UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINITRACION

LA AUDITORIA APLICADA EN INFORMATICA. (CONTROL Y SEGURIDAD)

SEMINARIO DE INVESTIGACION CONTABLE
QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN CONTADURIA

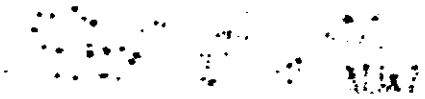
PRESENTA:

HUGO TELLEZ ZAVALA

ASESOR DEL SEMINARIO:

C.P. Y L.A. JOSE ANTONIO ECHENIQUE GARCIA

MEXICO, D.F. 1999



Es una satisfacción muy grande e importante el haber realizado uno de mis más grandes sueños, culminar mis estudios de Licenciatura y gracias a esto he logrado desarrollarme en el ámbito personal y profesional.

A la Universidad Nacional Autónoma de México por se la institución que me permitió forjarme como profesionista.

A la Facultad de Contaduría y Administración por ser la escuela en la que aprendí las bases profesionales.

A mis maestros por la dedicación y la comprensión que me tuvieron, por haber inculcado en mi la inquietud por el estudio y porque gracias a los conocimientos recibidos puedo poner en alto a la máxima casa de estudios.

Con un reconocimiento muy especial les doy las gracias a mis padres Juan y Gloria, porque gracias a su cariño, consejos y gran ayuda moral he logrado cumplir mi sueño, por esta razón estaré eternamente agradecido.

A mis hermanos Rodrigo, Jacqueline y Juan Pablo, por lo que representan para mí.

A mi Abuelita Milagros por su valioso y sincero cariño.

A mi Tío Salvador y Tía Lilia por el apoyo y cariño que siempre me han tenido.

Agradezco al C.P. José Antonio Echenique García por su guía y la confianza que siempre me tuvo.

A la C.P. Martha Valle Solis y al Maestro Enrique Schmidt Orozco por su guía, apoyo y comprensión que me brindaron siempre incondicionalmente.

A Alejandro Ceja por brindarme su apoyo y sincera amistad.

A Martha Avelino Hernandez, por el amor y cariño brindado durante todo este tiempo.

INDICE

INTRODUCCIÓN.

La contabilidad como la sociedad moderna está viviendo un profundo y creciente proceso de automatización cobrando una importancia significativa en el desempeño de las actividades de las organizaciones.

Después del elemento humano, uno de los recursos más valiosos para cualquier organización es sin duda el de la información, siendo el equipo y los sistemas, elementos que ayudan a incrementar ese valor al mejorar su oportunidad, contabilidad, uso y almacenamiento.

Por consiguiente es necesario tener un conocimiento claro de esta área dentro de las organizaciones, ya que, dependiendo del uso que se le dé, puede alcanzar altos niveles de utilidad, o por el contrario puede ser una amenaza potencial para la misma ya que son mayores las carencias en el campo de la organización y la gestión informática, en donde el valor de la información alcanza cifras muy altas, y su utilización resulta cada vez más amplía e imprescindible para la gestión de la propia organización.

Durante el proceso normal de generación de la información, llega un momento en que el volumen es tal, que manejarla en forma manual desde su recopilación y análisis hasta su síntesis, sería demasiado complicado, y es en este momento donde surge la unión del área de informática y la contabilidad dentro de la organización.

Esta área se convierte rápidamente en un factor estratégico ya que utiliza los equipos de cómputo más modernos para el manejo de información desde su capacidad de almacenamiento, como el procesamiento de grandes volúmenes de información. No por eso podemos olvidar que existen riesgos que amenazan el buen funcionamiento de las actividades en una organización.

Estos riesgos se pueden clasificar desde externos o internos, humanos o naturales, accidentales o voluntarias, así como la posibilidad de pérdida con la

capacidad del proceso, la posibilidad de decisiones erróneas y un mal uso de la computadora ocasionan que la información sea vulnerable o susceptible de ser distorsionada, extraviada, destruida o robada. Los efectos de estas vulnerabilidades pueden ser disminuidos, mediante la aplicación y ejercicio de controles. Si estos controles son débiles o inexistentes, la organización estará expuesta a más riesgos, con una mayor probabilidad de ocurrencia y con efectos adversos de mayor repercusión.

La Auditoría en informática es un área de estudio relativamente nueva por lo que la presente investigación ha sido desarrollada con la finalidad de proporcionar al lector conceptos y lineamientos actualizados, la cual surge por la necesidad actual de contar con una función encargada de vigilar el entorno informático, unas de las posibles debilidades que inciden básicamente esta área son:

1. - Toma de decisiones incorrecta.
2. - Abuso del equipo de cómputo.
    3.1. - Valuación del hardware
    3.2. - Valuación del software.
3. - Costos por pérdida de información.
4. - Costos elevados de errores de cómputo.
5. - Seguridad de la información.
    5.1. - Personal
    5.2. - Grupo

El proceso de Auditoría informática se puede concebir como la fuerza que ayuda a las organizaciones a lograr sus objetivos, minimizando las debilidades y riesgos antes mencionados, además de redituar en la integridad de datos y la eficiencia y eficacia de los sistemas de información. Esta función se desarrollará en las organizaciones con base al tamaño, contexto y complejidad de los sistemas.

CAPITULO 1.

METODOLOGÍA.

1.1. JUSTIFICACIÓN.

Para cualquier organización el realizar todas aquellas funciones relacionadas con el desarrollo de la información representan importancia de primer orden dentro de los planes de la Organización. Una de las maneras mediante la cual se logra una parte del objetivo del desarrollo de la información, es mediante la aplicación de Auditorías a sus sistemas las cuales logran elevar la eficiencia individual o colectiva de los departamentos que la desarrollan.

La importancia que reviste la aplicación de una Auditoría no proviene del simple hecho de apegarse a las disposiciones fiscales y legales, la cual obligan a las organizaciones a proporcionar información, la Auditoría debe satisfacer carencias o deficiencias en conocimientos, habilidades o actividades de los sistemas de información.

Es necesario el que toda organización sobresalga dentro del mercado y que se destaque por la calidad del producto o servicio prestado, pues bien, para ello es importante que cuente con la información, por medio de la realización de Auditorías se puede llegar a ese nivel de calidad, por así decirlo.

La aplicación de las Auditorías le brinda a la empresa, un elemento valioso para poder sobrevivir en el mercado.

1.2. PLANTEAMIENTO DEL PROBLEMA.

1.2.1. DEFINICIÓN DEL PROBLEMA.

1. - Desaprovechamiento del equipo de cómputo o incorrecta designación de los recursos computarizados.

2. - Justificar la ineficiencia del personal con fallas del sistema.

3. - Manipulación de datos o introducir intencionalmente datos incorrectos.

4. - Alteración o reproducción de los registros de las bases de datos.

5. - Modificación del software legalmente adquirido con programas no autorizados.

6. - Perdida de datos transmitidos por sistemas de telecomunicación.[1]

1.2.2. OBJETIVOS.

1. - Establecimiento de una planeación en función auditora de los sistemas informativos, en las áreas más importantes de la empresa.

2. - Actuación del auditor informático sobre el entorno del administrador de los sistemas de información de la empresa.

3. - Aplicación de técnicas necesarias para el ejercicio de la función auditora.

---

[1] *CFR. CUEVAS GUZMAN, MA. TERESA, ET. AL; CONTROL Y AUDITORÍA EN* CENTROS DE CÓMPUTO, TESIS DE LICENCIATURA, FACULTAD DE INGENIERÍA, *UNAM, MÉXICO, 1987. PAG. 102-103.*

1.2.3. HIPÓTESIS.

Desarrollar una actividad de análisis y síntesis que ha de tener siempre un sistema de referencia o modelo. El sistema de referencia del auditor informático no es otro que el análisis detallado de los procesos informáticos y con las posibles propuestas de solución.

1.2. TRABAJOS INICIALES.

La investigación consta de cinco capítulos principales y cada uno contiene diversos subcapítulos afines.

En el contenido de cada capítulo se proporcionará diversas citas textuales con objeto de proporcionar una bibliografía que sirva de referencia para obtener mayor información y profundizar en el tema que se desee.

El capítulo I se proporciona los puntos iniciales de toda un investigación con el objeto de proporcionar una referencia para obtener una mayor información de esta investigación.

El capítulo II introduce a los Conceptos Generales que serán tratados y mencionados a lo largo de la investigación, con objeto de formar un criterio y puntos de vista homogéneos; definiciones básicas de control, auditoría, informática y auditoría en informática; así también se propone una ubicación jerárquica del área mencionada en una organización; el idóneo perfil del auditor en informática, y finalmente se identifican las áreas de participación del mismo.

El capítulo III, nos introduce a los aspectos relevantes del desarrollo de Auditorías, así como a los riesgos que conlleva un inadecuado control sobre éstas.

El capítulo IV, expone las técnicas operativas y de control que el auditor informático maneja, así como las principales herramientas de trabajo disponibles para el mismo.

El capítulo V, expone los métodos de trabajo que conducen los pasos del auditor informático, desde la presentación, la revisión, hasta que se entrega el informe final.

1.4. FORMULACIÓN DEL PLAN DE TRABAJO PARA LA INVESTIGACIÓN.

PROGRAMA DE TRABAJO.

AÑO 1998.

MES/ACTIVIDAD	VIII	XI	X	XI	XII	I
MARCO TEORICO.						
1. LAS EMPRESAS.		XX				
METODOLOGIA DE INVESTIGACIÓN.						
1. PROBLEMATICA.		XX				
2. IMPORTANCIA.		XX				
3. OBJETIVOS.		XX				
4. VARIABLES.			XX			
5. HIPOTESIS.			XX			
6. PLAN DE INV.			XX	XX		
7. DES. DE INV.			XX	XX	XX	
OBTENCION DE RESULTADOS.						XX
PRES. Y DISCUSION DE RESULTADOS.						XX

1.5. RECOLECCIÓN DE LA INFORMACIÓN.

La información se recolecto de los siguientes lugares:

Biblioteca Alfredo Adam Adam de la F.C.A.

Datos en INTERNET

Biblioteca Central

Maestros con Experiencia en Auditoría

Instituto Mexicano de Contadores Públicos

CAPITULO 2.

CONCEPTOS GENERALES.

2.1. CONSIDERACIONES PRELIMINARES.

Al finalizar el presente capítulo, el lector tendrá una visión y perspectiva mayor de los conceptos básicos generales, para la mejor comprensión de esta investigación.

2.2. RIESGOS A QUE ESTA EXPUESTA LA INFORMACIÓN.

La parte más vulnerable de las organizaciones de hoy en día es el área de informática, ya que es aquí en donde se encuentra no sólo una gran inversión en equipo, sino aún más importante, la información que sirve de base para el funcionamiento normal de las organizaciones y para una adecuada toma de decisiones.

Al no estar la información y el área de informática protegida ante cualquier eventualidad que pudiera presentarse, estará expuesta a una serie de riesgos que de no ser conocidos, contemplados o controlados podrán repercutir en fatales consecuencias para la empresa.

Antes de desarrollar el tema a mayor detalle, se exponen dos definiciones de riesgo:

"Es el valor de la incertidumbre de que se presente un desastre o contingencia, *medido en términos del número de amenazas posibles*". [2]

"Una acción o evento el cual puede causar una pérdida". [3]

---

[2] Cf. Franco Romo, Alfonso, Et. al., Planención de la Recuperación Informática en caso de desastre, Facultad de Contaduría y Administración, UNAM, México 1990, pág. 8. MIMEO.

[3] Cf. Weber Ron, EDP Auditing. Conceptual Foundations and Practice Edit. Mc Graw-Hill, 2a. Ed., Pág. 248.

El auditor en informática tiene entre sus funciones la responsabilidad de evaluar la eficiencia de las medidas adoptadas para abatir la posibilidad de que los riesgos se materialicen, y en caso de que suceda tener los elementos y controles adecuados para disminuir la pérdida, la posibilidad de recuperación de la información y el restablecimiento de los sistemas en el menor tiempo posible.

Por lo anterior es importante conocer los diferentes riesgos que amenazan a la información y a el área de informática.

2.2.1 RIESGOS EXTERNOS.

Son todos aquéllos que se presentan en el ambiente físico y social que rodea a un centro de trabajo, los cuales, si bien no se pueden eliminar, si es posible tomar las medidas necesarias que minimicen la probabilidad de pérdida de información o destrucción de las instalaciones. A su vez, los riesgos externos se clasifican en tres tipos: naturales, humanos y materiales.

1. -Riesgos naturales

a) Temblor. Se refiere a los movimientos en la corteza terrestre qué pueden afectar en forma parcial o total a las instalaciones.

b) Incendio. Es la propagación de fuego que puede tener como origen la misma instalación o bien en instalaciones adyacentes.

C) Inundación. Fugas o desbordamientos de corrientes de agua, estas representan un peligro muy grande para los equipos de cómputo, por la sensibilidad de los componentes que los integran.

D) Tormenta. Son fenómenos físicos que descargan acumulaciones de energía

eléctrica, estas provocan variaciones de energía, averías en el equipo de Cómputo o al menos impedir que se pueda laborar en condiciones relativamente normales.

Estos riesgos están determinados por la localización geográfica del centro de trabajo y del medio ambiente que lo rodea.

2. - Riesgos humanos.

a) Robo. "Artículo 367 Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley."[4] motivado por la introducción de terceras personas ajenas a la organización, este puede ser tangibles (maquinas, discos) o intangibles (programas, datos).

b) Sabotaje. Igualmente provocado por una persona o grupo de personas que tengan conocimiento del tipo de información que se encuentra dentro del equipo de cómputo.

El sabotaje puede ser interno o externo; esto quiere decir que puede estar dirigido y organizado desde adentro o desde afuera de la Organización

Otra variante es la extorsión, la cual es la utilización de los archivos o programas como medio de presión hacia los dirigentes de una organización.

[4] Cf. Código Penal Anotado, Raúl Caranca y Trujillo Raúl Carranca y Rivas, Editorial Porrúa México 1996, Pág. 911

El código Penal define la extorsión como: "Artículo 390 ...al que sin derecho obligue a otro a hacer, tolerar o dejar de hacer algo, obteniendo un lucro para sí o para otro y causando un perjuicio patrimonial". [5]

c) Motines Sociales. El código Penal define al motín como: "Articulo 131 ... a quien para hacer uso de un derecho o pretextando su ejercicio o para evitar el cumplimiento de una ley, se reúnan tumultuariamente y perturben el orden público como empleo de violencia en las personas o sobre las cosas, o amenacen a la autoridad para intimidarla u obligarla a tomar alguna determinación."[6] Con la definición anterior se puede referir a la destrucción del centro de trabajo como resultado de un conflicto social ajeno a la organización.

d) Fraude. "Artículo 386 Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido".[7]

3. - Riesgos materiales

a) Descompostura de Equipo. Lo que limitará la producción normal del centro de trabajo y generará pérdidas cuantiosas en caso de no obtener los medios necesarios para efectuar las reparaciones pertinentes.

---

[5] Cf. Código Penal Anotado, Raúl Caranca y Trujillo Raúl Carranca y Rivas, Editorial Porrúa México 1996, Pág. 966

[6] Cf. Código Penal Anotado, Raúl Caranca y Trujillo Raúl Carranca y Rivas, Editorial Porrúa México 1996, Pág. 371

[7] Cf. Código Penal Anotado, Raúl Caranca y Trujillo Raúl Carranca y Rivas, Editorial Porrúa México 1996, Pág. 947

b) Fallas de Energía. Sobrecargas o bien bajas de voltaje que afectan la confiabilidad del sistema o que pueden dañar los componentes internos del equipo.

2.2.2. RIESGOS INTERNOS.

Estos tipos de riesgos son los mas comunes dentro de la organización, primordialmente donde se encuentra ubicado el equipo de cómputo. Estos riesgos son más sencillos de preever y en consecuencia, perfeccionar las medidas para contrarrestarlos. Sin embargo y aún cuando parezca contradictorio, la posibilidad de que éstos se manifiesten es muy grande, ya que el conocimiento de los procedimientos operativos y de control interno de la organización facilitará el camino a quien desee hacer un daño irreparable.

Los riesgos internos se clasifican en seis tipos: robo, sabotaje, destrucción, huelga, fraude, errores y omisiones.

1. - Robo

Se clasifica de 3 tipos:

1.1) De Material. Es el robo de los activos flotantes de la organización, tales como: papelería y discos.

1.2) De Recursos. La utilización del tiempo/máquina en aplicaciones, pertenecientes a actividades diferentes y completamente ajenas a la organización.

1.3) De información. Es la sustracción física de los programas, archivos y en general de los datos que se encuentran en un centro de trabajo. Esto también puede dar lugar a la extorsión y abuso de confianza. El código Penal define al abuso de confianza como: "Articulo 382 Al que, con

perjuicio de alguien, disponga para sí o para otra de cualquier cosa ajena mueble, de la que se le haya transmitido la tenencia y no el dominio...".[8]

2. - Sabotaje

Tiene la misma connotación que el inciso (b) de los riesgos humanos externos, con la diferencia de que en este caso, éste se puede presentar a través de los Virus Informáticos. Un virus es un programa que se usa para infectar una computadora, mediante de un código que se oculta dentro de un programa existente. Una vez que el programa se ejecuta, el código del virus se activa y agrega copias de él mismo a otros programas en el sistema. El virus puede variar desde una simple travesura que hace aparecer de repente un mensaje den la pantalla, a la verdadera destrucción de programas y datos.

3. - Destrucción

Se clasifica de 2 tipos:

3.1) De datos.- Archivados en medios electromagnéticos, de documentación y de archivos de respaldo.

3.2) De recursos.- La destrucción física de los elementos que componen a los equipos de cómputo, tales como las unidades de cintas, discos, cualquier equipo periférico.

Se incluyen también los recursos de papelería y soporte que complementan los elementos de producción de un centro de trabajo.

En este caso encontramos que la destrucción, tanto de los datos como de los recursos se puede dar en forma voluntaria como un ataque directo a la organización, o bien

[8] Cf. Código Penal Anotado, Raúl Caranca y Trujillo Raúl Carranca y Rivas, Editorial Porrúa México 1996, Pág. 940

en forma involuntaria debido a errores u omisiones de los operadores o usuarios de un *sistema.*

4. - Huelgas

Del personal, que impedirían el funcionamiento de las actividades ocasionando una paro total en las actividades del centro de trabajo.

5. - Fraudes

En este caso hablamos de los desfalcos, robos, abuso de confianza o utilización indebida, sea de los elementos que se encuentran en el centro de trabajo, o de la información que se maneja, a fin de obtener beneficios que se traducen directamente en pérdidas para la organización.

El fraude informático es cometido de las siguientes maneras:

A.- Desaprovechar el tiempo de computadora o robar recursos computarizados.

B.- Al utilizar a la computadora como pretexto de ineficiencia.

C.- Manipular datos de entrada o introducir intencionalmente datos incorrectos.

D.- Alterar o copiar los registros de la base de datos.

E.- Modificar el software o sustituir programas inválidos para validar información.

F.- Al interceptar datos transmitidos sobre los sistemas de comunicación".[9]

6. - Errores y omisiones

Finalmente la falta de información íntegra y consistente debido a errores y omisiones provocadas por el personal interno en el desarrollo de sus actividades. Este tipo

[9] *Cf.* Cuevas GUZMAN, Ma. Teresa de Jesús, *Et. al*; *Control y Auditoría en Centros de cómputo, TESIS* de Licenciatura, Facultad de Ingeniería, UNAM, México, 1987. Pág. 102-103.

de riesgo es el de mayor incurrencia y es fuente de los principales problemas en el área de sistemas y de las organizaciones en general.

Es importante hacer notar que estos riesgos, en el caso de presentarse, no siempre significarán un beneficio para la persona que lo origina, pero invariablemente se traducirán en pérdidas para la organización tomando en cuenta los efectos secundarios que tendrían alguno de los riesgos antes mencionados, por lo que es necesario reconocer su existencia para estar en posibilidades de contrarrestarlos.

2.2.3. CONTROLES Y MEDIDAS DE SEGURIDAD.

En los dos puntos anteriores se expusieron los diversos riesgos a los que está expuesta la información y el centro de cómputo, la existencia de procedimientos y medidas claramente definidas permitirán garantizar la prevención y detección de los mismos.

Se define como seguridad física " ...a la protección de hardware y software contra daños o destrucción ocasionadas por incendios, inundaciones o sabotaje".[10] La seguridad física es la implantación de medias de seguridad adecuadas que permiten garantizar la integridad del equipo y recursos en el centro de cómputo.

Los objetos principales que se pretenden alcanzar al asegurar físicamente el centro de cómputo son:

a) La reducción de la probabilidad de que ocurra algún siniestro y si este ocurriera reducir sus efectos. Ya que una instalación de cómputo representa una fuerte inversión que es necesaria proteger.

b) Asegurar la continuidad del servicio que otorga a la organización. Ya que es el lugar físico donde se procesa la información necesaria para la toma de decisiones.

[10] Sanders H., Donald, Informática: Presente y Futuro. Edit. McGraw-hill. México, 1985, Pág. 538.

Con los objetivos anteriores se determina que para tener un centro de cómputo operacional se debe evaluar:

1) Ubicación física dentro de la organización: El centro de cómputo deberá estar ubicado en un área que proporcione máxima protección para que no sufra daños, y alcance el máximo de vida útil.

   a) Suministro de energía eléctrica: El centro de cómputo deberá de contar con un adecuado suministro de energía, independiente de cualquier otra instalación, un suministro de energía inadecuado puede dañar al equipo de cómputo.

   b) Orden y limpieza: En este punto aparte de hacer sentir al personal que labora en un buen ambiente de trabajo, evita que se cometan errores u omisiones en el manejo de la información y reduce la posibilidad de un riesgo interno. El orden y la limpieza no pueden lograrse si se realizan de manera ocasional se necesita ser algo continuo y darle la suficiente atención.

   c) Control de acceso: Es la colocación de vigilantes y la implantación de procedimientos de entrada (registros, gafetes y tarjetas de acceso). Los controles de acceso varían según las distintas horas del día, cabe mencionar que es importante asegurar que los controles durante la noche sean tan o más estrictos que durante el día.

   d) Seguridad contra incendios: El fuego es un riesgo alto que amenaza a cualquier tipo de organización, se debe considerar los materiales para la construcción del centro de cómputo sin olvidar las áreas adyacentes al mismo. Será necesario contar con lugares especiales de almacenamiento para

las cintas y los discos así como para toda la documentación de los sistemas y programas, lo mas recurrente es el uso de cajas de seguridad que son resistentes al humo, calor y fuego.

2) Planes de contingencia: Es un plan formal que describe pasos apropiados que se deberán seguir en caso de una emergencia.

3) Planeación para recuperación en casos de desastre: Es un conjunto de procedimientos de recuperación para minimizar las pérdidas, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

4) Seguros: Los Seguros es un contrato por el cual una persona o una organización, se obliga a indemnizar, reparar o compensar perdidas o daños que ocurran en los bienes asegurados que corran un riesgo. El seguro para un centro de cómputo no solamente se debe de asegurar las áreas de evidente riesgo, sino también se debe de incluir los medios de almacenamiento, los programas y sistemas estos se deberán asegurar por el valor de reposición y no por su costo. Se entiende por valor de reposición la cantidad que exigiría la adquisición de un bien nuevo de la misma especie, clase y capacidad, incluyendo el costo de transporte, montaje, impuestos u derechos adherentes si los hubiere. La cobertura del seguro debe revisarse periódicamente para tener la seguridad de que es adecuada a las circunstancias.

2.3. CONTROL.

La obtención de resultados en una organización se basa en gran medida en la eficiencia lograda en las diversas áreas que la forman, y a través de la estructura de control desarrollada e implantada.

Bajo esta premisa es posible garantizar que la probabilidad de riesgo que pudiera afectar el éxito de una organización se mantendrá en niveles mínimos y ante la ocurrencia de algún riesgo, se contará con medidas preventivas que permitirán disminuir con oportunidad y eficiencia los efectos que de ésta se deriven.

Se puede afirmar que uno de los propósitos fundamentales de la Auditoría en informática será el determinar el riesgo existente en la organización y promover la optimización permanente del control o su propia implantación y medidas para que en caso de que sucedan se puedan restaurar la información.

2.3.1. DEFINICIÓN.

William Mair define al Control como "... Todo aquello que tiende a causar la reducción de los riesgos. El control puede lograr reducir, ya sea, los efectos nocivos del riesgo o la frecuencia de su ocurrencia".[11]

El incremento directo de controles aumenta la Exactitud, Integridad y Protección de la información, así como de su costo.

La mayoría de los controles pueden también incrementar la Efectividad y Eficiencia del procesamiento en un punto aceptable, después del cual la implantación de más controles resultan inútiles. El objetivo de la organización en general es alcanzar el punto óptimo. La implantación de controles excesivos o muy estrechos reduce la Efectividad y Eficiencia a tal grado que en un punto, tiende a afectar a la Exactitud, Integridad y a su Producción.

[11] Vid. Mi3ir, William, St. Al., Control y Auditoría del Computador, Instituto Mexicano de Contadores Públicos, México 1976, Pág. 41.

Dentro de la estructura general de controles existe un tipo de Control denominado, "Control Interno" que se describe a continuación.

2.3.2. CONTROL INTERNO

El estudio y evaluación del Control interno es de suma importancia, debido a que el alcance y la magnitud de las organizaciones han llegado a un punto donde su estructura jerárquica se ha vuelto tan compleja y extensa que resulta más difícil controlar eficazmente las operaciones.

Asimismo, la responsabilidad de salvaguardar los activos de las organizaciones y prevenir errores y fraudes descansa principalmente en la administración, por lo que un buen control interno le permite depositar mayor confianza en la veracidad de los datos.

Por lo antes expuesto se puede definir el Control Interno como: "El plan de organización y el conjunto de métodos y procedimientos que en forma coordinada se adoptan en una organización para: proporcionar una seguridad razonable de que los activos están protegidos y que la información es oportuna y confiable; para promover la eficiencia en las operaciones; e impulsar el cumplimiento de las políticas de la dirección, las leyes y regulaciones".[12]

De esta definición obtenemos los objetivos propios del Control interno, los cuales se constituyen en medios para el logro de los objetivos institucionales.

- La protección de activos del Procesamiento Electrónico de Información.
- Producción de información íntegra, correcta y oportuna.
- La promoción de la eficiencia y efectividad de los sistemas y operaciones.
    - Eficiencia, es consumir recursos de manera óptima

[12] Vid. Instituto Mexicano de Contadores Públicos, Normas y Procedimientos de Auditoría, Novena edición, México, 1989, Pág. 101.

- Efectividad, es la medida con la cual se cumplen los objetivos para lo cuales fue desarrollado el sistema

- El cumplimiento de las políticas de la Dirección, las leyes y demás regulaciones.

Los activos del Procesamiento Electrónico de Información representan el total de recursos, bienes y derechos con que cuenta el área de sistemas para realizar sus operaciones.

La información es el elemento sobre el que se toman las decisiones operativas y administrativas.

El aprovechamiento de recursos y tiempo se reflejan en la productividad del área. Los lineamientos obligatorios, internos y externos, fijan el curso de las actividades de la organización dentro del marco social, económico, fiscal y laboral en que se encuentra.

Para lograr dichos objetivos se requiere de todo un sistema de Control Interno

2.4. AUDITORÍA.

Para definir las funciones y responsabilidades de Auditoría en Informática es conveniente referirse al papel que juega la Auditoría en general dentro de un esquema de organización.

Al terminar de revisar y actualizar los objetivos de la organización de acuerdo con las características del entorno y las de la propia organización en sus aspectos internos.

Se llevara a cabo la especificación y/o actualización del plan de acción para el logro de los resultados que se deben alcanzar.

Este plan de acción involucra la participación de cuatro áreas:

- Productivas
- De Apoyo

- De Control

- De Evaluación del control

Las áreas Productivas son aquéllas que tienen participación directa con el giro de la organización y son las que con su acción determinan, principalmente, el éxito o fracaso de un negocio.

Las áreas de Apoyo, no necesariamente participan en forma directa con el giro de la organización, sin embargo su acción es indispensable para el desarrollo adecuado de las áreas operacionales, como sucede con las áreas de Personal, Sistemas, Contabilidad y Control.

Las áreas de Control tienen características especiales dado que su responsabilidad se ejerce en forma distribuida, cada área productiva y de apoyo tiene como parte de su responsabilidad la aplicación de controles adecuados al tipo de función que realizan, sin embargo, existen áreas especiales cuya responsabilidad básica radica en el establecimiento de controles, como es el caso de las áreas de Contraloría y Seguridad.

El área responsable de la Evaluación del control en toda la organización, es el área de Auditoría, la cual esta manifestada dentro de la estructura jerárquica como un apéndice del más alto nivel directivo de la organización.

La obtención de resultados en una organización, se basa en la eficiencia lograda en las áreas productivas y de apoyo a través de la estructura de controles desarrollada, implantada y evaluada periódicamente.

El equilibrio existente entre productividad y control, es la participación de las áreas involucradas, el adecuado funcionamiento de cada área y la congruencia de los objetivos específicos, deben ser motivo de evaluación permanente por parte del área de auditoría.

El propósito de una área de Auditoría es determinar el nivel de riesgo que existe en la organización y promover la el adecuado funcionamiento de cada área y la congruencia de los objetivos específicos para una actualización optima de los controles internos existentes.

2.4.1. DEFINICIÓN.

Etimológicamente la palabra auditoría proviene de la raíz latina "auditorius", que significa tener la virtud de oír; derivada de los términos "audis", oír y "auditor", el que escucha.

La palabra auditoría ha sido mal empleada ya que es considerada como una evaluación cuyo único fin es detectar errores y señalar fallas. Sin embargo, dicho término tiene un significado más amplio y requiere del ejercicio de un juicio profesional sólido y maduro para juzgar los procedimientos y lineamientos que deben de seguirse para evaluar los resultados obtenidos, ya que de ninguna manera es una actividad que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo sean de carácter indudable.

Para Carlos Slosse, la Auditoría es: "el examen de la información por parte de una tercera persona, distinta de la que la prepara, con la intención de establecer su razonabilidad dando a conocer los resultados de su examen, a fin de aumentar la utilidad que tal información posee".[13]

Como concepto personal " La Auditoría, es una evaluación analítica y sistemática valiéndose de un conjunto de técnicas y procedimientos que aplica el auditor para que por medio de análisis y pruebas, proporcione un juicio.

[13] Vid. Slosse, Carlos, Et. Al., Auditoría. Un Nuevo Enfoque Empresarial, Ed. Ediciones Macchi, segunda edición, Buenos Aires, Argentina, Pág. 4.

2.4.2. DIFERENTES TIPOS DE AUDITORÍA.

La auditoría, como cualquier disciplina toma características diferentes de acuerdo al campo de acción o área de aplicación en que se desenvuelve.

De acuerdo a las personas que la realizan se pueden reconocer dos tipos de auditoría, la Auditoría externa o independiente y la Auditoría interna.

2.4.2.1. AUDITORÍA INTERNA.

"Es una evaluación independiente de las operaciones realizadas por los empleados o funcionarios de la organización con propósitos de control".[14]

La auditoría interna es una función gerencial que mide y valora la eficacia de los controles, políticas y procedimientos definidos por la organización para que se cumplan de acuerdo a lo establecido.

Esta auditoría es una actividad apreciativa, independiente de los sectores objeto de revisión. Por lo tanto reporta directamente a los máximos niveles de la organización y de los cuales depende de ellos. Tiene por objeto la revisión de las operaciones para servir de base a la administración. Por este motivo, es un control que se describe como independiente puesto que mide y evalúa la eficacia de otros controles.

La auditoría interna deberá trabajar en forma separada a las operaciones de la organización.

Sus funciones incluyen:

* Revisión de las operaciones para verificar la autenticidad, exactitud y efectividad con las políticas y procedimientos establecidos por la organización.

[14] Vid. Slosse, Carlos. Pág. 7.

* Comprobar la contabilidad de los datos de la administración generados dentro de la organización.

* Evaluar la calidad de desempeño en la ejecución de las actividades asignadas.

* Revisión para conocer si los procedimientos fueron aplicados en forma consistente con las normas establecidas.

De acuerdo al objetivo específico de la auditoría existen dos tipos:

1. Auditoría contable/financiera

El Instituto de Contadores Públicos determina que "...el objetivo de esta auditoría es el de proporcionar una base razonable para expresar una opinión sobre los estados tomados en su conjunto. Por otro lado, una revisión limitada no proporciona una base para la expresión de tal opinión..."[15] Esta auditoría la realiza un Licenciado en Contaduría el cual examina los estados financieros de una organización con el fin de dictaminar sobre su razonabilidad y verificar que las operaciones se hayan registrado de acuerdo a principios de contabilidad.

2. Auditoría administrativa/operativa

El C.P. y L.A. José Antonio Echenique define a la Auditoría administrativa como: "...el examen comprensivo y constructivo de la estructura de una organización, de una institución o cualquier parte de un organismo, en cuanto a sus planes, políticos y objetivos; sus metas y estructura orgánica; funciones; niveles de autoridad y responsabilidad; su forma de operación y sus recursos, sistemas y procedimientos generales".[16]

---

[15] Vid. Instituto Mexicano de Contadores Públicos, Normas y Procedimientos de Auditoría, Décima octava edición, México, 1998, Pág. 4060-4.

[16] Cf. Echenique, José Antonio, Auditoría en Informática, Facultad de Contaduría y Administración, UNAM, México, 1990, Pág. 16.

El objetivo de esta auditoría es la evaluación de la efectividad de la toma de decisiones.

La auditoría administrativa/operativa ayuda a complementar a la administración en determinadas áreas, depura los medios de control, y pugna por el mejor uso de los recursos humanos, materiales, financieros y tecnológicos.

Cualquier tipo de organización tiene áreas generales sujetas a investigaciones y que permiten obtener una evaluación de la administración.

La auditoría administrativa/operativa evalúa la forma en que se llevan a cabo los procedimientos para registrar un determinado tipo de operación a fin de detectar posibles deficiencias de control, esfuerzos duplicados, problemas de funcionalidad, corregir los efectos de las decisiones administrativas o cualquier proceso susceptible de ser optimizado para alcanzar los objetivos establecidos por la Dirección.

2.4.2.2. AUDITORÍA EXTERNA.

"Es la auditoría que se realiza a solicitud de las organizaciones con el objeto de presentar una opinión profesional independiente acerca de la razonabilidad y contabilidad de la información y los recursos a examinar expresada bajo los principios y políticas de la misma"[17]

La labor de auditoría externa implica una competencia profesional singular, caracterizada por una serie de atributos tales como independencia, conocimientos especializados.

[17] Vid. Slasse, Carlos, Auditoría. Un nuevo enfoque empresarial Op. Cit., Pág. 8.

El auditor externo está capacitado para implicar cualquier examen de información, operaciones, procedimientos, actividades y proyecciones, que necesiten de un juicio profesional independiente.

Se concluye que estos dos tipos de auditoría deberán trabajar en forma coordinada, ya que el alcance de revisión del auditor externo es inferior al del auditor interno, en razón a su tiempo de permanencia en la organización. por lo cual el primero se deberá apoyar en el trabajo del cuerpo de auditoría de la organización.

2.5. INFORMÁTICA.

2.5.1. DEFINICIÓN.

Etimológicamente el concepto informática se deriva de la palabra francesa "informatique" que a su vez se compone de los vocablos "information", información, y "automatique", automática que al unirlas significa Información Automática.

"Es la ciencia que se encarga del estudio y tratamiento de los sistemas de información utilizando regularmente dispositivos electrónicos de procesamiento". Para analizar la definición se estratificará en los elementos claves que le dan origen. El primer elemento de la definición es el relativo al concepto de Ciencia.

Los elementos que conforman a la ciencia se apegan al método científico, ya que se orientan a lo objetivo, razonable y sistemático, porque se obtiene mediante razonamiento lógico, el cual incluye sistemas, pasos y etapas para llevarlo acabo. Desde el punto de vista dinámico se considera a la ciencia como un proceso, es decir, como una disciplina o actividad encaminada a mejorar las cosas, predominando el criterio de utilidad practica.

El segundo elemento de la definición es el de sistema de información; este término en su connotación actual se refiere al conjunto de elementos y procedimientos ordenados,

que al ser ejecutados proporcionan información para apoyar la toma de decisiones y el control en la organización.

La informática nace de la idea de ayudar al hombre en los trabajos rutinarios y repetitivos, generalmente de cálculo y de gestión de datos. Ente las principales funciones de la Informática son:

- El desarrollo de nuevas tecnologías
- El desarrollo de nuevos métodos de trabajo
- La construcción de aplicaciones informáticas
- Mejoramiento de los métodos y aplicaciones ya existentes

2.6. AUDITORÍA EN INFORMÁTICA.

2.6.1. DEFINICIÓN.

Para Mair William, "la Auditoría en informática es: "la verificación de los controles en las tres áreas de organización:

- Aplicaciones (programas en producción).
- Desarrollo de programas.
- La instalación del centro de cómputo"[18]

Marc Thorin define a la auditoría en informática como: "el examen para obtener un juicio de un sistema de información"[19].

[18] Vid. Mair, ;fillism, Et. al., Computer Control & Audit, The Institute of Internal Auditors, U.S.A., 1978, Pág. 17.
[19] Vid. Thorin, Marc, La Auditoría en Informática, Masson, París, 1981, Pág. 33

En un concepto más sencillo la Auditoría en Informática es "el examen y validación de los controles, técnicas y procedimientos utilizados en el centro de cómputo y que están cumpliendo en forma satisfactoria y oportuna de acuerdo a los objetivos y políticas establecidas por la organización".

2.6.2. LOCALIZACIÓN DEL ÁREA DE AUDITORÍA INFORMÁTICA EN LA EMPRESA.

Cuando nos referimos a la ubicación que debe ocupar el área de Auditoría en Informática, nos encontramos ante una situación polémica, ya que dependerá del tamaño, contexto y complejidad de toda la organización, así como del nivel de automatización de la misma.

Considerando lo anterior, la función o área debe estar ubicada de manera separada a las áreas usuarias; al área de sistemas, así como de la gerencia y dirección donde se realiza la toma de decisiones; esto es a nivel Staff. Esto permite al área el poder contar con autoridad propia y bien definida a fin de realizar sus actividades y actuar con un criterio imparcial e independiente para obtener como producto de sus funciones, resultados objetivos.

2.6.3. PERFIL DEL AUDITOR EN INFORMÁTICA.

El aspecto fundamental en la definición del perfil más adecuado para llevar a cabo las funciones de Auditoría en informática, es personal con perfil de informática, al que se le capacita en funciones de control y el perfil de auditor, al que se le da capacitación en tecnología de cómputo".[20]

La estrategia que se debe de adoptar en este sentido es la de localizar personal con experiencia y conocimientos en informática, de preferencia en desarrollo de sistemas, que

[20] Cf. Colegio de Contadores Públicos de México., Diferentes enfoques de Auditoría en informática, Op. Cit. Pág. 13.

cuente con claras inclinaciones hacia el control, manifestados en la utilización por convicción del proceso de planeación, la aplicación de metodologías, técnicas, estándares y de todos aquellos elementos que constituyen el marco de control, bajo el que debe de operar la función de sistemas.

Como complemento para lograr un equilibrio adecuado entre conocimientos de informática y auditoría, se debe reclutar personal con experiencia y conocimientos en auditoría que tengan una clara tendencia hacia la sistematización a través de una precisa idea conceptual de lo que comprende la función de sistemas en operación y bajo desarrollo.

A través de la interacción entre estos dos tipos de elementos es como consideramos que existe la posibilidad de llevar a cabo en forma adecuada la función de auditoría en informática.

Ahora bien, "por perfil de un profesional hemos de entender las características, aptitudes o requisitos mínimos que debe reunir una persona para ejercer una profesión"[21].

2.6.4. ÁREAS EN LAS QUE PARTICIPA EL AUDITOR EN INFORMÁTICA.

Las Áreas de participación primordial del Auditor en informática dentro de la organización:

Auditoría al desarrollo de sistemas

Auditoría a sistemas en operación

Auditoría a centros de cómputo

[21] Vid. López, Elizondo, La Profesión Contable. Selección y desarrollo, Edit. ECABA, tercera edición, México, 1984., Pág. 104.

CAPITULO 3.

CLASES Y TIPOS DE AUDITORÍAS INFORMÁTICAS.

3.1. ÁREAS GENERALES Y ESPECÍFICAS

Los Departamentos de Informática tienen una gran trascendencia respecto a las demás organizaciones usuarias de ella. La Informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa. Así, existirá la "auditoría Informática de Usuario".

Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. Consecuentemente, existirá una "Auditoría Informática de actividades Internas".

El enlace del Departamento de Informática con el exterior, es decir, con el usuario se realiza en principio por medio de la Dirección. La figura de la Dirección de Informática es especialmente importante y peculiar, en tanto que es capaz de interpretar las necesidades de la Compañía.

En el flujo inverso, una informática eficiente y eficaz requiere el apoyo continuo de su Dirección frente al "exterior". Revisar estas interrelaciones constituyen el objeto de la "auditoría Informática de Dirección".

La "Auditoría Informática de la Seguridad" es la encargada de revisar las actividades de la Dirección, a los Usuarios y a la propia informática.

Con lo expuesto resulta que se han enumerado las cuatro Áreas Generales de la Auditoría Informática más importantes.

Dentro de las áreas generales, es posible establecer las siguientes divisiones:

Auditoría Informática de Explotación

Auditoría Informática de Sistemas

Auditoría Informática de Comunicaciones

Auditoría Informática de Desarrollo de Proyectos

Auditoría Informática de Seguridad [22]

Siendo esta última también un área general.

Son estas últimas, las cinco Areas Específicas de la Auditoría Informática más importantes.

Debe resaltarse la dualidad de generalidad y especificidad que posee la Seguridad Informática. Según ella, puede realizarse una Auditoría Informática de la Seguridad del contexto informático globalizando, mientras que en otras ocasiones podrá realizarse una auditoría informática de una aplicación concreta, en donde será necesario analizar la seguridad de la misma.

Realizando una combinación de las Áreas Generales con las Áreas Específicas se han considerado diecinueve tipos distintos de Auditorías:

1. Auditoría Informática de Explotación Interna
2. Auditoría Informática de Explotación en Dirección
3. Auditoría Informática de Explotación en Usuario
4. Auditoría Informática de Explotación en Seguridad
5. Auditoría Informática de Sistemas Internos
6. Auditoría Informática de Sistemas en Dirección
7. Auditoría Informática de Sistemas en Usuario
8. Auditoría Informática de Sistemas en Seguridad

[22] Alonso Rivas, G. Auditoría Informática, Ed. Díaz de Santos S.A. 1988.

9. Auditoría Informática de Comunicaciones Internas

10. Auditoría Informática de Comunicaciones en Dirección

11. Auditoría Informática de Comunicaciones en Usuario

12. Auditoría Informática de Comunicaciones en Seguridad

13. Auditoría Informática de Desarrollo de Proyectos Internos

14. Auditoría Informática de Desarrollo de Proyectos en Dirección

15. Auditoría Informática de Desarrollo de Proyectos en Usuario

16. Auditoría Informática de Desarrollo de Proyectos en Seguridad

17. Auditoría Informática de Seguridad Interna

18. Auditoría Informática de Seguridad en Dirección

19. Auditoría Informática de Seguridad en Usuario

20. Auditoría Informática de Seguridad en Seguridad

Consecuentemente, cada área informática específica puede ser auditada desde los siguientes criterios generales, a saber:

a) Desde su propio funcionamiento interno

b) Desde el apoyo que recibe de la dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.

c) Desde la perspectiva de los usuarios, destinatarios reales de la informática.

d) Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.[23]

Las combinaciones descritas pueden ser ampliadas o reducidas, según las características de la empresa auditada. Ha de ponerse de manifiesto que las auditorías

[23] Alonso Rivas, G. Auditoría Informática, Ed. Díaz de Santos S.A. 1988.

más usuales son las referidas a las actividades específicas e internas de la propia actividad informática.

3.2. AUDITORÍA INFORMÁTICA DE EXPLOTACIÓN.

La explotación informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos soportados magnéticamente para otros informáticos, órdenes automatizadas para lanzar o modificar procesos industriales.

Para realizar la explotación informática se dispone de una materia prima, los datos, los cuales serán transformados y qué se someten previamente a controles de integridad y calidad.

La transformación se realiza por medio del proceso informático, el cual está regido por programas. Obteniendo el producto final, los resultados son sometidos nuevamente a uno a varios controles de calidad y finalmente son distribuidos al cliente, ó al usuario. En ocasiones, el propio cliente realiza funciones de revaluación del producto terminado.

Es significativa la evolución de la profesión de operador hacia la ocupación de otros puestos de trabajo dentro de la explotación, o fuera de ella. Las instalaciones han evolucionado y son tan eficientes que cuentan con un porcentaje apreciable de técnicos de sistemas, incluso de analistas, procedentes de explotación. Es así porque cada día es más evidente el acercamiento de conocimientos entre las diversas funciones de la empresa, y entre explotación y las demás áreas informáticas, como la rápida generación de funciones frontera, especialmente entre explotación y técnica de sistemas.

El factor más importante es que la tecnificación y automatización de la producción exige capacidad de programación propia. Pero ya aplicado en la vida cotidiana se ha demostrado que muchos departamentos de Explotación se han dotado de su propio desarrollo interno para atender sus propias necesidades.

El concepto de centro productivo ayuda a la elaboración de la auditoría de la explotación. Auditar explotación consiste en auditar las secciones que la componen y sus interrelaciones, estas son la planificación de la producción y la producción misma de resultados informáticos.

La Operatividad es prioritaria, al igual que el "plan crítico diario de producción", ya que toda la organización informática está sujeta a la obtención de resultados en plazo y calidad, siendo subsidiario a corto plazo cualquier otro objetivo.

La Explotación informática se divide en tres grandes áreas, a saber: Planificación, Producción y Soporte Técnico.[24]

3.2.1. CONTROL DE ENTRADA DE DATOS.

Existen diversas formas de captura de datos, la exactitud de los datos de entrada es un problema continúo, los errores de captura pueden ocurrir cuando los datos son registrados, cuando son convertidos a forma legible, cuando son manejados y cambiados de lugar o transmitidos. Hay varías técnicas de control que pueden ser incorporadas a los procedimientos de captura. El cumplimiento de plazos y calendarios de tratamiento y entrega de datos. Revisión o verificación de la conversión y el uso de dígitos de comprobación. La correcta transmisión de datos entre entornos diferentes, y se verificará realmente que los controles de integridad y calidad de datos se realicen.

3.2.2. 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, salvo excepciones con éste. Deberán realizarse muestreos selectivos de la documentación de las aplicaciones explotadas.

---

[24] de Juan Rivas, A. Pérez Pascual, A. La Auditoría en el desarrollo de Proyectos Informáticos, Ed. Díaz de Santos S.A. 1988.

Como función responsable de construir y optimizar las cadenas de control de trabajos-procedimientos, se analizarán la documentación que se tenga en cuento a su organización y en lo relacionado con la posible existencia de planificadores automáticos o semiautomáticos.

Se indagará sobre la anticipación de contactos con desarrollo para la planificación a mediano y largo plazo. Actualmente se maneja un tiempo de mediano plazo de la informática porque oscila entre los dieciocho y veinticuatro meses. [25]

3.2.3. CENTRO DE CONTROL Y SEGUIMIENTO DE TRABAJOS.

La forma y modo de auditar depende del sistema que se encuentre en operación como puede ser una Mainframe, Red en Línea, u proceso Batch, etcetera.

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. la explotación informática ejecuta procesos por cadenas o lotes sucesivos (Batch), o en tiempo real (Teleproceso).[26]

Mientras que las aplicaciones de teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo batch absorbe una buena parte de los efectivos de Explotación. En muchos centros procesamiento de datos, este órgano recibe el nombre de centro de control batch. Este grupo determina en gran medida el éxito de la explotación, en cuanto es uno de los factores más importantes en el mantenimiento de la producción.

[25] IEEE Computer Sociery Symposium. Proceeding: Research in Segurity and Privacy. 1990. Fuente Internet.
[26] Hannan, J. Ed. Guías prácticas Chip-Auerbach, traducción de ediciones Arcadia. 1984.

3.2.4. OPERATIVIDAD.

Para un mejor desempeño esta área trabaja de noche a turnos. Destaca el factor de responsabilidad ante incidencias y averías. Se verificará la existencia de un responsable de sala en cada turno de trabajo. Se analizarán el grado de automatización de comandos. Verificando la existencia y el grado de uso de los manuales de operación.

Se analizará la existencia de planes de formación, como también el que se aplique y el tiempo transcurrido para cada operador desde el último curso recibido.

Se cuantificarán y se estudiarán los respaldos realizados de la información. La actualización de software y la verificación del papel impreso tanto por hora como por día.

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 relacionando con la organización de comunicaciones software de técnica de sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos.

Se verificará la existencia de un punto local único, desde el cual sean perceptibles todas las líneas asociadas a los sistemas.

El Centro de Diagnosis es el área en donde se atienden las llamadas de los usuarios - clientes que han sufrido averías o incidencias, tanto de software como de hardware. En función del cometido descrito, y en cuanto a software, está relacionado con el Centro de Control de Red.

El Centro de diagnosis es uno de los elementos que más contribuyen a configurar la imagen de la informática de la empresa. Debe ser auditado desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispensa. No

basta con comprobar la eficiencia técnica del centro. es necesario analizarlo simultáneamente en el ámbito de Usuario.

3.3. AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS.

El área específica de desarrollo de proyectos o de aplicaciones es objeto frecuente de la auditoría informática.

La función de desarrollo es una evolución del llamado análisis, programación y la aplicación de los sistemas. La función desarrollo engloba a su vez muchas áreas, tantas como sectores informatizables que integran a la empresa

Una aplicación recorre las siguientes fases:

a) Prerrequisitos del Usuario (tanto individuales como colectivos), y del entorno.

b) Análisis funcional.

c) Análisis orgánico. (Preprogramación y programación).

d) Pruebas

e) Entrega a Explotación y alta para el Proceso.[27]

La importancia de la metodología utilizada en el desarrollo de los proyectos informáticos. Esta metodología debe ser semejante al menos en los proyectos correspondientes a cada área de la organización, aunque preferiblemente debería extenderse a la empresa en conjunto.

La utilización de una metodología común o similar, y el desarrollo de una aplicación debe estar sometido a un exigente control interno de todas las fases antes citadas. En caso contrario, además del disparo de los costos, podrá producirse fácilmente la insatisfacción del usuario, si éste no ha participado o no ha sido

[27] Alonso Rivas, G. Auditoría Informática, Ed. Díaz de Santos S.A. 1988.

consultado periódicamente en las diversas fases del mismo, y no solamente en la fase de prerrequisitos.

La auditoría informática deberá comprobar la "seguridad" de los programas, en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Una Auditoría Informática de Aplicaciones pasa indispensablemente por la observación y el análisis de estas tres consideraciones:[28]

a)Revisión de las metodologías utilizadas.

Se analizarán éstas, de modo que se asegure la modularidad de las futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas. Los sistemas metodológicos más conocidos, como los de Warnier, Merise, Jackson, los cuales pueden ser sustituidos por metodologías elaboradas internamente en cada empresa o en la informática de la misma. En cualquier caso, lo fundamental reside en una filosofía de normas de actuación, más que en un método concreto.

b) Control Interno de las Aplicaciones

La auditoría informática de Desarrollo de Aplicaciones deberá revisar las mismas fases que presuntamente ha debido seguir el área correspondiente de desarrollo. Las principales, son:

1.- Estudio de Vialidad de la Aplicación: Es muy importante para los casos de aplicaciones largas, complejas y de elevado costo.

2.- 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.

[28] de Juan Rivas, A. Pérez Pascual, A. La Auditoría en el desarrollo de Proyectos Informáticos, Ed. Díaz de Santos S.A. 1988.

3.- Desarrollo Técnico de la Aplicación. Se verificará que éste sea ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles.

4.- Diseño de Programas. Deberán poseer la máxima modularidad, sencillez y economía de recursos.

5.- 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.

Cuando existan entornos diferenciados de pruebas y explotación, se realizarán en el entorno de pruebas; Sólo cuando éstas hayan terminado con éxito, se realizarán pruebas finales en explotación, al tiempo de la entrega de dicha aplicación en explotación para su ejecución periódica.

6.- Documentación. Cumplirá la normativa establecida en la instalación, tanto la de desarrollo como la de entrega de aplicaciones a explotación.

7.- Equipo de Programación. Deben fijarse las tareas de análisis puro, de programación, y las intermedias. En aplicaciones complejas se producirán variaciones en la composición del grupo, pero éstas deberán estar previstas.

La coordinación de actividades corresponde al Jefe del Proyecto, el cual reporta al responsable del Área de Desarrollo.

c) Satisfacción de Usuarios

Una Aplicación técnicamente eficiente bien desarrollada teóricamente, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. Surgen

nuevamente las premisas fundamentales de la informática eficaz: fines y utilidad. No puede desarrollarse de espaldas al usuario, sino contando con sus puntos de vista durante todas las etapas del proyecto. La aprobación del usuario proporcionará además grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

d) Control de Procesos y Ejecuciones de Programas Críticos

El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones.

Se está diciendo que el auditor habrá de comprobar indiscutiblemente y personalmente la correspondencia biunívoca y exclusiva entre el programa codificado y el producto obtenido como resultado de su compilación y su conversión en ejecutable, mediante el montador de enlace. (Linkage Editor)

Las consecuencias de todo tipo que podrían derivarse del hecho de que los programas fuente y los programas módulos no coincidieran: desde errores de bulto que producirían graves retrasos y altos costos de mantenimiento, hasta fraudes de incalculables dimensiones, pasando por acciones de sabotaje, espionaje industrial-informático.

Esta problemática ha llevado a establecer una normativa muy rígida en todo lo referente al acceso a la documentación del programa. Una informática medianamente desarrollada y eficiente dispone de un solo juego de documentación del programa de instalación.

Explotación debe ingresar programas fuentes, y solamente fuentes. Estos son aquellos que desarrollo haya dado como buenos.

Explotación, asumirá la responsabilidad de:[29]

1. Copiar el programa fuente que Desarrollo de Aplicaciones ha dado por bueno en la documentación de Fuentes de Explotación, a la que nadie más tiene acceso.

2.- Compilar y montar ese programa, depositándolo en la documentación de módulos de explotación, a la que nadie más tiene acceso.

3.- Copiar los programas fuente que les sean solicitados para modificarlos, arreglarlos, en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente al primer punto.

La información se ha dotado de herramientas de seguridad sofisticadas que permiten identificar la personalidad del que accede a esa documentación. El auditor intervendrá los programas críticos, compilando y ejecutando nuevamente los mismos para verificar su forma biunivocidad.

3.4. AUDITORÍA INFORMÁTICA DE SISTEMAS.

Se ocupa de analizar la actividad propia de lo que se conoce como "Técnica de Sistemas" en todas sus facetas. En la actualidad, 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"[30]

[29] Thorin. M.La Auditoría Informática. Métodos, Reglas, Normas. Ed. Masson. S.A. 1989

[30] Weber, Ron. EDP Auditing, Conceptual Foundations and Practice. 2ª. Edición Ed. Mc Graw-Hill 1985.

3.4.1. SISTEMAS OPERATIVOS.

Se entienden por tales, los proporcionados por el fabricante junto con la máquina. Engloba los subsistemas de teleproceso, entrada/salida. Debe verificarse en primer lugar que los sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si éstas se han producido. El análisis de las versiones de los sistemas operativos, permite descubrir las posibles incompatibilidades entre algunos otros productos de software básico adquiridos por la instalación y determinadas versiones de aquellos.

3.4.2. SOFTWARE BÁSICO.

Lo constituye el conjunto de productos que, sin pertenecer al sistema operativo, configuran completamente los sistemas informáticos, haciendo posible la realización de *funciones básicas no incluidas en aquel.*

El software básico, o una gran parte de él, es abonado por el cliente a la firma creadora, mientras que el sistema operativo y algunos productos muy básicos, se incorporan a la máquina sin cargo alguno para el cliente.

Es difícil decidir si una función concreta debe estar incluida en el sistema operativo o puede ser omitida de él. Iguales dudas podrían establecerse respecto a una serie de utilidades, por ejemplo las copias, exportación e importación de archivos.

Con independencia del interés teórico que pueda tener la discusión de sí una función concreta es o no integrante del sistema operativo, para el auditor es fundamental conocer los productos de software básico que han sido adquiridos aparte y se encuentran instalados en la máquina. *Esto es por razones económicas y por comprobar de que si ese* software adquirido no sea necesario para el funcionamiento de la computadora.

Los conceptos de sistema operativo y software básico tienen fronteras comunes y que con independencia del entorno que corresponde, la política comercial de cada

compañía y sus relaciones con los clientes determinan finalmente el precio y los productos gratuitos o facturables.

Es importante recordar del software básico, la implementación y el desarrollo en los sistemas informáticos por el área de sistemas de la empresa, los cuales son desarrollos internos para el manejo de su información. El auditor, en este punto, debe verificar que ese software no agrede, ni condiciona al sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.

3.4.3. SOFTWARE DE PROCESO.

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. Los controles y medidas habituales que realiza el personal de técnica de sistemas.

Posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados.

Pueden realizarse:

a) Cuando existe la sospecha de deterioro del comportamiento parcial o general del Sistema.

b) De modo sistemático y periódico.

El auditor informático deberá conocer el número de Tunnigs 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.

3.4.4. *OPTIMIZACIÓN DE SISTEMAS.*

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la información diaria obtenida a través de Log Accounting. Actúa

igualmente como consecuencia de la realización de Tunnigs 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.

3.4.5. ADMINISTRACIÓN DE BASES DE DATOS.

Es un área que ha adquirido una gran importancia al hilo de la proliferación de usuarios y de las "descentralizaciones" habidas en las informáticas de las empresas.

El diseño de las bases de datos, ya sean relacionadas o jerárquicas, se han 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 los usuarios de la empresa.

El conocimiento del diseño y arquitectura de dichas bases de datos por parte de sistemas, ha cristalizado en que la administración de las mismas les sea igualmente encomendada. Aunque esta adscripción es la más frecuente en la actualidad, los auditores informáticos han observado algunas disfunciones derivadas de la relativamente escasa experiencia que tiene sobre la problemática general de los usuarios de las bases de datos.

Comienzan a percibirse hechos relativos a la separación del diseño y la construcción de las bases de datos de la administración de las mismas, que sería realizada por explotación. Sin embargo, esta tendencia es aún poco significativa.

El auditor informático de bases de datos deberá 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. Tendrá que revisar que la base de datos sea depurada y actualizada con consultas sin afectar desempeño de la base de datos.

En caso de que la base de datos se dañara el auditor revisara si esta se pudiera restaurar a su estado anterior con una copia de respaldo reciente, y se aplicaría una copia de respaldo de todas las post-imágenes salvadas entre la fecha en que se hizo la copia de respaldo y el momento de la falla de la base de datos. Así, puedes salvar todas las actualizaciones realizadas antes de la falla.

Por último revisará la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

3.4.6. INVESTIGACIÓN Y DESARROLLO.

El campo informático sigue evolucionando rápidamente. Multitud de Compañías de Software aparecen en el mercado.

Sólo muy recientemente, las empresas que necesitan de desarrollos informáticos han comprendido que sus propios departamentos pueden desarrollar aplicaciones y utilidades que, al pensarse inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo la competencia a las compañías del ramo.

Como consecuencia algunas empresas no dedicadas en principio a la venta de productos informáticos, están potenciando la investigación de sus equipos de técnica de sistemas y desarrollo, de forma que sus productos puedan convertirse en fuentes de ingresos adicionales.

La auditoría informática deberá cuidar de que la actividad de investigación y desarrollo de las empresas no vendedoras, no interfieran ni dificulte las tareas fundamentales internas. En todo caso, el auditor advertirá en su informe de los riesgos que haya observado.

La propia existencia de aplicaciones para la obtención de estadísticas desarrollados por los técnicos de sistemas de la empresa auditada, y su calidad, proporciona al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los sistemas. La correcta elaboración de esta información conlleva al buen conocimiento de la carga de la instalación.

3.5. AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES.

La creciente importancia de las Comunicaciones han determinado que se estudien separadamente del ámbito de técnica de sistemas. Naturalmente, siguen siendo términos sobrepuestos en los conceptos generales de sistemas y de arquitectura de los sistemas informáticos.

Se ha producido un cambio conceptual muy profundo en el tratamiento de las comunicaciones informáticas y en la construcción de los modernos sistemas de información, basados principalmente en redes de comunicaciones muy sofisticadas.

Para el informático y para el auditor informático, el armado conceptual que constituyen las redes nodales, (líneas, concentradores, multiplicadores), redes locales, no son sino el soporte físico - lógico del tiempo real. A mí parecer el siguiente concepto es de suma importancia "Las comunicaciones son el soporte físico - lógico de la informática en tiempo real".[31]

El auditor informático tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre si, pero como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales. No debe olvidarse que algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios.

[31] Sanchis, F. Planificación y Explotación de Sistemas Informáticos. E.U.I. de la U.P. de Madrid, 2ª. Edición.

Respecto a las comunicaciones en este punto se debe manejar con mucho cuidado, ya que se encuentra condicionado a la participación del monopolio telefónico que preste el servicio.

En algunas empresas solicitan líneas dedicadas y exclusivas, pero esto produce un costo excesivo, y él pagó anual por arrendamiento de líneas resulta que es más dinero que el invertido en hardware y software, y es casi igual o tanto como en gastos de personal. Resulta de ello la necesidad de un especial cuidado en la contratación de líneas telefónicas y de enganche a las redes públicas de transmisión de datos.

El auditor de comunicaciones deberá averiguar 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. La desactualización de esta documentación significaría una grave debilidad.

La inexistencia de datos sobre cuántas líneas existen, cómo son y dónde están instaladas, son problemas de seguridad y de acceso es una de las causas de la inoperatividad informática, pero la debilidad más frecuente e importante en la informática de las comunicaciones se encuentran en las disfunciones organizacionales. La contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes. Todas estas actividades deben estar coordinadas y de ser posible dependientes de una sola organización.

3.6. AUDITORÍA DE LA SEGURIDAD INFORMÁTICA.

La seguridad en la informática depende mucho del tipo de instalación, si el equipo esta en red o solo son Pc's solas, al determinar los conceptos anteriores revisará la seguridad física del centro de proceso de datos en su sentido más amplio, a si como la seguridad lógica d datos, procesos y funciones informáticas mas importantes.

La Seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales. Igualmente, a este ámbito pertenece la política de seguros.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. Se ha tratado la doble condición de la seguridad informática: como área general y como área específica (Seguridad de Explotación, Seguridad de las Aplicaciones, etc.). Así, podrán efectuarse auditorías de la seguridad global de una instalación informática (Seguridad General), y auditorías de la seguridad de un área informática determinada (Seguridad Específica).[32]

Los accesos y conexiones indebidos a través de las redes de comunicación, han acelerado el desarrollo de productos de seguridad lógica y la utilización de sofisticados medios criptográficos.

[32] Lamére, J.E. La securité informatique. Aproche metodologique. Traducción La Seguridad Informática. Metodología. Ed. Arcadia. 1987.

CAPITULO 4.

TÉCNICAS, HERRAMIENTAS Y CONTROLES DE LA AUDITORÍA INFORMÁTICA.

4.1. CUESTIONARIOS.

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los Informes 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, también llamados evidencias.

Suele ser habitual comenzar solicitando el llenado de cuestionarios preimpresos que se envían a las personas concretas que el auditor estima adecuados, sin que sea obligatorio que dichas personas sean las personas responsables oficiales de las diversas áreas a auditar.

Estos preimpresos no pueden ni deben ser repetidos para instalaciones distintas sino diferentes y muy específicos para cada situación, y muy precisos en su fondo y en su forma.

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

4.2. ENTREVISTAS.

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:[33]

a) Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

b) Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

c) 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 un mejor reflejo, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, que consiste 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 sólo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

4.3. LISTAS DE VERIFICACIÓN.

El conjunto de estas preguntas que redacta el auditor informático recibe el nombre de checklist. Las checklist's deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

[33] Derrier, Y. Les Techniques de Láudit Informatique, De. Dunod, 1992

Según la claridad de las preguntas y el talento 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, ha sido muy 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 celosamente sus checklist's, pero de poco sirven si el auditor no las utiliza adecuadamente y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor profesional y experto es aquel que actualiza frecuentemente el contenido de sus cuestionarios en función de los escenarios auditados. 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. Por lo contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la complementación sistemática de sus Cuestionarios, de sus checklist's. Las entrevistas y los cuestionarios se hacen también a usuarios reales y potenciales es decir o todas los usuarios que estén trabajando en el centro de trabajo.

Existen opiniones que descalifican el uso de cheklist. Sin duda se refieren a la situación antes descrita de un inexperto auditor que recita preguntas y espera respuestas. Pero esto no es utilizar Checklist's, esto es una evidente falta de profesionalidad.

La profesionalidad pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. La profesionalidad pasa por poseer preguntas muy estudiadas que ha de formularse flexiblemente.

El auditor deberá aplicar la checklist de modo que el auditado responda clara y brevemente. 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 aquel a que exponga con mayor amplitud un tema concreto, y en cualquier caso se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las checklist's utilizadas para cada sector, deben ser repetidas, es decir el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrá descubrir con mayor facilidad los puntos contradictorios; el auditor analizara los matices de las respuestas y actualizara preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El método descrito es habitual en toda auditoría. Proporcionando el necesario rigor del análisis de la situación.

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.

Los cuestionarios o checklist responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación.

a) Checklist de Rango

Contiene preguntas que el auditor debe sumar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo la 1 la respuesta más negativa y 5 el valor más positivo).

b) Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Sí o No. Aritméticamente, equivalen a "1" o "0", respectivamente.

Las Checklist's de Rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que la Checklist Binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las Checklist's Binaria siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del "Sí o No" frente a la mayor riqueza del intervalo.

4.4. SOFTWARE

4.4.1. 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 utilerias más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante.

El auditor informático emplea preferentemente la amplia información que proporciona el propio sistema, en donde se encuentra la producción completa de aquel, y los "Log" de dicho Sistema, en donde se recogen las modificaciones de datos y se designa la actividad general.

Del mismo modo el sistema genera automáticamente información exacta sobre el tratamiento de errores de máquina central, periféricos, y otros.

La auditaría financiero - contable convencional emplea trazas con mucha frecuencia. Son programas encaminados a verificar lo correcto de los cálculos de nominas, primas.

Las herramientas informáticas utilizadas en estos casos son la mejor expresión del concepto de auditoría económica con el apoyo de la informática, no de la auditoría informática propiamente dicha.

4.4.2. SOFTWARE DE INTERROGACIÓN.

Los productos software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada.

Estos productos son utilizados solamente por los auditores externos, mientras que los auditores internos disponen del software nativo propio de la instalación.

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 computadoras personales y mainframe, de modo que el auditor informático copia en su propio PC la información más relevante para su trabajo.

El auditor se halla obligado (dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los diferentes productos descritos.

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.

CAPITULO 5.

METODOLOGIA DE TRABAJO EN LA AUDITORÍA INFORMÁTICA.

Una vez definida la Auditoría Informática, sus fines y utilidades, así como expuestas sus clases y tipos, describiremos el método de trabajo que el auditor en informática ha de seguir, desde la orden de la Dirección (según la auditoría de que se trate externa o interna), hasta la confección y entrega por escrito del Informe Final. Toda la función auditora se compendia en la entrega del mencionado Informe a quien lo solicitó.

El método de trabajo auditor pasa por las siguientes fases:

1. Alcance y objetivos de la auditoría informática.
2. Estudio inicial del entorno auditable.
3. Determinación de los recursos necesarios para efectuar la auditoría.
4. Elaboración del plan y de los programas de trabajo.
5. Actividades propiamente dichas de la auditoría (Análisis, entrevistas).
6. Confección y redacción del informe final.
7. Redacción de la carta de introducción o carta de presentación del informe final.[34]

[34] de Juan Rivas, A. Pérez Pascual, A. La Auditoría en el desarrollo de Proyectos Informáticos, Ed. Díaz de Santos S.A. 1988.

5.1 ALCANCE Y OBJETIVOS DE LA AUDITORÍA INFORMÁTICA.

El alcance de la Auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones auditadas.

En la auditoría de una explotación deberá fijarse previamente si ha de incluirse o no la función de soporte técnico, dependiendo de su ubicación en el organigrama. Se fijará de antemano la percepción de los usuarios, y la eficiencia interna de explotación.

Especial importancia tendría la determinación del ámbito de la auditoría cuando se incluyan áreas no informáticas de la empresa u oficinas de servicios informáticos ajenos a la misma.

A estos efectos, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, manifestar por escrito cuáles materias o funciones no van a ser auditadas. Tanto el alcance de la auditoría como las excepciones del mismo, han de figurarse al comienzo del documento final.

La Auditoría ha de conocer con la mayor precisión los objetivos que sus acciones pretenden. Debe comprender con exactitud los deseos y pretensiones del cliente, de forma que los objetivos perseguidos sean susceptibles de ser cumplidos.

Bien determinados los objetivos, en lo sucesivo llamados objetivos específicos, el auditor tendrá siempre presente que éstos se añadirán a los dos objetivos generales y comunes a toda auditoría informática: La operatividad de los sistemas y los controles generales de gestión informática.

Los objetivos más habituales pueden ser:

- Evaluación de funcionamiento de áreas informáticas.
- Aumentos de Seguridad y Fiabilidad.
- Conectividad
- Compatibilidad
- Aumento de Calidad
- Costos o Plazos.

Dentro de este apartado de alcance y objetivos debe incluirse la fijación de los interlocutores del equipo auditor. El concepto de interlocución comprende la determinación previa de las personas que tienen poder de decisión y de validación dentro de la empresa. Los auditores conocerán con exactitud la persona o personas destinatarias del informe.

5.2 ESTUDIO INICIAL DEL ENTORNO AUDITABLE.

La metodología de trabajo del equipo auditor comporta un estudio inicial de la situación general, aún en el caso de que la auditoría a realizar sea solamente sectorial.

Para realizar dicho estudio han de examinarse las funciones y actividades generales de la informática, esas serán:

a) Organización.

Para el equipo auditor, el conocimiento de quien ordena, diseña y ejecuta es fundamental. No podrá realizar su misión sin conocer con bastante aproximación la estructura organizativa de la informática sujeta a auditoría. Al menos, se deberán fijar los conceptos que siguen:

1. Organigrama.

El organigrama expresa inicialmente la estructura oficial de la organización a auditar. El propio equipo auditor solicitará el organigrama oficial con todo detalle, sin omitir las casillas que realicen funciones auxiliares o complementarias no informáticas. Si el número de niveles es elevado se fraccionará. Los textos de las cajas deberán ser autoexplicativos.

Se tomará como referencia al organigrama oficial, el auditor podrá comprobar con facilidad la identidad que debe existir entre lo oficial y lo real.

Si se descubriera a través de los flujos de información y de las relaciones funcionales y jerárquicas que existe un organigrama diferente al oficial, se pondrá de manifiesto tal circunstancia y las derivadas de ella.

2. Departamentales.

Se entienden ahora como departamentos los órganos que siguen inmediatamente tras la Dirección. El auditor analizará las funciones más importantes de las cajas que constituyen cada una de ellas, y las que dependen directamente de éste.

3. Relaciones jerárquicas y funcionales entre órganos de la organización

Además del organigrama y de las funciones principales de cada Departamento, el auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas, o por el contrario, detectará, por ejemplo, si algún empleado tiene dos jefes.

Las relaciones de jerarquía implican la correspondiente subordinación. Las funcionales, por el contrario, indican relaciones de naturaleza complementaria y no estrictamente subordinables. Estas relaciones deben estar bien definidas por el nivel inmediato superior, el cual deberá informar a sus propios grupos horizontales de la existencia de tales relaciones, así como de cualquier variación en ellas.

En principio, las relaciones no jerárquicas contribuyen a proporcionar mayor flexibilidad a las estructuras. Sin embargo, y también como principio, deberán restringirse al máximo las dependencias funcionales.

Al referirnos a flujos de información, significa que las dependencias funcionales significan imprecisiones organizativa de diversa importancia y género, las cuales son aceptables tan sólo en circunstancias excepcionales, y siempre que estas desaparezcan a plazo fijo.

4. Flujos de Información.

Las corrientes verticales interdepartamentales y de las directrices de la Dirección, la estructura organizativa, cualquiera que sea, produce corrientes de información horizontales y oblicuas extra departamentales.

Los flujos de información entre los grupos de una organización son necesarios y aún imprescindibles para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

Las organizaciones crean expontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales de información alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que lo representa.

En la realidad no existe el organigrama perfecto, por lo que puede resultar inevitable la existencia de flujos de información no deseados, pero esta realidad no debe excusar la proliferación de dichos flujos. Generalmente la aparición de flujos de información son indeseables y producen graves perturbaciones en la organización, y en otras ocasiones sirven para un mejor manejo de la información. Particular importancia tienen los llamados puenteos en el vocabulario empresarial, sobre todo cuando está involucrada la propia Dirección.

5. Número de Puestos de Trabajo.

El Auditor comprobará que los nombres de los puestos de trabajo de la organización auditada corresponden a funciones reales distintas. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes en los diferentes grupos de la instalación.

Esta situación pone de manifiesto deficiencias estructurales; los auditores pondrán de manifiesto tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes. Es difícil que existan más de cinco o seis puestos operativos distintos por cada rama informática, mientras que en muchas organizaciones aparecen hasta diez o doce denominaciones por rama.

6. Número de personas por Puesto de Trabajo

Este es un parámetro que los auditores informáticos deben considerar la normatividad y la dependencia corporativa, para una adecuada distribución del personal o la falta de plantilla en algunas secciones y el exceso en otras, también determina que el número de personas que realizan las mismas funciones, rara vez coinciden con la estructura oficial de la organización.

Los auditores deberán exponer el número de empleados reales de cada sección auditada. Con esta acción, se expone una distribución ineficiente de recursos o la necesidad de una reorganización para modificar la estructura oficial.

a) Entorno Operacional.

El auditor en informática debe poseer una adecuada referencia del entorno en el que ha de desenvolverse. Este conocimiento previo se logra determinando, funcionalmente, los siguientes puntos:

1. Situación geográfica de los Sistemas.

Se determinará la ubicación geográfica de los Centros de Proceso de Datos distintos de la empresa. De acuerdo con dicha ubicación, se verificará la existencia de responsables por cada uno de ellos, así como el uso de los mismos estándares de trabajo.

2. Arquitectura y configuración de Hardware y Software.

Cuando existen varios centros de procesamientos de datos, es fundamental revisar la normatividad en la cual de proporcionara la configuración para constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica informática de las compañías.

3. Inventario Hardware y Software.

El auditor recabará información escrita de la empresa, en donde figuren todos los equipos físicos y lógicos de la instalación. En cuanto a hardware, figurarán los CPU'S, procesadores intermedios, unidades de controles tanto locales y remotos, periféricos de todo tipo, terminales, computadoras personales. Es conveniente que en el inventario físico figuren igualmente las líneas disponibles con los datos fundamentales de cada una de ellas.

El inventario 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.

4. Comunicaciones y Redes de Comunicaciones.

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 existirá ningún inconveniente para que toda la información de líneas y redes figuren en el mismo inventario que el software y hardware. Por el contrario, debe estimularse la construcción de un inventario de hardware y software único.

En caso de la ausencia o desactualización de los datos anteriores suponen una inconsistencia importante que el auditor deberá recoger con severidad.

a) Aplicaciones Informáticas, Bases de Datos y Ficheros.

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. El entorno auditable se pone de manifiesto principalmente por medio de las siguientes características:

1. Volumen, antigüedad y complejidad de las Aplicaciones.

El auditor en informática hallará un promedio de los conceptos epigrafiados. Se pondrá especial énfasis en la periodicidad de ejecuciones de la carga.

2. Metodología del Diseño

Se calificará globalmente la existencia total o parcial de metodologías en el desarrollo de las aplicaciones. Si se han utilizado varios a lo largo del tiempo, se pondrá de manifiesto tal circunstancia.

Usualmente el hecho de que se haya desarrollado simultáneamente varias aplicaciones con metodologías diferentes, da como resultado un evidente desaprovechamiento de recursos.

3. Documentación.

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes. Una documentación correcta es aún más importante que la homogeneidad metodológica. La documentación de programas disminuye grandemente el mantenimiento de los mismos.

La actividad de mantenimiento de aplicaciones es en la actualidad uno de los problemas más importantes, y representa a veces hasta un 70% del total de los recursos de desarrollo.

4. Cantidad y complejidad de Bases de Datos y Ficheros

El auditor recabará información de tamaño y características de las bases de datos, clasificándolas en relacionales y jerárquicas. Hallará un promedio de número de accesos a ellas por horas o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos. Estos datos proporcionan una visión aceptable de las características de la carga informática.[35]

[35] **Lamére, J.E. La securité informatique.** Aproche metodologique. Traducción La Seguridad Informática. Metodología. Ed. Arcadia. 1987.

5.3 DETERMINACIÓN DE LOS RECURSOS NECESARIOS PARA EFECTUAR LA AUDITORÍA.

Al obtener los resultados del estudio inicial, se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos Materiales.

Su determinación es muy importante, ya que la mayoría de ellos son proporcionados por el cliente, sobre el cual gravita el aumento de carga y las interferencias sobre el desarrollo normal de su trabajo.

Las herramientas software propias del auditor van a utilizarse igualmente en el Sistema auditado, por lo que han de acordar en lo posible las fechas y horas de uso entre auditor y cliente.

a) Recursos Materiales Software.

- Programas propios de la auditoría. Se indicó que son muy potentes y *flexibles. Se añaden a las ejecuciones de los procesos del cliente para* verificar los recorridos de aquellos.
- Monitores. Se utilizan en función del grado de desarrollo observando 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. Es una máxima de la auditoría informática que los procesos de control deben efectuarse necesariamente en los equipos del auditado.

Habrán de acordar, fundamentalmente, "el tiempo de máquina y oportunidad de fecha, hora y duración de las sesiones. También la cantidad de pantallas, espacio en disco, impresoras ocupadas y líneas de comunicación a utilizar y si es necesario de utilizar una línea en exclusiva".[36]

El auditor deberá calcular con la mayor precisión posible los incrementos de carga por él generados.

Recursos Humanos.

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado depende de la materia auditable. Una auditoría general, es habitual la presencia de personas no informáticas pero expertas en temas de organización y análisis de costos.

La auditoría informática y la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

En el siguiente cuadro sinóptico [37] se ha relacionado los perfiles profesionales de lo que podría ser un equipo de auditoria informática para abordar una revisión general de la informática de una organización.

Profesión	*Actividades y conocimientos deseables*
Informático	Con experiencia amplia en Auditoría. Deseables que su labor se haya desarrollado en explotación y en desarrollo de proyectos. Conocedor de Sistemas.

[36] Perry, W.E. Standard for Auditing Computer Applications. Auerbach Publishers Inc. 1986.
[37] de Juan Rivas, A. Pérez Pascual, A. La Auditoría en el desarrollo de Proyectos Informáticos, Ed. Díaz de Santos S.A. 1988.

Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de Proyectos. Experto analista. conocedor de las metodologías de desarrollo más importantes.
Experto de Sistemas	Experto en sistemas operativos y software básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de explotación.
Experto en Base de Datos y Administración de las mismas	Con experiencia en mantenimiento de base de datos. Conocimiento de Productos compatibles y equivalentes. Buenos conocimientos de explotación.
Experto en Software de Comunicaciones	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Experto en subsistemas de teleproceso.
Experto en Explotación y Gestión de Centro de procesamientos de datos	Responsable de algún centro de cálculo. Amplia experiencia en automatización de Trabajos. Experto en relaciones humanas. Buenos conocimientos de los Sistemas.
Experto de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Experto de evaluación de Costos	Economista con conocimiento de informática. Gestión de costos.

5.4 ELABORACIÓN DEL PLAN Y DE LOS PROGRAMAS DE TRABAJO.

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores se establece un plan de trabajo. Decidido éste, se procede a la programación del mismo por parte del responsable de cada sector o de cada especialista, que los reportan al mencionado responsable de la auditoría para la aprobación final.

El Plan de Auditoría se elaborara teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión ha de realizarse por áreas generales o áreas específicas: En el primer caso, la elaboración final es más compleja y costosa, lo cual redunda en una superior calidad.

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 la auditoría parcial el plan no se consideran calendarios porque se manejan recursos genéricos y no específicos.
- En la auditoría global el plan se establecen los recursos y esfuerzos conjuntos que van a ser necesarios.
- El plan establece las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El plan establece la disponibilidad futura del personal y de los demás recursos durante la duración de la revisión.
- El plan estructura las tareas a realizar por cada integrante del equipo.

- En el plan se expresan toda la ayuda que el auditor ha de recibir del auditado.

Una vez elaborado el plan, se procede a la programación de actividades. Esta ha de ser lo suficiente flexible como para permitir modificaciones a lo largo del proyecto. Los programas de trabajo son las cuantificaciones del plan.

En ellos se asignan los recursos humanos y materiales concretos para cada sector del plan. En el programa de trabajo se establece el calendario real de actividades a realizar. La auditoría informática necesita de planificación y programación detallada. Posee la naturaleza de un verdadero proyecto, y por ello le son aplicables las reglas generales de los mismos.[38]

5.5 ACTIVIDADES PROPIAMENTE DICHAS DE LA AUDITORÍA.

Se hará un repaso de las acciones auditoras, las técnicas concretas que se utilizan y las herramientas de las que se ayuda.

Auditoría por temas generales o por áreas específicas

La Auditoría informática general se realiza por áreas generales o por áreas específicas. El método de trabajo es diferente: Si se examina por grandes temas, por ejemplo desde el punto de vista de la seguridad, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Después de revisar la seguridad,

[38] Instituto Mexicano de Contadores Públicos. Normas y Procedimientos de Auditoría. Décimosexta Edición, México, 1996.

pasaríamos luego a la identificación de la Dirección con el modelo informático de la empresa en todas sus áreas, luego a la percepción de los usuarios finales respecto a la explotación, el desarrollo, y finalmente al funcionamiento interno de la informática como centro de trabajo.

Por el contrario, cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a las mismas, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Cuando se aborda la auditoría de desarrollo de aplicaciones, se tienen en cuenta todos los factores qué le afectan, como la seguridad, la percepción del usuario. Una vez finalizada la revisión del área de desarrollo, no es preciso volver sobre el mismo concepto, sino comenzar el análisis de otra rama específica.

Técnicas de Trabajo

Basta con enumerarlas. Ya qué se han conocido a través de los Capítulos anteriores:

- Análisis de la información recabada del auditado
- Análisis de la información propia
- Cruzamiento de las informaciones anteriores
- Entrevistas
- Simulación
- Muestreos

CONCLUSIONES.

La mayor dificultad que tienen las firmas de auditoría en relación con auditorías informáticas, es la asignación de personal a las auditorías con personal adecuadamente entrenado en métodos de computación. A mi parecer hay pocos auditores han recibido entrenamiento formal en la cuestión de sistemas de información.

El auditor debe ser suficientemente competente en métodos y técnicas de auditoría de sistemas para que pueda conducir la auditoría adecuadamente. La experiencia requerida que esta afirmación implica varía dependiendo de la complejidad del sistema que será auditado. La auditoría de una empresa que tenga una instalación pequeña de procesamiento de datos orientada a lotes requiere menos experiencia que una auditoría que implique un complejo sistema de equipo de cómputo.

La auditoría de un sistema basada en una computadora requiere que el auditor posea un buen entendimiento básico de los métodos de procesamiento de datos. Como también es importante un entendimiento específico por parte del auditor de la organización de la documentación, los controles, de las medidas de protección y de las técnicas de auditoría del sistema.

El auditor deberá ser capaz de elegir y poner en práctica el mejor método para cada instalación de procesamiento de datos y para cada prueba de auditoría, sin olvidarse de las características del sistema y del costo y efectividad. También deberá evaluar lo adecuado de los controles asociados con una aplicación particular con objeto de establecer la extensión de los procedimientos de auditoría.

Herramientas

Solamente las mencionaremos:

- Cuestionario general inicial.
- Cuestionarios – Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de Datos).
- Paquetes de Auditoría (*Generadores de Programas*)
- Matrices de Riesgo.[39]

Es conveniente resaltar en este último concepto, ya qué tienen la doble particularidad de que deben ser incorporadas al informe final y de que pueden considerarse también como elemento fundamental para la realización de una audiioría informática de seguridad.

[39] Perry, W.E. Standard for Auditing Computer Applications. Auerbach Publishers Inc. 1986.

BIBLIOGAFÍA.

1. CARRANCA RAÚL Y TRUJILLO, RAÚL CARRANCA Y RIVAS, CÓDIGO PENAL ANOTADO.
2. COLEGIO DE CONTADORES PÚBLICOS DE MÉXICO., DIFERENTES ENFOQUES DE AUDITORÍA EN INFORMÁTICA.
3. CUEVAS GUZMAN, MA. TERESA DE JESÚS, CONTROL Y AUDITORÍA EN CENTROS DE CÓMPUTO, TESIS DE LICENCIATURA.
4. DE JUAN RIVAS, A. PÉREZ PASCUAL, A. LA AUDITORÍA EN EL DESARROLLO DE PROYECTOS INFORMÁTICOS.
5. DERRIER, Y. *LES TECHNIQUES DE LÁUDIT INFORMATIQUE*, DE. DUNOD.
6. ECHENIQUE, JOSÉ ANTONIO, AUDITORÍA EN INFORMÁTICA.
7. FRANCO ROMO, ALFONSO. PLANENCIÓN DE LA *RECUPERACIÓN INFORMÁTICA* EN CASO DE DESASTRE.
8. GUZMAN, MA. TERESA, CONTROL Y AUDITORÍA EN CENTROS DE CÓMPUTO, TESIS DE LICENCIATURA.
9. HANNAN, J. ED. GUÍAS PRÁCTICAS CHIP-AUERBACH.
10. IEEE COMPUTER SOCIERY SYMPOSIUM. PROCEEDING: RESEARCH IN SEGURITY AND PRIVACY.
11. INSTITUTO MEXICANO DE CONTADORES PÚBLICOS. NORMAS Y PROCEDIMIENTOS DE AUDITORÍA.
12. LAMÉRE, J.E. LA SECURITÉ INFORMATIQUE. APROCHE METODOLOGIQUE. TRADUCCIÓN LA SEGURIDAD INFORMÁTICA. METODOLOGÍA.
13. LÓPEZ, ELIZONDO, LA PROFESIÓN CONTABLE. SELECCIÓN Y DESARROLLO.
14. MAIR, ;FILLISM, COMPUTER CONTROL & AUDIT, THE INSTITUTE OF INTERNAL AUDITORS.

15. Perry, W.E. Standard for Auditing Computer Applications. Auerbach Publishers Inc.

16. Rivas Alonso G. Auditoría Informática.

17. Sanchis, F. Planificación y Explotación de Sistemas Informáticos.

18. Sanders H., Donald, Informática: Presente y Futuro.

19. Slosse, Carlos, Auditoría. Un Nuevo Enfoque Empresarial.

20. Thorin, M.La Auditoría Informática. Métodos, Reglas, Normas.

21. Thorin, Marc, La Auditoría en Informática.

22. Weber Ron, EDP Auditing. Conceptual Foundations and Practice

23. William, St. Al., Control y Auditoría del Computador.