

10623  
9



**UNIVERSIDAD NACIONAL AUTONOMA  
DE MEXICO**

---

**FACULTAD DE ESTUDIOS SUPERIORES  
CUAUTITLAN**

"DESARROLLO DE UNA METODOLOGIA PARA LA  
AUDITORIA EN INFORMATICA".

**TESIS**

**PARA OBTENER EL TITULO DE  
LICENCIADA EN INFORMATICA**

**P R E S E N T A ;  
KARINA MARGARITA SILVA MARTINEZ**

**TESIS CON  
FALLA DE ORIGEN**

ASESOR: L.C. CARLOS PINEDA MUÑOZ.

CUAUTITLAN IZCALLI, EDO. DE MEXICO

2003

1



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



**FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN  
UNIDAD DE LA ADMINISTRACION ESCOLAR  
DEPARTAMENTO DE EXAMENES PROFESIONALES**

ASUNTO: VOTOS APROBATORIOS

**TESIS CON  
FALLA DE ORIGEN**

**DR. JUAN ANTONIO MONTARAZ CRESPO**  
DIRECTOR DE LA FES CUAUTITLAN  
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares  
Jefe del Departamento de Exámenes  
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:

Desarrollo de una metodología para la auditoría en informática.

que presenta la pasante: Karina Margarita Silva Martínez  
con número de cuenta: 09605836-3 para obtener el título de:  
Licenciada en Informática

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

**A T E N T A M E N T E**

**"POR MI RAZA HABLARA EL ESPIRITU"**

Cuautitlán Izcalli, Méx. a 29 de Agosto de 2003

PRESIDENTE	<u>L.C. Carlos Pineda Muñoz</u>	
VOCAL	<u>L.E. Rogelio Moisés Sánchez Arrastio</u>	
SECRETARIO	<u>Ing. Oscar Hernández Sánchez</u>	
PRIMER SUPLENTE	<u>C.P. Carlos Francisco Román Rivera</u>	
SEGUNDO SUPLENTE	<u>L.C. Jaime Navarro Mejía</u>	

Para mi Dios por las puertas que ha abierto para lograr este paso.

Para mi papá, mi orgullo, mi apoyo, siempre ejemplo de lucha.

Para mi mamá, eterno agradecimiento de mi vida, forjándome cada instante al triunfo.

Para mi hermana Miriam, surtidora de sonrisas y apoyo hasta en los días nublados.

Para mis hermanos Juan y Alan los cuales hacen de mi vida la aventura más divertida.

Para mi Tita, maestra del amor puro y sincero.

Para mis amigos, por compartir los días soleados y las noches lluviosas. David sin tu apoyo esto se hubiera convertido en un mar de dudas y un sin fin de razones.

Para mi asesor L.C Carlos Pineda Muñoz, por sus mejores regalos para mí, conocimiento, experiencia y paciencia.

Agradezco sinceramente a mis sinodales por su tiempo y consejos,

Ing. Oscar Hernández Sánchez,

L.E Rogelio Moisés Sánchez Arrastio,

C:P Carlos Francisco Román Rivera,

L.C Jaime Navarro Mejía.

TESIS CON  
FALLA DE ORIGEN

Universidad Nacional Autónoma de México  
Raíz de la ciencia, arte del fruto.

## INDICE

1. Antecedentes de la Auditoría Informática.....	1
1.1 Terminología de la auditoría Informática.....	1
1.2 Tipos de auditoría en informática.....	12
1.3 El entorno de la informática.....	26
1.4 Estrategias para la implementación formal de la función de auditoría Informática.....	29
1.5 Estructura organizacional.....	31
1.6 Administración de la función de auditoría en informática.....	36
1.7 Las dificultades de la auditoría de una aplicación informatizada.....	37
2. Análisis de las propuestas existentes.....	38
2.1 Metodología para el desarrollo e implementación de la auditoría en Informática de Mario Piatinni.....	39
2.2 Metodología para el desarrollo e implementación de la auditoría en Informática de Jose Antonio Echenique.....	43
2.3 Metodología para el desarrollo e implementación de la auditoría en Informática de Enrique Hernández Hernández.....	46
2.4 Metodología para el desarrollo e implementación de la auditoría en Informática de Yann Derrien.....	49
3. Propuesta de una Metodología para el desarrollo e implementación de la auditoría en Informática en busca de la eficiencia.....	51
3.1 Etapa de preauditoría.....	52
3.2 Etapa de inicio.....	54
3.3 Etapa de análisis.....	56
3.4 Etapa de desarrollo.....	60
3.5 Etapa final.....	62
4. Características y Ética del Auditor en Informática.....	65
4.1 Perfil del auditor informático.....	65
4.2 Principios éticos del Auditor en Informática.....	67
Conclusiones.....	69
Bibliografía.....	70

## 1. ANTECEDENTES DE LA AUDITORÍA EN INFORMÁTICA.

### 1.1 TERMINOLOGÍA DE LA AUDITORIA EN INFORMÁTICA.

Para poder entender lo relacionado con la Auditoria en Informática, es necesario conocer los términos que se utilizan a lo largo de este escrito, es por ello que abarcaremos los más importantes esperando ampliar nuestros conocimientos en esta área que tan difícilmente ha logrado llegar a un punto en que las organizaciones la consideren como una necesidad, para poder enfrentar los requerimientos que se están exigiendo para el desarrollo y calidad de las empresas de cualquier giro comercial en nuestro país.

Para esto mencionaremos los conceptos que se han definido tanto de algunos autores como de las organizaciones que están altamente relacionadas con la auditoria en informática.

#### *Informática:*

Etimológicamente, la palabra informática se deriva del francés *informatique*. Este neologismo proviene de la conjugación de *information* (información) y *automatique* (automática).

En 1966, la academia Francesa reconoció este nuevo concepto, definiéndolo:

*Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación en los ámbitos técnicos, económico y social.*

El principal esfuerzo por redefinir el concepto de informática lo realizó a principios de los sesentas la Oficina Intergubernamental de Informática (IBI), en aquel tiempo órgano asociado a la UNESCO. Este organismo, a través de los comités expertos convocados para ello, formuló en 1975 esta definición:

*Aplicación racional, sistemática de la información para el desarrollo económico, social y político.*

José Antonio Echenique <sup>1</sup> define que en algunas ocasiones se han empleado como sinónimo los conceptos de proceso electrónico, computadora e informática. El concepto de informática es más amplio, ya que considera el total del sistema y el manejo de la información, la cual puede usar los equipos electrónicos como una de sus herramientas.

<sup>1</sup> Auditoria en Informática, pp 3

TESIS CON  
FALLA DE ORIGEN

También es común confundir el concepto dato con el de información . La información es una serie de datos clasificados y ordenados con un objetivo común. El dato se refiere únicamente a un símbolo, signo o a una serie de letras o números, sin un objetivo que dé un significado a esa serie de símbolos, signos, letras o números.

Enrique Hernández <sup>2</sup> define:

La *informática* se desarrolla con base en normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional.

Se recomienda leer los textos sugeridos en la bibliografía y así se definen los siguientes términos:

La *informática* es el campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionadas con las computadoras y el manejo de la información por medios electrónicos, el cual comprende las áreas de la tecnología de información orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya de manera oportuna, veraz, confiable.

También es el proceso metodológico que se desarrolla de manera permanente en las organizaciones para el análisis, evaluación, selección, implantación y actualización de los recursos humanos (conocimientos, habilidades, normas, etc.) y financieros (inversiones) encaminados al manejo de la información, buscando que no se pierdan los propósitos de calidad, confiabilidad, oportunidad, integridad y veracidad, entre otros propósitos.

*Hardware:*

Se refiere a los componentes físicos y tangibles de las computadoras.

*Software:*

Implica la parte no física de las computadoras. Esto significa que es la porción intangible de los equipos de cómputo, es decir, programas con orientaciones específicas para la administración de la información y el uso eficiente de los recursos de cómputo.

*Sistemas de información:*

Son el conjunto de módulos computacionales o manuales organizados e interrelacionados de una manera formal para la administración y uso eficiente de todos los recursos ( humanos, materiales, financieros, tecnológicos, etc.) de un área específica de la empresa ( manufactura, administración, dirección, etc.) con la finalidad de representar los procesos reales del negocio, y orientar los procedimientos, políticas y funciones inherentes para el logro de las metas y objetivos del negocio.

<sup>2</sup> Auditoría en Informática, Hernández Hernández Enrique, pp 1

### ***Sistemas de información estratégica (SIE):***

Son aquellos que de manera permanente proporcionan a la alta dirección una serie de parámetros y acciones encaminadas a la toma de decisiones que apoyarán al negocio en el seguimiento de la rentabilidad y competitividad respecto de la competencia.

### ***Metodología:***

Es un conjunto de etapas ( fases o módulos) formalmente estructurados, de manera que brinden a los interesados los siguientes parámetros de acción en el desarrollo de sus proyectos:

### ***Técnicas:***

Es el conjunto de procedimientos y pasos ordenados que se usan en el desarrollo de un proyecto con el propósito de finalizar las etapas, fases, o módulos definidos en el proceso metodológico.

### ***Herramientas:***

Es el conjunto de elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica. Antes del auge de las computadoras, así como de otros elementos tecnológicos las herramientas eran simples máquinas o utensilios manuales que apoyaban el desarrollo de las tareas de cada uno de los proyectos.

### ***Control Interno:***

Este comprende el plan organizacional y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración.



### **Auditoría:**

La palabra auditoría viene del latín auditorius, y de ésta proviene "auditor", el que tiene la virtud de oír; el diccionario lo define como "revisor de cuentas colegiado"<sup>3</sup>

Para José Antonio Echenique<sup>4</sup> opina que la palabra auditoría se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Por eso se ha llegado a usar la frase "tiene auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto Auditoría es mas amplio; no sólo detecta errores: es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.

El boletín C de normas de auditoría del Instituto Mexicano de Contadores nos dice: <sup>5</sup>

La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos.

Así como existen normas y procedimientos específicos para la realización de auditorías contables, debe haber también normas y procedimientos para la realización de auditorías en informática como parte de una profesión. Estas pueden estar basadas en las experiencias de otras profesiones, pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y que además la auditoría debe de evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

**Auditoría:** Es un proceso formal y necesario para las empresas con el fin de asegurar que todos los activos sean protegidos en forma adecuada. Así mismo, la alta dirección espera que de los proyectos de auditoría surjan las recomendaciones necesarias para que se lleven acabo de manera oportuna y satisfactoria las políticas, controles y procedimientos definidos formalmente, con objeto de que cada individuo o función de la organización opere de modo productivo en sus actividades diarias, respetando las normas generales de honestidad y trabajo aceptadas.<sup>6</sup>

<sup>3</sup> Nuevo diccionario español Sopena

<sup>4</sup> Auditoría en Informática, Echenique JA, pp2

<sup>5</sup> Normas y procedimientos de auditoría, Instituto

<sup>6</sup> Auditoría en Informática, Hernández Hernández Enrique, pp16

TESIS CON  
FALLA DE ORIGEN

#### Tareas principales de la auditoría:

- Estudiar y actualizar permanente las áreas susceptibles de revisión.
- Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por los organismos generalmente aceptados a nivel nacional e internacional.
- Evaluación y verificación de las áreas requeridas por la alta dirección o responsables directos del negocio.
- Elaboración del informe de auditoría ( debilidades y recomendaciones)
- Otras recomendadas para el desempeño eficiente de la auditoría.

#### *Auditoría Interna y Auditoría Externa:*

La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

Por otro lado, la auditoría externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoría externa, las cuales no son tan perceptibles como en las auditorías convencionales. La auditoría interna tiene la ventaja de que puede actuar periódicamente realizando revisiones globales, como parte de su plan anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las auditorías, especialmente cuando las consecuencias de las recomendaciones habidas benefician su trabajo.

En una empresa, los responsables de Informática escuchan, orientan e informan sobre las posibilidades técnicas y los costos de tal sistema. Con voz, pero a menudo sin voto, informática trata de satisfacer lo más adecuadamente posible aquellas necesidades. La empresa necesita controlar su informática y ésta necesita que su propia gestión esté sometida a los mismos Procedimientos y estándares que el resto de aquella. La conjunción de ambas necesidades cristaliza en la figura del auditor interno informático.

En cuanto a empresas se refiere, solamente las más grandes pueden poseer una auditoría propia y permanente, mientras que el resto acuden a las auditorías externas. Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la auditoría interna de la empresa cuando ésta existe. Finalmente, la propia informática requiere de su propio grupo de control interno, con implantación física en su estructura, puesto que si se ubicase dentro de la estructura informática ya no sería independiente. Hoy, ya existen varias organizaciones informáticas dentro de la misma empresa, y con diverso grado de autonomía, que son coordinadas por órganos corporativos de sistemas de información de las empresas.

Una empresa o institución que posee auditoría interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

- Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- Contrastar algún Informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- Servir como mecanismo protector de posibles auditorías informáticas externas decretadas por la misma empresa.
- Aunque la auditoría interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas como para tener una visión desde afuera de la empresa.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

#### *Auditoría con informática.*

Los procedimientos de auditoría con informática varían de acuerdo a la técnica de cada organización y departamento de auditoría en particular. Existiendo ciertas técnicas y procedimientos que son compatibles en la mayoría de los ambientes de informática.

Estas técnicas caen en dos categorías: métodos manuales y métodos asistidos por computadora.

#### *Utilización de las técnicas de auditoría asistidas por computadora*

El auditor puede utilizar la computadora en la ejecución de la auditoría ya que esta herramienta permitirá ampliar la cobertura del examen, reduciendo el tiempo / costo de las pruebas y procedimientos de muestreo, que de otra manera tendrían que efectuarse manualmente.

Existen diferentes paquetes que permite elaborar auditorías a sistemas financieros y contables que se encuentran en medios informáticos. Además, el empleo de la computadora por el auditor le permite familiarizarse con la operación del equipo en el centro de cómputo de la institución. Una computadora puede ser empleada por el auditor en:

- Transmisión de información de la contabilidad de la organización a la computadora del auditor.
- Verificación de cifras totales y cálculos para comprobar la exactitud de los reportes.
- Clasificación de datos
- Impresiones
- Verificar la conexión y consistencia de los programas de computadora corriendo el proceso.

Entonces concretamos que la Auditoría con Informática se define "como el empleo de la computadora constituyéndose como una herramienta que facilita la realización de las actividades de revisión tales como:"

- Traslado de datos del sistema a un ambiente del control del auditor.
- Llevar a cabo la selección de datos.
- Verificar la exactitud de los cálculos: muestreo estadístico.
- Visualización de datos.
- Ordenamiento de la información. Producción de reporte e histogramas.

No olvidemos tomar en cuenta que un auditor debe tener ciertas habilidades principalmente; Habilidades para manejar paquetes de procesadores de texto, hojas de cálculo, uso de Internet, manejo de bases de datos, un paquete básico de contabilidad.

#### *Auditoría en Informática.*

La definición de Mair William es la siguiente:

*"Auditoría en Informática es la verificación de los controles en las siguientes tres áreas de la organización informática:"*

- Aplicaciones (programa de producción)
- Desarrollo de sistemas.
- Instalación del centro de proceso.

Para Ron Weber en Auditing Conceptual Foundations and Practice sobre auditoría informática:

*"Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente."*

<sup>7</sup> Auditoría en Informática, Echenique JA, pp11

TESIS CON  
FALLA DE ORIGEN

La auditoría en informática es :<sup>8</sup>

- a) *Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente.*
- b) *Las actividades ejecutadas por los profesionales del área de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.). Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual ha de contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y optimización permanente de la tecnología de informática en el negocio.*
- c) *El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de que todos los recursos de informática operen en un ambiente de seguridad y control eficiente, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que pasa por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etc.*
- d) *Proceso metodológico que tiene el propósito principal de evaluar todos los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opera con un criterio de integración y desempeño de niveles altamente satisfactorios para que apoyen la productividad y rentabilidad de la organización.*

Por lo tanto, puedo decir en mi opinión que auditoría en Informática "es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, así como una sugerencia para hacer uso de la tecnología de la manera mas eficaz y eficiente , ayudando a la toma de decisiones asertivas."

---

<sup>8</sup> Auditoría en Informática, Hemández Hemández Enrique, pp17

### Síntomas de necesidad de una Auditoría Informática:

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse de la siguiente manera:

- Síntomas de descoordinación y desorganización:
  - No coinciden los objetivos de la informática de la compañía con los de la propia compañía.
  - Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.
  - (Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna norma importante o cambio de software y hardware.)
- Síntomas de mala imagen e insatisfacción de los usuarios:
  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en las terminales de usuario, refrescamiento de paneles, variación de los archivos que deben ponerse diariamente a su disposición, etc.
  - No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
  - No se cumplen en todos los casos los plazos de entrega de resultados periódicos, pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.
- Síntomas de debilidades económico-financiero:
  - Incremento desmesurado de costos.
  - Necesidad de justificación de inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
  - Desviaciones presupuestarias significativas.
  - Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a desarrollo de proyectos y al órgano que realizó la petición).
- Síntomas de Inseguridad: Evaluación de nivel de riesgos
  - Seguridad lógica
  - Seguridad física
  - Confidencialidad

(Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales)

  - Continuidad del servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante planes de contingencia totales y locales.
  - Centro de proceso de datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

Los factores que pueden influir en una organización a través del control y la auditoría en informática son:

- Necesidad de controlar el uso evolucionado de las computadoras.
- Controlar el uso de las computadora, que cada día se vuelve más importante y costosa.
- Los altos costos que producen los errores en una organización.
- Abuso en las computadoras.
- Posibilidad de pérdida de capacidades de procesamiento de datos.
- Posibilidad de decisiones incorrectas.
- Valor del hardware, software y personal.
- Necesidad de mantener la privacidad individual.
- Posibilidad de pérdida de información o de mal uso de la misma.
- Toma de decisiones incorrectas.
- Necesidad de mantener la privacidad de la organización.

La auditoría en Informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimientos específicos, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad, personal (desarrollador, operador, usuarios) y obtención de información. En esto se deben incluir los equipos de cómputo.  
Campos de la auditoría de la Informática.<sup>9</sup>

El campo de acción de la auditoría informática es:

- A) La evaluación administrativa del área de informática.
- B) La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información. La evaluación de la eficiencia y eficacia con la que se trabaja.
- C) La evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, base de datos, comunicaciones, instalaciones)
- D) Seguridad y confidencialidad de la información.

Para lograr los puntos antes señalados se necesita:

- A) La evaluación administrativa del área de informática. Esto comprende la evaluación de:
  - Los objetivos del departamento, dirección o gerencia.
  - Metas, planes, políticas y procedimientos de procesos electrónicos estándares.
  - Organización del área y su estructura orgánica.
  - Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
  - Integración de los recursos materiales y técnicos.
  - Dirección.

<sup>9</sup>Auditoría en Informática. Echenique JA, pp20

- Costos y controles presupuestales.
- Controles administrativos del área de procesos electrónicos.

B) La evaluación de los sistemas y procedimientos, y de la eficiencia y eficacia que se tienen en el uso de la información, lo cual comprende:

- Evaluación del análisis de los sistemas y sus diferentes etapas.
- Evaluación del diseño lógico del sistema.
- Evaluación del desarrollo físico del sistema.
- Control de proyectos.
- Control de sistemas y programación.
- Instructivos y documentación.
- Formas de implantación.
- Seguridad física y lógica de los sistemas.
- Confidencialidad de los sistemas.
- Controles de mantenimiento y forma de respaldo de los sistemas.
- Utilización de los sistemas.
- Prevención de factores que puedan causar contingencias; seguros y recuperación en caso de desastre.
- Productividad.
- Derechos de autor y secretos industriales.

C) La evaluación del proceso de datos y de los equipos de cómputo que comprende:

- Controles de los datos fuente y manejo de cifras de control.
- Control de operación.
- Control de salida.
- Control de asignación de trabajo.
- Control de medios de almacenamiento masivos.
- Control de otros elementos de cómputo.
- Control de medios de comunicación.
- Orden en el centro de cómputo.

D) Seguridad y confidencialidad de la información.

- Seguridad física y lógica.
- Confidencialidad.
- Respaldos.
- Seguridad del personal.
- Seguros.
- Seguridad en la utilización de los equipos.
- Plan de contingencia y procedimientos de respaldo para casos de desastre.
- Restauración de equipos y de sistemas.



## 1.2 TIPOS DE AUDITORÍA EN INFORMÁTICA

Se explicará a continuación las áreas donde la Auditoría en informática se desempeña logrando sus objetivos.

### "Auditoría informática de explotación:"

La explotación informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fábrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la explotación informática se dispone de una materia prima, los datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar explotación consiste en auditar las secciones que la componen y sus interrelaciones. La explotación informática se divide en tres grandes áreas: planificación, producción y soporte técnico, en la que cada cual tiene varios grupos.

#### Control de entrada de datos:

Se analizará la captura de la información en soporte compatible con los sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a norma.

#### Planificación y recepción de aplicaciones:

Se auditarán las normas de entrega de aplicaciones por parte de desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la documentación de las aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con desarrollo para la planificación a medio y largo plazo.

#### Centro de control y seguimiento de trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación informática ejecuta procesos por cadenas o lotes sucesivos (Batch\*), o en tiempo real (Tiempo Real\*). Mientras que las aplicaciones de teleproceso están permanentemente activas y la función de

TESIS CON  
FALLA DE ORIGEN

explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de explotación.

En muchos centros de proceso de datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

\*Batch y tiempo real:

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

*Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.*

Operación. Sala de computadoras:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificará la existencia y grado de uso de los manuales de operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada operador desde el último curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de control de red y centro de diagnosis:

El centro de control de red suele ubicarse en el área de producción de explotación. Sus funciones se refieren exclusivamente al ámbito de las comunicaciones, estando muy relacionado con la organización de software de comunicaciones de técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todas las líneas asociadas al sistema. El centro de diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de software como de hardware. El centro de diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en

TESIS CON  
FALLA DE ORIGEN

un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del centro, es necesario analizarlo simultáneamente en el ámbito de usuario.

**"Auditoría informática de desarrollo de proyectos o aplicaciones:"**

La función de desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una aplicación recorre las siguientes fases:

- Prerrequisitos del usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Preprogramación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costos, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoría de aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. *Revisión de las metodologías utilizadas:* Se analizarán éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de las mismas.
2. *Control Interno de las Aplicaciones:* se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de desarrollo:
  - Estudio de viabilidad de la aplicación. (importante para aplicaciones largas, complejas y caras)
  - Definición lógica de la aplicación. (Se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto)
  - Desarrollo técnico de la aplicación. (Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles)

TESIS CON  
FALLA DE ORIGEN

- Diseño de programas. (Deberán poseer la máxima sencillez, modularidad y economía de recursos)
  - Métodos de pruebas. ( Se realizarán de acuerdo a las Normas de la Instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales)
  - Documentación. (Cumplirá la normativa establecida en la instalación, tanto la de desarrollo como la de entrega de aplicaciones a explotación)
  - Equipo de programación. (Deben fijarse las tareas de análisis puro, de programación y las intermedias. En aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos).
3. *Satisfacción de usuarios:* Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la aplicación.
4. *Control de Procesos y Ejecuciones de Programas Críticos:* El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podrían provocar, desde errores de bulto que producirían graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las librerías de programas; aquellos programas fuente que hayan sido dados por bueno por desarrollo, son entregados a explotación con el fin de que éste:
1. Copie el programa fuente en la librería de fuentes de explotación, a la que nadie más tiene acceso
  2. Compile y monte ese programa, depositándolo en la librería de módulos de explotación, a la que nadie más tiene acceso.
  3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como este sistema para auditar y dar el alta a una nueva aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta aplicación use la aplicación como si la estuviera usando en producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Sign Off ("Esto está bien"). Toda esta revisión, auditoría lo tiene que controlar, tiene que evaluar que la revisión sea correcto, que exista

TESIS CON  
FALLA DE ORIGEN

un plan de revisión, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan. Auditoría tiene que corroborar que el U.A.T. prueba todo y que el Sign Off del usuario sea un Sign Off por todo.

#### "Auditoría Informática de Sistemas:"

Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones, líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de sistemas.

#### Sistemas operativos:

Engloba los subsistemas de teleproceso, Entrada / Salida, etc. Debe verificarse en primer lugar que los sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los sistemas operativos permite descubrir las posibles incompatibilidades entre otros productos de software básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las librerías más importantes de los sistemas, por si difieren de los valores habituales aconsejados por el constructor.

#### Software básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agrada ni condiciona al sistema. Igualmente, debe considerarse el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.

#### Software de teleproceso (Tiempo Real):

No se incluye en software básico por su especialidad e importancia. Las consideraciones anteriores son válidas para éste también.

#### Tunning:

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de técnica de sistemas. El tunning posee una

TESIS CON  
FALLA DE ORIGEN

naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- Cuando existe sospecha de deterioro del comportamiento parcial o general del sistema
- De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

**Optimización de los sistemas y subsistemas:**

Técnica de sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización\* fueron efectivas y no comprometieron la operatividad de los sistemas ni el plan crítico de producción diaria de explotación.

\*Optimización:

Por ejemplo: cuando se instala una aplicación, normalmente está vacía, no tiene nada cargado adentro. Lo que puede suceder es que, a medida que se va cargando, la aplicación se va poniendo cada vez más lenta; porque todas las referencias a tablas es cada vez más grande, la información que está moviendo es cada vez mayor. Lo que se tiene que hacer es un análisis de performance, para luego optimizarla, mejorar el rendimiento de dicha Aplicación.

**Administración de base de datos:**

El diseño de las bases de datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de técnica de sistemas, y de acuerdo con las áreas de desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de sistemas, se les encomienda también su administración. Los auditores de sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que técnica de sistemas tiene sobre la problemática general de los usuarios de bases de datos.

TESIS CON  
FALLA DE ORIGEN

La administración tendría que estar a cargo de explotación. El auditor de base de datos debería asegurarse que explotación conoce suficientemente las que son accedidas por los procedimientos que ella ejecuta. Analizará los sistemas de salvaguarda existentes, que competen igualmente a explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

#### Investigación y Desarrollo:

Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las compañías del ramo. La auditoría informática deberá cuidar de que la actividad de investigación y desarrollo no interfiera ni dificulte las tareas fundamentales internas.

La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas.

#### "Auditoría Informática de Comunicaciones y Redes:"

Para el Informático y para el auditor informático, el entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc. no son sino el soporte físico-lógico del tiempo real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios).

El auditor de comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la red de comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la inoperatividad informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (Pantallas, servidores de redes locales, computadoras con tarjetas de comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

TESIS CON  
FALLA DE ORIGEN

**"Auditoría de la Seguridad informática:"**

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

*En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.*

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

TESIS CON  
FALLA DE ORIGEN



## Herramientas y Técnicas para la Auditoría Informática:

### **Cuestionarios:**

La auditoría en informática se materializa recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la documentación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

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

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

TESIS CON  
FALLA DE ORIGEN

### *Entrevistas:*

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

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

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

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo.

El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

### *Checklist:*

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la documentación sistemática de sus cuestionarios, de sus checklists.

Hay opiniones que descalifican el uso de los checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de checklist. Salvo excepciones, las checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y habilidad del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de auditoría informática guardan sus checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar el checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que se ponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de los checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

TESIS CON  
FALLA DE ORIGEN

### **Trazas y / o Huellas:**

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática de sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio sistema: Así, los archivos de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log> de dicho sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general. Del mismo modo, el sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc. (La auditoría financiero-contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nóminas, primas, etc.)

### **\*Log:**

El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar cronológicamente que es lo que sucedió con la información que está en el sistema o que existe dentro de la base de datos.

### **Software de Interrogación:**

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente "paquetes de auditoría", capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de archivos y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadores personales y mainframe, de modo que el auditor informático copia en su propia computadora personal la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la compañía.

Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de procesadores de texto, paquetes de gráficos, hojas de cálculo, etc.

**Los principales objetivos de la auditoría informática son los siguientes:**

- **Salvaguardar los activos.** Se refiere a la protección del hardware, software y recursos humanos.
- **Integridad de datos.** Los datos deben mantener consistencia y no duplicarse.
- **Efectividad de sistemas.** Los sistemas deben cumplir con los objetivos de la organización.
- **Eficiencia de sistemas.** Que se cumplan los objetivos con los menores recursos.
- **Seguridad y confidencialidad.**

La auditoría en Informática debe de evaluar todo ( informática, organización del centro de cómputo, computadoras, comunicación y programas), con auxilio de los principios de auditoría administrativa, auditoría interna , auditoría contable/ financiera y , a su vez, pueden ser una herramienta para la realización de cualquiera de las auditorías.

La adecuada salvaguarda de los activos, la integridad de los datos y la eficiencia de los sistemas solamente se pueden lograr si la administración de la organización desarrolla un adecuado sistema de control interno.

Como se ve, la evaluación que se debe desarrollar para la realización de la auditoría en informática debe ser hecha por personas con un alto grado de conocimiento en informática y con mucha experiencia en el área.

La información proporcionada debe ser confiable, oportuna, verídica, y debe manejarse en forma segura y con la suficiente confidencialidad, pero debe estar contenida dentro de parámetros legales y éticos.

TESIS CON  
FALLA DE ORIGEN

### 1.3 EL ENTORNO DE LA INFORMÁTICA.

#### Entorno.

Son las características dominantes del mercado en cada una de las ramas o criterios relacionados con la tecnología de informática, que definen el rumbo de la misma en gran parte de los negocios.

La función de informática ha de estructurar sus servicios y proyectos con base en los requerimientos específicos del negocio, apoyándose en la tecnología de vanguardia que domina el mercado, así como en las tendencias de la misma. El grado de apoyo que se buscará en el medio tecnológico depende en gran medida de la orientación y justificación que se le asigne al enfocarlo a cada estrategia del negocio.

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

- a) **Situación geográfica de los Sistemas:**  
Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- b) **Arquitectura y configuración de Hardware y Software:**  
Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.
- c) **Inventario de Hardware y Software:**  
El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.  
El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d) **Comunicación y Redes de Comunicación:**

En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, poseerán información de las redes locales de la empresa.

No todo lo que ofrece el mercado como estándares y soluciones tecnológicas garantiza el desempeño eficiente de la función de informática en una organización; el auditor en informática deberá verificar la existencia de un análisis costo / beneficio en cada proyecto de inversión orientado a la adquisición de nueva tecnología o estándares (normas) para el uso y manejo de la misma.

En las últimas décadas, el entorno de la información ha sido uno de los campos con mayor ritmo de crecimiento en todas sus áreas de acción, por lo cual existen:<sup>10</sup>

- a) Mejores equipos de cómputo, ya que cuentan con características nunca antes proporcionadas, como conectividad, escalabilidad, etc.
- b) Lenguajes de programación y paquetes de software más flexibles y dinámicos que permiten a los desarrolladores de aplicaciones ser mas productivos además de ofrecer un alto grado de participación a los usuarios en el proceso de desarrollo e implantación de soluciones de negocio
- c) Innovaciones tecnológicas en telecomunicaciones, ya que se pueden transmitir voz, datos e imágenes. Con ello, se ha logrado enlazar diferentes empresas con clientes y proveedores a través de redes locales (LAN), redes metropolitanas (MAN) y redes abiertas (WAN). Se ha obtenido la capacidad de manejar grandes volúmenes de información, velocidad de transmisión y protección de los datos con la aparición del cable coaxial y la tecnología de redes digitales integradas, por ejemplo.
- d) Metodologías, técnicas y herramientas para la administración de la función de informática y la planeación y desarrollo de sistemas que han venido formalizándose y apegándose a los estándares aceptados a nivel nacional e internacional, lo que ha sido un factor de suma utilidad para el desempeño eficiente de las tareas y servicios inherentes a la informática y a la misma auditoría en informática.
- e) La integración de especialidades profesionales en asociaciones profesionales reconocidas formalmente a nivel nacional, como la Asociación Mexicana de Auditores en Informática (AMAI) e internacional, como la Auditors Association, Inc. (EDP) entre otras. Dichas asociaciones proporcionan la oportunidad a las instituciones y organizaciones privadas y de gobierno de tener un contacto directo y oportuno con los conocedores o impulsores de las tendencias dominantes del medio en sus áreas económica, social y tecnológica, por mencionar sólo algunas.

<sup>10</sup> Auditoría en Informática, Hernández Hernández Enrique, pp22

TESIS CON  
FALLA DE ORIGEN



**Objetivo del auditor en informática al estudiar el entorno y su impacto en el negocio.**

La finalidad principal del auditor es evaluar y dar seguimiento oportuno al conjunto de proyectos de auditoría en informática que serán ejecutadas en un plazo determinado con el fin de apoyar directa o indirectamente las estrategias del negocio, considerando los diversos factores internos y externos que se relacionan con la organización. Es conveniente señalar que cada uno de estos proyectos deberá estar enmarcado en los límites definidos para la función, esto es, debe enfocarse al control, seguridad y auditoría de los diferentes elementos que tengan contacto directo o indirecto con la tecnología informática.

**TESIS CON  
FALLA DE ORIGEN**

#### 1.4 ESTRATEGIAS PARA LA IMPLEMENTACIÓN FORMAL DE LA FUNCIÓN DE AUDITORÍA INFORMÁTICA

##### I) Formalizar la auditoría en informática en la organización a través de:

- a) Justificar el desarrollo de la función de auditoría en informática en el negocio.
- b) Presentar a la alta dirección del documento de justificación
- c) Aprobación de la alta dirección
- d) Difusión de la auditoría en informática en las áreas relacionadas directa e indirectamente con informática.
- e) Desarrollo del proceso de auditoría en informática en el negocio.

##### II) Proporcionar a la empresa o institución un proceso de auditoría en informática permanente con el objeto de garantizar a la alta dirección:

- a) Que la seguridad, políticas y procedimientos sean eficientes y confiables.
- b) Apoyo a los objetivos del negocio al tomar decisiones con base en información que cumpla con los requisitos mínimos exigidos por auditoría, como exactitud, totalidad, autorización, actualización, etc. Así mismo, se cumplirán los requerimientos exigidos de calidad y oportunidad.
- c) La verificación del uso de tecnología de vanguardia que se requiere.
- d) La elaboración y desarrollo formal de un proceso de planeación en informática que se oriente al plan del negocio.
- e) El uso formal de metodologías, técnicas y herramientas por el personal de informática para el desempeño eficiente de sus tareas.
- f) Promover que el personal de informática se desarrolle en un ambiente de profesionalismos y de alta productividad tomando como base sus habilidades, conocimientos y perfiles requeridos por la organización.

##### Curso de acción.

1. Lograr que la alta dirección, las áreas o departamentos usuarios y el personal de informática tomen conciencia de las necesidades de contar con una función de auditoría en informática asegurando y orientando el uso eficiente de los recursos involucrados con la misma.
2. Formalizar un procedimiento que contemple:
  - divulgación
  - asimilación de los planes
  - objetivos
  - beneficios
  - áreas de oportunidad

TESIS CON  
FALLA DE ORIGEN

3. Dar a conocer a los usuarios y personal el grado de compromiso y participación que se requiere por parte de todos los involucrados.
4. Lo primero a lo que se procede una vez autorizado el proyecto es a la planeación y desarrollo formal.
5. El proceso de planeación, primordialmente debe de reflejar las prioridades de la alta dirección, áreas de oportunidad del negocio y evaluaciones que garanticen calidad y uso eficiente de los recursos informáticos.
6. Cubrir las expectativas que justificaron en el proyecto.
7. Preparar una presentación ejecutiva para darle a conocer a la alta dirección todos los proyectos , así como la asignación de los responsables directos.
8. Formalizar las visitas y reuniones necesarias al personal involucrado en el proyecto.
9. Ejecutar el proyecto de al margen de lo planeado.
10. Entregar a la alta dirección informes detallados de cada proyecto.
11. Seleccionar metodología de auditoría en informática, con objeto de orientar los requerimientos actuales y futuros de la organización, tomando en cuenta políticas, procedimientos y estándares.

TESIS CON  
FALLA DE ORIGEN

## 1.5 ESTRUCTURA ORGANIZACIONAL.

### Ubicación jerárquica de la función

El criterio básico de independencia personal jerárquica, es el desempeño de las actividades profesionales en el proceso de evaluación y control que no debe verse afectando por aspectos emocionales ni de autoridad emanados de los responsables e involucrados en el momento de la auditoría. Debemos de ubicar la función auditoría informática en un nivel organizacional que le asegure la independencia y soporte requerido de la alta dirección, a fin de contar con una entidad confiable y eficiente.

Esto se va dando en medida en que la dirección establezca políticas claras que especifiquen que la función del auditor es asegurar el control y la seguridad de todos los elementos relacionados con la informática y que esto es apoyado y aceptado por la alta dirección, para que las áreas involucradas participen brindando su apoyo.

Se recomienda que si la auditoría en informática es ejercida por personal externo a la empresa, el seguimiento, coordinación, apoyo y aprobación del trabajo sea llevado a cabo por la alta dirección.

Ejemplo de Tipos de estructura donde se ubica la auditoría en informática manejada desde el punto de vista externo.

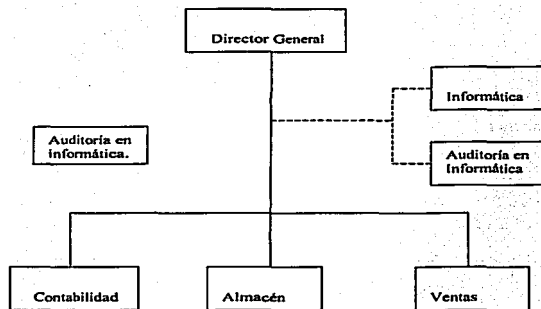
Un objeto primordial para la alta dirección es asegurar que los auditores cuenten con:

- Independencia funcional.
- Libertad de acción.
- Facultad para la toma de decisiones.
- Negociación con los niveles gerenciales.
- Involucramiento en proyectos de alto impacto en el negocio.

Una manera de estructurar la función de auditoría en informática en la organización puede ser a un nivel estratégico o un nivel táctico; por el nivel estratégico se tiene la ventaja de una comunicación formal, de tener apoyo y soporte con la alta dirección, y la característica primordial es la independencia funcional; por el nivel táctico la alta dirección la considera una función indispensable para observar el cumplimiento de políticas y procedimientos de informática, se debilita el compromiso y soporte de la alta dirección, y no hay independencia funcional respecto a otras direcciones. Esto podría variar de acuerdo con el giro de cada organización.

Organizacionalmente la función de auditoría en informática se encuentra dentro del área de auditoría y en un menor número en el área de Informática, teniendo así diferentes enfoques y alcances al momento de ejecutar su trabajo.

TESIS CON  
FALLA DE ORIGEN

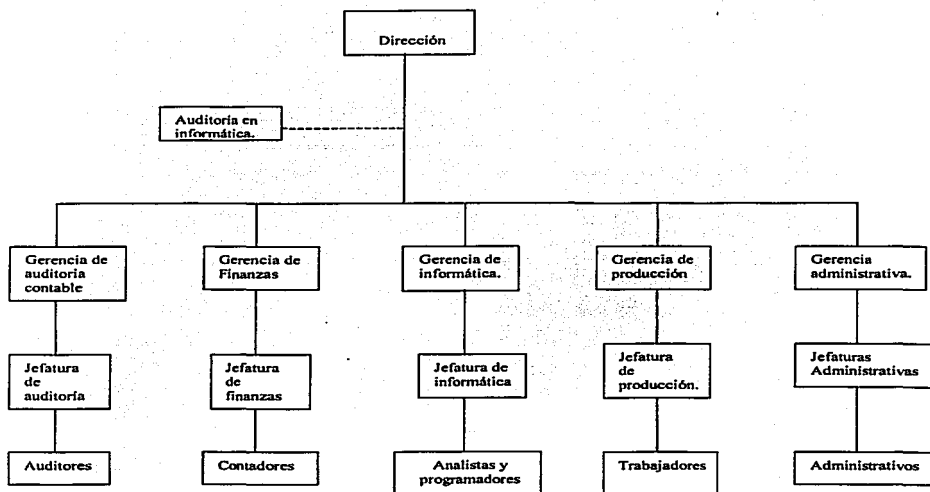


## ESTRUCTURA 1

Asesoría a la pequeña empresa.

En esta estructura se considera a una organización pequeña, donde es indispensable las asesorías ya que es cuando la organización requiere de apoyo para su crecimiento y desarrollo, la informática y la auditoría en informática se maneja externamente, ya que una empresa pequeña no podría tener un departamento de informática por el momento.

TESIS CON  
FALLA DE ORIGEN

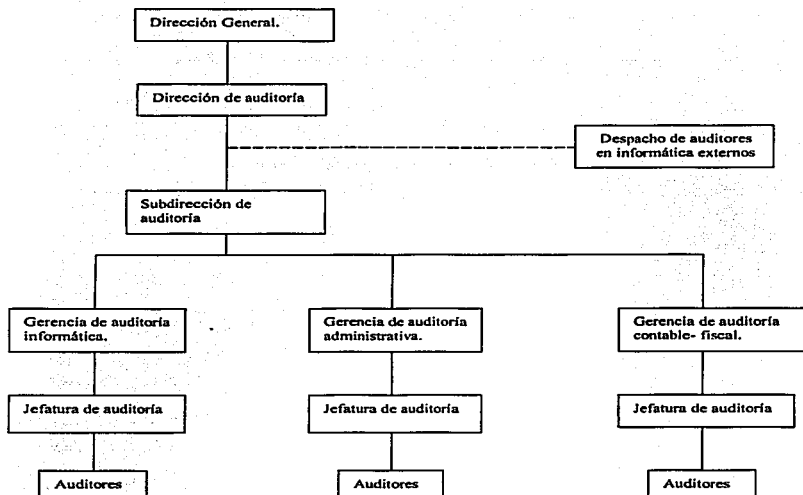


## ESTRUCTURA 2

Asesoría y soporte a la alta dirección.

En esta estructura se maneja como un personal de apoyo la Auditoría en Informática (staff) ubicándose entidad estratégica, hay un compromiso de generar resultados, las áreas se comprometen a cumplir las políticas y controles de informática y es donde se justifica el perfil de ejecutivo del auditor en informática, la alta dirección tiene la ventaja de evaluar constantemente. Tomar en cuenta para un organización mediana, porque su desarrollo es mas cercano y así poder lograr en un futuro la gerencia de auditoría en informática

TESIS CON  
FALLA DE ORIGEN



**ESTRUCTURA 3. (Organigrama parcial)**

Soporte directo al nivel gerencial de auditoría.

Este podría ser la estructura mas funcional para la auditoría en informática externa, como staff, en una empresa grande donde se cuenta con la gerencia de auditoría en informática llevando acabo un trabajo continuo pero el despacho externo es para revisar las funciones de la gerencia de auditoría en informática interna para hacer una exhaustiva revisión y así los proyectos con los asesores serían coordinados por la dirección de auditoría.

Finalmente las diferentes formas de la estructura organizacional dependen de cada organización dando como resultado la elaboración de un conjunto de opiniones experimentadas para así ubicar la auditoría en informática en el nivel que satisfaga las condiciones necesarias para el auditor mostrando el actual plan de organización.

En el presente trabajo se plantea que independientemente del tamaño de la organización realizar auditoría en informática es un proceso sano, que incluye ventajas y como se puede observar en los ejemplos anteriores existen varias posibilidades de insertar el área de auditoría en informática procurando que no resulte una carga costosa para la organización.



## 1.6 ADMINISTRACIÓN DE LA FUNCIÓN DE AUDITORIA EN INFORMÁTICA

Una vez formalizada la función en cualquiera de las situaciones organizacionales señaladas, se define un mecanismo de administración y control de la función.

El mundo complejo de las empresas en el que nos movemos, con industrias emergentes y con una tendencia globalizadora en los negocios, hace muy necesario la buena administración, es así que entonces la función de la auditoría en informática debe realizar un amplio abanico de actividades objetivas.

Este mecanismo garantizará que todos los recursos y proyectos involucrados en el proceso de desempeño y gestión, obediendo los principios básicos de un proceso administrativos.

Los elementos indispensables son:

- La *planeación* la administración de la función implica el desarrollo de una matriz de la planeación de auditoría en informática para determinar áreas que serán en cierto periodo , de los planes de auditoría en informática emanarán los proyectos específicos para cierto periodo.
- El *personal* debe ser seleccionada y reclutada de acuerdo a las habilidades y perfiles establecidas en sus políticas y procedimientos, tomando en cuenta que las habilidades profesionales inherentes de un auditor en informática son: experiencia, educación, adaptabilidad, entendimiento, determinación y diligencia.
- El *control* es llevado por la supervisión oportuna asegurando que las asignaciones a las auditorías sean planeadas apropiadamente para obtener un producto consistente y de calidad, involucrando las áreas y ayudando a la preparación de los planes de la auditoría en informática en el desarrollo y control de los presupuestos de la función.
- Los *reportes de desempeño* son una herramienta para evaluar: productividad y calidad de los proyectos, resultados, avances de los proyectos, áreas susceptibles de control y seguimiento tanto individual y de grupo

Los objetivos principales de la administración de la auditoría en informática:

- Asegurar que la función de auditoría cubra y proteja los mayores riesgos.
- Asegurar que los recursos de informática como hardware, software, telecomunicaciones, servicios, personal sean orientados al logro de objetivos y estrategias.
- Elaboración y difusión de políticas, controles y procedimientos definidos en cada proyecto así como el cumplimiento de estas.

## 1.7 LAS DIFICULTADES DE LA AUDITORÍA DE UNA APLICACIÓN INFORMATIZADA.

La auditoría ha cambiado notablemente en los últimos años con el enorme impacto de las técnicas informáticas así que las dificultades a las que nos enfrentamos para poder llevar a cabo la auditoría no es la elección de la metodología que utilizaremos o los ajustes que se hacen previamente al tener conocimiento de las necesidades del negocio; sino saber explicar en base a estos cambios el apoyo que requerimos para poder desempeñar y lograr los objetivos de la auditoría, ya sea ha mencionado lo importante que es el apoyo del personal de las áreas que serán auditadas, muchas veces existe personal dentro de la organización que esto lo considera externo, y que no son labores obligatorias, entonces el auditor se enfrenta a el convencimiento de estas personas explicando la necesidad que se tiene por analizar el desempeño de los sistemas informáticos ya que de esto depende un mejor trabajo para ellos, al estar teniendo eficiencia y fluidez en sus labores, logrando así una mejora a la organización, que mas adelante se verá proyectada en cifras monetarias.

Ahora bien, por parte de las personas que autorizan el proyecto y dan el visto bueno, el auditor se enfrenta a lo impensable que sería una análisis minucioso de los conjuntos de los registros para así lograr el convencimiento de la alta dirección, y una de las cosas que un auditor debe de explicar desde un principio es la realidad de los objetivos que pueden ser alcanzados en la auditoría, pero no hay que ser tan pesimistas ya que una de las partes a las que se enfrentan actualmente los negocios, a nivel internacional primordialmente son los 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.

Dejando ver la rapidez de los cambios, los directivos tomaran conciencia de que para evitar fallos de control significativos deben reevaluar y reestructurar sus sistemas.

La manera en que se evitan las dificultades para la aceptación de la auditoría es la explicación de la actuación proactiva antes de que surjan los problemas. Tomando medidas audaces para su propia tranquilidad, así como para garantizar a los consejos administración, accionistas, comités como por ejemplo, que a la empresa le serán diseñados adecuadamente los controles para hacer frente a los retos del futuro y asegurar la integridad en el momento actual.

Logrando así que el auditor obtenga todo el apoyo necesario de toda las áreas necesarias y la confianza para que se le proporciona el acceso a toda la información necesaria concluyendo con calidad el proyecto.

TESIS CON  
FALLA DE ORIGEN

## 2. ANALISIS DE LAS PROPUESTAS EXISTENTES.

En este capítulo se hará un análisis de las metodologías de diferentes autores, ya que cada autor tiene un método diferente de llevar a cabo una auditoría en informática.

Cada uno de los autores que se han elegido, dentro de la auditoría en informática se han desempeñado de manera amplia en este campo y cuentan con gran experiencia, la cual será el motivo de estudio en este capítulo.

Método "es el modo de decir o hacer con orden una cosa", así mismo define la palabra Metodología "como un conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal."<sup>11</sup>

La informática es una ciencia compleja que se basa en metodologías, por tanto la auditoría en informática tiene sus métodos que la hacen un trabajo formal.

La proliferación de metodologías en el mundo de la auditoría y el control informáticos se pueden observar en los primeros años de la década de los ochenta, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas. Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas que utilizan estos como práctica habitual.

---

<sup>11</sup>Diccionario de la Lengua de la Real Academia Española.

TESIS CON  
FALLA DE ORIGEN

## 2.1 METODOLOGÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE LA AUDITORÍA INFORMÁTICA DE MARIO PIANTINNI.

Mario Gerardo Piatinni Velthuis, doctor Ingeniero en informática por la Universidad Politécnica de Madrid.

Máster en Auditoría en informática (GENEI).

Especialista en la aplicación de Tecnologías de la Información a la Gestión Empresarial (CEPADE-UPM).

CISA (Certified Information System Auditor) por la ISACA (Information System Audit and Control Association).

Diplomado en Psicología (UNED).

Ha sido director del departamento de desarrollo de la empresa SIE y socio fundador de Cronos Ibérica, S A en la que ha sido director de los departamentos de Formación y Metodologías e Investigación y Desarrollo.

Ha trabajado como consultor y profesor para numerosos organismos y empresas, entre las que destacan:  
Ministerio de Industria y Energía, Ministerio de Administraciones Públicas, Ministerio del Interior, Siemens-Nixdorf, Unisys, Hewlett-Packard, Oracle, ICM, etc.

Actualmente es profesor titular en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en ciudad Real, donde dirige el grupo de investigación Alarcos, especializado en Sistemas de Información, Base de datos e Ingeniero de Software.

Piatinni opina que existen diferencias entre el control informático y la auditoría informática:

El control informático debería ser independiente del departamento controlado. Ya que "por segregación de funciones la informática no debería controlarse así misma". Partiendo de la base de un concepto en el que la seguridad de sistemas abarca un campo mucho mayor de lo que es la seguridad lógica, podríamos decir que:

- El área informática implementa los procesos informáticos seguros.
- El control interno implementa los controles.
- La auditoría Informática evalúa el grado de control.<sup>12</sup>

<sup>12</sup> Auditoría en Informática, Piatinni, pp.68

TESIS CON  
FALLA DE ORIGEN

Conociendo este punto de vista de Piatinni, podríamos decir que existen diferencias muy marcadas entre las funciones de control informático y las de auditoría en Informática.

Mencionaremos las funciones que Piatinni describe tanto para la auditoría en Informática como para el control interno Informático, ya que de este punto partiremos a la metodología que el realiza.

#### La auditoría Informática.

- Tiene la función de vigilancia y evaluación mediante dictámenes, y todas sus metodologías van encaminadas a esta función.
- Tiene sus propios objetivos distintos a los auditores de cuenta, aunque necesarios para que éstos puedan utilizar la información de sus sistemas para sus evaluaciones financieras y operativas.
- Evalúan eficiencia, costo y seguridad en su más amplia visión.
- Operan según el plan auditor.
- Utilizan metodologías de evaluación del tipo cualitativo con la característica de las pruebas de auditoría.
- Establecen planes quincenales como ciclos completos.
- Sistemas de evaluación de repetición de la auditoría por nivel de exposición del área auditada y el resultado de la última auditoría de esta área.
- La función de soporte informático de todos los auditores.

#### Control Interno Informático.

- Tiene funciones propias (administración de la seguridad lógica, etc.).
- Funciones de control dual con otros departamentos.
- Función normativa y del cumplimiento del marco jurídico.
- Operan según procedimientos de control en los que se ven involucrados y que luego se desarrollarán.
- Al igual que en la auditoría y de forma opcional pueden ser el soporte informático de control interno no informático.

Son una gran cantidad de funciones para desarrollarlas desde el inicio de la implementación, pero nos sirve conocerlas para no perder el objetivo que considera Piatinni: el control informático es el componente de la actuación segura entre los usuarios, la informática y control interno, todo esto auditado por los auditores en informática.

TESIS CON  
FALLA DE ORIGEN

Expliquemos que Piatinni maneja 2 metodologías para poder cubrir los 2 aspectos más importantes que el maneja que son:

1. Clasificación de la Información y
2. Procedimientos de control.

1. Para la clasificación de la información maneja la metodología de PRIMA la cual se define en:

- Estratégica (información muy restringida, muy confidencial).
- Restringida (a los propietarios de la información).
- De uso interno (a todos los empleados).
- De uso general (sin restricción).

Siguiendo así los siguientes pasos de la Metodología:

- Identificación de la Información.
- Inventario de entidades de información residentes y operativas.(Inventario de programas, archivos de datos, estructura de datos, soportes de información, etc.)
- Identificación de propietarios.(Son los que usan o custodian la información)
- Definición de jerarquías de información.
- Definición de la matriz de clasificación. (Definir las políticas, estándares, objetivos de control y jerarquías de información).
- Confección de la matriz de clasificación.
- Realización del plan de acciones.(plan detallado de acciones)
- Implantación y Mantenimiento. (Se implanta el plan acciones y se mantiene actualizado).

2. Para la obtención de control maneja otra metodología "La obtención de los Procedimientos de Control", esta metodología nos ayuda a saber si es suficiente y como mejorar el control informático.

Fase I. Definición de objetivos de control.

Tarea 1. Análisis de la empresa. Se estudian los procesos, organigramas y funciones.

Tarea 2. Recopilación de estándares. Se estudian todas las fuentes de información.

Tarea 3. Definición de los Objetivos de Control.

TESIS CON  
FALLA DE ORIGEN

**Fase II. Definición de los Controles.**

Tarea 1. Definición de los Controles.

Tarea 2. Definición de necesidades tecnológicas (hardware y herramientas de control).

Tarea 3. Definición de los procedimientos de control.

Tarea 4. Definición de las necesidades de recursos humanos.

**Fase III. Implantación de los controles.**

Una vez definidos los controles, las herramientas de control y los recursos humanos necesarios, no resta más que implantarlos en forma de acciones específicas.

Terminado el proceso de implantación de acciones habrá que documentar los procedimientos nuevos y revisar los efectuados de cambio.

Finalmente, estas 2 metodologías son las que Piatinni considera para la realización de la Auditoría en Informática, desde mi punto de vista observo que el tener dos metodologías para trabajar propicia que a una se le de mas importancia que a la otra; Para Piatinni es de suma importancia el control interno.

El que Piatinni le de también un trato especial a la información logra manejar mucha seguridad para esta y para todos los responsables.

**TESIS CON  
FALLA DE ORIGEN**

## 2.2 METODOLOGÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE LA AUDITORÍA INFORMÁTICA DE JOSÉ ANTONIO ECHENIQUE.

José Antonio Echenique García, secretario adjunto de la facultad de Contabilidad y Administración de la Universidad Nacional Autónoma de México.

Una parte muy importante que se manejan de manera muy cuidadosa y detallada es la planeación de la auditoría en informática, para Echenique esta debe de contener:

- Objetivos
- Revisión preliminar.
- Revisión detallada
- Examen y evaluación de la información.
- Pruebas de consentimiento.
- Pruebas de controles del usuario.
- Pruebas sustantivas.
- Evaluación de los sistemas de acuerdo al riesgo.
- Investigación preliminar.
- Personal participante.

Y la metodología que Echenique maneja los siguientes puntos:

1. Para la evaluación de la dirección de informática se llevarán a cabo las siguientes actividades:
  - Solicitud de los manuales administrativos, organización, funciones, planes, políticas, estándares utilizados y programas de trabajo.
  - Solicitud de costos y presupuestos de informática.
  - Elaboración de un cuestionario para la evaluación de la dirección.
  - Aplicación del cuestionario al personal y realización de entrevistas.
  - Entrevistas a líderes de proyectos y a usuarios más revelantes de la dirección informática.
  - Análisis y evaluación del informe.
  - Elaboración del informe.
2. Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:
  - Estudios de viabilidad y costo/ beneficio.
  - Solicitud del análisis y diseño de los sistemas en operación y en desarrollo.
  - Solicitud de documentación de los sistemas en operación (manuales técnicos, de operación, de usuario, diseños).
  - Solicitud del plan de trabajo.

TESIS CON  
FALLA DE ORIGEN



- Solicitud de contratos de compra o renta de software.
- Solicitud de licencias y derechos de autor.
- Plan de contingencia y recuperación en caso de desastre.
- Recopilación y análisis de los procedimientos administrativos de cada sistema.
- Análisis de base de datos.
- Análisis de la seguridad lógica y confidencialidad.
- Evaluación de los proyectos en desarrollo, prioridades y personal asignado.
- Evaluación de la participación de auditoría interna.
- Evaluación de controles.
- Evaluación de las licencias, la obtención de derechos de autor y de la confidencialidad de la información.
- Entrevistas con usuarios de los sistemas.
- Evaluación directa de la información obtenida contra las necesidades y requerimientos de los usuarios.
- Análisis objetivo de la estructuración y flujo de los programas.
- Análisis y evaluación de la información compilada.
- Elaboración de informe.

3. Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:

- Solicitud de los estudios de viabilidad, costo / beneficio y características de los equipos actuales, proyectos sobre adquisición o ampliación de equipo y su actualización.
- Solicitud de contratos de compra o renta de los equipos.
- Solicitud de contratos de mantenimiento de los equipos.
- Solicitud de contratos y convenios de respaldo.
- Solicitud de contratos de seguro.
- Bitácoras de los equipos.
- Elaboración de cuestionario sobre la utilización de equipos, archivos, unidades de entrada/salida, equipos periféricos y su seguridad.
- Visita a las instalaciones y a los lugares de almacenamiento de archivos magnéticos.
- Visita técnica de comprobación de seguridad física y lógica de las instalaciones.
- Evaluación técnica del sistema eléctrico y ambiental de los equipos y en general de las instalaciones.
- Evaluación de los sistemas de seguridad de acceso.
- Evaluación de la información recopilada, obtención de gráficas, porcentajes de utilización de los equipos y justificación.
- Elaboración del informe.

TESIS CON  
FALLA DE ORIGEN

**4. Elaboración del informe final, presentación y discusión del mismo, y presentación de conclusiones y recomendaciones.**

Para Echenique la alta dirección juega un papel importante, ya que es en la alta dirección donde se toman las decisiones de un proyecto de auditoría, de esta manera Echenique nos muestra en su libro un ejemplo de propuesta de servicios de auditoría en informática.

La metodología que maneja Echenique es muy concreta, se basa en los objetivos de la auditoría en informática logrando así la auditoría de los sistemas en operación como en desarrollo, evalúa los equipos, se presenta reporte final incluyendo conclusiones y recomendaciones.

El buscar costo / beneficio, logra llegar a la parte que a todos los de la alta dirección les llama la atención y apoyan, ya que se entiende que la auditoría en informática esta beneficiando a la organización a un costo bajo.

Para una empresa que busca eficiencia, esta es una metodología que pudiera acoplarse mas para una auditoría en informática

TESIS CON  
FALLA DE ORIGEN

### 2.3 METODOLOGÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE LA AUDITORÍA INFORMÁTICA DE ENRIQUE HERNÁNDEZ HERNÁNDEZ.

Lic. Enrique Hernández Hernández profesionalista en el campo de la auditoría en informática pretende facilitar e impulsar el desempeño formal de los negocios e instituciones educativas donde se encuentra la tecnología de informática.

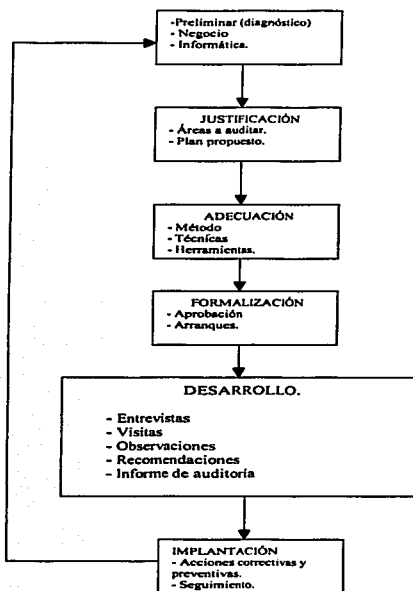
La auditoría en informática debe ser respaldada por un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la empresa. Al igual que otras funciones en el negocio, la auditoría en informática efectúa sus tareas y actividades mediante una metodología.

Esta es la importancia con la que Hernández respalda el uso de una metodología, otro de lo que enuncia respecto al uso de una metodología es que no es recomendable basar esta función en experiencia, habilidades, criterio y conocimientos sin una referencia metodológica.

Hernández nos muestra en una tabla las etapas, productos terminados, requerimientos, responsable e involucrados siendo esto el proceso de su metodología para entonces así tener "un enfoque practico".

TESIS CON  
FALLA DE ORIGEN

Para Hernández con su enfoque práctico se puede presentar de la siguiente manera:



TESIS CON  
FALLA DE ORIGEN

Proceso metodológico general de la auditoría en informática visto con un diagrama de flujo, en la cual las etapas preliminar y justificación son la revisión informal; la adecuación y formalización son la revisión formal y la aprobación formal se da en la etapa de desarrollo para seguir con la implantación.

La estrategia que el autor muestra nos da pauta a que la tomemos en 2 etapas la cual es la revisión informal y la formal, en las cuales se integran todos los pasos para lograr nuestra implantación, esta visión que nos da cubre todas las necesidades para llevar a cabo nuestro proceso de acuerdo a mi punto de vista.

En cualquiera de las metodologías el primer paso es un análisis exhaustivo, ya que se lleva a cabo el diagnóstico del negocio y de informática.

En la justificación se realiza un análisis de riesgo y áreas de oportunidad y esto se lleva a cabo con una matriz de riesgos además se elabora el plan de auditoría en informática que es el que define los responsables de las actividades así como los tiempos.

La adecuación como su nombre lo dice, es donde se busca el plan y la metodología adecuada para nuestro proyecto ya habiendo revisado nuestras áreas de oportunidad, este plan detalla las tareas y tiempos.

La formalización es la aprobación de la alta dirección, comprometiéndose a dar respaldo y apoyo al proyecto.

El desarrollo lo llevamos a cabo después de la aprobación de la alta dirección y nos dedicamos a auditar las áreas seleccionadas dando como conclusión un informe de auditoría en informática; en la implantación se toman las recomendaciones dadas y se tiene que verificar que se esta haciendo el cumplimiento del plan ya elaborado.

Siendo así la manera que Hernández maneja para llevar a cabo la auditoría en informática.

TESIS CON  
FALLA DE ORIGEN

## 2.4 METODOLOGÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE LA AUDITORIA INFORMÁTICA DE YAN DERRIEN.

Yan Derrien, Ingeniero I.D.N., diplomado experto contable, ha ejercido durante varios años las funciones de jefe de proyectos en una S.S.I.I., la SLIGOS.

De 1982 a 1989 dirigió en un importante gabinete de auditoría, el BEFEC, varios dossier de consulta y auditoría en materia de informática, organización y contabilidad.

Actualmente es Director de Estudios en el servicio de auditorías de la Caisse des Dépôts et Consignations.

Yan Derrien tiene un enfoque técnico lo que hace que su metodología se desarrolle con ciertas características muy diferentes a los demás autores que hemos citado a lo largo de este capítulo, así a continuación analizaremos su propuesta.

Para Derrien hay 4 partes que integran lo que llama la "Presentación general de la gestión":

### 1. Los participantes:

En esta parte Derrien comenta acerca del auditor de cuentas, el cual tiene como responsabilidad la verificación de que las cuentas presentadas estén regularizadas, sean verdaderas y que proporcionen una imagen fiel de la situación de la empresa, la presencia de estos auditores la veremos en casi todas las empresas comerciales.

La gestión del auditor de cuentas tiene como objetivo detectar los puntos fuertes y débiles del control interno y también aislar los principales factores de riesgo concernientes a la fiabilidad de las cuentas.

Bajo el término de auditoría en informática hay tres tipos de intervenciones por parte del auditor de cuentas, el primero es un examen de control interno de la función informática, el segundo aborda el examen de aplicaciones informatizadas dando un examen de fiabilidad de las aplicaciones en caso de que los ciclos de la empresa estén altamente informatizadas; Y por último la utilización de la informática para controles contables.

TESIS CON  
FALLA DE ORIGEN

## 2. El plan plurianual de auditoría en informática.

Esto se refiere al conjunto de los componentes de riesgo informáticos planteados a cierto tiempo, esto es difícil de calcular porque todas las empresas tienen diferentes prioridades.

Este es el momento de la primera intervención, haciendo un primer diagnóstico sobre la función informática y se van preparando las misiones futuras.

## 3. El programa anual de trabajo.

El programa establece las fechas, los movimientos y la carga de trabajo como lo puede ser en jornadas-hombre.

## 4. Las herramientas del auditor informático.

Hay herramientas importantes con las cual puede trabajar el auditor en informática para realizar sus actividades; Los métodos de riesgo informáticos y software de auditoría.

Yan Derrien se concreta en 4 puntos como ya los mencionamos, la manera en el que los maneja nos lleva a una intervención a la empresa de manera interna, cuando uno se encuentra dentro de la organización es factible manejar las misiones para así tener un plan para lograr nuestros objetivos y esto es una de las partes que Derrien le da mucha importancia. Además el que se lleve un control de los planes a futuro son los que nos llevan a un control de nuestras actividades y objetivos planteados.

El proceso es incompleto ya que hay muchas situaciones que no son contempladas por el autor. Sin embargo nos ha permitido ver su metodología de un punto de vista diferente.

En función a lo expuesto en este capítulo y basados en las metodologías estudiadas, en el próximo capítulo se presenta la propuesta de metodología la cual es objeto de este trabajo de tesis.

TESIS CON  
FALLA DE ORIGEN

### 3. PROPUESTA DE UNA METODOLOGÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE LA AUDITORÍA EN INFORMÁTICA EN BUSCA DE LA EFICIENCIA.

Este capítulo está dedicado a la formulación de una propuesta de metodología que nos proporcione la eficiencia necesaria para llevar a cabo una auditoría en informática con éxito para ello debemos tener en cuenta que el proceso que se lleva a cabo para lograr nuestros objetivos debe ser llevado a la práctica para que se cumpla el tiempo programado, los costos estipulados así como los resultados esperados.

Cabe mencionar que esta propuesta metodológica ha sido considerada para tamaños de empresas diferentes tales como pequeñas, medianas y grandes; y se basa en las propuestas expuestas en el capítulo precedente. Toda empresa sin tomar en cuenta su tamaño requiere de Auditoría en Informática para poder maximizar la tecnología, métodos y manejo de información entre otros.

Una empresa pequeña, requiere de una amplia supervisión y manejo para poder desarrollarse, la empresa mediana también requiere de esto y agregar tecnología y la empresa grande ya habiéndose desarrollado, con utilización de tecnología de punta buscará la eficiencia de cada uno de sus equipos de cómputo y aplicaciones cuales quiera maneje.

Proponiendo así esta metodología la cual será ajustada a las necesidades requeridas de la empresa, existiendo el paso de adaptación donde se consideran las características de la empresa.

Se recomienda el seguimiento en orden de esta metodología para obtener los resultados de cada fase y lograr llevar a cabo la auditoría en informática de la empresa elegida.

Conociendo los puntos más importantes podemos sugerir lo siguiente:

Metodología para el desarrollo e implantación de la auditoría en informática en busca de la eficiencia.

TESIS CON  
FALLA DE ORIGEN



### 3.1 ETAPA DE PREAUDITORÍA.

Quando un auditor es solicitado por alguna empresa, este no tiene un conocimiento de la misma, para este requiere de un tiempo, para conocer puntos muy específicos y así el auditor realice un diagnóstico en el cual se examinen las funciones y actividades generales de la informática, en la organización.

Y debe tener conocimiento de:

- 1) Organigrama: en el cual encontramos la estructura oficial de la organización.
- 2) Departamentos: de estos describirá brevemente las funciones de cada uno de ellos.
- 3) Relaciones Jerárquicas y funcionales entre órganos de la Organización: el auditor verificara las relaciones funcionales y jerárquicas
- 4) Flujos de Información: estos nos ayuda a encontrar si en la organización se han llevado a cabo canales alternativos de información, sin los cuales no podrían ejercerse con eficacia estos son producidos por fallos en la estructura.
- 5) Políticas referentes a informática: esto es con el fin de saber la manera en que organizan y ejercen control.
- 6) Número de Puestos de trabajo: esto nos sirve para encontrar si hay alguna labor idéntica realizada por personas diferentes bajo el mismo nombre.
- 7) Apoyo al negocio: el auditor debe de saber cual es el apoyo que se requiere de la función de informática, el apoyo para la alta dirección, las gerencias, niveles operativos.
- 8) Fortaleza de informática: estas pueden ser propuestas por la alta dirección, usuarios o informática.
- 9) Debilidades de informática: estas pueden ser propuestas por la alta dirección, usuarios o informática.

10) **Áreas de oportunidad:** es donde se detectan todas las características que facilitarán la implantación de soluciones brindadas por informática, teniendo un impacto relevante en el negocio.

En esta fase del proceso metodológico se estiman las áreas de informática que se auditarán y nos damos una idea del tiempo, costos, recursos que necesitaremos para llevar a cabo nuestro proyecto con esto tenemos una visión mas clara y objetiva del lugar donde se desarrollará el proyecto.

En el diagrama de flujo que aparece al final del capítulo podemos observar que si se cumple el resultado esperado el cual es obtener el conocimiento previo de la empresa que van a ser auditadas y con esta información el auditor podrá decidir si esta empresa es óptima para que le sea realizada una auditoría en informática, con base en el conocimiento previo de la organización, pasaremos a la siguiente fase de lo contrario volvemos a esta etapa ya que no podremos continuar sin esta información.

### 3.2 ETAPA DE INICIO.

#### *Justificación.*

En esta fase se justifica la revisión o evaluación de las áreas o funciones críticas relacionadas con informática.

Para ello nos apoyaremos en:

- Matriz de riesgos: definiendo las áreas que serán auditadas, así como las de mayor riesgo.

Las áreas serán diagnosticadas pudiendo variar según el tamaño y estructura del negocio.

- Plan general de auditoría en informática: una vez elaborada la matriz de riesgo se procede a la formulación del plan general de informática, en el cual básicamente se plantea las tareas, los tiempos y costos, teniendo en cuenta:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- En el plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- En el plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El plan establece disponibilidad futura de los recursos durante la revisión.
- El plan estructura las tareas a realizar por cada integrante del grupo.
- En el plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Esta fase es en la cual se busca la aprobación del proyecto es por ello que es muy importante lograr que el plan que se esta elaborando contenga la información mas relevante que se tomará en cuenta para el proyecto; Así que como se muestra en el diagrama de flujo debemos obtener los resultados para poder continuar.

TESIS CON  
FALLA DE ORIGEN

### *Formalización.*

Esta fase es la que involucra la autorización de la alta dirección, el objetivo primordial es la justificación del desarrollo del proyecto con base en todos los argumentos y detalles encontrados, analizados en las fases anteriores.

Se recomienda que el auditor en informática documente lo expuesto en cada entrevista explicando los puntos tratados y las conclusiones.

Tomar muy en cuenta 3 puntos muy importantes a especificar en esta fase que son:

- **Prioridades:** Acciones que deben llevarse a cabo antes que las demás sugeridas en el proyecto, ya que de alguna manera tienen mas urgencia el mejorar un hecho.
  
- **Restricciones:** Hechos o circunstancias identificables que afectarán directa o indirectamente el proyecto, estas pueden ser limitaciones que no se podrán resolver inmediatamente.
  
- **Alcance:** Específicamente los que el proyecto abarca, cubre, resultados esperados.

Después de esto se hace la presentación formal del plan de auditoria en informática, contando con todo lo documentado a presentar, buscando la manera de explicar la importancia del proyecto.

En el siguiente paso la alta dirección da su autorización; algunas veces se realizarán cambios o aclaraciones, se autorizan las fechas de inicio del proyecto, y si no se ha logrado la autorización se continua justificando y documentando hasta lograr este paso; si se autoriza el proyecto sin ningún cambio se procede a la firma del contrato. También se corre el riesgo que en esta fase nos cancelen el proyecto.

TESIS CON  
FALLA DE ORIGEN

### 3.3 ETAPA DE ANÁLISIS

#### *Análisis detallado.*

La primera fase que se debe llevar es un análisis detallado del proyecto a emprender, para esto debemos dar a conocer los objetivos generales y particulares a las personas que realizan la auditoría conociendo las pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez explicados y analizado los objetivos estos se añadirán a toda la auditoría en Informática.

Los resultados de esta fase son la comprensión y detalle de nuestros objetivos así como las metas de modo que se cubran los requerimientos del cliente. En el diagrama de flujo no podemos continuar hasta cumplir con estos resultados, al cumplir continuamos con la fase siguiente.

### **Entorno.**

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando:

- a) **Situación geográfica de los Sistemas:**  
Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- b) **Arquitectura y configuración de Hardware y Software:**  
Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías.
- c) **Inventario de Hardware y Software:**  
El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.  
  
El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.
- d) **Comunicación y Redes de Comunicación:**  
En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.  
Igualmente, poseerán información de las Redes Locales de la Empresa.

Los resultados que debemos obtener de esta fase son:

- Conocer los responsables de cada área donde se procesen datos de la empresa.
- Conocer la configuración y arquitectura de los equipos con los que cuenta la empresa.
- Conocer las políticas lógicas.
- Conocer la información del hardware y software así como toda la información respecto a las redes locales de la empresa.

TESIS CON  
FALLA DE ORIGEN

### *Determinación de recursos*

Es indispensable saber cuales son los recursos con los que contamos para poder pasar a nuestra siguiente fase, así que tomaremos en cuenta lo siguiente:

- Recursos materiales.

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente. Los recursos materiales del auditor son de dos tipos:

#### A) Recursos materiales software

*Programas propios de la auditoria:* Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

*Monitores:* Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

#### B) Recursos materiales hardware

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado.

Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas, etc.

- Recursos humanos.

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable.

Este tema lo mencionaremos ampliamente en el capítulo 4.

Los resultados que debemos obtener de esta fase serán los recursos con los que contamos para llevar a cabo la auditoria en informática, tales como software para la auditoria y cuantas computadoras o equipo de hardware nos proporcionaran.

TESIS CON  
FALLA DE ORIGEN

### **Formalización.**

Esta fase es la que involucra la autorización de la alta dirección, el objetivo primordial es la justificación del desarrollo del proyecto con base en todos los argumentos y detalles encontrados, analizados en las fases anteriores.

Se recomienda que el auditor en informática documente lo expuesto en cada entrevista explicando los puntos tratados y las conclusiones.

Tomar muy en cuenta 3 puntos muy importantes a especificar en esta fase que son:

- **Prioridades:** Acciones que deben llevarse a cabo antes que las demás sugeridas en el proyecto, ya que de alguna manera tienen más urgencia al mejorar un hecho.
- **Restricciones:** Hechos o circunstancias identificables que afectarán directa o indirectamente el proyecto, estas pueden ser limitaciones que no se podrán resolver inmediatamente.
- **Alcance:** Específicamente los que el proyecto abarca, cubre, resultados esperados.

Después de esto se hace la presentación formal del plan de auditoría en informática, contando con todo lo documentado a presentar, buscando la manera de explicar la importancia del proyecto.

En el siguiente paso la alta dirección da su autorización; algunas veces se realizarán cambios o aclaraciones, se autorizan las fechas de inicio del proyecto, y si no se ha logrado la autorización se continúa justificando y documentando hasta lograr este paso; si se autoriza el proyecto sin ningún cambio se procede a la firma del contrato. También se corre el riesgo que en esta fase nos cancelen el proyecto.

**TESIS CON  
FALLA DE ORIGEN**



### 3.3 ETAPA DE ANÁLISIS

#### *Análisis detallado.*

La primera fase que se debe llevar es un análisis detallado del proyecto a emprender, para esto debemos dar a conocer los objetivos generales y particulares a las personas que realizan la auditoría conociendo las pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez explicados y analizado los objetivos estos se añadirán a toda la auditoría en Informática.

Los resultados de esta fase son la comprensión y detalle de nuestros objetivos así como las metas de modo que se cubran los requerimientos del cliente. En el diagrama de flujo no podemos continuar hasta cumplir con estos resultados, al cumplir continuamos con la fase siguiente.

**Entorno.**

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando:

- a) **Situación geográfica de los Sistemas:**  
Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- b) **Arquitectura y configuración de Hardware y Software:**  
Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías.
- c) **Inventario de Hardware y Software:**  
El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.  
  
El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.
- d) **Comunicación y Redes de Comunicación:**  
En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.  
Igualmente, poseerán información de las Redes Locales de la Empresa.

Los resultados que debemos obtener de esta fase son:

- Conocer los responsables de cada área donde se procesen datos de la empresa.
- Conocer la configuración y arquitectura de los equipos con los que cuenta la empresa.
- Conocer las políticas lógicas.
- Conocer la información del hardware y software así como toda la información respecto a las redes locales de la empresa.

TESIS CON  
FALLA DE ORIGEN

### ***Determinación de recursos***

Es indispensable saber cuales son los recursos con los que contamos para poder pasar a nuestra siguiente fase, así que tomaremos en cuenta lo siguiente:

- Recursos materiales.

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente. Los recursos materiales del auditor son de dos tipos:

#### **A) Recursos materiales software**

*Programas propios de la auditoria:* Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

*Monitores:* Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

#### **B) Recursos materiales hardware**

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado.

Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas, etc.

- Recursos humanos.

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable.

Este tema lo mencionaremos ampliamente en el capítulo 4.

Los resultados que debemos obtener de esta fase serán los recursos con los que contamos para llevar a cabo la auditoría en informática, tales como software para la auditoría y cuantas computadoras o equipo de hardware nos proporcionaran.

TESIS CON  
FALLA DE ORIGEN

### Adaptación.

Esta fase se enfoca en el análisis, adecuación y actualización detallados de todos los elementos que intervienen en un proyecto de auditoría en informática.

Las tareas de esta fase ejecutadas nos llevan a la adecuación de todo el proyecto a las características del negocio, tomando muy en cuenta el cumplimiento de estándares, políticas y procedimientos.

Una vez especificados todos los requerimientos de éxito y conociendo los factores tecnológicos, humanos que intervienen, el auditor puede actualizar el plan de trabajo y detallar las fechas, tiempos, funciones y responsabilidades y ahora si poder estimar gastos y el número de personas que participaran en el proyecto.

Además se definen las técnicas y herramientas necesarias para la revisión adecuada y eficiente.

Una de la técnicas mas importantes son los cuestionarios los cuales son nuestro apoyo en la evaluación, y se derivan entrevistas, visitas a los departamentos, etc.

Los cuestionarios deben tener la característica fundamental de una buena estructuración para obtener información confiable del personal entrevistado.

En esta propuesta de metodología se plasma la idea de apoyarse en tecnologías de información como lo pueden ser:

- Redes de computadoras y sus servicios (correo electrónico, internet, etc.)
- Base de datos para procesar los cuestionarios y almacenar toda la información referente al proyecto.
- Procesadores y hojas de cálculo para el desarrollo de gráficas, estadísticas y documentos de informe.
- Un software para el desarrollo y seguimiento del proyecto.

En cuanto al análisis de Hardware se recomienda el uso de programas de Benchmark, monitores de flujos de información en redes (para ruteadores, switches, etc.)

Como resultado de esta fase definiremos las técnicas y herramientas, se elaboran los cuestionarios, mas no se utilizan aún.

TESIS CON  
FALLA DE ORIGEN

### 3.4 ETAPA DE DESARROLLO.

#### *Uso de técnicas y herramientas.*

Esta fase es la mas importante ya que da inicio la parte práctica del proyecto, en esta etapa es donde el auditor pone de manifiesto toda sus conocimientos, profesionalismo, técnicas, experiencia profesional, ética, etc.

Esta fase comprende:

- Concertación de fechas para entrevistas, visitas, aplicaciones de cuestionarios.
- Clasificación de técnicas y herramientas.
- Efectuar entrevistas.
- Aplicar cuestionarios.
- Efectuar visitas de verificación.
- Elaborar informe preliminar
- Elaborar plan de implantación.
- Aprobar informe preliminar y plan de implantación.
- Aprobar informe final.

Las actividades mas importantes del auditor en informática en esta fase son las de ejecutar las tareas de acuerdo con el plan detallado, respetar el proceso metodológico, coordinar los recursos humanos con eficiencia, impulsar apoyo de la alta dirección, documentar las entrevistas, visitas, cuestionario, debilidades, falta de políticas y procedimiento de control para poder lograr una eficiencia en cada una de las actividades del realizadas por el auditor en informática en el proyecto.

En el diagrama de flujo esta es una de las fases mas importantes ya que si nuestra elección de técnicas y herramientas fue erróneo nos llevara a un proceso delicado después de nuestra implantación.

TESIS CON  
FALLA DE ORIGEN

### *Implementación.*

En esta fase se ejecutan las acciones en los tiempos definidos en el plan, se asignan los usuarios de informática responsables de la implantación, el apoyo de la alta dirección sigue siendo de suma importancia para facilitar la realización de esta fase.

El resultado de esta fase es el logro de los tiempos cubriendo todo el plan propuesto en la fase de justificación. Llamado en nuestro diagrama de flujo como el éxito obtenido, continuamos con nuestro dictamen y se programan revisiones posteriores que aseguren a la empresa el funcionamiento del proyecto.

TESIS CON  
FALLA DE ORIGEN

### 3.5 ETAPA FINAL

#### *Informe.*

Una vez que el proyecto de Auditoría en informática ha terminado se elabora un documento final en el cual se expliquen los objetivos, observaciones, recomendaciones y conclusiones del proceso.

La característica mas importante que debe cubrir este informe es la veracidad de la información para que tanto las consideraciones y conclusiones que se ofrezcan sean con la certeza de que los datos son reales y de buena fuente.

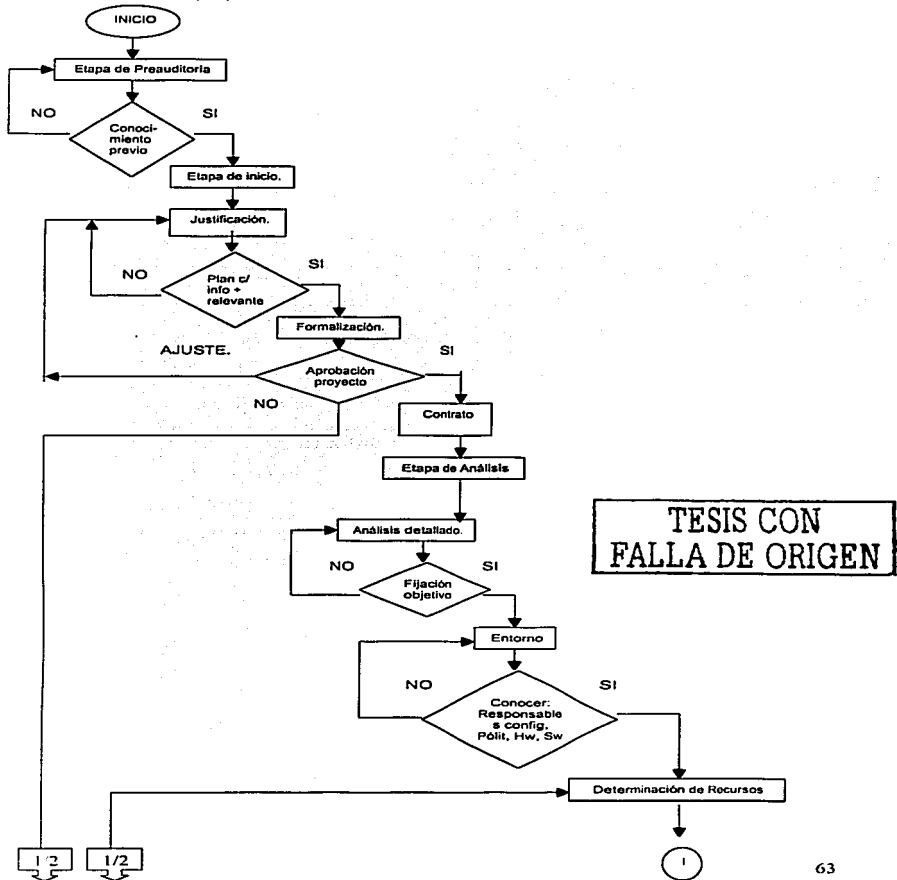
El informe final ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias

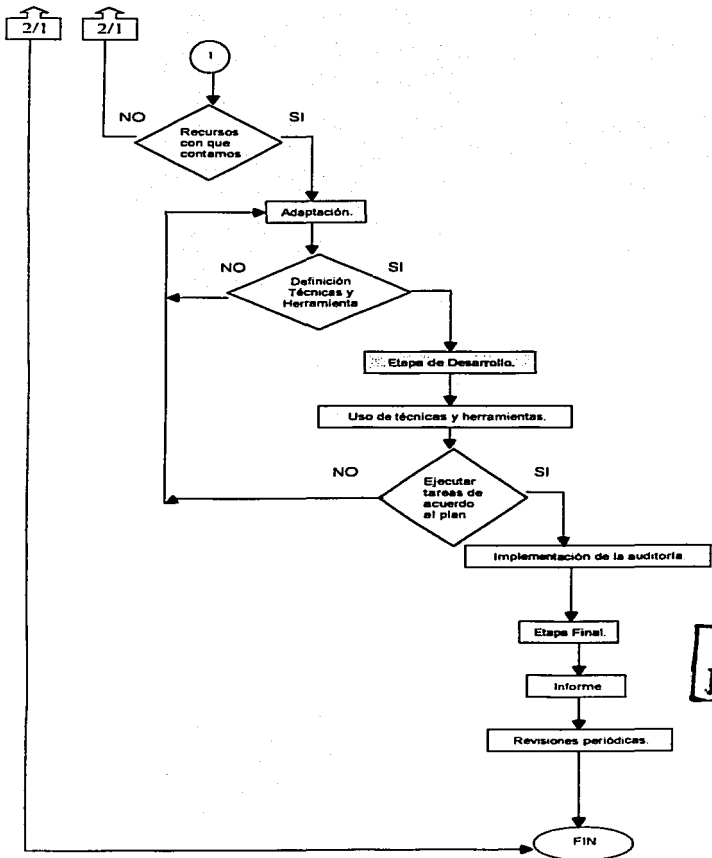
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- Contendrá recomendaciones y soluciones para cada observación.
- Reflejar las áreas de oportunidad y cursos de acción, estas áreas son detectadas en el transcurso del proyecto por el auditor en informática.

TESIS CON  
FALLA DE ORIGEN

Por medio de este diagrama de flujo podemos apreciar la metodología propuesta.







**TESIS CON FALLA DE ORIGEN**

#### 4. CARACTERÍSTICAS Y ÉTICA DEL AUDITOR EN INFORMÁTICA.

##### 4.1 Perfil del auditor informático.

Una vez hecha la propuesta de metodología en el capítulo anterior definiremos aquí las características que de acuerdo a esa propuesta debe tener el profesional de la informática que realice trabajos de auditoría.

La persona que integre esta función debe contemplar en su formación básica ser Licenciado en Informática y para los casos de administración, legales, fiscales, financieros, etc. se asesorará de profesionales expertos en esas áreas.

Conocimientos básicos que debe tener el Lic. en Informática:

- Desarrollo informático; gestión de proyectos y del ciclo de vida de un proyecto de desarrollo.
- Gestión del departamento de sistemas.
- Análisis de riesgos en un entorno informático.
- Sistemas operativos.
- Telecomunicaciones.
- Gestión de base de datos.
- Redes locales.
- Seguridad física.
- Operaciones y planificación informática; efectividad de las operaciones y del rendimiento de los sistemas.
- Gestión de la seguridad de los sistemas y de la continuidad empresarial a través de planes de contingencia de la información.
- Gestión de problemas y de cambios en entornos informáticos.
- Administración de datos.
- Ofimática.
- Comercio electrónico.
- Prospectiva tecnológica.
- Encriptación de datos.<sup>13</sup>

Para Piattini una de las características que el auditor informático debe tener siempre el concepto de Calidad total; como parte de un colectivo empresarial ya sea como un auditor interno o externo, el concepto de calidad total hará que sus conclusiones y trabajo sea reconocido como un elemento valioso dentro de la organización y que los resultados sean aceptados en su totalidad.

<sup>13</sup> Auditoría informática, Piattini, pp.111

TESIS CON  
FALLA DE ORIGEN

Además de lo anterior otras características del auditor en informática son:

- Habilidad de comunicación: tanto oral como escrita.
- Habilidad para el continuo desarrollo: pericia profesional
- Habilidades de manejo de conflictos: manejar los conflictos con un criterio amplio.

Para la constitución del equipo de Auditoría en Informática podemos considerar la siguiente tabla de Perfiles Profesionales de los auditores informáticos.

<b>Profesión</b>	<b>Actividades y conocimientos deseables</b>
<b>Informático Generalista</b>	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
<b>Experto en Desarrollo de Proyectos</b>	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
<b>Técnico de Sistemas</b>	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
<b>Experto en Bases de Datos y Administración de las mismas</b>	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
<b>Experto en Software de Comunicación</b>	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
<b>Experto en Explotación y Gestión de CPD'S (centro de procesamiento de datos)</b>	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
<b>Técnico de Organización</b>	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
<b>Técnico de evaluación de Costos</b>	Economista con conocimiento de Informática. Gestión de costos.

Sin embargo de acuerdo a lo planteado en este inciso , este grupo deberá ser asesorado por otros profesionistas.

**TESIS CON  
FALLA DE ORIGEN**

#### 4.2 Principios éticos del Auditor en Informática.

Los principios morales en contraposición con los preceptos normativos materiales, deben ser asumidos individual y colectivamente como propios en forma voluntaria y con independencia.

Los principios contenidos en los códigos deontológicos dan a conocer la obligación moral que tienen los auditores en informática de advertir a la sociedad sobre los riesgos y dependencias que la informática puede provocar y sobre las medidas que deben adoptarse para prevenirlos, debiendo servir los códigos deontológicos de ejemplo y cauce para transmitir sus percepciones.

Ahora bien describiremos los principios que un auditor en informática se le sugiere tomar en cuenta para poder desarrollar una mejora de prestigio y un trabajo con calidad.

- Principio de beneficio del auditado: conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada y no los propios.
- Principio de la calidad: en caso de que los medios ofrecidos por la empresa impidan o dificulten seriamente la realización de la auditoría negarse a realizarla hasta que se le garantice un mínimo de condiciones técnicas.
- Principio de capacidad: el auditor debe estar plenamente capacitado para la realización de la auditoría.
- Principio de cautela: el auditor debe ser consciente de que sus recomendaciones deben estar bien basadas en la experiencia, no haciéndolo por simples intuiciones.
- Principio de la confianza: el auditor debe incrementar su confianza con base en una actuación transparente, basándose en una comunicación mutua.
- Principio del criterio propio: el auditor deberá actuar con criterio propio y no permitir que este sea subordinado por otros profesionistas.
- Principio de discreción: el auditor deberá mantener discreción en la divulgación de los datos, y toda la información que se le haya dado durante la ejecución de la auditoría.
- Principio de fortalecimiento y respeto a la profesión: lograr que se mantenga un respeto las actividades desarrolladas por los auditores.

TESIS CON  
FALLA DE ORIGEN

- Principio de independencia: esto se refiere a lograr una autonomía e independencia en su trabajo ya sea que actúe de manera interna o externa para la empresa.
- Principio de legalidad: el auditor deberá evitar utilizar sus conocimientos para facilitar a los auditados o terceras personas la contravención de la legalidad vigente.
- Principio de no discriminación: el auditor en su actuación previa, durante y posterior a la auditoría deberá negarse a cualquier situación discriminatoria, así mismo mantener una igualdad de trato profesional con la totalidad de personas con las que se tenga que relacionar.
- Principio de publicidad adecuada: la oferta y promoción de los servicios de auditoría deberán ajustarse a las características, condiciones y finalidades perseguidas sin mentir, sin exagerar la capacidad de querer solucionar los problemas.
- Principio del secreto profesional: la confidencialidad y la confianza son las características esenciales de la relación entre el auditado y el auditor, guardando el secreto de los hechos e información que se conozca en el ejercicio de la actividad.

Cabe mencionar que hay mas principios dependiendo el autor, pero los arriba mencionados son los mas relevantes y no repetitivos.

TESIS CON  
FALLA DE ORIGEN

## CONCLUSIONES.

Los centros de cómputo antes no eran planeados para una organización, es mas, no eran tomados en cuenta con alguna importancia, en la actualidad han ido creciendo y su distribución ha cambiado logrando una descentralización, esto hace que su administración sea cada vez mas compleja en áreas críticas y que requiera de evaluaciones periódicas, formales e imparciales, para ello un apoyo exterior con una metodología eficiente ayuda a controlar los centros de cómputo.

Las herramientas específicas definidas en esta propuesta de metodología son utilizadas para lograr que la empresa sea administrada y dirigida eficientemente en el ámbito de las tecnologías de información.

El uso de tecnologías de información facilitan la auditoría en Informática ya que a lo largo del tiempo han ido desarrollándose con el objetivo de utilizarlas para maximizar sus beneficios y así proyectarlo en la actividad que se realice.

Al llevar a cabo una Auditoría en Informática los directivos sabrán si se está administrando y dirigiendo de manera correcta todos los recursos informáticos contando con un proceso de auditoría en informática digerible, práctico y eficiente que facilite tanto el planteamiento oportuno de las recomendaciones, como los cursos de acción requeridos para dar una solución integral. De esta manera, la auditoría en Informática se convierte en un impulsor de las organizaciones para obtener los resultados esperados de dicha tecnología en los tiempos, costos, beneficios, calidad y otros factores recomendados para acercarse a ser una organización de alta calidad y competir en terrenos de las tecnologías de información.

Por último cabe mencionar que esta metodología está a nivel de propuesta y se espera en poco tiempo poder llevarla a la práctica y encontrar de manera total los beneficios que se obtendrán.

TESIS CON  
FALLA DE ORIGEN

## **BIBLIOGRAFÍA.**

**Auditoría en informática "Un enfoque metodológico y práctico".**  
Enrique Hernández Hernández.  
Ed. CECSA  
1 era ed.  
México, 1995.

**Auditoría en informática**  
José Antonio Echenique García  
Ed. Mc Graw Hill  
2nda ed.  
México, 2002

**Auditoría en informática: Un enfoque práctico.**  
Mario Gerardo Piattini Velthuis y Emilio del Peso.  
Ed. Alfaomega, Ra-Ma  
2nda ed. Ampliada y revisada.  
México

**Técnicas de la auditoría informática.**  
Yan Derrien.  
Ed. Alfaomega, marcombo.  
1era ed.  
México, 1995.

**Auditoría de la investigación.**  
Roberto Hernández Sampieri  
Carlos Fernández Collado  
Pilar Baptista Lucio  
Ed. McGraw-Hill  
3era ed.  
México, 2003.

**Benchmarking.**  
Robert C. Camp  
Ed. Panorama  
1 era ed.  
México, 1993.

**TESIS CON  
FALLA DE ORIGEN**

**Auditoría Informática en la empresa\***  
J. José Acha Iturmendi.  
Ed. Paraninfo  
1 era ed.  
México, 1994.

**Programas de Auditoría**  
Francisco Javier Sánchez Alarcón  
Ed. ECASA  
México, 1996

**Arquitectura de computadoras**  
Felix García Merayo  
Javier Portillo García  
Francisco Ormaechea Sahuguillo.  
Eduardo Alcalde Lancharro  
Ed. McGraw-Hill  
México.

**Fundamentos de Informática.**  
L. Alfonso Ureña López.  
Antonio Miguel Sánchez Solana  
María Teresa Martín Valdivia  
José Miguel Mantas Ruiz.  
Ed. Alfaomega RA-MA  
1 era ed.  
México, 1999.

**Metodología de la programación.**  
Osvaldo Cairó Battistutti.  
Ed. Computec  
México, 1996.

**Base de Datos**  
Irene Luque Ruiz.  
Miguel Angel Gómez Nieto.  
Enrique López Espinoza  
Gonzalo Cerruela García  
Ed. Alfaomega RA-MA  
México, 2002.

**Computación Metodología, Lógica computacional y Programación.**  
Ma. Del Rosario Beres Rangel  
Roman Rosales Becerri  
Ed. McGraw Hill  
México, 1993.

**TESIS CON  
FALLA DE ORIGEN**



Introducción a la computación.  
Peter Norton  
Ed. McGraw Hill  
México, 1995.

Conoce las auditorías  
J. R Santillana González  
Ed. ECASA  
México, 1992.

TESIS CON  
FALLA DE ORIGEN