrato colectivo no tiene mucha importancia ya que en vez de lograr un ambiente sano puede generar parálisis y no la flexibilidad como se recomienda en este tipo de proceso. En cambio en el rubro de la capacitación e incentivos son esenciales para un trabajador de confianza.

3.9. Control Interno

Tradicionalmente en materia de control interno se adoptaba un enfoque bastante restringido limitado a los controles contables internos. En tanto se relacione con la información financiera, el control interno era un tema que interesaba principalmente al personal financiero de la organización y, por supuesto, al auditor externo.

El concepto de control interno de mucha gente no incluía muchas actividades operativas claves destinadas a prevenir los riesgos efectivos y potenciales a los que se enfrentan las organizaciones.

Además de la mayor atención que prestan las autoridades al problema, se observan importantes cambios en las empresas. Dichos cambios someten a una gran tensión a los controles internos existentes. La mayoría de las organizaciones han acometido varias iniciativas en tal sentido, tales como:

- La reestructuración de los procesos empresariales (BPR – Bussiness Process Re-engineering)

- La gestión de la calidad total (TQM –Total Quality Management).

- El redimensionamiento por reducción o por aumento del tamaño hasta el nivel correcto.

- La contratación externa (Outsourcing)

- La descentralización

El mundo en general está cambiando cada vez más rápidamente, sometiéndose a las empresas a la acción de muchas fuerzas externas tales como la creciente necesidad de acceder a los mercados mundiales, la consolidación industrial, la intensificación de la competencia, y las nuevas tecnologías. Las tendencias externas que influyen sobre las empresas son entre otras, las siguientes:

- La globalización

- La diversificación de actividades

- La eliminación de ramas de negocios no rentables o antiguas

- La introducción de nuevos productos como respuesta a la competencia

- Las fusiones y la formación de alianzas estratégicas.

Ante la rapidez de los cambios los directivos toman conciencia de que para evitar fallos de control significativo deben reevaluar y reestructurar sus sistemas de controles internos. Deben actuar de manera proactiva antes de que surjan los problemas, tomando medidas audaces para su propia tranquilidad, así como para garantizar a los consejos de administración, accionistas, comités y público que los controles internos de la empresa están adecuadamente diseñados para hacer frente a los retos del futuro y asegurar la integridad en el momento actual.

Un centro informático de una empresa del sector terciario suele tener una importancia crucial por soportar los sistemas de información del negocio, por el volumen de recursos y presupuestos que maneja, etc. Por lo tanto, aumenta la complejidad de las necesidades de control y auditoría, surgiendo en las organizaciones, como medidas organizativas, las figuras de control interno y auditoría informáticos.

La auditoría ha cambiado notablemente en los últimos años con el enorme impacto que han venido cobrando las técnicas informáticas en la forma de procesar la información para la gerencia. La necesidad de adquirir y mantener conocimientos actualizados de los sistemas informáticos se vuelve cada vez más acuciante, si bien los aspectos básicos de la profesión no han variado.

Los auditores informáticos aportan conocimientos especializados, así como su familiaridad con la tecnología informática. Se sigue tratando las mismas cuestiones de control en la auditoría, pero los especialistas en auditoría informática de sistemas basados en computadoras prestan una ayuda valiosa a la organización y a los auditores en todo lo relativo a los controles sobre dichos sistemas.

En muchas organizaciones, el auditor ha dejado de centrarse en la evaluación y la comprobación de los resultados de procesos, desplazando su atención a la evaluación de riesgos y la comprobación de controles. Mucho de los controles se incorporan en programas informáticos o se realizan por parte de la función informática de la organización, representada por el Control Interno Informático.

El enfoque centrado en controles normalmente exige conocimientos informáticos a nivel de la tecnología utilizada en el área o la organización que se examina.

3.10. Control Interno Informático (CII)

El CII controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la organización y/o la Dirección de Informática así como requerimientos legales.

La misión de CII es asegurar que las medidas que se obtiene de los mecanismos implantados por cada responsable sean correctas y válidas. El CII suele ser un órgano staff de las Dirección del Departamento de informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.

- Asesorar sobre el conocimiento de las normas

- Colaborar y apoyar el trabajo de auditoría Informática, así como de las auditorías externas al grupo.

- Definir, implementar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del Servicio Informático, lo cual no debe considerarse como que la implementación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implementación de los medios de medida adecuados.

Realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC's, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de diferentes actividades operativas sobre:

- El cumplimiento de procedimientos, normas y controles dictados. Merece resaltarse la vigilancia sobre el control de cambios y versiones del software.
- Controles sobre la producción diaria.

- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.

- Controles en las redes de comunicaciones

- Controles sobre el software de base.

- Controles en los sistemas microinformáticos.

- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien pueda asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano).

    o Usuarios, responsables perfiles de uso de archivos y bases de datos o Normas de seguridad

- Control de información clasificada
- Control dual de la seguridad informática.

- Licencias y relaciones contractuales con terceros
- Asesorar y transmitir cultura sobre el riesgo informático.

3.11. Ejecución de la auditoría informática (AI)

La auditoría informática (AI) es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficientemente los fines de la organización y utiliza eficientemente los recursos. De este modo la AI sustenta y confirma la consecución de los objetivos de la auditoría.

- Objetivos de protección de activos e integridad de datos
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por computadoras.[35]

El auditor es responsable de revisar e informar a la Dirección de la organización sobre el diseño y el funcionamiento de los controles implementados y sobre la

fiabilidad de la información. Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implementación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes.

- Revisar y juzgar los controles implementados en los sistemas informáticos para verificar su adecuación a las ordenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ente errores y fraudes.

- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

3.12. Administración de Riegos

Al hablar de riesgos en una organización hablamos de la amenaza por evento u acción que puede afectar de forma adversa la habilidad para lograr los objetivos y ejecutar con éxito los planes futuros de una organización.

Derivado de lo anterior debemos pensar en el manejo efectivo de esas empresas, ya que las consecuencias de estas sobre los resultados de la organización pueden ser desastrosos, es por ello que la ciencia administrativa se ha ocupado entre otras cosas, de su manejo, siguiendo el proceso administrativo que consiste en los pasos siguientes: Planeación, organización, integración, dirección y control de todas y cada una de las áreas de la organización que pudieran verse afectadas con estas amenazas, ya que en las labores cotidianas existen riesgos de diversa índole que es necesario evaluar continuamente, ya que están en constante cambio por lo que son impredecibles de calcular.

Hoy en día los riesgos no solo deben considerarse desde el ámbito externo o de mercado, sino además, se tiene que ver la introspectiva empresarial para

conservar el impacto que los riesgos intrínsecos pueden tener y el grado de correlación de estos con los factores extrínsecos ; sin embargo el estar conscientes de ello no es suficiente hay que además, cuantificar su impacto y establecer planes de acción para prevenirlos y/o mitigarlos; es por ello que la administración, las estrategias y las técnicas, entre otras áreas, se han preocupado por el estudio y prevención de estos, estableciendo métodos cuantitativos y pro balísticos para su análisis.

4. EL AUDITOR

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

4.1. 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.

4.2. 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 auditoría 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 auditoría 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 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).

Es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio.

- La auditoría de tecnología de la información (T.I) como se le conoce actualmente, (auditoria informática o auditoria de sistemas en nuestro medio), se ha consolidado en el mundo entero como cuerpo de conocimientos cierto y consistente, respondiendo a la acelerada evolución de la tecnología informática de los últimos 10 años.
- La INFORMACION es considerada un activo tan o más importante que cualquier otro organización.

Existe pues, un cuerpo de conocimientos, normas, técnicas y buenas prácticas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad y disponibilidad de la INFORMACION tratada y almacenada a través del computador y equipos afines, asi como la eficacia, eficiencia y economía con que la administración de un ente están manejando dicha INFORMACION y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo el anterior con el objetivo de emitir una opinión o juicio, para la cual se aplican técnicas de auditoria de general aceptación y conocimiento técnico especifico.

4.3. 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

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

1. **Participación en el desarrollo de nuevos sistemas:**

    a. **Evaluación de controles**

Esta 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 de evaluar todo: informática, organización de centros de información, software y hadware.

4.4. Objetivos específicos de la auditoria de sistemas.

En muchas ocasiones, cuando se habla de controles internos las percepciones de su significado son muy distintas, dependiendo del usuario, preparador,

auditor o dirección. Para algunos usuarios, control interno se refiere a los procedimientos de conciliaciones y autorizaciones; para otros, pudieran ser los controles relativos a fraude; y para otros, ser solo políticas y procedimientos establecidos en las empresas.

Sin embargo, de manera general se puede comentar que los controles internos son las respuestas de la administración de una empresa o negocio para mitigar un factor identificado de riesgo o alcanzar un objetivo de control.

Los objetivos de los controles pueden agruparse en cuatro categorías:

- Estratégicos.
- De información financiera.
- De operaciones.
- De cumplimiento de las disposiciones legales y reglamentos.

Si bien las empresas requieren establecer controles internos para mitigar los riegos asociados con estos temas; para efectos de la auditoría de estados financieros, el control interno relevante es el relacionado con la información financiera.

En el presente artículo se analizará la evaluación del control interno y sus componentes en la auditoría de estados financieros, tomando en cuenta las disposiciones de las Normas Internacionales de Auditoría (NIA) para efectos de exponer la finalidad, el alcance y la naturaleza del control interno sobre la información financiera, incluyendo los cinco componentes que debe evaluar el auditor de los estados financieros.

b. Cumplimiento de la metodología.

2. Evaluación de la seguridad en el área informática.

Cuando se habla de la función informática generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, etc.

Sin embargo se suele pasar por alto o se tiene muy implícita **la base** que hace posible la existencia de los anteriores elementos. Esta base es la *información*.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo está basado en tecnología moderna, para esto se debe conocer que la información:

- esta almacenada y procesada en computadoras
- puede ser confidencial para algunas personas o a escala institucional
- puede ser mal utilizada o divulgada
- puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información está centralizada y que puede tener un alto valor y los últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Pensemos por un momento que hay se sufre un accidente en el centro de cómputo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

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.**

Más personas, más mercadería, más dinero circulando, más situaciones que no puedes controlar en forma permanente…más riesgos.
Anticípate a situaciones complejas y aplica buenas prácticas para el cuidado de tus bienes tangibles e intangibles.
Algunas formas de proteger el esfuerzo (y dinero) invertido en poner en marcha y sostener tu negocio son:

- **Mecanismos de control interno.** Arqueos sorpresivos, controles cruzados, controles al ingreso y egreso del personal, normas de seguridad, se vuelven imprescindibles en la medida que una empresa incorpora nuevos integrantes con acceso a bienes de valor. Organizar a las personas y crear puestos con responsabilidad de supervisión ayuda a aumentar el control. Estos mecanismos permiten evitar problemas o detectarlos rápidamente, a la vez que actúan como disuasivos

- **Observación directa.** El control de los lugares clave o los momentos críticos de la operación puede resultar difícil de delegar totalmente. Pero “el ojo del amo” ya no tiene por qué ser real. Con cámaras web es hoy posible mirar en tiempo real la fábrica, la caja del restaurante o la actividad en la oficina, desde una computadora, celular o dispositivo móvil.

- **Alarmas.** Utilízalas tanto para detectar incendios como intrusos. Los sistemas con monitoreo permiten poner en marcha planes de acción inmediatamente.
- **Seguros.** A las coberturas básicas de incendio, robo, mercadería y vehículos, los seguros comerciales agregan opciones que protegen ante rotura de vidrieras,

demandas civiles, falta de pago de clientes, daños en equipos electrónicos o caída brusca de la actividad.

- **Tecnología.** En algún momento accesible sólo para las grandes empresas, hoy las pymes pueden utilizar sistemas tecnológicos para proteger sus lugares de trabajo, depósitos y mercaderías. Seguimientos satelitales, cámaras, inventarios con códigos de barras, sensores de movimiento, controles de acceso, son algunas de las herramientas que pueden mantener a salvo tu patrimonio.
- **Seguridad informática.** La información de tu empresa puede ser tan o más valiosa que los bienes tangibles. Aplica buenas prácticas para resguardar datos confidenciales, proteger tu infraestructura, bloquear programas maliciosos, y administrar el acceso de tus empleados.

5. Control de modificación a las aplicaciones existentes.

a. Fraudes

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de Delito puede ser más compleja. Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta. El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar,

confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos. Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso. Este es el panorama de este nuevo fenómeno científico tecnológico en las sociedades modernas.

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.

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

a. Quién accede a los datos.
b. Cuándo se accedió a los datos.
c. Desde qué tipo de dispositivo/aplicación.
d. Desde que ubicación en la Red.
e. Cuál fue la sentencia SQL ejecutada.
f. Cuál fue el efecto del acceso a la base de datos.

Objetivos: Disponer de mecanismos que permitan capturar de una auditoría la relación del personal con el acceso a las bases de datos incluyendo la capacidad de generar, modificar y/o eliminara datos.

Importancia: Dentro de los aspectos de mayor importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que se utilizan, además que toda la información financiera de una compañía reside en una de estas, ya que debe existir controles adecuados y relacionados con el acceso a las mismas.

a. Estructura sobre la cual se desarrollan las aplicaciones.

DISEÑO Y CARGA: En esta fase se llevarán a cabo los diseños lógico y físico de la base de datos, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente; determinando si la definición de datos contemplan además de su estructura, las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad.

9. Auditoría de la red de teleprocesos.

El teleproceso es un elemento de importancia crítica en las funciones de la entidad deberá verificarse que existen los elementos adecuados de respaldo para la red de teleproceso de modo que ante estos fallos claves (concentradores, ordenadores para comunicaciones, controladores, etc.) la actividad del centro no se vea paralizada. En determinados casos puede ser interesante desarrollar un estudio de viabilidad para la implementación de una versión más reducida del teleproceso de forma que se garantice, cuanto menos, la continuidad de las transacciones vitales en espera de la total restauración de servicio tras una caída grave.

10. Desarrollo de software de auditoría.

La auditoría informática viene siendo la revisión y el completo análisis del servicio informático ofrecido por la empresa. Una revisión profunda que permita conocer, supervisar y verificar todos los procesos involucrados con esta área de la organización. 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

4.4. 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.

4.5. Tipos de auditoria

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

4.5.1 **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

4.5.2. **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

4.5.3. **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.

4.5.4. **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.

Las auditorias de Performance o de gestión incluyen las auditorias de economía, de eficiencia y las de programas.

Las auditorias de economías y de eficiencia pueden determinar:

a) si la entidad está adquiriendo, protegiendo y utilizando sus recursos de manera económica y eficiente

b) las causas de las ineficiencias o prácticas antieconómicas.

Las auditorias de programas pueden determinar:

a. hasta qué punto se está consiguiendo los beneficios o los resultados buscados

b. la eficacia de las organizaciones, programas, actividades o de las funciones.

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.

4.6. Justificación 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.

4.7. Pasos a seguir para implementar auditoría en un sistema de información

Se requieren varios pasos para realizar una auditoría. 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 auditoría 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.

4.8. 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 relacionadas con 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.

5. CONTROLES INFORMÁTICOS Y RIESGOS

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.

5.1. Clasificación general de los controles

5.1.1. 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.

5.1.2. Controles detectivos

Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más 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.

5.1.3 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 detectives sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

5.2. Principales controles físicos y lógicos

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

5.2.1. Autenticidad

Permiten verificar la identidad

- Passwords
- Firmas digitales

5.2.2. Exactitud

Aseguran la coherencia de los datos

- Validación de campos
- Validación de excesos

5.2.3. Totalidad

Evitan la omisión de registros así como garantizan la conclusión de un proceso de envió:

- Conteo de registros
- Cifras de control

5.2.4. Redundancia

Evitan la duplicidad de datos

- Cancelación de lotes
- Verificación de secuencias

5.2.5. Privacidad

Aseguran la protección de los datos

- Compactación
- Encriptación

5.2.6. Existencia

Aseguran la disponibilidad de los datos

- Bitácora de estados
- Mantenimiento de activos

5.2.7. Protección de Activos

Destrucción o corrupción de información o del hardware

- Extintores
- Passwords

5.2.8. Efectividad

Aseguran el logro de los objetivos

- Encuestas de satisfacción
- Medición de niveles de servicio

5.2.9. Eficiencia

Aseguran el uso óptimo de los recursos

- Programas monitores
- Análisis costo-beneficio
-

5.3. 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.

5.4. 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.

5.5. 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.

6. Controles automáticos o lógicos

6.1. Periodicidad de cambio de claves de acceso

Los cambios de las claves de acceso a los programas se deben realizar periódicamente. Nomalmente 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.

6.2. 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

6.2.1. 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.

6.2.2. Confidenciales

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

6.2.3. No significativas

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

6.3 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.

6.3.1 Conteo de registros

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

6.3.2. 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.

6.3.3. Verificación de límites

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

6.4. 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 sí.

6.5. Dígito auto verificador

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 décimo dígito de la cédula de identidad, calculado con el módulo 10 o el último dígito del RUC calculado con el módulo 11.

6.6. 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.

7. 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

7.1.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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 cómputo 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.

7.6. Controles en el uso del microcomputador

Es la tarea más difícil pues son equipos más 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.

8. 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 críticas.
- Comunicación de resultados.

8.1. 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.

8.2. 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 críticas, Revisión de procesos históricos (backups), Revisión de documentación y archivos, entre otras actividades.

8.3. Examen detallado de áreas criticas.-Con las fases anteriores el auditor descubre las áreas críticas 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.

8.4. **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.

8.5. Estructura de una empresa idónea.

La misión, visión y objetivos son él porque de la empresa. Dentro de la problemática de la empresa el cumplimiento de estos parámetros no se han logrado satisfacer y se ha tenido la necesidad de redefinirlos constantemente ya sea porque se generan nuevos requerimientos o porque en algunos rubros no se puedan satisfacer.

Cabe mencionar, que es importante fijar la atención en toma de decisiones en todo momento. Se induce que la empresa debe y requiere que su infraestructura tecnológica, equipos, programas, procedimientos y personal, se actualicen y modernicen constantemente:

Misión

Garantizar el procesamiento y flujo de la información entre los participantes del SAR, con la más **alta eficiencia** y seguridad, al menor costo y satisfacer las necesidades de sus accionistas vía soluciones **de alta tecnología** que den como resultado mejoras en su información, procesos y rentabilidad.

Visión

Ser reconocida por el sistema como la empresa más:

- **Automatizada** (poca intervención humana)
- **Optimizada** (operar el mejor proceso posible)
- **Capacitada** (que el personal del equipo conozca bien el proceso)
- Satisfecha (que al personal le guste su trabajo)
- **Monitoreada** (mecanismos de control: detección, corrección y de contingencia)
- Eficientada (operar a los menores costos)
- Consultada (tener siempre disponible la información)
- Propositiva (identificar desviaciones y coordinar soluciones)
- Estandarizada (ejecutar igual todas las veces)

Objetivos Estratégicos

- Maximizar el aprovechamiento de recursos

- Fomentar el talento humano especializado

- Operar orientado en la administración de procesos Implementar reingeniería de procesos

- **Optimización** de los sistemas

- Aprovechar el desarrollo tecnológico

- Fusionar la seguridad y una continua operación

- Aplicar en los servicios un valor agregado

- Integrar control y monitoreo y un sistema de administración de la calidad total.

9. Título de auditoria.

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

9.1. Normas Generales

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

9.1.1. 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.

9.2. Independencia

9.2.1. 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.

9.3. 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.

9.4. Ética y normas profesionales

9.4.1 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.

9.5. 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.

9.6. Idoneidad

9.7. 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.

9.8. Educación profesional continúa

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

9.9. Planificación

9.9.1. 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.

9.10. Ejecución del trabajo de auditoría

9.11. 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.

9.12. 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.

9.13. Informes

9.14. 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.

9.15. Actividades de seguimiento

9.16. 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

10. 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 pre numerados 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.

Solución 3.

El no contar con un esquema de migración de sistemas ha provocado pérdidas que han puesto en duda la continuidad de la empresa, cuyos procesos operativos dependen principalmente y podría decirse totalmente de su capacidad tecnológica, de la innovación, de la continua actualización y rápida adaptación al cambio en el área de sistemas para lograr cumplir con sus metas y justificar su existencia.

De los resultados desalentadores de proyectos de migración de sistemas, surge la necesidad de analizar y determinar: ***¿cuáles y que factores intervienen en mayor o en menor grado en un proceso de migración de tecnología y sistemas de información, cuál es su relación con el desempeño y la productividad de la empresa, y cómo es posible mejorar este proceso?.***

Por otro lado, también se desea aportar información que sirva como referencia y ayuda para toda aquella empresa que desee implementar cambios tecnológicos ya que actualmente existe escasa información que describa experiencias reales y retos de este tipo de proyectos (migración de sistemas) contando solo con referencias subjetivas y con una basta literatura generalizada que solo establece patrones muy superficiales.

Por lo tanto esta investigación evalúa el desempeño antes, durante y después de la de proceso de migración con objeto de contestar la anterior pregunta de investigación para desarrollar un esquema de referencia para la toma de decisiones y asegurar en mayor grado el cumplimiento de objetivos.

11. Federación De Asociaciones Mexicanas de Informática.

La **Federación de Asociaciones Mexicanas de Informática, AC** (FAMI) es una asociación civil mexicana formada para potenciar, apoyar y facilitar la coordinación entre las asociaciones relacionadas con la informática, computación, y áreas afines. Fue creada en 1996, con sede en la Ciudad De México

En México existen diversas organizaciones de la sociedad civil relacionadas con el ámbito informático. El 11 de abril de 1996 se integró el Comité Coordinador de Asociaciones en Informática, considerando que sería de utilidad tratar de mejorar la coordinación e intercambio de información entre este tipo de agrupaciones, con objeto de facilitar la cooperación y la búsqueda de consensos con miras a apoyar al desarrollo del país a través de esta disciplina y presentar un frente común en los aspectos de interés de los miembros.

Firmaron la carta de intención correspondiente los presidentes de las asociaciones siguientes:

- Asociación de Informática para la Ingeniería (AMII)
- Academia Mexicana de Informática (AMIAC)
- Asociación Mexicana de Telemática (AMT)
- Asociación Mexicana de Ejecutivos en Informática (AMEI)
- Asociación Mexicana de Informática Médica (AMIM)
- Comité Permanente de Peritos en Informática y Computación del CIME
- Asociación Nacional de la Industria de Programas para Computadora
- Asociación Mexicana de Auditores en Informática
- Asociación Nacional de Profesionales en Informática

- Asociación de Alta Dirección en Informática
- Asociación Nacional de Instituciones de Educación en Informática
- Asociación Mexicana de Sistemas de Información Geográfica
- Asociación Mexicana de Ingenieros Mecánicos Electricistas
- Instituto Nacional De Geografía Estadística e Informática
- Firmó además el Ing. Enzo Molino Ravetto, promotor de la reunión y ex presidente de la AMIAC

En la asamblea de este Comité Coordinador celebrada el 11 de junio de 1996, se acordó que era conveniente dar mayor formalidad al grupo y que debería formarse una Asociación Civil denominada FAMI. Esa reunión, como asamblea constitutiva designó la primera mesa directiva de la FAMI, para el periodo 1996-1998, misma que quedó integrada del modo siguiente:

- Presidente: Enzo Molino Ravetto
- Vicepresidente (y presidente del siguiente periodo): Jorge Hernández Aguilar
- Secretario: Yolanda Campos Campos
- Tesorero: Guillermo Mallen Fullerton.
- Coordinador administrativo: Antonio Ayestaran

La protocolización se realizó ante notario el 29 de agosto de 1996.

El instituto Mexicano de auditores informáticos es una asociación civil mexicana, fundada el 7 de septiembre de 1976. Su propósito principal es agrupar a los informáticos de mayor relevancia en el país.

El 14 de mayo de 1976 se celebró en el Hotel Alameda de la Ciudad de México la reunión en la que se acordó formar el instituto mexicano de Informática.

La formalización ante notario requirió algún tiempo, y se realizó el 7 de septiembre de ese año, en la Notaría 26 del DF.

El primer presidente de la Academia (1976-78), en esa época coordinaba las actividades de Informática en la Secretaría de Hacienda y Crédito Público. Una vez fundada el instituto, el coordinó la realización del I Seminario de Informática en 1978, inaugurado por el Presidente de la República, Lic. José López Portillo, y en el cual participaron 2 Premios Nobel, además de importantes personalidades nacionales e internacionales.

El segundo presidente (1978-1980. Bajo su presidencia se incorporó la AMIAC a la International Medical Informatics Association (IMIA) y se organizó en México, del 7 al 12 de febrero de 1982, el Congreso Mundial de Informática Médica y los Países en Desarrollo.

Propósitos y Estrategias.

Objetivos

La FAMI se creó para la unidad y el mejoramiento de la informática en México y para la proyección y defensa de las asociaciones que la forman. Entre los objetivos específicos cabe destacar:

a. Representar los intereses comunes de las asociaciones miembro, tanto a nivel nacional como internacional, sin limitar la autonomía de estas.

b. Integrar grupos e intereses de todas las vertientes y áreas de especialidad de la informática y de las diferentes regiones del país.

c. Ser un órgano independiente de consulta y diálogo sobre informática ante los diversos sectores que conforman la sociedad mexicana.

d. Ser un foro de comunicación e intercambio de ideas, experiencias e información que permita mejorar la interacción de las diferentes asociaciones y grupos con interés en la informática.

e. Proponer, recomendar, difundir y promover lineamientos, proyectos y acciones, tendientes a mejorar el aprovechamiento y desarrollo de la informática, ante las instancias correspondientes.

f. Definir, emitir y promover normas y lineamientos para la formación y capacitación de los informáticos, asesorar en el diseño de los planes de estudio correspondientes y en general, velar porque se imparta educación adecuada en el campo de la informática.

g. Apoyar la profesionalización de la informática, incluyendo la emisión de recomendaciones, lineamientos y criterios de evaluación y certificación.

h. Impulsar la informática en todos sus aspectos, incluyendo la investigación, la docencia y el ejercicio profesional.

i. Fomentar la cultura informática para apoyar el desarrollo del país.

Estrategias

Para sus actividades, la FAMI considera las estrategias siguientes:

a. Operar a través de esquemas que faciliten y promuevan la colaboración y la suma de esfuerzos.

b. Ser un medio de concertación en relación con los objetivos especificados.

d. Mantener independencia de ideologías políticas, credos, religiones, intereses económicos particulares, así como de otras instituciones o empresas.

Actividades Realizadas

- Co-organizador con la Comisión Federal de Telecomunicaciones y la Sociedad Internet de México, de la reunión con proveedores de servicio Internet, celebrada el 27 de enero de 1997
- Presentación de opinión, a solicitud de la Secretaría de Relaciones Exteriores, sobre la propuesta francesa a la OECD para reglamentar Internet
- Co organizador con la Sociedad Internet de México de la primera reunión sobre seguridad en redes de cómputo, celebrada los días 24 y 25 de abril de 1997
- Instalación de un servidor WEB para difundir información sobre la propia FAMI
- Participación los días 21 y 22 de septiembre de 1996 en el foro de consulta sobre el futuro de Internet en México, organizado por CONACYT y la Comisión Federal de Telecomunicaciones
- Participación en el Comité de normalización de EDI
- Participación en la organización del foro “Gobierno Digital” (1998)
- Colaboración para la organización de la Olimpiada Informática

- Realización de la auditoría técnica al Programa de resultados electorar el preliminares (PREP) del Instituto Federal Electoral (México) para incrementar la confianza en los sistemas informáticos de las elecciones federales de 1997 en México.

- Elaboración, en 2001, del documento "Opciones estratégicas para el desarrollo informático de México", para apoyo a la toma de decisiones del Gobierno de México

11.2. 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.

12. La Auditoría Interna:

En el territorio mexicano existen dos tipos de normas que son objeto de auditoria por los organismos pertinentes, las primeras son las normas oficiales mexicanas (NOM) estas son de carácter obligatorio, las normas mexicanas (NMX) no son de carácter obligatorio.

12.1. Norma Oficial Mexicana NOM

Artículo. 3, Fracción XI. Norma Oficial Mexicana: la regulación técnica de observancia obligatoria expedida por las dependencias competentes, conforme a las finalidades establecidas en el artículo 40, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado y las que se refieran a su cumplimiento o aplicación.

Estas normas ordinariamente se publican íntegramente en el Diario Oficial de la Federación e incluso se publican en medios electrónicos, por lo que se pueden considerar de acceso público y libre distribución, siempre y cuando no se alteren, aunque para referirse a ellas deben tomarse las publicadas por el Diario Oficial de la Federación.

12.2. Norma Mexicana NMX

Las normas mexicanas, conocidas por sus siglas como normas NMX, creadas en el Artículo 3 Fracción X de la Ley Federal sobre Metrología y Normalización, que dice:

Artículo 3, Fracción X. Norma mexicana: la que elabore un organismo nacional de normalización, o la Secretaría, en los términos de esta Ley, que prevé para un uso

común y repetido reglas, especificaciones, atributos, métodos de prueba, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado.

La aplicación de este tipo de normas puede ser obligatorio si es referida en una NOM para realizar algo, tal y como ocurre en el caso de la **NOM-002-SEDE-1999**, con respecto a las normas **NMX-J-116-ANCE** y la **NMX-J-169-ANCE**.

12.3. 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.

13. Normas Generales

La unidad de Auditoría Interna es la única unidad 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, 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 ambigüedades.

  Ser remitidos oportunamente a las autoridades a quienes corresponda y presentados ante el Comité de Auditoría.

  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 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 Auditoría 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.

14. 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).

15. 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%C 3%B3n

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

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

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

APA. (1994). **Manual de estilo de publicaciones**. México.: Manual Moderno

Ackoff, Russell L. (1997). **Planificación de la empresa del futuro**. México.: LIMUSA

Andrade, Ma. Antonieta y otros. (2002). **Investigación Administrativa.** No. 90. Año 31. México.: ESCA-IPN.

Andrade, Ma. Antonieta. (1998). **Apuntes sobre metodología de la Investigación.** México: ESCA-IPN.

Badia, Albert. (2002). **Calidad ISO 9001 versión 2000**. México.: Deusto.

Bijon, Claude. (1993**). Las estrategias de ruptura**. México.: UNIANDES

Davis, Gordon. (1989). **Sistemas de Información Gerencial**. México.: Mc. Graw Hill

El economista.(sep 2002). Tecnología aplicada (En red). Disponible: www.eleconomista.com.mx

Fred R. David. (1997). **Conceptos de administración estratégica**. México.: PHH

Hall, Richard H. (1996). **Organizaciones. Estructura, procesos y resultados (6ª ed).**
México.: PHH

IDS. (2003). **Manuel de procedimientos**. México: IDS