UNIVERSIDAD DE EL SALVADOR

FACULTAD CIENCIAS ECONOMICAS

ESCUELA DE CONTADURIA PÚBLICA

"LINEAMIENTOS TÉCNICOS PARA EL DISEÑO DE LA PLANEACIÓN DE AUDITORIA A LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS (SIC)"

Trabajo de Graduación Presentado por:

Funes Ayala, Glenda María
Henríquez Miranda, Cecilia Bersabé
Sibrián de Gómez, Susana Elizabeth

Para obtener el grado de:

LICENCIADO EN CONTADURIA PÚBLICA

Octubre del 2008

San Salvador, El Salvador, Centro América

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	: Master Rufino Antonio Quezada Sánchez
Secretario	: Licenciado Douglas Vladimir Alfaro Chávez
Decano de la Facultad de Ciencias Económicas	: Master Roger Armando Arias Alvarado
Secretaria de la Facultad de Ciencias Económicas	: M.A.E José Ciriaco Gutiérrez Contreras
Asesor Director	: Licenciado Héctor Alfredo Rivas Núñez
Jurado Examinador	: Master Héctor Alfredo Rivas Núñez Licenciado Roberto Carlos Jovel Jovel

Octubre del 2008

San Salvador, El Salvador, Centro América

AGRADECIMIENTOS

Agradezco en primer lugar a Dios todo poderoso por brindarme sabiduría y perseverancia para culminar mis estudios universitarios; a mis padres José Manuel Funes y María Ayala de Funes, por su apoyo incondicional en todo momento; a mis hermanos Jorge, Karla y Mauricio, por sus consejos y apoyo; a mi asesor técnico que nos dio los lineamientos correctos para concluir nuestra investigación; a mis compañeras de trabajo por compartir con migo tantos momentos bonitos y difíciles en el desarrollo de este documento; a mis amigas y amigos por brindarme su cariño y apoyo a lo largo de mi carrera universitaria y en general a todos aquellos que de una u otra manera contribuyeron al logro de éste anhelo.

Glenda María Funes Ayala.

En primer lugar este trabajo fue realizado gracias a la ayuda de nuestro **Dios** quien me ha permitido culminar mis estudios universitarios, a través de la sabiduría, entendimiento y constancia; también a mis padres Ramón Arturo y Maria Dolores por su gran amor, por su apoyo, por su paciencia y comprensión en todo momento; a mis hermanos Juan Ramón y Oscar Antonio por sus valiosos consejos a lo largo de mi carrera; mis compañeras de trabajo de graduación Susana y Glenda porque juntas hemos compartido bonitos momentos en el desarrollo de nuestra investigación y para nuestro asesor Lic. Héctor Rivas por su orientación profesional tan importante para realizar el presente documento.

Cecilia Bersabé Henríquez Miranda.

Agradezco a **"DIOS"** todo poderoso por haberme permitido perseverar y culminar uno de mis grandes retos; a mi madre Celia de los Ángeles Ruiz, quien me apoyo y comprendió a lo largo de la carrera; a mis hermanas y mi hermano por creer y confiar en mi; a mi queridísimo esposo que es un soplo de energía para seguir adelante; a mi asesor Héctor Alfredo Rivas Núñez por el empeño y disposición que mantuvo en el desarrollo de nuestro trabajo; a mis compañeros por compartir buenos y difíciles momentos en el proceso de desarrollo del trabajo de graduación, a mis amigas por su aprecio, y en general, a todas las personas que de una u otra forma hicieron posible este sueño tan anhelado.

Susana Elizabeth Sibrián Ruiz.

LINEAMIENTOS TÉCNICOS ACTUALIZADOS PARA EL DISEÑO DE LA PLANEACIÓN DE AUDITORIA A LOS SISTEMAS DE INFORMACION COMPUTARIZADOS (SIC)

CONTENIDO **PÁG**

RESUMEN EJECUTIVO

Los sistemas de información computarizados han producido un impacto muy significativo en el procesamiento de la información en las empresas. La confianza que la empresa deposita en estos es uno de los principales riesgos que representan dichos sistemas, pues muchos de ellos tienden a tener fallas o ser vulnerables a las manipulaciones y generar información errónea. A nivel mundial se han producido muchos fraudes auxiliados por los sistemas de información computarizados.

El auditor para realizar una auditoria a los sistemas de información computarizados requiere de una planeación especial, en la cual incorpore procedimientos para determinar la vulnerabilidad del sistema, además debe evaluar los diferentes riesgos del sistema y de su ambiente.

Una de las dificultades que enfrenta el auditor, es la de no contar con lineamientos técnicos específicos para realizar una auditoria a los sistemas de información.

En vista de la falta de lineamientos técnicos para el diseño de la planeación de auditoria a los sistemas de información computarizados, que permita desarrollar una auditoria eficiente, se decide realizar un estudio de tipo descriptivo, explicativo y correlacional, que no solo busca describir el fenómeno relacionado al desarrollo de una auditoria de sistemas eficiente, sino que además explicar las razones o causas que provocan dicho fenómeno, en que condiciones se da y como una variable incide o produce efecto en la otra.

El objetivo principal de la investigación fue, elaborar lineamientos técnicos para el diseño de la planeación de auditoria a los sistemas de información computarizados (SIC).

La investigación se centró en la obtención de lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los SIC, mediante la recopilación de información bibliográfica y de campo. Los métodos e instrumentos que se utilizaron fueron la síntesis bibliográfica, análisis documental y la encuesta.

Se creó la hipótesis de trabajo para identificar una posible solución al problema, la cual fue comprobada por medio de una encuesta dirigida a los auditores independientes, inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria.

El resultado de la investigación indicó la necesidad de los auditores de contar con lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los sistemas de información computarizados; la cual contiene los métodos para evaluar el control interno de los sistemas, los procedimientos para determinar las áreas de riesgo, los procedimientos para evaluar el riesgo, los lineamientos para elaborar los procedimientos de auditoria y la descripción de los criterios para identificar los papeles de trabajo.

INTRODUCCIÓN

Habiendo realizado una investigación previa con los auditores independientes que prestan servicios de auditoria de sistemas, se detectó que los auditores tenían dificultad al diseñar la planeación de auditoria, por no contar con lineamientos técnicos actualizados; por lo cual utilizan más tiempo y recursos para desarrollar la auditoria.

Es así como el presente trabajo está orientado a desarrollar una herramienta para el auditor que contenga lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los sistemas de información computarizados, que garantice una auditoria eficiente.

La estructura del trabajo de investigación contiene cuatro capítulos, descritos a continuación:

Capítulo I. Este comprende el desarrollo del marco teórico, que contiene las generalidades sobre la auditoria de sistemas de información computarizados, que constituyen la base teórica del trabajo de investigación desarrollado; los conceptos concernientes al tema en estudio; la parte teórica referente a los sistemas de información computarizados y las características fundamentales de la auditoria de sistemas. Con la diversidad de conceptos incluidos en este capítulo los auditores estarán capacitados para abordar la parte operativa de la auditoria de sistemas de información computarizados.

Capítulo II. Presenta un panorama detallado de la metodología aplicada en el desarrollo de la investigación; se define el área de estudio y los resultados que se espera obtener.

La metodología de la investigación define las técnicas, métodos e instrumentos que se han de utilizar en la recolección de información necesaria para sustentar el trabajo.

Capítulo III. Presenta el desarrollo de lineamientos técnicos actualizados, que está diseñada para ser consultada por los auditores, la cual muestra una síntesis de las Normas Internacionales de Auditoria (NIAs) aplicables a la auditoria de sistemas; así como lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los sistemas de información computarizados; también contiene un apartado en el cual se desarrollan los lineamientos técnicos actualizados para la obtención del legajo de los papeles de trabajo, la elaboración de los programas de auditoria y la elaboración del informe final de auditoria. Por lo tanto, es una guía de apoyo y fuente de consulta a los auditores, a profesionales de otras ramas afines, estudiantes y público en general que deseen conocer técnicas y herramientas enfocadas para el área de sistemas de información computarizados.

Capítulo IV. Se plantean las principales conclusiones y recomendaciones que, según criterio del grupo de trabajo, merecen destacarse y que su puesta en práctica posibilitaría a los auditores independientes, superar en alguna medida las deficiencias y limitantes detectadas en la etapa de investigación.

1. MARCO TEÓRICO

1.1. AUDITORIA DE SISTEMAS DE INFORMACIÓN COMPUTARIZADA

1.1.1. ANTECEDENTES DE AUDITORIA DE SISTEMAS

ANTECEDENTES INTERNACIONALES

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

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

A finales del siglo XVIII, en Inglaterra durante el reinado de Eduardo I, aparece por primera vez el término auditor.

En diversos países de Europa, durante la edad media, muchas eran las asociaciones profesionales, que se encargaban de ejecutar funciones de auditoria, destacándose entre ellas los consejos Londinenses (Inglaterra) en 1310 y el Colegio de Contadores de Venecia (Italia) en 1581.

La revolución industrial llevada a cabo en la segunda mitad del siglo XVIII, imprimió nuevas direcciones a las técnicas contables, especialmente a la auditoria, pasando a atender las necesidades

creadas por la aparición de las grandes empresas donde la naturaleza del servicio es prácticamente obligatorio.

En 1845 "Railway Companies Consolidation Act" obliga a los auditores a verificar anualmente los balances realizados en las compañías.

También en los Estados Unidos de Norteamérica, una importante asociación cuida las normas de auditoria, la cual publicó diversos reglamentos, de los cuales el primero que conocemos data del mes de octubre de 1939, en tanto otros consolidaron las diversas normas en diciembre de 1939, marzo de 1941, junio de 1942 y diciembre de 1943, años en los cuales se tienen antecedentes de las auditorias.

En la actualidad los procedimientos utilizados se han revolucionado con la llegada de los sistemas de información computarizada.

Los sistemas de información computarizada, que forman parte de la organización de una empresa y que solamente proporcionan servicio a otras divisiones, áreas o departamentos de la misma empresa.

Los sistemas de información computarizados han producido un impacto muy significativo en el procesamiento de datos. Muchos de los atributos de un sistema afectan al auditor y al trabajo que este desempeña.

El cambio en los rastreos de auditoria, la velocidad y exactitud de la computadora, así como sus capacidades de revisión, exigen al auditor examinar los procedimientos tradicionales y efectivos para los sistemas electrónicos.

ANTECEDENTES NACIONALES

En El Salvador a partir de la década de los 50´S, los negocios crecían de forma acelerada en lo económico y en lo complejo, de igual manera el sector público sufría el mismo fenómeno estableciendo nuevos requisitos fiscales, imposición y controles. Por ello los grandes negociantes necesitaban reducir tiempo en obtener la información fidedigna y precisa, labor que se dificultaba por el volumen de transacciones que se realizaban; lo cual motivo a la utilización del sistemas de información computarizados agilizando dichas labores.

El uso de equipos de procesamiento electrónico ha venido a facilitar la administración y control en las empresas e instituciones públicas, mejorando los sistemas de información y reduciendo el tiempo de procesar volúmenes de datos.

En la década de los 60´s se extiende la utilización del procesador electrónico de datos en las empresas e instituciones gubernamentales y bancarias; sin embargo, estos procesadores requieren de una instalación especial y una persona capacitada, esto incide el aumento de los costos y la generación de errores.

Hoy en día existen diversidad de procesadores electrónicos; en el país los sistemas de información computarizados se hacen mayormente bajo el proceso de lotes en el cual los departamentos usuarios envían periódicamente pequeños grupos o lotes de transacciones controladas al departamento de cómputo, en éste se transcriben las transacciones

en un formato legible para la máquina y el computador procesa las transacciones correspondientes en un sistema específico. Otro proceso de los sistemas de información computarizados es el proceso en línea, que permite a los departamentos usuarios introducir directamente las transacciones, muchas veces sin los controles que se aplican al proceso en lote.

Muchas empresas aún no utilizan los sistemas de información computarizados debido a imposibilidades económicas, la resistencia al cambio, desconocimiento de los beneficios o la falta de personal capacitado.

1.1.2. CONCEPTUALIZACIÓN

Un sistema es una red de procedimientos relacionados entre sí y desarrollados de acuerdo a un esquema integrado, para lograr una mejor actividad de la empresa.

El concepto de procedimiento, según MLeod Jr, en su obra Sistemas de Información General es:

La sucesión cronológica y secuencial de operaciones concatenadas entre sí constituyen una unidad, en función de la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación.

Sistemas de información computarizados, según J Emey, es un conjunto ordenado de procedimientos (operaciones y métodos), relacionados entre sí, que contribuyen a realizar una función.

Auditoria de sistemas se define según Erick L. Kohler, como cualquier auditoria que conlleva a la revisión y evaluación de todos los aspectos (o cualquiera de sus partes) de un sistema automatizado de procesos de información que están relacionados y las interfaces entre ellos.

El auditor de sistemas actúa sobre el área de los sistemas de información, que normalmente está representada por los siguientes componentes:

- Desarrollo de sistemas de información.
- Asesoría y apoyo técnico a usuarios.
- Desarrollo de sistemas de información.
- Base de datos.
- Manejo de personal.

1.1.3. IMPORTANCIA DE LOS SISTEMAS

La importancia del sistema de información computarizada es que mejora el desempeño de las empresas apoyando la calidad de las decisiones gerenciales. Un sistema de información eficaz reúne, clasifica, guarda, resume y presenta información de tal manera que responda a las interrogantes de importancia de la gerencia que ayuden a la toma de decisiones.

1.1.4. IMPACTO DE LOS SISTEMAS DE INFORMACIÓN

La implantación y uso de un sistema de información dentro de una organización regularmente desencadena una serie de consecuencias, de las cuales unas son positivas y otras negativas.

A continuación, algunas de las ventajas de contar con un sistema de información y algunos puntos negativos que las organizaciones deben enfrentar al implantar un sistema de información:

Entre las ventajas de la utilización de un sistema de información computarizado se mencionan:

- Control más efectivo de las actividades de la organización.
- Integración de las diferentes áreas que conforman la organización.
- Integración de nuevas tecnologías y herramientas de vanguardia.
- Ayuda a incrementar la efectividad en la operación de las empresas.
- Proporciona ventajas competitivas y valor agregado.
- Disponibilidad de mayor y mejor información para los usuarios en tiempo real.
- Elimina la barrera de la distancia, trabajando con un mismo sistema en puntos distantes.

- Disminuye errores, tiempo y recursos superfluos.
- Permite comparar resultados alcanzados con los objetivos programados, con fines de evaluación y control.

Entre las limitaciones se puede mencionar:

- El tiempo que pueda tomar su implementación.
- La resistencia al cambio de los usuarios.
- Problemas técnicos, si no se hace un estudio adecuado, como fallas de hardware, de software o funciones implementadas inadecuadamente para apoyar ciertas actividades de la organización.

1.1.5. COMPONENTES DE LOS SISTEMAS DE INFORMACIÓN

Los sistemas de información dependen de otros subsistemas componentes para poder llevar a cabo las actividades de entrada, proceso, salida, almacenamiento y control, que convierten los datos en productos de información. Estos subsistemas incluyen personas, hardware, software, procedimientos y datos. A continuación se detallan cada uno de ellos.

Personas: Un sistema de información computarizada involucra una variada gama de personas relacionadas con el mismo, puesto que su construcción, mantenimiento y uso representan una labor con cierto grado de complejidad. Se pueden dividir en dos grandes grupos los cuales son:

- Los usuarios finales son aquellos que operan o interactúan directamente con el sistema a través de una estación de trabajo o incluso, quienes reciben reportes e información generada por el sistema.

- Entre los profesionales se encuentran los analistas de los sistemas de información, encargados de idear soluciones cuando se requiere un nuevo sistema, actualizarlo, modificarlo o reconstruirlo; los programadores, que crean los programas de cómputo que forman parte de los sistemas de información; los administradores del sistema, encargados de mantener el sistema en buenas condiciones y los capacitadores, que instruyen y preparan a los usuarios para la utilización del sistema.

Según J. Emey en su obra "Sistemas de Planteamiento y Control de la Empresa"

Hardware: consiste en los equipos, dispositivos y medios necesarios que constituyen la plataforma física mediante la cual, el sistema de información puede funcionar. Se incluyen aquí, los que permiten las comunicaciones y los enlaces de red; estos recursos son por ejemplo: computadoras, monitores, impresoras, disquetes o componentes de almacenamiento de información externos, disco óptico, papel de impresión, cableado de red, y otros.

Software o programas: son el componente lógico, es decir, los programas, las rutinas e instrucciones que conforman el sistema de información. Se les suele denominar aplicación de sistema de

información. Es así como los sistemas de información pueden tener aplicaciones particulares, por ejemplo, para el área de ventas, de contabilidad, de personal o de compras. La aplicación que conforma un sistema de información completo contiene subconjuntos de programas que se encargan de apoyar las distintas actividades propias de la organización.

Un sistema comprende tres niveles:

1. El nivel de datos fuente (Entrada)
2. El nivel de procesamiento de datos (Procesamiento)
3. El nivel de reportes (Salida)

Procedimientos: consiste en los pasos secuenciales para indicar que datos se necesitan y cuando, así como donde obtenerlos y en que forma utilizarlos.

El procesamiento de datos es la capacidad de la computadora para ejecutar instrucciones en clave (codificadas) y lleva a cabo estas instrucciones por medio de una unidad de control y un sistema de circuitos electrónicos. Las instrucciones propiamente dichas reciben el nombre de programas.

Durante el procesamiento, los datos se almacenan en la unidad central de procesamiento, este almacenamiento interno o memoria de la computadora se conoce como almacenamiento temporal.

Los datos: son el documento fuente, del cual procede la información que será procesada en el sistema; entre estos documentos fuente se pueden mencionar facturas, acuerdos, nóminas, declaraciones y otros.

Normalmente los datos se trasmiten a la unidad central de procesamiento por medio de tarjetas perforadas, cintas de papel, cintas magnéticas, caracteres magnéticos y discos magnéticos.

1.1.6. EL CONTROL INTERNO RELACIONADO A LOS SIC

El autor J. Emey define el control interno como:

El plan de organización y todos los métodos coordinados y medidas adaptadas dentro de un negocio para salvaguardar sus activos, verificar la exactitud y confiabilidad de sus datos, mejorar la eficiencia de las operaciones y alentar el apego a las políticas prescritas.

La finalidad del control interno es asegurar el SIC. La utilización de éste exige emplear nuevos controles; mientras que ciertas medidas tradicionales de control posiblemente han disminuido.

La división de las responsabilidades funcionales debe trazar una clara separación entre las funciones de iniciar y autorizar la transacción, el registro de la transacción por escrito y la custodia de los activos resultantes.

La división de funciones brinda las eficiencias derivadas de la especialización, permite efectuar una verificación cruzada que de precisión y aumente la efectividad de un sistema de control directivo.

La automatización ha producido una mayor centralización de las actividades de procesamiento de datos y la concentración de las funciones de dicho proceso.

Uno de los principios fundamentales del control interno es la separación entre las personas que autorizan una transacción, las que ejercen custodia sobre los activos adquiridos, y quienes registran la contabilidad de dichos activos.

Es necesario separar la función de planeamiento de los sistemas y programación; tal separación es importante por las siguientes razones:

- Proporciona una eficaz verificación cruzada de la exactitud y corrección de los cambios introducidos en el sistema.
- Impide al personal de operación efectuar revisiones sin previa autorización y plena verificación.
- Evita que el personal ajeno a la operación tenga acceso al equipo.

- Mejora la eficiencia, puesto que las capacidades, el adiestramiento y las pericias que se requieren para desempeñar diversas actividades, difieren notablemente.

Controles de los datos fuente[1]

Las finalidades perseguidas por los controles de los datos fuente son:

- Determinar que todas las transacciones se hayan registrado correctamente en su punto de origen o fuente.

- Determinar que todas las transacciones se trasmitan del punto de registro al de procesamiento.

Registro correcto: En los sistemas de información computarizados, en que el documento fuente se elimina o está en tal forma que no permite la revisión humana, existen dos soluciones básicas para garantizar su registro correcto. La primera es retroceder el control hacia el punto de origen a fin de permitir que el acceso al equipo de transmisión, registro, y el uso del mismo, queden debidamente controlados para evitar su uso desautorizado o impropio. Una segunda solución consiste en dejar que la computadora ejerza la misma revisión de la transacción que la que efectuaran personas.

[1] J, Emey, España 2004 "Sistemas de Planteamiento y Control de la Empresa", edición Pirámide.

La capacidad de revisión y corrección de la computadora puede utilizarse para descubrir, en la preparación del material de entrada, errores que no habían sido advertidos por la revisión humana.

Las verificaciones programadas para determinar la validez de los datos de entrada o fuente son:

1. Verificación de existencia
2. Verificación de combinación
3. Verificación de totalidad
4. Verificación de razonabilidad

Las verificaciones de existencia, se usan para determinar si un cierto código (clave) de transacción continua es válido.

Las verificaciones de combinación, se usan en aquellas transacciones en las cuales diversos sectores o campos del registro se relacionan lógicamente entre sí.

Las verificaciones de totalidad, tienen por objeto asegurar que la entrada tenga el número total de datos prescritos en todas las categorías de información.

Las verificaciones de razonabilidad, se usan para probar los campos de registro y ver si no se han excedido ciertos límites predeterminados.

Transmisión de todas las transacciones. El segundo objeto de ejercer control de los registros es determinar que todas las transacciones se transmitan desde el punto de registro hasta el punto de procesamiento. Para lograr este objetivo en los sistemas de información computarizados, se han usado técnicas de pruebas totales, o de lote cuando los documentos fuente se convierte en datos de entrada traducidos a lenguaje de máquina y las transacciones se ordenan en una secuencia de acuerdo con el orden de los registros en el archivo.

Controles del procesamiento

El centro de los sistemas de información computarizados se ocupa exclusivamente de procesar los datos que se le remitan de acuerdo con instrucciones y procedimientos previamente establecidos. La exactitud del procesamiento depende de la precisión y veracidad de la programación de las verificaciones diseñadas e incorporadas al equipo por el fabricante; así como las verificaciones programadas que el usuario incluya en sus programas. La exactitud y precisión de la programación depende de la concepción cuidadosa y la realización esmerada tanto del diseño de los sistemas como de las instrucciones del programa, de la adecuada documentación, así como de su acertada revisión y aprobación.

La exactitud del procesamiento de datos en un sistema de información computarizado, se logra mediante verificaciones programadas; las

cuales pueden clasificarse en relación con los objetivos básicos de los controles del procesamiento.

Los objetivos básicos de los controles de procesamiento son los siguientes:

- Descubrir la pérdida de datos o la falta de su procesamiento.
- Determinar que las funciones aritméticas se ejecuten correctamente.
- Determinar que todas las transacciones se asienten en el registro indicado.

Controles de salida

La función de los controles de salida, es determinar que los datos procesados no incluyan ninguna alteración desautorizada por la sección de operación de la computadora, y que los datos son sustancialmente correctos o razonables[2].

El control de salida más básico es la comparación de los totales de control de los datos procesados con los totales obtenidos independientemente de procesos anteriores o de los datos fuente originales. El muestreo sistemático de renglones individuales procesados proporciona otro control de salida.

Además de los controles de organización y de procedimientos, todo sistema de información computarizado necesita controles

[2] J, Emey, "Sistemas de Planteamiento y Control de la Empresa", edición Pirámide, España 2004.

administrativos. Estos controles pueden asociarse con la formulación, documentación y administración de los métodos y prácticas de operación en el diseño de sistemas, la programación y las operaciones de la computadora.

Controles sobre las operaciones de la computadora[3]

Uno de los más importantes controles sobre las operaciones de la computadora, es el riesgo que se mantiene para marcar el tiempo de análisis; este registro de utilización consigna las operaciones de la computadora, el uso del equipo y el tiempo consumido en procesar un trabajo; tal registro debe ser analizado y revisado por personal de operación responsable, para determinar el tiempo que se requiere para procesar cada uno de los trabajos y las razones de todas las demoras.

1.1.7. EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

La evaluación del sistema de control interno mide la calidad del sistema y proporciona al auditor las bases sobre las cuales este construirá su examen y derivará sus conclusiones.

El mejor punto de partida para evaluar el control interno es revisar la documentación, después observar las actividades de procesamiento

[3] J, Emey "Sistemas de Planteamiento y Control de la Empresa", edición Pirámide, España 2004

de datos, e interrogar a las personas encargadas de desempeñar esas actividades. Tal revisión es necesaria para determinar la existencia de un sistema de información, así como para evaluar los controles empleados para fomentar el apego a las políticas de las empresas y para lograr eficiencias de operación[4].

1.1.8. PRINCIPALES FRAUDES EN LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS[5]

Entre los fraudes más comunes que se presentan en los sistemas de información computarizados, figuran entre otros los siguientes:

a) Manipulación de datos: ha sido el método más utilizado para la comisión de fraudes, en ambientes automatizados.

b) La técnica de salami: que consiste en sustraer pequeñas cantidades de un gran número de registros, mediante la activación de rutinas incluidas en los programas aplicativos corrientes.

c) Técnica del caballo de troya: consiste en insertar instrucciones de programación, en los programas aplicativos, con objetivos de fraude, de manera que, además de las funciones propias del programa, también ejecuten funciones no autorizadas por la administración.

---

[4] Gómez Girón, José Alfredo; Año 1999, "Diseño de un Modelo de Evaluación de los Niveles de Riesgo en la Auditoria de Sistemas de Procesamiento Electrónico de Datos", Trabajo de graduación, Universidad de El Salvador.

[5] http/bibliotec.bcv.org.ve/cgi_win/b_alex.exe
Aguilar Molina, Jennifer Magali, "La auditoria forense como herramienta para combatir fraudes y delitos", Universidad de El Salvador, 2005

d) Bombas lógicas: son una técnica de fraude, en ambientes computarizados, que consiste en diseñar instrucciones fraudulentas en software autorizado, para ser activadas cuando se cumpla una condición o estado específico.

e) Juego de la pizza: es un método relativamente fácil para lograr el acceso no autorizado a los centros de procesamiento de datos, así estén adecuadamente controlados.

f) Ingeniería social: esta técnica de fraude informático consiste en planear la forma de abordar a quienes puedan proporcionar información valiosa o facilitar de alguna forma la comisión de hechos ilícitos.

g) Trampas-puertas: son deficiencias del sistema operacional desde las etapas del diseño original.

h) "Superzaping": permite adicionar, modificar y/o eliminar registros de archivos, datos de registros o agregar caracteres dentro de un archivo maestro, sin dejar rastro y sin modificar ni correr los programas normalmente usados para mantener los archivos.

i) Evasiva astuta: se trata que los programadores de sistemas se inventaron la forma de comunicarse con la computadora a través del lenguaje de máquina (es un método fácil para entrar en la computadora, cambiar las cosas, hacer que algo suceda y hasta recambiarlas para que vuelvan a su forma original sin dejar rastros para auditoria).

j) Recolección de basura: es una técnica utilizada para obtener información abandonada dentro o alrededor del sistema de computación, después de haber realizado una operación cualquiera.

k) Ir a cuenta para tener acceso no autorizado: es una técnica para lograr el acceso no autorizado a los recursos del sistema, entrando detrás de alguien influyente ("piggyback") o por imitación (suplantación).

i) Puertas levadizas: consiste en la utilización de datos sin la debida autorización, mediante rutinas involucradas en los programas o en los dispositivos de hardware.

l) Técnica del taladro: consiste en utilizar una computadora para llamar con diferentes códigos hasta cuando uno de ellos resulte aceptado y permita el acceso a los archivos deseados.

m) Intercepción de líneas de comunicación: esta técnica de fraude consiste en establecer una conexión secreta telefónica o telegráfica para interceptar mensajes, también es técnicamente posible la intercepción de comunicaciones por micro-ondas y vía satélite.

1.1.9. IMPORTANCIA DE LA AUDITORIA DE SISTEMAS

La modernización de las empresas es sinónimo de alta tecnología combinada con la reingeniería en sus sistemas, tanto a nivel organizacional como en sus productos y servicios.

A medida que avanza la tecnología, se presentan nuevas necesidades de información, se generan nuevos servicios, se facilitan las transacciones, se complican los controles aplicados a los sistemas, se incrementan los volúmenes de información procesada, se incrementan incalculablemente los niveles de riesgo para las empresas, entre otros; es por esto necesario desarrollar una auditoria de sistemas con el fin de detectar y minimizar los riesgos que significan daños y prejuicios para las empresas.

1.1.10. RIESGOS DE LA AUDITORIA DE SISTEMAS

El auditor al crear su trabajo de planeación deberá considerar el riesgo de la auditoria, éste es el riesgo de proporcionar una conclusión errónea sobre el funcionamiento de los sistemas de información computarizados.

El auditor está expuesto a la suspensión temporal o definitiva del ejercicio, debido a litigios u otros acontecimientos que surjan con relación a sus conclusiones.

Existen tres tipos de riesgos a considerar en el desarrollo de la auditoria de sistemas los cuales son:

Riesgo inherente: Es la susceptibilidad de cada una de las áreas de los sistemas, ya sea en lo individual o cuando se integra con otras áreas, suponiendo que no hay controles relacionados.

Riesgo de control: Es el riesgo de fallas o vulnerabilidad en cada una de las áreas de los sistemas, ya sea en lo individual o cuando se integra con otras áreas y no se prevenga o detecte y corrija oportunamente por el control interno de la entidad.

Riesgo de detección: Es el riesgo de que el auditor no detecte una falla o susceptibilidad que existe en los sistemas. El riesgo de detección es una función de la efectividad de un procedimiento de auditoria y de su aplicación por parte del auditor.

1.1.11. PROCESO DE LA AUDITORIA DEG SISTEMAS

Las auditorias de sistemas son cambiantes y dinámicas para acomodarse a las actividades a que se dedica el cliente, las cuales representan una infinidad de variadas operaciones, por lo que en el ciclo de auditoria deben desarrollarse ocho pasos que necesariamente se ejecutan de forma integrada y secuencial, o combinadas, los cuales son:

1. Compresión de los sistemas.
2. Registro de la comprensión.
3. Evaluación preliminar del control interno de los sistemas.
4. Confirmación de controles.
5. Evaluación del riesgo.
6. Determinación de áreas criticas.
7. Emisión del informe.

1.1.12. ENFOQUE DE LA AUDITORIA TRADICIONAL

La palabra auditoria se ha empleado incorrectamente y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a acuñar la frase (tiene auditoria) como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo auditoria. El concepto de auditoria es más amplio; no solo detecta errores, sino que es un examen crítico que se realiza con objeto de evaluar la eficacia y eficiencia de una sección o de un organismo con miras a corregir o mejorar la forma de actuación.

1.1.13. ENFOQUE DE LA AUDITORIA MODERNA - EL AUDITOR DE SISTEMAS

Los profesionales responsables del auditor en ambientes computarizados, deben poseer una sólida formación en administración, control interno, informática y auditoria.

En administración deben manejar con habilidad y destreza las funciones básicas del proceso administrativo, tales como: planeación, organización, dirección y control; con una mentalidad de hombre de negocios y dentro de las modernas teorías de la planeación estratégica y la calidad total.

En materia de control interno, el auditor informático, debe estar en capacidad de diagnosticar su validez técnica desde un punto de vista sistémico total, esto quiere decir que deberá entender el control interno como sistema y no como un conjunto de controles distribuidos de cualquier manera en las organizaciones.

El auditor deberá analizar y evaluar la estructura conceptual del sistema de control interno, teniendo en cuenta para ello los controles preventivos, detectivos y correctivos. Comprometerse con una conclusión objetiva e independiente, en relación con el grado de seguridad y de confiabilidad del sistema de control vigente en el área de informática.

En esencia, un sistema de control interno, para el área de informática, comprende por lo menos los siguientes elementos: objetivos, políticas y presupuestos perfectamente definidos; estructura de organización sólida; personal competente; procedimientos operativos y de control, efectivos y documentados; sistema de información confiable y oportuno; sistema de seguridad de todos los recursos y sistema de auditoria efectivo.

Como puede observarse, la función de auditoria es un elemento de control interno, que goza de un privilegio muy especial y es el de monitorear permanentemente los otros controles y operaciones del ente auditado.

La temática del concepto de control interno exige del auditor una formación avanzada en administración de recursos informáticos, sobre

la base de que no se puede diagnosticar una determinada realidad sin estar en condiciones de conocerla y entenderla plenamente.

En la era de la informática, el auditor debe entender que su papel profesional debe ser el de asesor gerencial para asegurar el éxito de la función y, en consecuencia, debe visualizar la empresa y su futuro en forma sistémico-estructural, articulando ordenadamente los objetivos del área informática con la misión y los objetivos de la organización en su conjunto.

En informática, el auditor debe conocer por lo menos, cómo funcionan los computadores, cuales son sus reales capacidades y limitaciones, las marcas, las potencialidades y la calidad de los componentes de hardware y de software, los ambientes de procesamiento, los sistemas operacionales, los sistemas de seguridad, los riesgos posibles, los principales lenguajes de programación, las tecnologías de almacenamiento y la metodología para la generación y mantenimiento de sistemas de información. En general el auditor de sistemas debe estar al día en los avances científico-tecnológicos sobre la materia.

En el campo de la auditoria, el auditor informático, debe conocer y manejar deseablemente la teoría básica de la auditoria, en términos de conceptos, filosofía, ética, taxonomía, normatividad, técnicas, procedimientos, metodología, papeles de trabajo e informes.

El auditor informático, debe ser una persona de muy buenas relaciones humanas, respetuoso de la opinión de los demás, analítico, crítico, buen oidor, amable, objetivo, de espíritu científico, con habilidad y

capacidad para trabajar bajo presión, con un amplio sentido de responsabilidad social y por sobre todo, que goce de un comportamiento ético a toda prueba.

1.1.14. ENFOQUES DE LA AUDITORIA INFORMÁTICA

Auditoria Alrededor del Computador[6]

En este enfoque de auditoria, los programas y los archivos de datos no se auditan.

La auditoria alrededor del computador concentra sus esfuerzos en la entrada de datos y en la salida de información. Es el más cómodo para los auditores de sistemas, por cuanto únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina. Naturalmente que se examinan los controles desde el origen de los datos para protegerlos de cualquier tipo de riesgo que atente contra la integridad, completitud, exactitud y legalidad.

La auditoria alrededor del computador no es tan simple como aparentemente puede presentarse, pues tiene objetivos muy importantes como:

- Verificar la existencia de una adecuada segregación funcional.

[6] Propuesta de una "Guía técnica en el área de auditoria de seguridad informática para verificar la confiabilidad de la información procesada en los sistemas contables computarizados", Moreno Salamanca, Universidad de El Salvador, año 2005.

- Comprobar la eficiencia de los controles sobre seguridades físicas y lógicas de los datos.

- Asegurarse de la existencia de controles dirigidos a que todos los datos enviados a proceso estén autorizados.

- Comprobar la existencia de controles para asegurar que todos los datos enviados sean procesados.

- Cerciorarse que los procesos se hacen con exactitud.

- Comprobar que los datos sean sometidos a validación antes de ordenar su proceso.

- Verificar la validez del procedimiento utilizado para corregir inconsistencias y la posterior realimentación de los datos corregidos al proceso.

- Examinar los controles de salida de la información para asegurar que se eviten los riesgos entre sistemas y el usuario.

- Verificar la satisfacción del usuario, en materia de los informes recibidos.

- Comprobar la existencia y efectividad de un plan de contingencias, para asegurar la continuidad de los procesos y la recuperación de los datos en caso de desastres.

Se puede apreciar la ambición de los objetivos planteados, pues solamente faltarían objetivos relacionados con el examen de los archivos y los programas, lo cual es parte de otro enfoque.

Informe de esta auditoria: deberá redactarse en forma sencilla y ordenada, haciendo énfasis en los riesgos más significativos e indicando el camino a seguir mediante recomendaciones económicas y operativamente posibles.

Pasos que se deben seguir en la auditoria:

- Metodología de la auditoria.
- Objetivos de la auditoria.
- Evaluación del sistema de control interno.
- Deficiencias de control interno.
- Procedimientos de auditoria.
- Papeles de trabajo.
- Informe de auditoria.

Auditoria a Través del Computador

Este enfoque está orientado a examinar y evaluar los recursos del software, y surge como complemento del enfoque de auditoria alrededor del computador, en el sentido de que su acción va dirigida a evaluar el sistema de controles diseñados para minimizar los fraudes y los errores que normalmente tienen origen en los programas.

Este enfoque es más exigente que el anterior, por cuanto es necesario saber con cierto rigor, lenguajes de programación o desarrollo de sistemas en general, con el objeto de facilitar el proceso de auditoria.

Objetivos de esta auditoria:

1. Asegurar que los programas procesan los datos, de acuerdo con las necesidades del usuario o dentro de los parámetros de precisión previstos.

2. Cerciorarse de la no-existencia de rutinas fraudulentas al interior de los programas.

3. Verificar que los programadores modifiquen los programas solamente en los aspectos autorizados.

4. Comprobar que los programas utilizados en producción son los debidamente autorizados por el administrador.

5. Verificar la existencia de controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.

6. Cerciorarse que todos los datos son sometidos a validación antes de ordenar su proceso correspondiente.

Informe de auditoria: deberá orientarse a opinar sobre la validez de los controles, en este caso de software, para proteger los datos en su proceso de conversión en información.

Auditoria con el Computador

Este enfoque va dirigido especialmente, al examen y evaluación de los archivos de datos en medios magnéticos, con el auxilio del computador y de software de auditoria generalizado y /o a la medida. Este enfoque es relativamente completo para verificar la existencia, la integridad y la exactitud de los datos, en grandes volúmenes de transacciones.

La auditoria con el computador es relativamente fácil de desarrollar porque los programas de auditoria vienen documentados de tal manera que se convierten en instrumentos de sencilla aplicación. Normalmente son paquetes que se aprenden a manejar en cursos cortos y sin avanzados conocimientos de informática. Los paquetes de auditoria permiten desarrollar operaciones y prueba, tales como:

- Recálculos y verificación de información, como por ejemplo: relaciones sobre nómina, montos de depreciación y acumulación de intereses, entre otros.
- Demostración gráfica de datos seleccionados.
- Selección de muestras estadísticas.
- Preparación de análisis de cartera por antigüedad.

Informe de auditoria: este informe deberá tratar sobre la confiabilidad del sistema de control interno para proteger los datos sometidos a proceso y la información contenida en los archivos maestros.

1.1.15. SIMILITUDES Y DIFERENCIAS DE LA AUDITORIA TRADICIONAL Y LA AUDITORIA DE SISTEMAS

SIMILITUDES:

- No se requieren nuevas normas de auditoria, son las mismas.
- Los elementos básicos de un buen sistema de control interno siguen siendo los mismos; por ejemplo: la adecuada segregación de funciones.
- Los propósitos principales del estudio y la evaluación del control interno son: la obtención de evidencia para respaldar una opinión y determinar la base, oportunidad y extensión de las pruebas futuras de auditoria.

DIFERENCIAS:

- Se establecen algunos nuevos procedimientos de auditoria.
- Hay diferencias en las técnicas destinadas a mantener un adecuado control interno.
- Una diferencia significativa es que en algunos procesos se usan programas o sistemas.
- El énfasis en la evaluación de los sistemas manuales está en la evaluación de transacciones, mientras que el énfasis en los sistemas informáticos, está en la evaluación del control interno.
- En la auditoria de sistemas, el auditor utiliza los sistemas informáticos para ejecutar su auditoria ya que le permite

ampliar la cobertura de su examen, reduciendo los costos en personal y tiempo que de otra forma (manual) llevarían más tiempo para su ejecución.

- La auditoria financiera efectúa un examen sistemático de los estados financieros, los registros y las operaciones correspondientes para determinar la observancia de los principios de contabilidad, de las políticas de la administración y la planificación; mientras que la auditoria de sistemas efectúa un examen sistemático y de evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad de la información que se procesa a través de los sistemas de información.

1.1.16. FASES DE LA AUDITORIA DE SISTEMAS[7]

Para el desarrollo eficiente y eficaz de la auditoria de sistemas de información computarizados se efectúan tres fases, las cuales son:

Planeación de la auditoria de sistemas

Para hacer una adecuada planeación de la auditoria de sistemas, hay que seguir una serie de pasos previos que permitirán dimensionar el

[7] http://www.mailxmail.com/curso/empresa/auditoriaelemental/capitulo11.htm

tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoria en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los siguientes objetivos:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar; para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base a ésto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

Ejecución

En esta fase se realizan diferentes tipos de pruebas y análisis a los sistemas de información computarizados, para determinar su funcionabilidad y razonabilidad; entre estos se encuentran:

1. Las pruebas de auditoria.
2. Técnicas de muestreo.
3. Evidencias de auditoria.

4. Papeles de trabajo.

5. Hallazgos de auditoria.

Se detectan los errores, si los hay, se evalúan los resultados de las pruebas y se identifican los hallazgos.

En ésta fase se elaboran las conclusiones y recomendaciones que se comunicarán a las autoridades de la entidad auditada.

Aunque las tres fases son importantes, esta fase viene a ser el centro de lo que es el trabajo de auditoria, donde se realizan todas las pruebas y se utilizan todas las técnicas o procedimientos para encontrar las evidencias de auditoria que sustentarán el informe de auditoria.

Informe (comunicación de resultados y el seguimiento).

En esta fase se analizan las comunicaciones que se dan entre la entidad auditada y los auditores, es decir:

a) Comunicaciones de la entidad, y

b) Comunicaciones del auditor

Entre las primeras comunicaciones de la entidad tenemos:

- ❖ Carta de representación.
- ❖ Reporte a partes externas.

En las comunicaciones del auditor están:

- Memorandum de requerimientos.
- Comunicación de hallazgos.
- Informe de control interno.
- Informe especial.
- Dictamen.
- Informe final.

Si en el transcurso del trabajo de auditoria surgen hechos o se encuentran algunos o algún hallazgo que a juicio del auditor es grave, se deberá hacer un informe especial, dando a conocer el hecho en forma inmediata, con el propósito de que sea corregido o enmendado a la mayor brevedad.

Así mismo, si al analizar el sistema de control interno se encuentran serias debilidades en su organización y contenido, se debe elaborar por separado un informe sobre la evaluación del control interno.

El informe final del auditor, debe estar elaborado de forma sencilla y clara, ser constructivo y oportuno.

Las entidades auditadas deben estar siendo informadas de todo lo que acontezca alrededor de la auditoria, por tanto, podrán tener acceso a cualquier documentación relativa a algún hecho encontrado.

1.2. NORMATIVA LEGAL Y TÉCNICA APLICABLE A LOS SIC

Normativa Legal

El auditor debe conocer sobre las diferentes leyes que regulan a los sistemas de información computarizados, para identificar los riesgos legales a los que pueden enfrentarse las empresas al utilizar dichos sistemas y determinar el apego o no a las regulaciones.

Existe diversidad de leyes y regulaciones; de las cuales son aplicables a los sistemas de información computarizada los siguientes:

- Código tributario.
- Ley de registro de comercio.
- Ley de impuesto sobre la renta.
- Ley de impuesto a la transferencia de bienes muebles y a la prestación de servicios.
- Ley de fomento y protección a la propiedad intelectual.
- Otras leyes o normativas vigentes en el país que tengan una relación directa con el tema en estudio.

Las leyes antes mencionadas abordan las regulaciones aplicables al entorno de los sistemas; además de estas existen normas internas de cada institución que deben ser consideradas, ya sean acuerdos, contratos, convenios, entre otros.

Normativa Técnica

En el país no existe una normativa técnica para el desarrollo de una auditoria a los sistemas de información computarizados, únicamente se encuentran vigentes las Normas Internacionales de Auditoria (NIAs), las cuales son dirigidas a auditorias de estados financieros; pero su aplicación se amplía a los diferentes tipos de auditoria incluyendo la auditoria a los sistemas de información computarizados.

Las Normas Internacionales de Auditoria (NIAs) son amplias; pero las normas empleadas en la realización de una auditoria de sistemas son las siguientes:

- NIA 230 Documentación de auditoria.
- NIA 240 Responsabilidad del auditor de considerar el fraude en una auditoria de estados financieros.
- NIA 300 Planeación de una auditoria de estados financieros.
- NIA 315 Entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa.
- NIA 500 Evidencia de auditoria.
- NIA 530 Muestreo de la auditoria y otros medios de pruebas
- NIA 620 Uso del trabajo de un experto.
- NIA 800 El dictamen del auditor sobre trabajos de auditoria con propósito especial.

Las normas mencionadas no son específicas para la realización de una auditoria de sistemas de información computarizados, pero proporcionan lineamientos generales para llevar a cabo una auditoria. Adicional a las Normas Internacionales de Auditoria (NIAs) se emitieron las Declaraciones Internacionales de Práctica de Auditoria (DIPAs) que tratan sobre los SIC las cuales son:

- ❖ DIPA 1001 Ambientes de CIS - Computadoras independientes.

  -Derogada en diciembre de 2004.

- ❖ DIPA 1002 Ambientes de CIS - Sistemas de computadoras en línea.

  - Derogada en diciembre de 2004.

- ❖ DIPA 1003 Ambientes de CIS - Sistemas de base de datos.

  - Derogada en diciembre de 2004.

- ❖ DIPA 1008 Evaluación del riesgo y el control interno - Características y consideraciones del CIS.

  - Derogada en diciembre de 2004.

- ❖ DIPA 1009 Técnicas de auditoria con ayuda de computadora.

  - Derogada en diciembre de 2004.

Las DIPAs en su mayoría han sido derogadas, y algunos lineamientos se han incorporado a las normas; es por eso que serán mencionadas en la presente investigación.

2. METODOLOGÍA Y DIAGNOSTICO DE INVESTIGACIÓN

2.1. DISEÑO METODOLÓGICO

2.1.1. TIPO DE INVESTIGACIÓN

El problema relacionado a la realización de una auditoria de sistemas de información computarizados (SIC) eficiente por parte del auditor, fue investigado mediante el enfoque hipotético deductivo, analizando desde una perspectiva general hasta descubrir la causa fundamental del fenómeno, con el propósito de plantear una alternativa de solución.

2.1.2. TIPO DE ESTUDIO

La metodología utilizada representa la forma en que se organizó el proceso de investigación y los resultados obtenidos; así como la consecución de los objetivos y alcance de la investigación.

En la investigación se utilizó el estudio de tipo descriptivo, explicativo y correlacional, que pretende no solo describir el fenómeno relacionado a la realización de una auditoria eficiente sobre el funcionamiento de los sistemas de información computarizados, sino explicar las razones o causas que provocan dicho fenómeno, en qué condiciones se da y como una variable incide o produce efecto en la otra.

2.1.3. DETERMINACIÓN DE LA POBLACIÓN

Para la investigación, se consideró como población todos los profesionales que ejerzan la auditoria, tomando como referencia el registro del Concejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria (CVPCPA), inscritos hasta el 31 de diciembre de 2007 (publicación del Diario Oficial, tomo 379, publicado el 09 de abril del 2008) y que tengan su sede en el municipio de San Salvador.

2.1.4. DETERMINACIÓN DE LA MUESTRA

Para la determinación de la muestra, por tratarse de una población finita se utilizó la fórmula del muestreo estadístico para población finita[8].

$$n = \frac{NPQZ^2}{(N-1)e^2 + Z^2PQ}$$

Donde:

n = Tamaño de la muestra = ? = 72 Auditores.

N = Población = 3,434 número de profesionales inscritos en el CVPCPA al 31 de diciembre de 2007.

Z^2 = Coeficiente de confianza al cuadrado = 1.96

P = Probabilidad de éxito (≤ 1) = 0.95

Q = Probabilidad de fracaso (1-p) = (1-0.95) = 0.05

e = Margen de error = 0.05

Aplicando la fórmula:

[8] Bonilla, Gildaberto "Como hacer una tesis con técnicas estadísticas"

$$n = \frac{3434\,(0.95)(0.05)(1.96)^2}{(3434-1)0.05^2 + 1.96^2(0.95)(0.05)} = 71.48 \approx 72$$

n= 72 auditores es la muestra de la población

Para el desarrollo de la investigación se consideró el 95% de probabilidad de éxito tomando como parámetro, el hecho de que los auditores hayan realizado auditorias de sistemas y un 0.5% de margen de error.

La selección de la muestra, se realizó de forma aleatoria simple sobre los auditores inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria que cumplan con la característica que tenga su sede en el municipio de San Salvador. La forma de escoger los elementos de la muestra se efectuó utilizando la tabla de números aleatorios.

2.1.5. UNIDAD DE ANÁLISIS

En la investigación la unidad de análisis que se consideró fue, el resultados de la encuesta dirigida a los profesionales que ejercen la auditoria y que se encuentren inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria, con el fin de analizar la incidencia de la falta de lineamientos técnicos en el desarrollo de una auditoria eficiente sobre el funcionamiento de los sistemas de información computarizados.

2.1.6. MÉTODOS E INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN

Las técnicas e instrumentos utilizada para la obtención de información referente al tema sujeto de estudio, se dividió en:

2.1.7. INVESTIGACIÓN DOCUMENTAL

Consiste en la información contenida en libros, revistas, tesis, brochures, boletines, páginas Web, entre otros. Dicha información fue utilizada para sustentar el criterio técnico, legal y genérico del tema en estudio. Para la recolección se utilizó la técnica de análisis y sistematización documental, para compilar los datos de las normas legales, normas contables, Normas Internacionales de Auditoria (NIAs), de libros, revistas, periódicos, trabajos de investigación e internet; relacionados con el tema de investigación.

2.1.8. INVESTIGACIÓN DE CAMPO

El instrumento utilizado en la investigación para la recolección de datos, fue un cuestionario que constó de preguntas cerradas y abiertas, dirigido a los auditores considerados en la muestra (ver anexo 1); se utilizó con el fin de determinar los lineamientos a seguir para la realización de auditoria a los sistemas de información computarizados (SIC) eficiente, además de los procesos que se utilizan para realizar dicha auditoria.

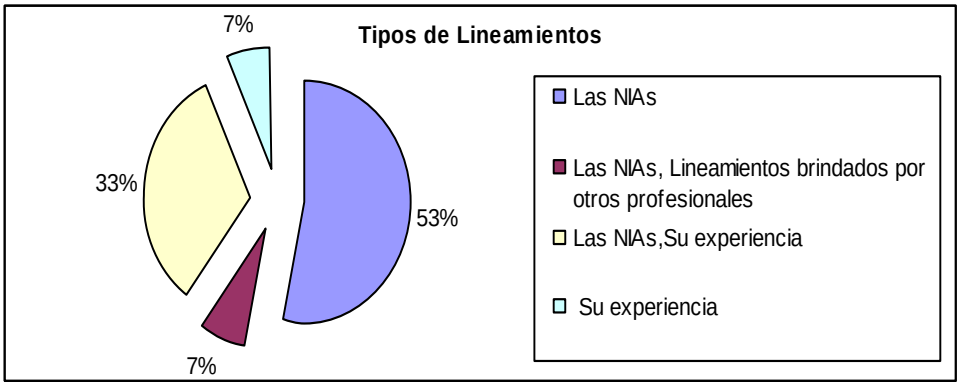
2.2. TABULACIÓN Y LECTURA DE DATOS DE LA INFORMACIÓN

Los datos se analizaron mediante las respuestas que se obtuvieron del cuestionario dirigido a los profesionales en auditoria; para lo cual se diseñaron las gráficas correspondientes a la problemática con su debido análisis que permita acertar o negar la presencia del problema y obtener elementos para el mejor planteamiento de una posible solución.

Pregunta N° 1

¿Qué tipo de lineamientos técnicos utiliza para realizar la auditoria a los sistemas de información computarizados?

Objetivos: Conocer los diferente lineamientos técnicos que utilizan los auditores para realizar la planeación de auditoria de sistemas de información computarizados.



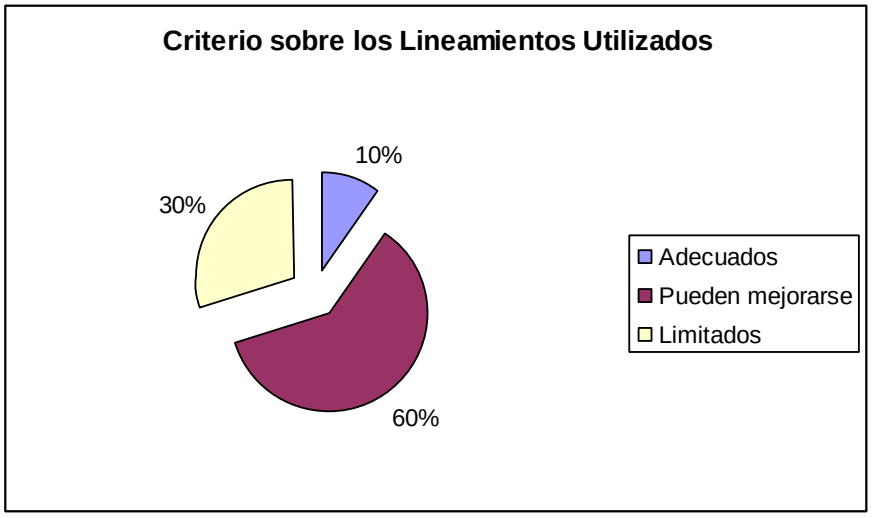
Análisis:

De los 72 auditores encuestados 38 contestaron que utilizan las NIAs los que representan un 53% de total, 24 auditores contestaron que para el desarrollo de la auditoria de sistemas utilizan las NIAs y su experiencia representando un 33% y el 14% restante utilizan otro tipo de lineamientos.

Pregunta N° 2

¿Cómo considera los lineamientos técnicos que utiliza?

Objetivo: Identificar el criterio de los auditores sobre los lineamientos técnicos que utilizan para realizar la auditoria a los sistemas de información computarizados.



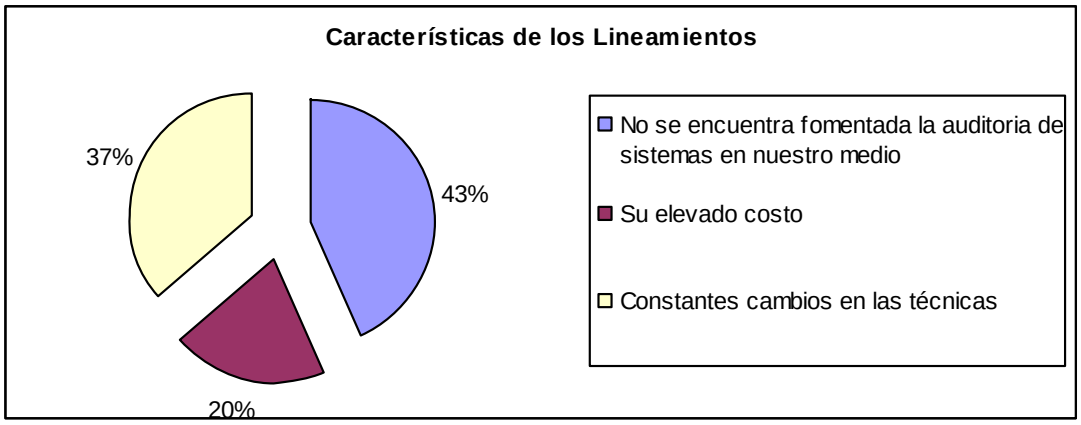
Análisis:

Los resultados obtenidos, indican que del total de 72 auditores encuestados 46 de ellos equivalentes al 63% consideraron que los lineamientos técnicos que utilizan pueden mejorarse y un 17% manifiesta que los lineamientos que utilizan son limitados; lo anterior evidencia la importancia de la creación de un documento que contenga lineamientos técnicos que permitan a los auditores realizar un trabajo de auditoria de manera eficiente.

Pregunta N° 3

¿A cuáles de los siguientes factores considera que obedece la poca existencia de lineamientos técnicos?

Objetivo: Determinar los factores a los que obedece la poca existencia de lineamientos técnicos para el desarrollo de la auditoria a los sistemas de información computarizados.



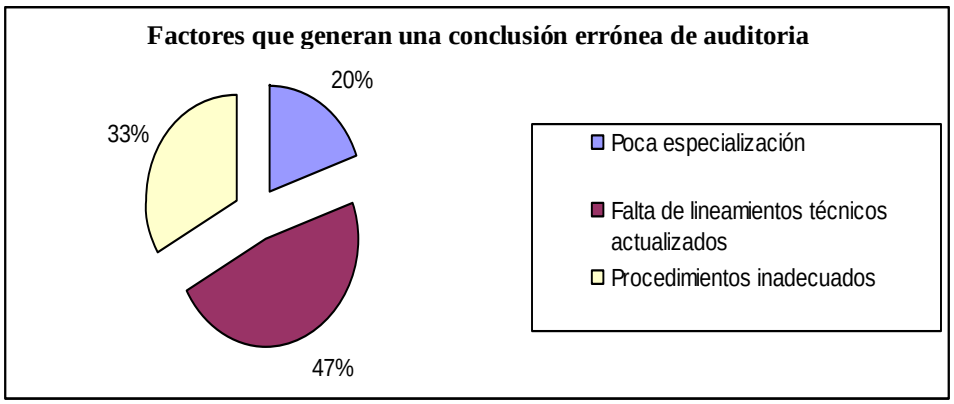
Análisis:

En cuanto a la poca existencia de lineamientos técnicos, de los 72 auditores encuestados el 43% del total manifiesta que el factor principal de dicha problemática es que no se encuentra fomentada la auditoria de sistemas, 37% respondió que obedece a su elevado costo y el resto opina que la causa son los constantes cambios en las técnicas; demostrando así que no se encuentra fomentada la auditoria de sistemas en nuestro medio.

Pregunta N° 4

¿De qué factores depende, según su opinión, que el auditor emita una conclusión errónea en la auditoria al funcionamiento de los sistemas de información computarizados?

Objetivos: Determinar los factores que influyen a que el auditor emita una conclusión errónea sobre el funcionamiento de los sistemas de información computarizados.



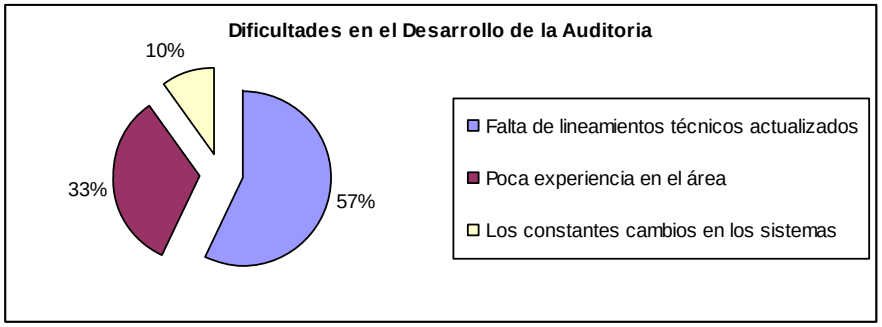
Análisis:

De la problemática sobre la emisión de una conclusión errónea sobre el funcionamiento de los sistemas, de 72 auditores encuestados el 47% opina que el factor principal que genera la problemática es la falta de lineamientos técnicos actualizados, el 33% opina que obedece a la implementación de procedimientos inadecuados y 20% opina que obedece a la poca especialización en auditoria de sistemas; con lo cual se confirma la necesidad de un documento que contenga lineamientos técnicos actualizados para el desarrollo de la auditora de sistemas que garantice una auditoria eficiente.

Pregunta N° 5

¿Cuál de las siguientes dificultades considera más influyentes, al desarrollar una auditoria a los sistemas de información computarizados?

Objetivo: Indagar sobre las dificultades más influyentes en el desarrollo de una auditoria de sistemas de información computarizados.



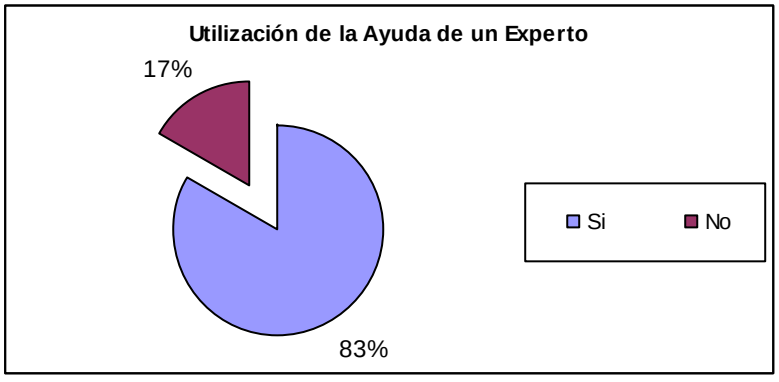
Análisis:

En el desarrollo de la auditoria de sistemas existen diversas dificultades, el 57% coincide que la dificultad que más se les ha presentado es la falta de lineamientos técnicos actualizados, el 33% coincide en que es la poca experiencia en el área y el resto opina que los constantes cambios en los sistemas, siendo evidente la falta de un documento que contenga lineamientos técnicos actualizados, los cuales disminuyan las dificultades en el desarrollo de la auditoria de sistemas.

Pregunta N° 6

¿Para la realización de la auditoria de sistemas utiliza la ayuda de un experto?

Objetivo: Conocer si para el desarrollo de la auditoria de sistemas de información computarizados, el auditor utiliza la ayuda de un experto.



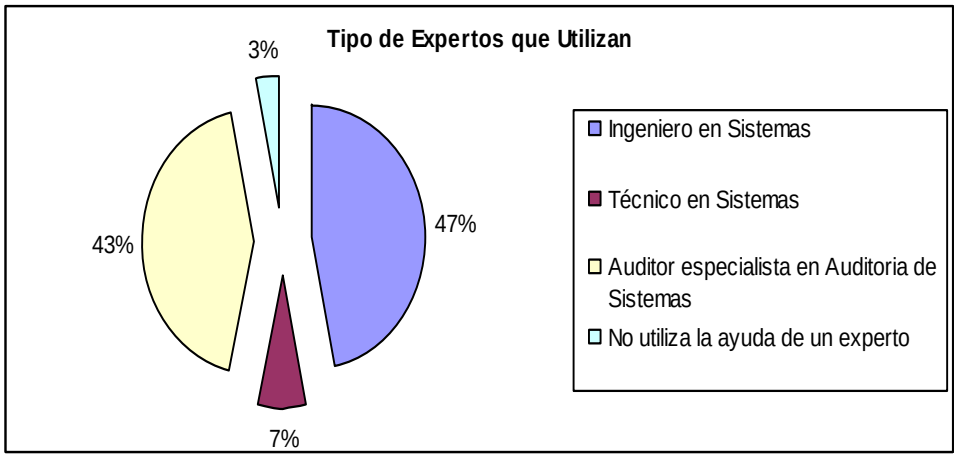
Análisis:

De 72 auditores encuestados el 83% del total considera necesaria la ayuda de un experto en sistemas para desarrollar la auditoria y el resto (17%) opina que no necesita la ayuda de un experto; por lo cual es recomendable que para el trabajo del auditor se apoye un experto en sistemas para efectuar una auditoria eficiente.

Pregunta N° 7

Si utiliza la ayuda de un experto, ¿cuál de los siguientes profesionales le es conveniente?

Objetivo: Determinar que tipo de experto consideran conveniente los auditores al desarrollar una auditoria de sistemas de información computarizados



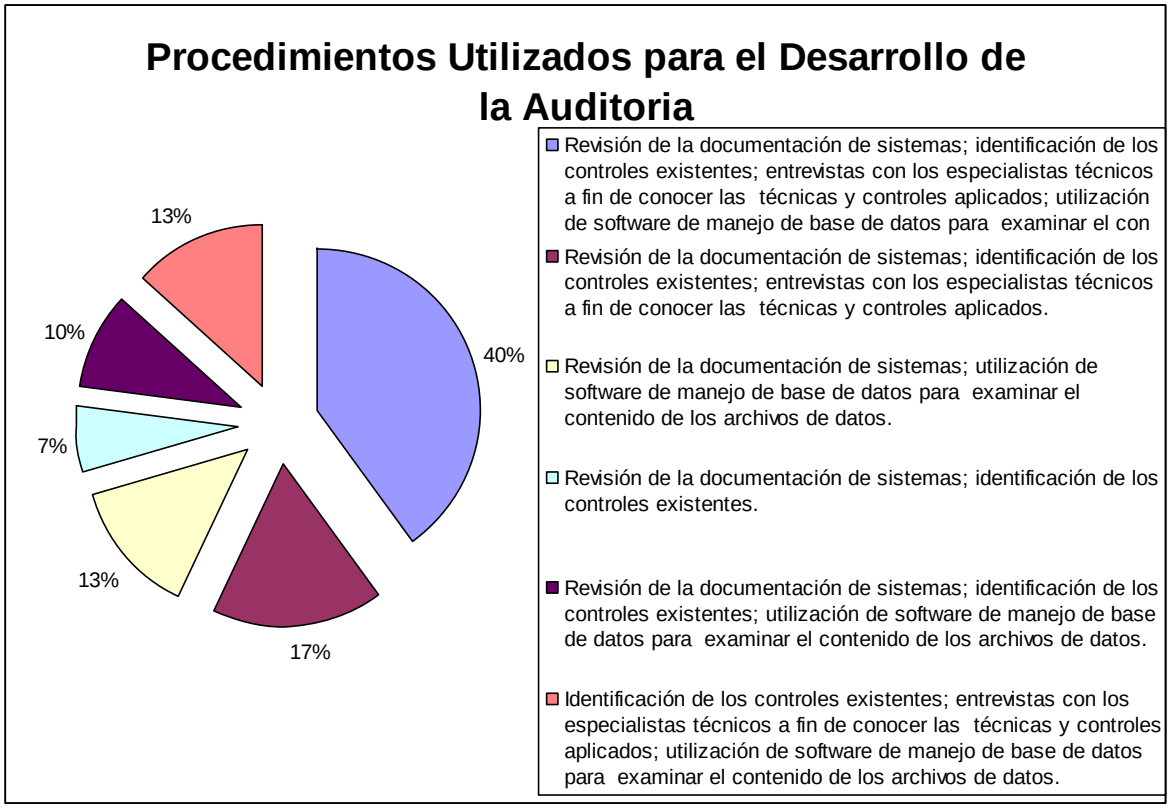
Análisis:

Para realizar la auditoria de sistemas es recomendable la ayuda de un experto, de 72 auditores encuestados el 47% contestó que era conveniente un ingeniero en sistemas, el 43% contestó que es conveniente la ayuda de un técnico en sistemas, el 7% considera útil la ayuda de un auditor especializado en sistemas y el 3% no considera conveniente la ayuda de un experto; en tal sentido la mayoría de auditores consideran conveniente el apoyo de un ingeniero en sistemas para el desarrollo de los procedimientos de auditoria.

Pregunta N° 8

Mencione cuáles procedimientos utiliza para desarrollar la auditoria a los sistemas de información computarizados.

Objetivo: Indagar sobre los procedimientos utilizados por el auditor para desarrollar una auditoria a los sistemas de información computarizados.



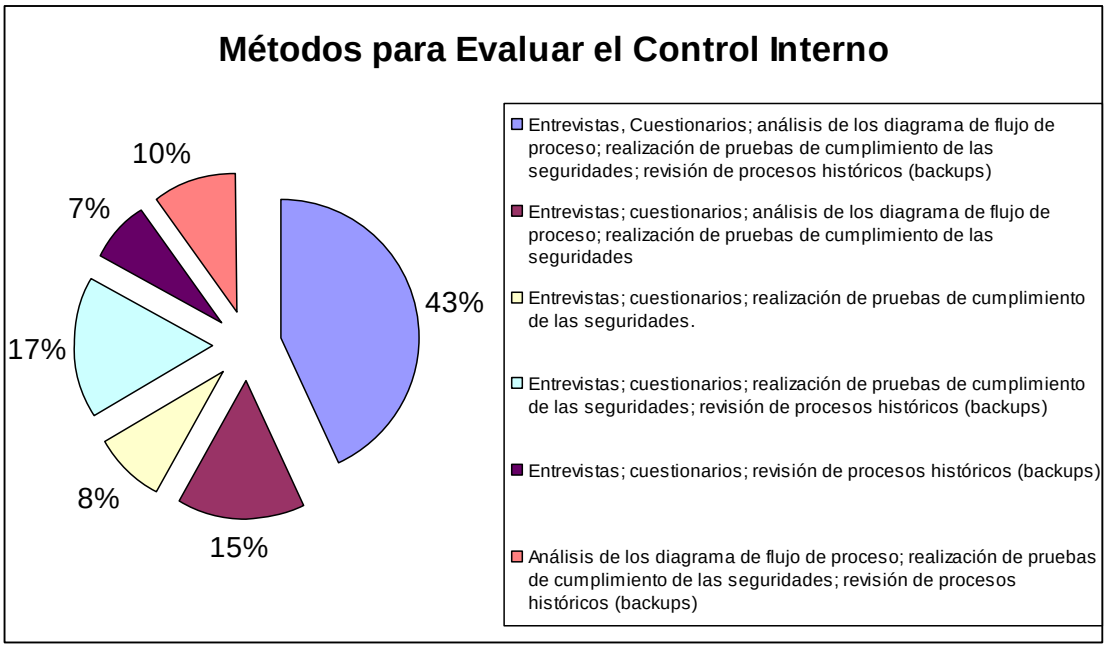
Análisis:

El 40% de los auditores encuestados, mencionan que los procedimientos utilizados para el desarrollo de la auditoria son la revisión de la documentación de sistemas, la identificación de los controles existentes, las entrevistas con los especialistas técnicos a fin de conocer las técnicas y controles aplicados y la utilización de software de manejo de base de datos para examinar el contenido de los archivos de datos. Estos procedimientos son esenciales para el desarrollo de una auditoria a los sistemas de información computarizados de manera eficiente.

Pregunta N° 9

¿De qué manera evalúa el control interno en la auditoria de sistemas de información computarizados?

Objetivo: Conocer los métodos utilizados para evaluar el control interno en la auditoria en sistemas de información computarizados.



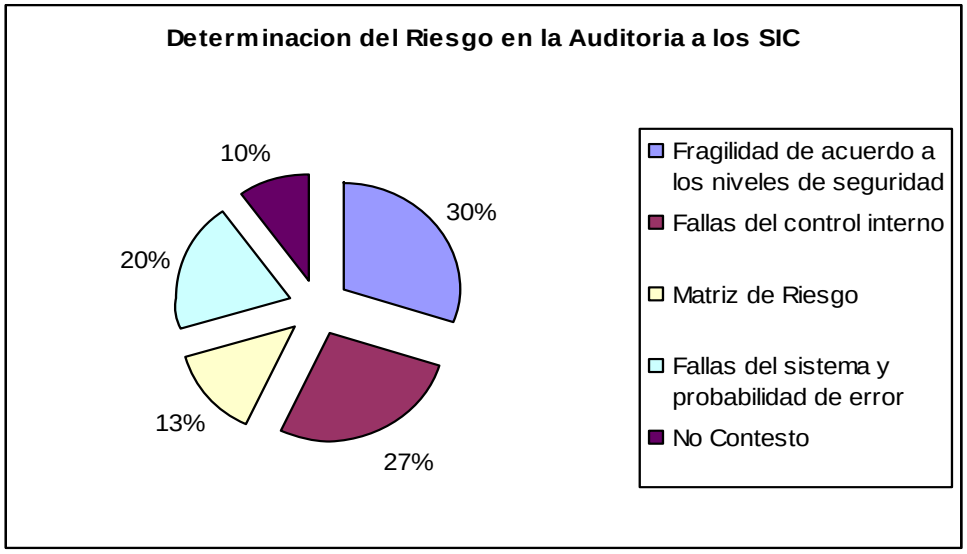
Análisis:

Una cantidad representativa de los auditores (43%) opina que los métodos utilizados para evaluar el control interno deben ser las entrevistas, los cuestionarios, el análisis de los diagramas de flujo de proceso, la realización de pruebas de cumplimiento de las seguridades y revisión de procesos históricos (backups); por tal motivo la implementación de estos métodos garantizan una evaluación de control interno eficiente.

Pregunta N° 10

¿De qué manera determina el riesgo en la auditoria a lo sistemas de información computarizados?

Objetivo: Conocer el criterio de los auditores para identificar los niveles de riesgo en la auditoria a los sistemas de información computarizados.



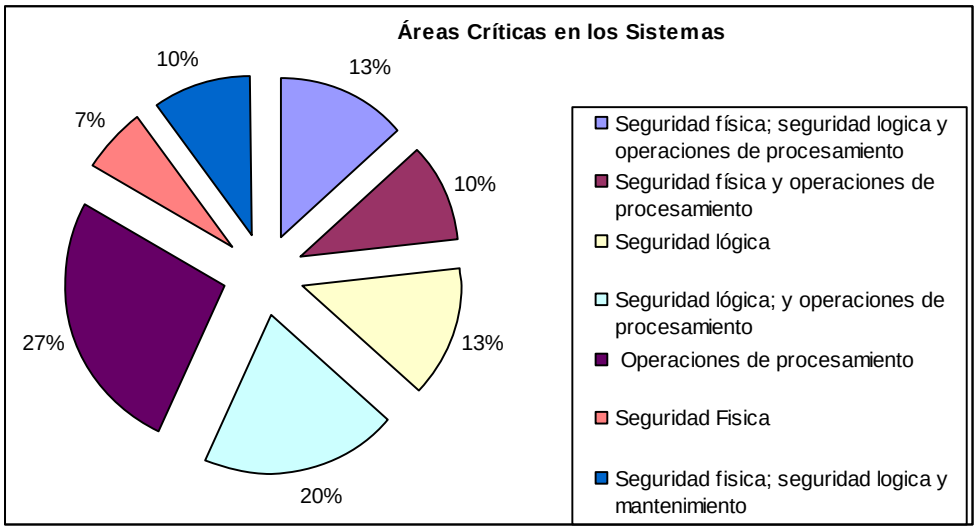
Análisis:

En el desarrollo del trabajo de una auditoria de sistemas de información computarizados, el 30% de los profesionales determinan el riesgo por medio de la fragilidad de acuerdo a los niveles de seguridad; mientras que el 27% contestó que determinan el riesgo a través de las fallas de control interno. Entre otras alternativas se mencionaron fallas del sistema, la probabilidad de error y a través de la matriz de riesgo, un pequeño porcentaje (10%) no contestó.

Pregunta N° 11

¿De las siguientes áreas cuáles considera usted que son las más críticas en los sistemas?

Objetivo: Identificar las áreas más críticas de los sistemas al desarrollar la auditoria a los sistemas de información computarizados.



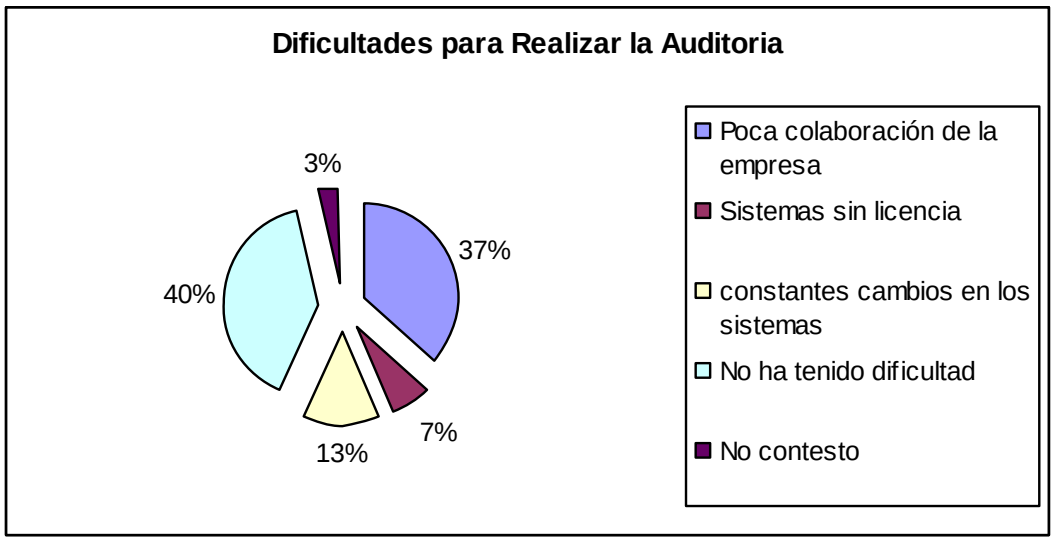
Análisis:

Entre las principales áreas críticas en los sistemas, según los profesionales en auditoria se encuentran en primer lugar las operaciones de procesamiento (27%) debido a que se considera como un punto susceptible además de vital importancia en la generación de información confiable y para los cuales debe contarse con controles encaminados a minimizar riesgos en los sistemas y su entorno; dejando en segundo lugar la seguridad lógica aunada al procesamiento de datos con un 20% luego con un 13% la seguridad física, lógica unidas al procesamiento de información.

Pregunta N° 12

¿Ha tenido dificultades para realizar la auditoria a los sistemas de información computarizados? Menciónelas.

Objetivo: Investigar si los auditores han tenido dificultad al desarrollar la auditoria a los sistemas de información computarizados y cuales son estas dificultades.



Análisis:

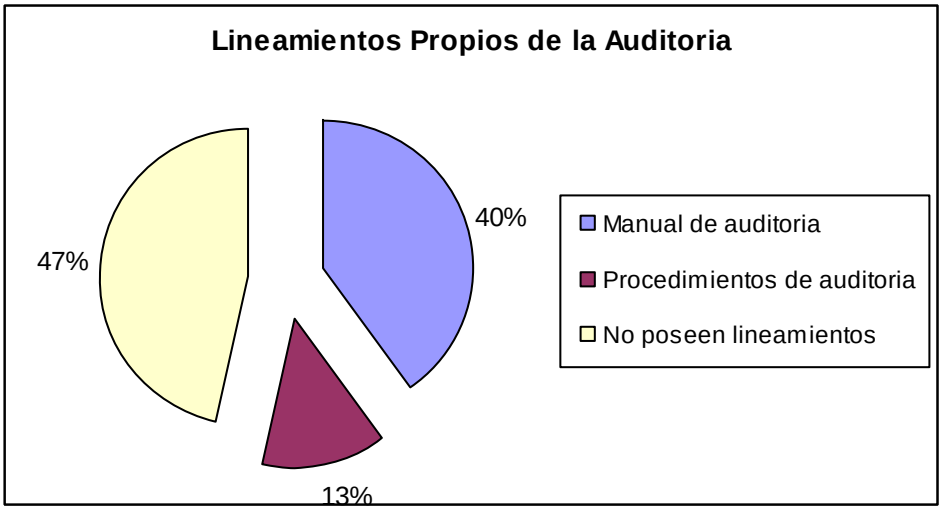
En cuanto a que si los auditores han tenido o no alguna dificultad al realizar la auditoria y cuales son dichas dificultades, el 57% de ellos las han tenido; de los cuales un 37% coincidieron en que la principal dificultad que tuvieron fue, la falta de colaboración de la empresa, el 7% respondió que es la falta de licencias de los sistemas que se usaban y el 13% dicen que los constantes cambios en los sistemas de información computarizados son la principal dificultad

que han tenido. El 40% del total de los auditores encuestados no tuvieron dificultades y el 3% se abstuvieron de contestar a la interrogante. Demostrando que la mayoría de auditores han tenido dificultades y la principal es la poca colaboración de los usuarios ocultando información, no colaborando con el auditor para llevar a cabo una auditoria de manera adecuada y eficiente.

Pregunta N° 13

En la firma de auditoria en donde usted labora, ¿cuenta con lineamientos propios para realizar la planeación de auditoria?; ¿En qué consisten?

Objetivo: Investigar si los auditores cuentan con lineamientos propios para el desarrollo de la auditoria a los sistemas de información computarizados y en que consisten.



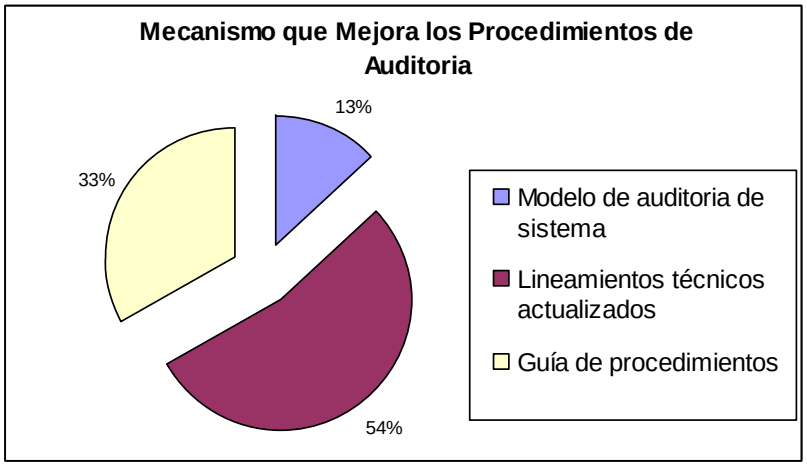
Análisis:

Del total de la muestra el 40% respondieron que contaban con lineamientos técnicos propios para realizar la planeación de auditoria en la firma donde laboran y que dichos lineamientos consisten en un manual de auditoria ; el 13% respondió que cuentan con una serie de procedimientos de auditoria y un 47% de auditores encuestados no cuenta con lineamientos técnicos propios para realizar una auditoria; con lo que se demuestra que un gran porcentaje de firmas de auditoria no tienen lineamientos propios para realizar una planeación de auditoria a los sistemas de información de computarizados.

Pregunta N° 14

¿Qué mecanismo considera que podría mejorar los procedimientos de auditoria?

Objetivo: Determinar el mecanismo que mejore los procedimientos de auditoria a los sistemas de información computarizados.



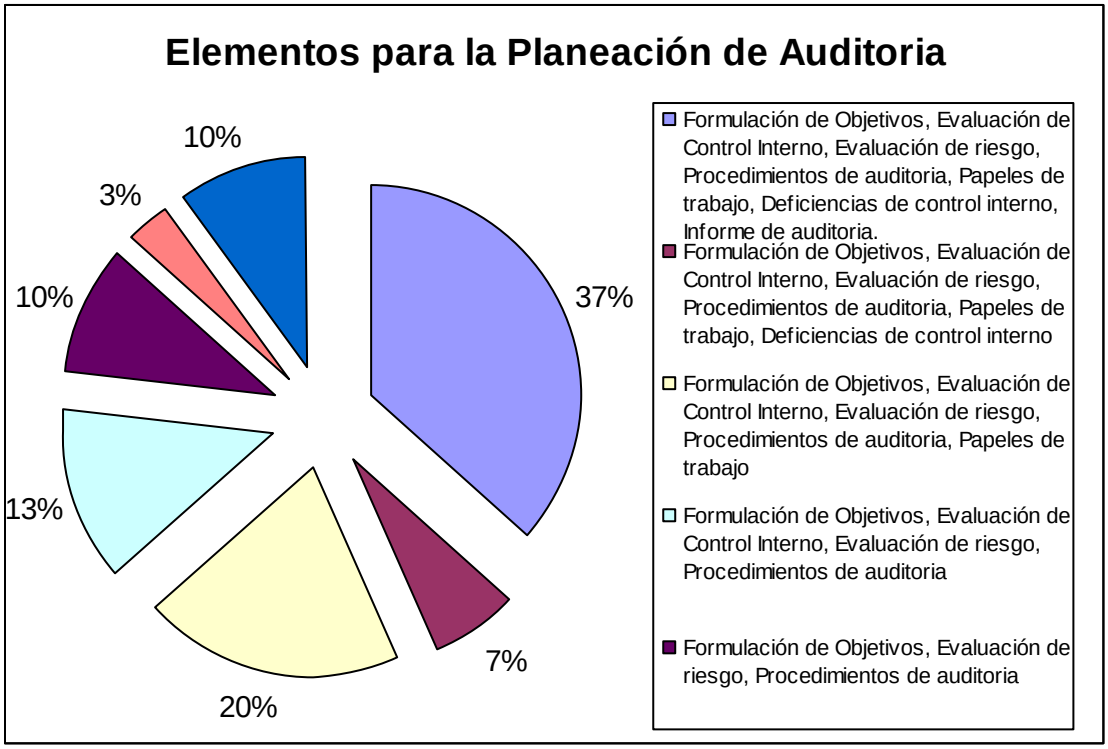
Análisis:

Un 54% de los auditores consideran que lineamientos técnicos actualizados son un mecanismo adecuado para mejorar los procedimientos de auditoria; mientras que 24 auditores que corresponden al 33% respondieron que lo mejor seria una guía de procedimientos; finalmente solo un 13% consideró la realización de un modelo de auditoria de sistemas como herramienta para mejorar los procedimientos de auditoria; en tal sentido es más útil y aceptable la realización de lineamientos técnicos actualizados.

Pregunta N° 15

¿Qué tipos de elementos debe contener una guía de lineamientos técnicos para el desarrollo de una auditoria?

Objetivos: Establecer los elementos que debe contener los lineamientos técnicos para el diseño de la planeación de auditoria a los sistemas de información computarizados.



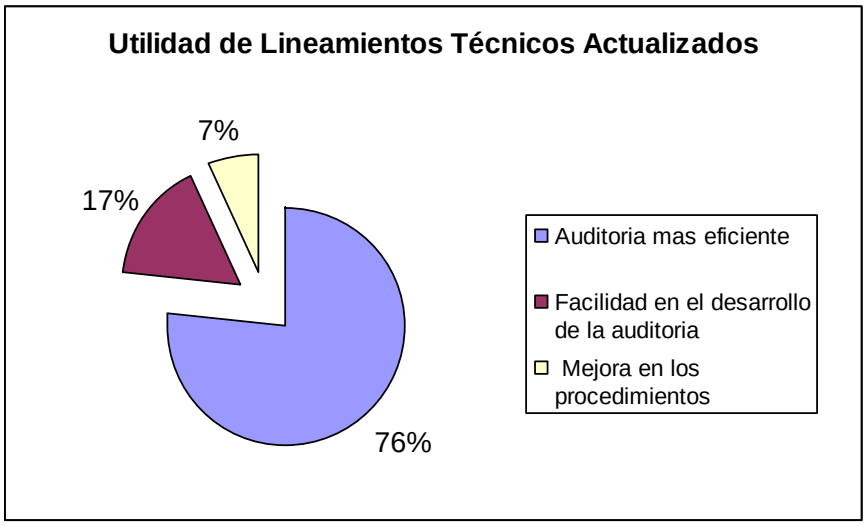
Análisis:

Para realizar la planeación de auditoria en sistemas que garantice una adecuada ejecución es necesario que cuente con ciertos elementos, de 72 auditores encuestados el 37% opina que una guía de lineamientos técnicos debe contener: la formulación de objetivos, la evaluación de control interno, la evaluación de riesgo, los procedimientos de auditoria, los papeles de trabajo, las deficiencias de control interno, y el informe de auditoria, el resto menciona la omisión de algunos de los elementos mencionados.

Pregunta N° 16

¿Qué utilidad podría tener para usted la existencia de lineamientos técnicos actualizados para la planeación de auditoria de sistemas de información computarizados?

Objetivo: Determinar la utilidad que tendrían los lineamientos técnicos actualizados en el desarrollo de la planeación de auditoria a los sistemas de información computarizados



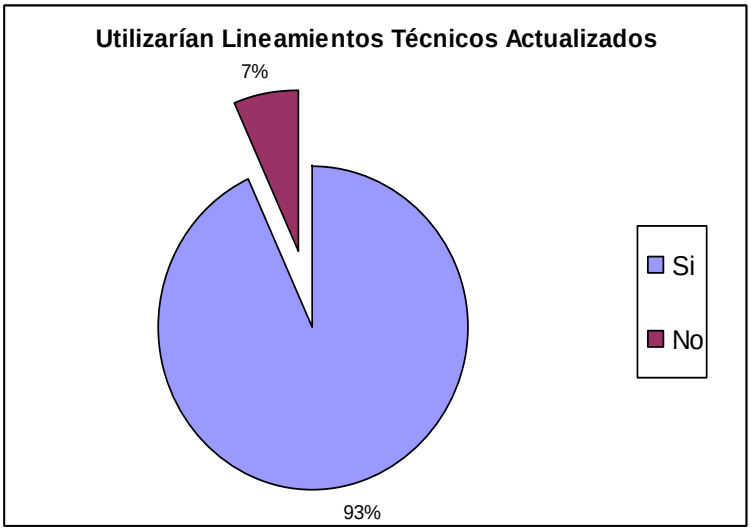
Análisis:

En cuanto a la utilidad que podría tener la existencia de lineamientos técnicos actualizados para la planeación de auditoria a los sistemas de información computarizados, la mayoría de los auditores encuestados (77%) respondieron que el beneficio obtenido de dicho documento seria la realización de una auditoria más eficiente; el 17% del total dicen que es la facilidad en el desarrollo de la auditoria y el resto respondió que les serviría para mejorar los procedimientos de auditoria al desarrollar una auditoria a los sistemas de información computarizados, lo cual confirma que existe la necesidad de contar con un documento que contenga lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los sistemas de información computarizados.

Pregunta N° 17

Usted utilizaría un documento que contenga lineamientos técnicos actualizados para elaborar la planeación de auditoria a los sistemas de información computarizados.

Objetivo: Conocer el grado de aceptación de los lineamientos técnicos actualizados para el diseño de la plantación de la auditoria a los sistemas de información computarizados.



Análisis:

En cuanto a que si utilizarían un documento que contenga lineamientos técnicos actualizados para elaborar la planeación de auditoria, del total de los auditores encuestados, la gran mayoría (93%) respondió que sí utilizarían el documento que contengan dichos lineamientos y solo el 3% que representan a 5 auditores no los utilizarían. Por tanto se demuestra que existe gran aceptación por parte de los auditores hacia un documento que contengan lineamientos técnicos actualizados para desarrollar la planeación de auditoria a los sistemas de información computarizados.

2.3. DIAGNOSTICO DE LA INVESTIGACIÓN

Lineamientos técnicos utilizados por los auditores para realizar la auditoria a los sistemas de información computarizados.

En lo que se refiere al uso de lineamientos técnicos para el desarrollo de la auditoria en sistemas, la mayoría de auditores utilizan las NIAs y una pequeña cantidad de auditores utilizan su experiencia y lineamientos brindados por otros profesionales.

Los auditores independientes consideraron que los lineamientos técnicos que utilizan se encuentran limitados y que pueden mejorarse.

De acuerdo a los resultados de la investigación, los auditores independientes manifiestan que no se encuentra fomentada la auditoria de sistemas en nuestro medio y que los lineamientos técnicos existentes poseen un elevado costo, además de los constantes cambios en las técnicas.

Algunos auditores independientes poseen lineamientos propios para el desarrollo de la auditoria de sistemas, entre ellos se pueden mencionar los manuales de auditoria y procedimientos de auditoria.

Existe la importancia de la creación de un documento que contenga lineamientos técnicos actualizados, que permitan a los auditores realizar su trabajo de manera eficiente y efectiva, los cuales disminuirán las dificultades en el desarrollo de la auditoria y

facilite la elaboración de los programas de auditoria; además proporcione lineamientos generales sobre la recolección de los papeles de trabajo y la elaboración del informe final de auditoria.

Utilización de la ayuda de un experto en la auditoria de sistemas de información computarizada.

En base a la Norma Internacional de Auditoria 620 "Uso del trabajo de un experto" para realizar una auditoria especializada (auditoria de sistemas de información computarizados) es recomendable la ayuda de un experto.

De acuerdo a los resultados de la investigación, la mayoría de auditores considera necesaria la ayuda de un experto en sistemas para desarrollar la auditoria.

Existen diferentes profesionales especializados en sistemas, de los cuales una cantidad considerable de auditores opinan conveniente la ayuda de un ingeniero en sistemas; mientras que otros opinan que es idónea la ayuda de un técnico en sistemas o de un auditor especializado en el área.

De acuerdo a lo anterior la mayoría de auditores desarrollan su trabajo apoyados por un experto.

Técnicas y Procedimientos para Desarrollar una Auditoria en Sistemas.

Para la realización de la auditoria de sistemas es necesaria la combinación de diversas técnicas y procedimientos, los auditores sugieren que los procedimientos utilizados para el desarrollo de la auditoria de sistemas deben ser: la revisión de la documentación de sistemas, la identificación de los controles existentes, las entrevistas con los especialistas técnicos a fin de conocer las técnicas y controles aplicados y la utilización de software de manejo de base de datos para examinar el contenido de los archivos de datos.

Los métodos a utilizar para la evaluación del control interno según los auditores deben ser: las entrevistas, los cuestionarios, el análisis de los diagramas de flujo de proceso, la realización de pruebas de cumplimiento de las seguridades, revisión de procesos históricos (backups); por lo tanto la implementación de estos métodos y procedimientos garantizan el desarrollo de una auditoria más eficiente.

En el desarrollo de una auditoria de sistemas de información computarizada los profesionales determinan el riesgo en primer lugar según la fragilidad del sistema en base a los niveles de seguridad y en segundo lugar lo establecen a través de las fallas de control interno. Entre otros factores que influyen para determinar el riesgo

de auditoria se mencionaron: fallas del sistema, la probabilidad de error y a través del establecimiento de la matriz de riesgo.

Mediante el uso de los procedimientos mencionados, los auditores establecen que las principales áreas críticas en los sistemas son: en primer lugar las operaciones de procesamiento, debido a que son un punto susceptible y de vital importancia en la generación de información confiable, para los cuales debe contarse con controles encaminados a minimizar riesgos en los sistemas y su entorno; dejando en segundo lugar la seguridad lógica y en tercer lugar una combinación de la seguridad física y lógica.

Algunos auditores creen que con la implementación de dichos métodos y procedimientos se garantiza el desarrollo de una auditoria eficiente y efectiva, que informe adecuadamente el funcionamiento de los sistemas de información de las empresas.

Para mejorar los procedimientos de auditoria de sistemas, la mayoría auditores consideran conveniente la utilización de lineamientos técnicos actualizados que contenga ejemplos de procedimientos de auditoria.

Según los auditores, el mecanismo que facilitaría y mejoraría los procedimientos de auditoria sería una guía de lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los sistemas de información computarizados.

Dificultades en el desarrollo de una Auditoria de Sistemas

En el desarrollo de la auditoria de sistema existen diversas dificultades, la mayoría de los auditores coinciden que la dificultad que más influye es la falta de lineamientos técnicos actualizados, seguida de la poca experiencia en el área y los constantes cambios en los sistemas.

Entre otras dificultades que se presentan al desarrollar una auditoria de sistemas, pueden mencionarse: la falta de colaboración de parte de la empresa, los constantes cambios en los sistemas de información computarizados y la falta de licencias de los sistemas que las empresas utilizan.

Elementos que deben contener una guía de lineamentos técnicos

Para realizar la planeación de auditoria de sistemas, que garantice una adecuada ejecución, es necesario que cuente con ciertos elementos; los auditores opinan que una guía de lineamientos técnicos debe contener: la formulación de Objetivos, la evaluación de control interno, la evaluación de riesgo, los procedimientos de auditoria, los papeles de trabajo, las deficiencias de control interno, y el informe de auditoria.

Uso y Utilidad de Lineamientos Técnicos para el Diseño de la Planeación de Auditoria a los Sistemas de Información Computarizados

Si existiera un documento que contenga lineamientos técnicos actualizados para diseñar la planeación de auditoria de sistemas, los auditores están dispuestos a utilizar dicho documento para desarrollar una auditoria eficiente y efectiva, que facilitaría los procedimientos.

En cuanto a la utilidad que podría tener la existencia de lineamientos técnicos actualizados para la planeación de auditoria a los sistemas de información computarizados, la mayoría de los auditores consideran que los beneficios obtenidos de dicho documento serían: facilitaría el desarrollo de la auditoria, realización de una auditoria más eficiente y mejoraría los procedimientos de auditoria a los sistemas de información computarizados.

El resultado de la investigación demuestra que existe gran aceptación por parte de los auditores hacia un documento que contenga lineamientos técnicos actualizados para el diseño de la planeación de auditoria a los sistemas de información computarizados con el fin de que ésta se desarrolle de una manera eficiente y efectiva.

3. LINEAMIENTOS TÉCNICOS PARA EL DISEÑO DE LA PLANEACIÓN DE AUDITORIA A LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

El tema relativo a la auditoria de sistemas de información computarizados, se refiere a las áreas de aplicación, que trata de los diferentes procedimientos que se van a emplear en el área de sistemas de información computarizados, así como también el procesamiento electrónico de datos, puesto que el auditor debe conocer el programa que va a utilizar.

Debido a las dificultades que enfrenta el auditor se ha creado una serie de lineamientos técnicos que describe los objetivos primordiales de una auditoria de sistemas, evaluación de la operatividad del sistema y el control de la función de sistemas de información computarizados, que influyen mucho en los resultados obtenidos (informe final); los procedimientos que se realizan en la auditoria consiste en la metodología que se va a aplicar para realizar el análisis correspondiente.

En la actualidad la auditoria de sistemas de información computarizados se encuentra evidentemente vinculada con la gestión empresarial es por esto que es de vital importancia que existan lineamientos técnicos para desarrollar una adecuada planeación de auditoria de sistemas de información computarizados, para analizar el desempeño y funcionamiento de los sistemas, de los cuales depende la organización.

3.1. SÍNTESIS DE LAS NORMAS INTERNACIONALES DE AUDITORIA APLICABLES A LA AUDITORIA DE SISTEMAS

NIA - 230 Documentación de Auditoria.

En esta norma se establece la naturaleza de la documentación de auditoria; como debe ser su forma, contenido y extensión, la compilación del archivo final y los cambios que pueden existir en la documentación.

La documentación eficiente y apropiada para una auditoria ayuda y enriquece la calidad de la misma, donde su forma, contenido y extensión ayudan a entender la naturaleza, oportunidad y extensión de los procedimientos de auditoria, los resultados de los procedimientos y la evidencia de auditoria obtenida entre otros asuntos de importancia para la conclusión de la misma.

Las formas en que puede registrarse la documentación de auditoria son:

- En papel.
- En forma electrónica u otros medios.

Como ejemplo se incluyen:

- Programas de auditoria.
- Listas de verificación.
- Correspondencia (correo electrónico).

Como un punto importante la norma establece que la documentación de auditoria pertenece al trabajo específico del auditor (archivo).

NIA - 240 Responsabilidad del auditor de considerar el fraude en una auditoria de estados financieros.

La susceptibilidad de los sistemas y su manejo se consideran de importancia relativa debido a la figura del fraude que lleva una parte importante en la realización de una auditoria; donde el auditor desempeña los procedimientos de evaluación de riesgo como averiguaciones con la administración o personal, considera factores de riesgo, revisión de situaciones inusuales o inesperadas y revisión de documentación (datos y documentos) útiles; lo anterior, el auditor lo realiza considerando el tamaño, la complejidad y características de la empresa y como ésta maneja su información, sea de forma manual o mediante el uso de sistemas de información computarizada.

Algunos ejemplos indican la posibilidad de fraude en los estados financieros entre los cuales se mencionan:

- Evidencia electrónica no disponible o faltante, inconsistente, con las prácticas o políticas en los registros de la entidad.
- Falta de capacidad para producir evidencia de desarrollo de sistemas clave, entre otros.

El auditor deberá realizar procedimientos adicionales de auditoria dirigidos a determinar el fraude y obtener evidencia suficiente y apropiada de auditoria.

NIA - 300 Planeación de una auditoria de estados financieros.

En esta norma se establecen y proporcionan lineamientos sobre las consideraciones y actividades aplicables para planear la auditoria.

En la planeación de la auditoria, se prepara una estrategia general para el trabajo y desarrollo; donde ello implica el desempeñar actividades preliminares que permitan comprender la naturaleza, oportunidad y extensión de los recursos necesarios para la realización del trabajo (personal, tiempo, entre otros).

La forma y extensión de la documentación del plan de auditoria dependen del tamaño y complejidad de la empresa (sistemas), así como también circunstancias especiales del trabajo.

La norma considera como puntos a tomar en cuenta en el establecimiento de la estrategia general de auditoria, el alcance del trabajo, el efecto de la tecnología de la información en los procedimientos de auditoria, incluyendo disponibilidad de datos y el uso esperado de técnicas de auditoria soportadas por computadora.

Es importante mencionar que se aplican estos principios básicos en la planeación de auditorias de sistemas, con la diferencia que en ésta se incluye un análisis y diseño detallado de los sistemas, como especificaciones de programas de cómputo, diseño de pistas de auditoria, estándares de documentación de programas, control interno dirigido al sistema, mantenimiento, entre otros aspectos donde intervienen la fuente, captura, procesamiento, almacenamiento y generación de informe o reportes entre otros.

NIA – 315 Entendimientos de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa

Esta norma es explícita, cuando en su párrafo 2 menciona que "el auditor debe obtener un entendimiento de la entidad y su entorno, incluyendo el control interno"; esto se aplica también en la auditoria de sistemas, al igual que en cualquier otro tipo de auditoria, esto para poder identificar y evaluar los riesgos de cualquier tipo que los sistemas pueden tener. El entendimiento de la entidad (sistema) debe ser suficiente, para diseñar y desempeñar procedimientos adicionales de auditoria, los cuales se determinan en el momento de la planeación de la auditoria; eso es posible debido a que el auditor usa el juicio profesional para determinar el grado requerido de entendimiento de la entidad y su entorno y así poder llevar a cabo la planeación de auditoria de una manera más acertada.

El auditor debe determinar si cualquiera de los riesgos requiere consideración especial de auditoria, o si existen riesgos para los que los procedimientos sustantivos solos no proporcionan evidencia suficiente y apropiada para la auditoria; es importante además, que el auditor evalúe los controles de la entidad sobre dichos riesgos y si se han implementado.

El entendimiento de la entidad (sistemas) y su entorno, es un aspecto esencial del desempeño de una auditoria y por ende de la planeación de la misma, debido a que un entendimiento adecuado y suficiente es

un excelente parámetro para el profesional de auditoria y para la planeación de la misma.

El juicio profesional proporciona el grado requerido de entendimiento de la entidad (sistemas), incluyendo el control interno, para evaluar los riesgos y diseñar los procedimientos de auditoria.

La obtención de un entendimiento de la entidad (sistemas) y su entorno, incluyendo el control interno, es un proceso dinámico de compilación, actualización y análisis de información en la auditoria (párrafo 6, NIA 315).

En la planeación de auditoria de sistemas computarizados es importante que el auditor tenga el conocimiento suficiente acerca del control interno que se tiene en los sistemas, para determinar el riesgo y poder llevar a cabo la planeación de la auditoria de tal manera que los resultados obtenidos sean adecuados.

El párrafo 17 de la norma 315, menciona que el equipo de trabajo debe discutir acerca de la auditoria que se va a hacer, pero no es necesario que se incluya a todos los miembros de éste, generalmente son los miembros claves del equipo; esto debido a que se incluye a las personas que tengan mayor conocimiento del área en el cual se está realizando la auditoria.

Existen casos en los cuales se necesita incluir a especialistas en alguna área en particular; como en caso de las tecnologías de

información en donde se requerirá la opinión de un experto para poder realizar la planeación de manera adecuada.

Dentro del entendimiento de los factores relevantes a la industria, es necesario conocer el desarrollo tecnológico, sobre todo cuando la auditoria se está realizando a los sistemas de información computarizados (SIC).

Control interno

El párrafo 4 de la NIA 315, es enfático al mencionar que "el auditor usa el control interno para identificar posibles errores y considerar factores que afectan a la empresa, dependiendo del área que se esté auditando". De igual forma esto sirve al auditor a poder considerar procedimientos adicionales en su planeación.

En el párrafo 56 de la norma 315, se menciona que los controles de una entidad no son suficiente prueba de la efectividad operativa de los controles; sin embargo, que los controles sean automatizados le da cierto grado de confianza a los datos que los sistemas automatizados proporcionan.

No importa lo bien diseñado y operado que este el control interno, puede proporcionar a una entidad solo una seguridad razonable sobre el logro de los objetivos referentes al funcionamiento de los sistemas de información computarizados.

NIA – 330 Procedimientos del auditor en respuesta a los riesgos evaluados

Dependiendo del tipo de riesgo y con la aplicación del juicio profesional del auditor, se puede determinar el grado de confiabilidad de de la evidencia de auditoria que busca el auditor con los procedimientos sustantivos.

Al considerar cuándo desempeñar procedimientos de auditoria, el auditor debe de tomar en cuenta una diversidad de factores, como los siguientes:

- El entorno del control.
- Cuándo está disponible la información relevante (por ejemplo, los archivos electrónicos pueden alterarse posteriormente a los procedimientos).
- La naturaleza de los riesgos.
- El ejercicio o fecha con que se relaciona la evidencia de auditoria.

Dentro de la Auditoria a los SIC (Sistemas de Información Computarizados), existen ocasiones en que se confía más de lo debido en la información que proporcionan, ya que se supone que están diseñados de acuerdo a las necesidades de la empresa, y el personal o los usuarios del mismo por lo general no tienen conocimiento extenso del área y por lo tanto existe un alto riesgo de que la información generada por los sistemas de información no sea adecuada; este tipo de información es más segura que la información generada manualmente.

NIA – 500 Evidencia de auditoria

El propósito de esta Norma Internacional de Auditoria (NIA) es establecer normas y proporcionar guías sobre lo que constituye evidencia de auditoria.

"Evidencia de auditoria" es toda la información que usa el auditor para llegar a una conclusión".

La información que el auditor puede usar como evidencia incluye manuales de controles; información obtenida por el auditor de procedimientos de auditoria como investigación, observación e inspección; y otra información desarrollada por, o disponible para el auditor que le permita llegar a conclusiones a través de un razonamiento válido.

La suficiencia es la medida de la cantidad de evidencia de auditoria. Lo apropiado es la medida de la calidad de evidencia de auditoria, es decir su relevancia y su confiabilidad para dar soporte.

La confiabilidad de la evidencia de auditoria es influida por su fuente y por su naturaleza y depende de las circunstancias individuales bajo las que se obtiene. Entre las formas de obtener evidencia se encuentran:

- La evidencia de auditoria que se obtiene directamente por el auditor (por ejemplo, observación de la aplicación de un control) la cual es más confiable que la evidencia de auditoria

que se obtiene de manera indirecta o por inferencia (por ejemplo, investigación sobre la aplicación de un control).

- La evidencia de auditoria es más confiable cuando existe en forma documental, ya sea en papel, en forma electrónica, o en otro medio.

En algunas situaciones el auditor puede determinar que se necesitan procedimientos adicionales de auditoria, estos por ejemplo, pueden incluir usar Técnicas de Auditoria con Ayuda de Computadora (TAACs) para volver a calcular la información o volver a desarrollar los procedimientos.

Procedimientos de auditoria para obtener evidencia de auditoria

El auditor obtiene evidencia de auditoria para llegar a conclusiones razonables mediante el desempeño de procedimientos de auditoria para:

(a) Obtener un entendimiento de la entidad (Sistemas) y su entorno, incluyendo su control interno, para evaluar los riesgos.

(b) Cuando sea necesario o cuando el auditor haya determinado hacerlo así, hacer pruebas de la efectividad operativa de los controles para prevenir, o detectar y corregir errores (los procedimientos de auditoria desempeñados para este fin se citan en las NIAs como pruebas de controles).

La observación proporciona evidencia de auditoria sobre el desempeño de un proceso o procedimiento, pero está limitada por el momento en que tiene lugar la observación y por el hecho de que el acto de ser observado puede afectar la manera en la cual se desempeña el proceso o procedimiento.

La investigación consiste en buscar información de personas bien informadas. La investigación es un procedimiento de auditoria que se usa de manera extensa en toda la auditoria y a menudo es complementaria al desempeño de otros procedimientos de auditoria. Las investigaciones pueden ir desde investigaciones formales por escrito hasta investigaciones orales informales. Evaluar las respuestas a las investigaciones es una parte integral del proceso de investigación.

Volver a calcular: consiste en verificar la exactitud matemática de los documentos o registros. El nuevo cálculo puede desempeñarse mediante el uso de tecnología de la información, por ejemplo, obteniendo un archivo electrónico de la entidad y usando TAACs para verificar la exactitud de la totalización del archivo.

Volver a desarrollar: es la ejecución independiente por el auditor de procedimientos o controles que originalmente se desarrollaron como parte del control interno de la entidad, ya sea manualmente o con el uso de TAACs.

NIA – 530 Muestreos de la auditoria y otros medios de pruebas

El propósito de esta Norma Internacional de Auditoria (NIA) es establecer normas y proporcionar lineamientos, sobre el uso de procedimientos de muestreo en la auditoria.

Al diseñar los procedimientos de auditoria, el auditor deberá determinar los medios apropiados para reunir suficiente evidencia apropiada de auditoria para cumplir los objetivos de los procedimientos de auditoria.

Para fines de esta NIA, "error" significa tanto, desviaciones de control, cuando se desempeñan pruebas de control, o representaciones erróneas, cuando se aplican pruebas de detalles. De modo similar, error total se usa para definir la tasa de desviación o una representación errónea total.

"Error anómalo" significa un error que surge de un suceso aislado que no es recurrente salvo en ocasiones identificables específicamente y por tanto, no es representativo de errores en el universo.

"Universo" significa el conjunto total de datos de los que se selecciona una muestra y sobre los cuales el auditor desea extraer conclusiones.

El "riesgo en el muestreo" surge de la posibilidad de que la conclusión del auditor, basada en una muestra pueda ser diferente de la conclusión alcanzada si todo el universo se sometiera al mismo procedimiento de auditoria. Hay dos tipos de riesgo en el muestreo:

(a) el riesgo de que el auditor concluya en el caso de una prueba de control, que los controles son más efectivos de lo que realmente son. Este tipo de riesgo altera la efectividad de la auditoria y es más probable que lleve a una conclusión de auditoria inapropiada.

(b) el riesgo de que el auditor concluya, en el caso de una prueba de control, que los controles son menos efectivos de lo que realmente son. Ese tipo de riesgo afecta la eficiencia de la auditoria ya que generalmente llevaría a realizar trabajo adicional para establecer que las condiciones iniciales fueron incorrectas.

Estratificación es el proceso de dividir un universo en sub-universos. Cada uno de los cuales es un grupo de unidades de muestreo que tienen características similares.

Procedimientos para evaluar el riesgo

De acuerdo con la NIA 315, "Entendimiento de la entidad (sistemas) y su entorno y evaluación de los riesgos. El auditor aplica procedimientos de evaluación del riesgo para obtener un entendimiento de la entidad (sistemas) y entorno, incluyendo su control interno. Ordinariamente, los procedimientos de evaluación del riesgo no implican el uso de muestreo de auditoria. Sin embargo, el auditor a menudo planea y aplica pruebas de controles a la vez que obtiene el entendimiento del diseño de los controles y determina si se han

implementado éstos. En tales casos, es relevante la discusión siguiente de las pruebas de control.

Pruebas de Control

El muestreo en la auditoria para pruebas de control, es generalmente apropiado cuando la aplicación del control deja evidencia de auditoria de su desempeño (por ejemplo, evidencia de autorización de incorporación de información a un sistema de procesamiento de datos basado en una microcomputadora).

Diseño de la muestra

Cuando se diseña una muestra de auditoria, el auditor deberá considerar los objetivos del procedimiento de auditoria y los atributos del universo del cual se extraerá la muestra.

El auditor debe considerar primero los objetivos específicos a lograr y la combinación de procedimientos de auditoria que es probable que cumplan mejor dichos objetivos. La consideración de la naturaleza de la evidencia de auditoria buscada y las condiciones de error posible u otras características relacionadas con dicha evidencia, ayudarán al auditor a definir qué constituye un error y qué universo usar.

Selección de la muestra

El auditor al realizar el muestreo debe de cerciorarse de que todos los elementos del universo tengan igual oportunidad de selección.

NIA - 620 Uso del trabajo de un experto.

Los aspectos que trata esta norma son sobre el uso del trabajo de un experto en una determinada auditoria, es decir el como determinar dicha necesidad, ver la competencia y objetividad del experto, cuál será el alcance de su trabajo y como expresar referencia a un experto en el dictamen del auditor.

Es un experto la persona o firma que posee la habilidad, conocimiento y experiencia especial en un campo en particular distinto del de la contabilidad y de la auditoria.

Entre los aspectos a considerar en el uso del trabajo de un experto se mencionan: conocimiento y experiencia, riesgo de representación errónea de importancia relativa respecto al asunto a considerar, la cantidad y calidad de la evidencia de auditoria que se espera obtener.

Un punto importante es evaluar la competencia profesional del experto, mediante la certificación o licencia profesional por organismos especializados, la experiencia y reputación en el campo donde el auditor está buscando evidencia.

Por ejemplo una certificación como auditor de sistemas de información (CISA) otorgada por Information Systems Audit and Control Association (ISACA), Asociación de Auditoria y Control de Sistemas de Información.

NIA – 800 El dictamen del auditor sobre compromisos de auditoria con propósito especial

El propósito de esta Norma Internacional de Auditoria (NIA) es establecer normas y proporcionar lineamientos en conexión con los compromisos de auditoria con propósito especial.

El auditor deberá analizar y evaluar las conclusiones extraídas de la evidencia de auditoria obtenida durante el trabajo de auditoria con propósito especial como la base para una expresión de opinión. El dictamen deberá contener una clara expresión escrita de conclusión.

La naturaleza, oportunidad, y alcance del trabajo que va ser desarrollado en un trabajo de auditoria con propósito especial variará con las circunstancias. Antes de emprender un trabajo de auditoria con propósito especial, el auditor deberá asegurarse de que hay acuerdo con el cliente sobre la naturaleza exacta del trabajo y la forma y contenido del dictamen que será emitido.

Al planear el trabajo de auditoria, el auditor necesitará una clara comprensión del propósito para el que se usará la información sobre la que se dictamine, y quién es probable que la use. Para evitar la posibilidad de que el dictamen del auditor sea usado para propósito que no son los planeados, el auditor puede desear indicar en el dictamen el propósito para el cual se prepara el dictamen y cualquier restricción sobre su distribución y uso.

El dictamen del auditor sobre un trabajo de auditoria con propósito especial, debería incluir los siguientes elementos básicos:

(a) Título;

(b) El destinatario;

(c) Un párrafo de entrada o introductorio

(i) Identificación del elemento auditado; y

(ii) Una declaración de la responsabilidad de la administración de la entidad y de la responsabilidad del auditor;

(d) Un párrafo de alcance (describiendo la naturaleza de una auditoria)

(i) Referencia a NIAs aplicables a trabajos de auditoria con propósito especial o a normas o prácticas nacionales relevantes; y

(ii) Una descripción del trabajo que el auditor desempeñó;

(e) Un párrafo de opinión conteniendo una expresión de la conclusión del auditor sobre la cuestión a auditor

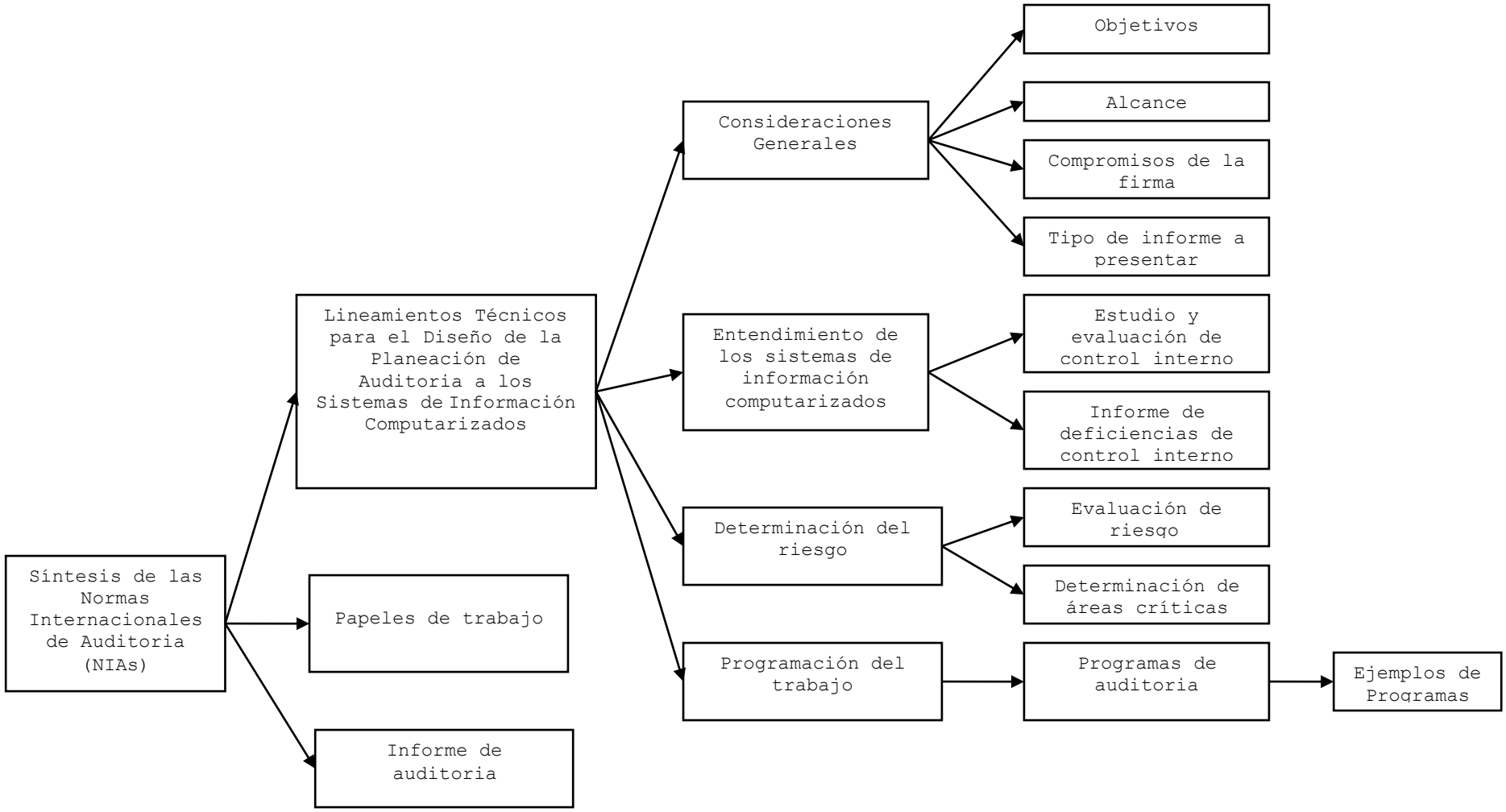
(f) La fecha del dictamen;

(g) La dirección del auditor; y

(h) La firma del auditor.

Es deseable una medida de uniformidad en la forma y contenido del dictamen del auditor porque ayuda a propiciar la comprensión del lector.

3.2. LINEAMIENTOS TÉCNICOS PARA EL DISEÑO DE LA PLANEACIÓN DE AUDITORIA A LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS.



3.2.1. CONSIDERACIONES GENERALES

En la planeación de auditoria de sistemas de información computarizados es necesario establecer las consideraciones generales del trabajo, en las cuales se incluye: los compromisos que adquiere el auditor, los objetivos a cumplir, el alcance de la auditoria y los tipos de informe a presentar.

3.2.1.1. COMPROMISOS DE LA FIRMA

Para llevar a cabo una auditoria de sistemas es esencial establecer los compromisos de la firma, en los cuales el auditor deberá determinar sus responsabilidades sobre el trabajo que realizará.

Dentro de las responsabilidades del auditor deben incluirse: que tipo de auditoria está realizando, en base a que normativa técnica realizará el trabajo y referente a que brindará su conclusión.

Ejemplo de compromisos de la firma

Realizar una auditoria especializada a los sistemas de información computarizados de forma adecuada, en base a la normativa técnica aplicable a los sistemas de información, permitiendo establecer una conclusión sobre el funcionamiento del sistema de información auditado. Se emitirá un informe final de auditoria el cual contendrá la conclusión final sobre el funcionamiento de lo sistemas y las posibles sugerencias de los hallazgos encontrados. La fecha tentativa ha ser entregado el informe es el 30 de agosto del presente año.

3.2.1.2. OBJETIVOS

Para el desarrollo de la auditoria a los sistemas de información computarizados es fundamental plantear el objetivo a seguir en el proceso de toda la auditoria.

En el diseño de la planeación de auditoria a los sistemas de información computarizados, es preciso establecer un objetivo general y una serie de objetivos específicos que contribuyan a lograr dicho objetivo general.

La auditoria de sistema de información tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema de información en que se sustenta.

Los principales objetivos de la auditoria de sistemas de información computarizados son: garantizar el funcionamiento de los sistemas de información computarizados, el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

Ejemplos de objetivos de la auditoria de sistemas de información computarizados

Objetivo General:

Emitir un informe sobre el funcionamiento de los sistemas de información computarizados (SIC), para asegurar el cumplimiento, la integridad, confiabilidad, confidencialidad y seguridad de los sistemas.

Objetivos Específicos:

1. Asegurar que los programas procesan los datos, de acuerdo con las necesidades del usuario o dentro de los parámetros de precisión previstos.
2. Cerciorarse de la no existencia de rutinas fraudulentas al interior de los programas.
3. Comprobar que los programas utilizados son los debidamente autorizados por el administrador.
4. Verificar la existencia de controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.
5. Cerciorarse que todos los datos son sometidos a validación antes de ordenar su proceso correspondiente.

3.2.1.3. ALCANCE

En el alcance de trabajo de auditoria a los SIC, se identifican los sistemas específicos o unidades de organización que se han de incluir en la revisión, así como el período de tiempo dentro del cual se desarrollará el trabajo de auditoria.

El alcance de auditoria a los sistemas debe contener los siguientes elementos:

1. Evaluación de los recursos informáticos disponibles.
2. Capacidad de soporte del negocio.

3. Oportunidad de la prestación del servicio.
4. Evaluación de los controles generales.
5. Evaluación de sistemas de información (usuarios, niveles de acceso, información, funcionalidades internas con otros sistemas, rechazos y rezagos, documentación y manuales).
6. Evaluación del uso de servicio de red como correo electrónico, internet, transferencias de archivos, impresión, etc.

La evaluación se realizará a través de las siguientes pruebas:

- ❖ Pruebas de control.
- ❖ Pruebas sustantivas.

El alcance establecido debe ser suficiente para satisfacer los objetivos del trabajo, teniendo en cuenta los sistemas, registros y personal involucrado con los sistemas; los auditores deben asegurar que el alcance del trabajo sea suficiente para cumplir los objetivos acordados, si existieran restricciones en el alcance durante el trabajo, éstas deberán tratarse con el cliente para determinar si se continúa o no con el trabajo.

En el alcance de auditoria se incluyen: la referencia a la legislación, reglamentos y pronunciamientos aplicables a los cuales se adhiere el auditor.

Ejemplo de un alcance de auditoria de sistemas de información computarizados.

La auditoria a los sistemas de información computarizados, se realizará tomando en cuenta los siguientes parámetros:

1. La evaluación de la captura de datos.
2. La evaluación de los controles internos aplicados a los sistemas.
3. La evaluación del procesamiento de datos, salida de la información, seguridad lógica y calidad de la información.

A través de las siguientes pruebas:

a. Pruebas de control de usuario, que abarca el manual del control interno a las bases de datos; a fin de comprender la ruta crítica de la captura de datos, el procesamiento de los mismos y relacionar con ello la información vinculada entre los diferentes módulos, además de entrevistas al personal de informática.

b. Pruebas sustantivas, que comprenden el procesamiento electrónico de datos en los sistemas de información; éstas tendrán como fin corroborar el cumplimiento de los siguientes aspectos:

   - ❖ Identificar los errores en el procesamiento.
   - ❖ Asegurar la calidad de los datos.

- Identificación de las inconsistencias en datos, reportes y liberación de información.
- Comparación de datos físicos vrs. digitalizados a través de fuentes externas.
- Verificación de la comunicación a través de las diversas interfases de red.
- Evaluación de las medidas de seguridad, tanto lógica como física de la información.

La auditoria de sistemas se realizará con base a las Normas Internacionales de Auditoria (NIAS), la cual se efectuará en un periodo de 15 semanas, pudiendo variar este periodo por circunstancias ajenas a nuestro control haciéndolo saber anticipadamente a la administración de la empresa.

3.2.1.4. TIPO DE INFORME A PRESENTAR

Los informes a presentar son importantes para indicar las observaciones y recomendaciones a la gerencia, se expone la opinión sobre lo adecuado o lo inadecuado de los controles o procedimientos revisados durante la auditoria.

Es responsabilidad de la firma presentar a la administración, información sobre los hallazgos importantes determinados en el examen

de los sistemas de información. Los informes que pueden presentarse son:

- ❖ Informe preliminar del estudio de control interno.
- ❖ Cartas a la gerencia.
- ❖ Informe final

Informe preliminar del estudio del control interno[9]

Este informe preliminar presenta un extracto de desviaciones y áreas de mejoramiento de control interno encontradas, así como una conclusión de auditoria sobre éstas.

Carta de gerencia

Contendrá los hallazgos de auditoria, en donde reflejan la condición actual, criterio, causa, efecto y oportunidades de mejora de estos hallazgos.

Informe final de auditoria

Éste contiene la conclusión final del auditor, incluye las respectivas sugerencias sobre los hallazgos reportados y no subsanados.

[9] El informe preliminar del control interno puede ser presentado dentro de la carta de gerencia.

3.2.2. ENTENDIMIENTO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS.

La comprensión del ambiente y sistemas de información computacionales conjuntamente con los controles relacionados, son áreas importantes para la auditoria, debido a que los resultados de éste se considerarán al determinar la estrategia del trabajo de auditoria y de esta forma desarrollar el plan global de auditoria. Para estudiar los sistemas se deben realizar las siguientes actividades:

- Comprender cómo está organizada el área de sistemas de información computarizados.
- Comprender cómo controla la dirección las actividades que realiza el sistema de información computarizado.
- Identificar las principales características de los sistemas y de su ambiente.
- Identificar los cambios significativos a los sistemas y de su ambiente.

Es necesaria la utilización de técnicas de auditoria para el establecimiento de los puntos que serán evaluados y considerar aspectos muy específicos de los sistemas computacionales, tales como:

- Observación de las actividades en las instalaciones, con el objetivo de dar al auditor una noción acerca de la organización y su relación con los reportes finales que se emiten para la toma de decisiones.

- Revisión de instalaciones físicas, para recopilar información sobre la estructura en que se organiza el área de sistemas y como realiza las operaciones, revisando aspectos como: la distribución de maquinas, del personal, espacio adecuado, operaciones que se realizan, entre otras.

- Revisión del sistema utilizado, se verifican algunos aspectos tales como: legalidad del sistema, si la empresa cuenta con manual del sistema, la utilización de manuales de usuario, principales módulos del sistema, el proceso de captura de datos, las salidas de información, entre otras.

- Identificación de seguridad lógica, revisando si la empresa aplica procedimientos para el resguardo, acceso de información, y autorizaciones por ejemplo: modalidades de acceso (claves), administración de base de datos, limitaciones a los usuarios, acceso a transacciones o diferentes módulos del sistema, backup, entre otros.

- Identificación de seguridad física, revisión de la aplicación de procedimientos o medidas de prevención ante amenazas a la información, controles y mecanismos de seguridad, tanto para protección de medios de hardware como de software y para el almacenamiento de datos. También permitir o negar acceso a áreas o sectores dentro de la empresa; por ejemplo: si existen guardias de seguridad, verificación de firmas, protección electrónica, detector de metales, entre otros.

3.2.2.1. ESTUDIO Y EVALUACIÓN DE CONTROL INTERNO

Para el entendimiento del sistema de información es necesario conocer los controles internos aplicables al ambiente SIC, a fin de unificar criterios y verificar el cumplimiento operativo de dichos controles.

Para el estudio y evaluación de control interno se utilizan procedimientos que verifican el cumplimiento de políticas relacionadas al control interno y dirigidas a los sistemas de la empresa a la que presta el servicio.

Entre los controles a verificar se encuentran:

- Controles sobre organización
- Controles de administración.
- Controles sobre la operación y procesamiento del sistema.
- Control del programa del cliente

Controles de organización

Básicamente, el auditor revisa el plan de organización y las responsabilidades funcionales, a fin de determinar si existe una separación de la autoridad, el mantenimiento de los registros y la custodia de los activos. Esta segregación de funciones se logra en los sistemas de información computarizados, por la separación de las funciones de análisis de sistemas y las de programación. Además, tal separación fomenta la eficiencia de operación, puesto que las

capacidades, conocimientos, capacitación y destrezas que se requieren para ejecutar estas funciones, difieren grandemente.

Para valorizar los controles de organización, el auditor debe revisar los diagramas y manuales de organización, observar las actividades del personal del sistema de información computarizada y plantear preguntas.

Controles administrativos

La evaluación de los controles administrativos consiste principalmente en revisar la documentación referente al diseño del sistema, programación y operaciones de computadoras. El auditor debe determinar la idoneidad de la documentación, revisando los diagramas de recorrido del sistema y de los programas, los libros de corridas de programas y de consola, los manuales de normas de programación, los registros de utilización del SIC, los procedimientos del mantenimiento del programa, y los procedimientos de biblioteca de SIC.

Controles de procedimientos

El aspecto principal de la evaluación de los controles internos, es determinar la existencia de un sistema de procesamiento de datos y la efectividad con que dicho sistema registre, procese y reporte los datos. Esta revisión es importante para poder determinar si se han establecido procedimientos financieros y contables para asegurarse de que:

1. Las transacciones son revisadas lo suficiente para establecer la idoneidad y exactitud de sus registros.

2. El recorrido del procesamiento de datos permite descubrir y corregir errores en los datos de operaciones y financieros, reduciendo dichos errores al nivel permitido por la gerencia.

3. Se exigen y preparan informes que reflejan la responsabilidad de la autorización, la ejecución y la revisión de transacciones financieras y contables.

El auditor necesitará entonces observar las diferentes actividades del procesamiento de datos, e interrogar a los encargados de ejecutarlas, a fin de comprender más a fondo el sistema y sus controles.

Control del programa del cliente

Uno de los procedimientos importantes para probar los sistemas de información computarizados de una empresa, consiste en asegurarse que el programa en estudio, es el mismo que la compañía usa efectivamente para procesar sus datos. Básicamente existen dos fórmulas de lograrlo.

La primera, es solicitar sorpresivamente el programa al bibliotecario de SIC, duplicarlo para el control del auditor, y usarlo en el procesamiento de los datos de prueba. El auditor también puede solicitar datos de prueba, previamente procesados con la copia del programa del auditor, para procesarlos con el programa de operación

del cliente; el auditor puede así comparar los resultados. Este método tiene la ventaja adicional de verificar cualquier intervención de los operadores de la computadora.

El segundo método consiste en que el auditor solicite inesperadamente y a base de sorpresa, que el programa de operación permanezca en la computadora después de haberse procesado totalmente los datos de operación, de tal manera que él pueda procesar sus datos de prueba con dicho programa. Este método tiene, sobre el anterior, la ventaja de que por lo general garantiza una versión vigente y actual del programa.

Una vez que ha obtenido el programa del procesamiento del cliente, el auditor debe duplicar el programa, conservar la copia para su propio uso, y observar el procesamiento de sus datos de prueba con esta copia controlada[10].

Prueba del sistema

El auditor tiene que probar el sistema de procesamiento de datos para determinar la existencia y efectividad de los procedimientos de procesamiento de información del cliente, así como de los controles programados. Al probar los sistemas de información computarizados, el auditor deberá elaborar datos de prueba para determinar con exactitud como reaccionará un sistema de procesamiento específico ante determinado tipo de transacciones; prácticamente, el auditor deja que

[10] Enrique García, José Antonio año 1995 "Auditoria en Informática" México, editorial Mc Graw-Hill

el SIC se haga una auditoria a sí mismo, presentando al sistema transacciones de prueba que éste no puede distinguir de las transacciones de operación. Entonces el auditor evalúa los resultados y determina si efectivamente las transacciones de prueba se procesaron de la manera descrita en la revisión del sistema.

La elaboración y el empleo de las transacciones de prueba tienen seis etapas las cuales son[11]:

1. Decidir el punto exacto del sistema donde han de introducirse las transacciones de prueba.

2. Determinar los tipos de transacciones que incluirán en los datos.

3. Obtener registros maestros para procesar con las transacciones de prueba y computar los resultados predeterminados para compararlos con los resultados de salida del procesamiento de prueba.

4. Considerar cuidadosamente los efectos que causará el procesamiento de las transacciones de prueba, en los resultados del sistema producido bajo condiciones normales de operación.

5. Obtener los programas regulares de procesamiento del cliente y comprobar que el programa se utilice para procesar las transacciones de prueba.

[11] Enrique García, José Antonio año 1995 "Auditoria en Informática" México, editorial Mc Graw-Hill

6. Hacer los arreglos necesarios para preparar y procesar las transacciones de prueba y obtener la salida en la forma deseada.

Además de determinar los tipos de transacción, obtener registros maestros y obtener el programa normal de procesamiento del cliente, el auditor debe diseñar cuidadosamente datos de prueba, obtener el equipo y el personal necesarios y solicitar tiempo de la computadora al personal autorizado, para preparar y procesar los datos de prueba y obtener la salida en la forma deseada.

La interpretación y evaluación que el auditor haga de los resultados de prueba, puede simplificarse y acelerarse mediante el empleo de claves especiales y nombres distintivos que permiten identificar fácilmente las transacciones de prueba.

3.2.2.2. INFORME PRELIMINAR DEL ESTUDIO DE CONTROL INTERNO

La función del entendimiento, estudio, y evaluación de los sistemas y sus controles, se materializa exclusivamente por escrito. Por lo tanto la elaboración de un informe sobre las deficiencias encontradas expone de mejor manera el trabajo realizado.

Es evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre las conclusiones del auditor y auditado.

El informe preliminar del estudio de control interno contendrá: la fecha de comienzo de la auditoria y la fecha de redacción del mismo; se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo.

La aparición de un hecho en un informe de deficiencias de control interno implica necesariamente la existencia de una debilidad que ha de ser corregida.

El informe preliminar del estudio y evaluación del control interno tiene dos formas de ser presentados, la primera en forma de cara de gerencia y la segunda en forma de reporte.

Contenido del informe preliminar de control interno en forma de cara de gerencia:

Flujo del hecho o debilidad:

1 Hecho encontrado.

- ❖ Ha de ser relevante para el auditor y para el cliente.
- ❖ Ha de ser exacto, y además convincente.
- ❖ No deben existir hechos repetidos.

2 – Consecuencias del hecho

- ❖ Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

3 – Repercusión del hecho

- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

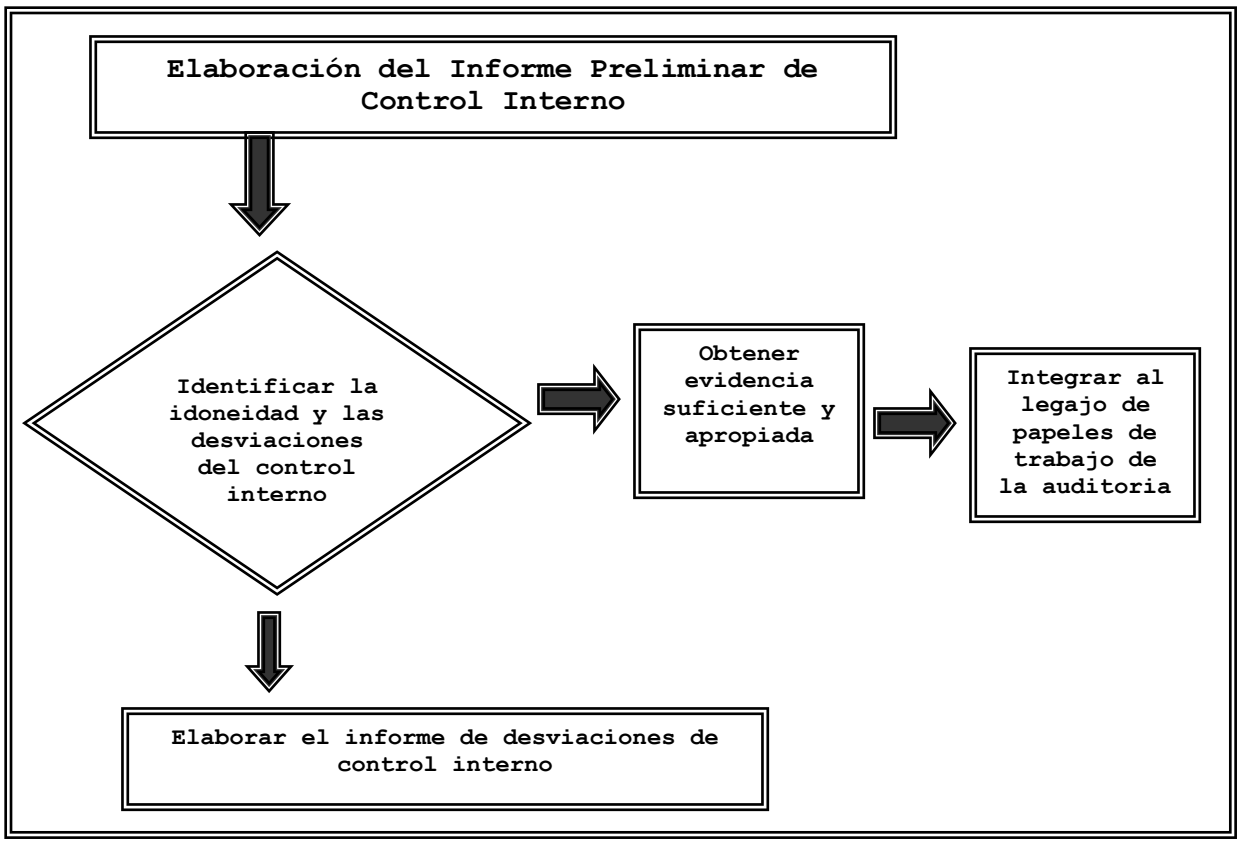
4 – Conclusión del hecho

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

5 – Recomendación del auditor informático

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

El informe preliminar de control interno puede ser presentado separado de la carta de gerencia, en el se resume la evaluación de auditoria realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoria.



El informe preliminar separado de la carta de gerencia poseerá los siguientes atributos:

- Deberá ser redactado de manera breve y clara.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- No se escribirán nunca recomendaciones.

3.2.3. DETERMINACIÓN DEL RIESGO

Una auditoria tal vez no detecte cada uno de los potenciales errores en un universo; pero si el tamaño de la muestra es lo suficientemente grande, o se utiliza procedimientos estadísticos adecuados, se llega a minimizar la probabilidad del riesgo de detección. De manera similar al evaluar los controles internos, el auditor de sistemas debe percibir que en un sistema dado se puede detectar un error mínimo, pero ese error combinado con otros, puede convertirse en un error material para todo el sistema.

RIESGOS ASOCIADOS AL ÁREA DE TI:

Hardware

- Descuido o falta de protección
- Condiciones inapropiadas
- Mal manejo
- Destrucción

Software:

- Uso o acceso (no autorizado)
- Copia (exportación de datos no autorizada).
- Modificación (no autorizada).
- Destrucción.
- Error u omisión

Archivos:

- Copia o modificación (no autorizada), destrucción, hurto.
- Usos o acceso (no autorizada).

Organización:

- Inadecuada: no funcional, sin división de funciones.
- Falta de seguridad.
- Falta de políticas y planes.

Personal

- Deshonesto, incompetente y descontento.

Usuarios:

- Enmascaramiento, falta de autorización, falta de conocimiento de su función.

3.2.3.1. EVALUACIÓN DE RIESGO

De acuerdo con la NIA 315 "Evaluación del riesgo y control interno", el auditor debería hacer una evaluación de los riesgos inherentes y de control, además el auditor debería considerar el ambiente SIC al diseñar los procedimientos de auditoria para reducir el riesgo de a un nivel aceptablemente bajo.

Al determinar que áreas funcionales deben auditarse, el auditor de sistemas debe evaluar todos los riesgos que pueden existir.

Existen tres motivos por los que se utiliza la evaluación de riesgos, estos son:

- Permitir que la gerencia asigne recursos necesarios para la auditoria.
- Garantizar que se ha obtenido la información pertinente
- Garantiza que las actividades de la función de auditoria se dirigen correctamente a las áreas de alto riesgo.

El nivel de importancia se determinará a juicio del auditor y dependerá del área del sistema de información que se está evaluando, por lo que se incluirán aquellos componentes que tengan materialidad sobre la evaluación.

El nivel de riesgo de detección se establecerá de acuerdo al nivel de riesgo inherente y al nivel de riesgo de control.

La determinación del riesgo se realiza de diversas formas, una de ellas es utilizando una matriz de riesgo.

Una matriz es una herramienta sencilla que permite realizar un diagnóstico objetivo de la situación global de riesgo en los sistemas de información.

Matriz de riesgo

N°	Evaluación del riesgo del sistema "x" por áreas de mejora	Controles alrededor del computador									Controles a través del computador								
		Inherente			Control			Detección			Inherente			Control			Detección		
		A	m	b	a	m	b	a	m	b	a	m	b	a	M	b	a	m	b
1	Instalación del software		■			■				■									
2	Inicio de programa	■				■				■									
3	Recopilación de la información												■			■		■	
4	Ordenar, clasificar documentos.	■				■			■										
5	Captura de datos		■			■			■										
6	Verificación de datos												■		■			■	
7	Desactualización de la información											■				■		■	
8	Consultas de datos												■		■			■	
9	Reportes	■				■			■				■		■			■	
10	Impresión											■			■				■
11	Backup	■					■		■										
10	Revisión de backup		■			■				■									

Donde:

a = alto

m = Medio

b = Bajo

Instalación del software.

Al evaluar los controles realizados alrededor del computador, y los diferentes controles aplicados esta área se determinó que el riesgo de detección es bajo, debido a que los riesgos inherentes y de control son medios, por tanto hay menor riesgo de que no se detecte oportunamente alguna falla o error.

Inicio de programa.

Al evaluar los diferentes controles que se aplican en el inicio del programa se determinó un riesgo de detección bajo, lo cual indica menor riesgo de no detectar fallas o errores.

Recopilación de la información.

Al evaluar esta área se identifico susceptibilidades de que los controles aplicados en la empresa, para éste tipo de actividades, no son suficientes; por tanto el riesgo de detección es medio, lo cual es un indicio de que los procedimientos implementados al realizar la auditoria no detecten el total de errores en esta área, y es necesario que se consideren realizar procedimientos adicionales que puedan reducir éste riesgo.

Ordenar y clasificar documentos.

Al ordenar y clasificar la información, se determinó, que existe un riesgo de control medio, debido a que los controles existentes aplicados para salvaguardar que estos procedimientos se realicen de manera fiable son medianamente eficientes, por lo tanto se determinó

un riesgo de detección medio, es decir que existe la posibilidad de que los procedimientos desarrollados, no detecten oportunamente fallas en esta área del sistema; por lo cual se considerará la realización de procedimientos adicionales de auditoria, con el fin de poder disminuir éste riesgo a un nivel aceptablemente bajo.

Captura de datos.

En la captura de datos existe susceptibilidad de errores y controles aplicados no son los adecuados para detectarlos, ya que éstos son medianamente efectivos, por lo tanto es necesario mejorarlos para poder reducir los riesgos a un nivel aceptablemente bajo, el riesgo de detección es medio, es decir que se deben desempeñar procedimientos adicionales a fin de reducir este riesgo a un nivel aceptablemente bajo.

Verificación de datos.

En éste tipo de procedimientos, se determinó un riesgo de detección medio debido a que el riesgo de susceptibilidades del sistema y de los controles aplicados al verificar los datos recopilados y procesados por el sistema son medianamente efectivos.

Áreas de desactualización de la información, consultas de datos y reportes.

Al evaluar el control interno en estas áreas se determinó un riesgo de detección medio, por tanto es necesario implementar nuevos

procedimientos, encaminados a reducir éste riesgo a un nivel aceptablemente bajo.

Áreas de impresión, backup y revisión de backup.

Al evaluar los diferentes tipos de riesgos en éstas áreas, tanto en los controles alrededor del computador como a través de él, se determinó que el riesgo de detección es razonablemente bajo, por tanto no será necesaria la realización de procedimientos adicionales de auditoria.

Definido el grado de riesgo (alto, medio, bajo), se debe elaborar una lista de medidas preventivas a tomar y las correctivas en caso de desastre señalando prioridades.

El riesgo de auditoria tiene una influencia directa sobre la cantidad de evidencia a recopilar, pues interviene en que el auditor de una conclusión correcta o equivocada.

3.2.3.2. DETERMINACIÓN DE ÁREAS CRÍTICAS

La evaluación del control interno proporciona la base para determinar el riesgo existente en cada área a examinar, así mismo conocer sus incidencias en el funcionamiento del sistema, y de las políticas y procedimientos establecidos para los sistemas de información computarizados.

Después de analizar los sistemas de información computarizados de la compañía, determinamos los riesgos en las principales áreas de los sistemas y se bebe poner énfasis en las áreas críticas o de mayor riesgo.

Para establecer un área crítica el auditor debe considerar la fragilidad de acuerdo a los niveles de seguridad; a través de las fallas de control interno, las fallas del sistema y la probabilidad de error.

Ejemplo de las principales áreas críticas de los sistemas

Entre las principales áreas críticas en los sistemas se encuentran: las operaciones de procesamiento, debido a que se considera como un punto susceptible además de vital importancia en la generación de información confiable y para los cuales debe contarse con controles encaminados a minimizar riesgos en los sistemas y su entorno; así también se consideran áreas críticas la seguridad lógica y la seguridad física de los sistemas.

3.2.4. PROGRAMACIÓN DEL TRABAJO

Dentro de la planeación de auditoria a los sistemas de información computarizados, es necesario incluir la programación del trabajo, en la cual se estipulan los procedimientos a seguir para identificar el cumplimiento del control interno, la calidad del funcionamiento del sistema y las evidencias que permitan formular una conclusión acertada sobre el funcionamiento del sistema.

3.2.4.1. PROGRAMAS DE AUDITORIA

Se requieren varios pasos para realizar una auditoria; el auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoria que consta de objetivos de control y procedimientos de auditoria que deben satisfacer esos objetivos. El proceso de auditoria exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoria que presente esos temas en forma objetiva a la gerencia.

Asimismo, la gerencia de auditoria debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoria además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

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

- Complejidad de los sistemas.
- Uso de lenguajes.
- Metodologías, son parte de las personas y su experiencia.
- Centralización de funciones.
- Controles del computador.
- Controles manuales y controles automatizados (procedimientos programados).
- Confiabilidad electrónica.

- ❖ Debilidades de las máquinas y tecnología.
- ❖ Transmisión y registro de la información en medios magnéticos, óptico y otros.
- ❖ Almacenamiento en medios que deben acceder a través del computador mismo.
- ❖ Centros externos de procesamiento de datos.
- ❖ Dependencia externa.

Desarrollo del programa de auditoria.

Un programa de auditoria es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoria planificados. El esquema típico de un programa de auditoria incluye lo siguiente:

1. **Tema de auditoria:** Donde se identifica el área a ser auditada.
2. **Objetivos de Auditoria:** Donde se indica el propósito del trabajo de auditoria a realizar.
3. **Planificación previa:** Donde se identifican los recursos y destrezas que se necesitan para realizar el trabajo; así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
4. **Procedimientos de auditoria:**
   - ❖ Recopilación de datos.
   - ❖ Identificación de lista de personas a entrevistar.

- Identificación y selección del enfoque del trabajo
- Identificación y obtención de políticas, normas y directivas.
- Desarrollo de herramientas y metodología para probar y verificar los controles existentes.
- Procedimientos para evaluar los resultados de las pruebas y revisiones.
- Procedimientos de comunicación con la gerencia.
- Procedimientos de seguimiento.

El programa de auditoria se convierte también en una guía para documentar los diversos pasos de auditoria y para señalar la ubicación del material de evidencia. Generalmente tiene la siguiente estructura:

NOMBRE DEL DESPACHO **PERIODO DE AUDITORIA** **PROGRAMAS DE AUDITORIA** **EMPRESA:** **FECHA:** **AREA:** **OBJETIVOS:**			REF	
N°	**Procedimiento**	**Hecho Por**	**Ref.**	**Descripción del procedimiento**

Los procedimientos involucran pruebas de cumplimiento o pruebas sustantivas, las pruebas de cumplimiento se hacen para verificar que los controles funcionan de acuerdo a las políticas y procedimientos

establecidos y las pruebas sustantivas verifican si los controles establecidos por las políticas o procedimientos son eficaces.

El auditor debe tener la habilidad para revisar y probar la integridad de los sistemas.

Algunos ejemplos de procedimientos de auditoria son:

- Revisión de la documentación de sistemas e identificación de los controles existentes. Entrevistas con los especialistas técnicos a fin de conocer las técnicas y controles aplicados.

- Verificar los controles y procedimientos de autorización de la utilización y captura de los datos, su proceso y salida de información, así como los programas que las generan. Es importante revisar los procedimientos para el mantenimiento de los programas y las modificaciones a los sistemas.

- Revisar las transacciones realizadas para asegurarse de que los archivos reflejan la situación actual.

- Revisar las transacciones y los archivos para detectar posibles desviaciones de las normas establecidas.

- Asegurarse de que las aplicaciones cumplan con los objetivos definidos en la planeación.

- Revisar todos los cambios hechos a los programas y sistemas para verificar la integridad de las aplicaciones.

3.2.4.2. EJEMPLO DE PROGRAMAS DE AUDITORIA DE SISTEMAS

AUDITORES HR Y ASOCIADOS

Auditoria a los Sistemas de Información Computarizados del 1 de marzo al 30 de agosto de 2008

Programa de Auditoria

Empresa: SINTEX S.A. DE C.V.

Fecha: 14 marzo de 2008

Área: **Captura de datos**

Objetivo: Conocer la forma en que se realiza la captura de datos a fin de garantizar su integridad para el procesamiento de estos

N°	Procedimiento	Hecho por	Ref.	Descripción
1	Verificar la captación de datos por parte de las personas encargadas			Se verificará a través de la base de datos la hora y la fecha en que captura los datos
2	Cerciorarse que la captura de datos se está haciendo a través del módulo y de la opciones adecuadas a fin de alimentar los diferentes módulos interrelacionados			Se verificará el ingreso de documento a través de registro de la tabla y se envían adecuadamente, con una base de Excel o similar a la base de datos

3	Se revisará la planeación de trabajo de la compañía, en función del cumplimiento de las metas de la misma			observe las siguientes situaciones: a) cada cuanto tiempo se elabora el programa, b) si se labora de forma interna, c) se señala las prioridades y posibles fechas de entrega
4	Verificar que la captura de datos coincida con los documentos fuentes reales			Se revisará a través del uso de documentos
5	Verifique que los documentos de compra ingresados en el sistema, estén de acuerdo a los CCF físico			Se verificará a través del boucher de la documentación
6	Verificar que el procesamiento de las órdenes estén en función de los datos reales			Se verificará a través de una muestra de dichas órdenes
7	Verifique que el ingreso del producto terminado esté en función de proceso de costeo en el módulo respectivo			Se verificará que el módulo de costos esté emitiendo adecuadamente la información para los módulos interrelacionados

3.3. PAPELES DE TRABAJO

Entender los pasos del proceso de auditoria del área de sistemas de información computarizados permite a los administradores del sistema saber lo que deben esperar de la auditoria; de esta forma pueden lograr los objetivos de cumplimiento normativo de su empresa y optimizar el proceso de auditoria para completarlo más eficazmente; posteriormente entregar a la gerencia un informe final con relación a lo auditado.

El legajo de los papeles de trabajo, por su naturaleza y contenido, es el aspecto fundamental para elaborar el informe de auditoria, y su uso es confidencial y exclusivo del auditor de sistemas. El contenido de los papeles de trabajo puede variar de un auditor a otro, ya que en cada auditoria existen técnicas, procedimientos y métodos de evaluación especiales, que obtienen diferente tipo de evidencia.

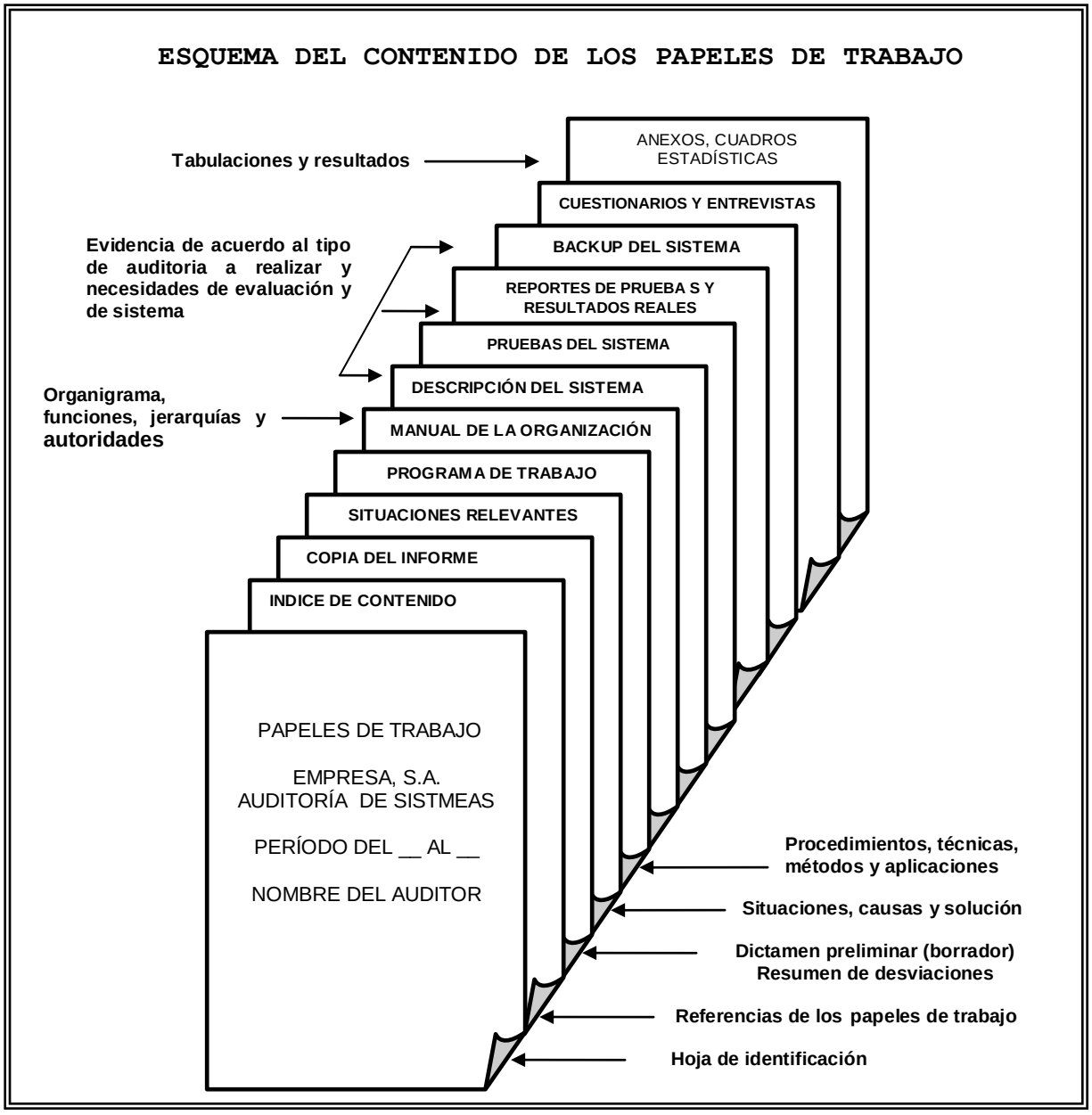
Entre alguna documentación que forman los papeles de trabajo están:

- Hoja de identificación
- Índice de contenido de los papeles de trabajo
- Resumen de deficiencias de control
- Programas de trabajo de auditoria
- Manual de organización
- Descripción organizacional del centro de cómputo
- Reporte de pruebas y resultados del sistema

- Respaldos (backup) de datos, disquetes, CD y programas de aplicación de auditoria
- Respaldo (backup) de las bases de datos y de los sistemas
- Guía de claves para el señalamiento de los papeles de trabajo
- Diagramas de flujos, de programas y de desarrollo de sistemas
- Testimonios, actas y documentos legales de comprobación y confirmación
- Análisis y estadísticas de resultados, datos y pruebas de comportamiento del sistema
- Otros documentos de apoyo para el auditor

En una auditoria de sistemas los papeles de trabajo representan el sustento para registrar los datos e información que se van recolectando durante la evaluación, por la especialidad de medios que se usan para el registro de la información de las áreas de cómputo, la recopilación de datos se puede realizar en documentos o medios electromagnéticos de captura y resguardo de datos, estos pueden ser discos duros, discos flexibles, cintas, CD-ROM, DVD, y otros medios electromagnéticos.

Existen múltiples formas de elaborar y utilizar los papeles de trabajo, las cuales estarán determinados por la experiencia, habilidad y conocimiento del auditor. La obtención del legajo de papeles de trabajo dependerá de la astucia del auditor y de la necesidad del documento.



Para que los papeles de trabajo puedan admitirse como soporte documental de auditoria de sistema, y para que fundamente los resultados y opiniones que presenta el auditor, es necesario que tanto en su diseño como en su uso, reúnan ciertos requisitos y formalidades, los cuales serán determinados por el auditor responsable de la auditoria.

3.4. INFORME DE AUDITORIA

Los informes de auditoria son el producto final del trabajo del auditor de sistemas, este informe es utilizado para indicar las observaciones y recomendaciones a la gerencia; aquí también se expone la conclusión sobre el funcionamiento de los sistemas y de sus controles o procedimientos revisados durante la auditoria, no existe un formato específico para exponer un informe de auditoria de sistemas de información.

Los pasos para elaborar el informe son los siguientes:

1. Aplicar instrumentos de recopilación.
2. Registrar los hallazgos encontrados durante la auditoria.
3. Encontrar las causas de los hallazgos y sus posibles soluciones.
4. Analizar, depurar y corregir los hallazgos.
5. Crear conclusiones sobre los resultados obtenidos.
6. Concentrar, depurar y elaborar el informe final de auditoria.
7. Presentar el informe a los directivos de la empresa.

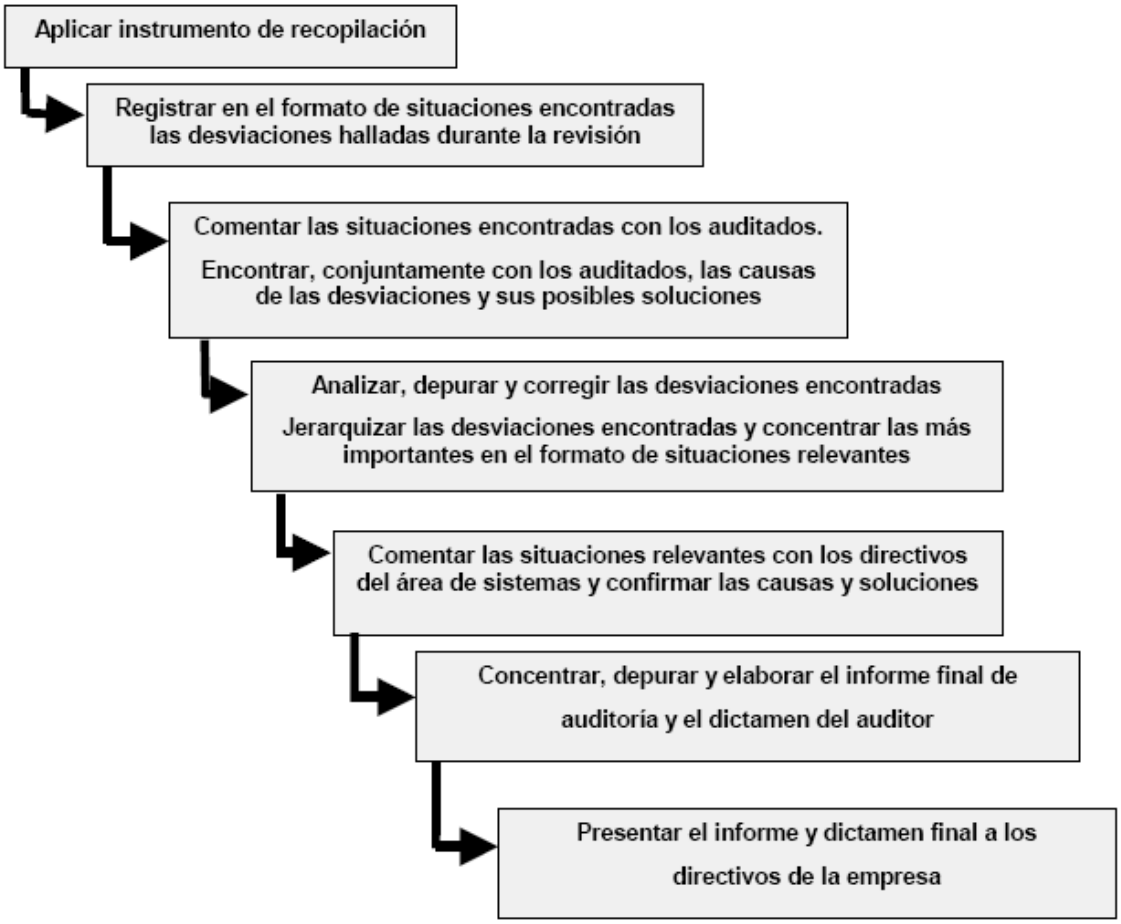
El informe debe tener ciertas características fundamentales referidas al contenido y forma del sistema.

Las características relativas a la forma, se refieren al cuido del auditor de que el informe esté acorde con la revisión efectuada, que la información que contenga sea veraz, confiable y oportuna, sin distorsiones ni tendencias, que muestre con simple lectura la situación

real de los sistemas y que el lector capte inmediatamente la conclusión del auditor.

Las características de forma que debe cumplir el informe, se refiere a la manera en que el auditor debe presentar el informe, en cuanto al estilo de redacción, sus partes y apéndices. Estas características consisten en la redacción clara, sencilla, sin excesos de tecnicismo, sin redundancias, sin errores ortográficos y sin ningún error en la forma de presentación.

Esquema del proceso de elaboración del informe de auditoria.



Generalmente tiene la siguiente estructura:

- Introducción al informe, donde se expresará los objetivos de la auditoria, el período o alcance cubierto por la misma, y una expresión general sobre la naturaleza o extensión de los procedimientos de auditoria realizados.

- Descripción del sistemas, en la cual se detalle cada uno de lo módulos del sistema que se esta auditando, la función de dichos módulos, el motivo por el cual fue adquirido dicho sistema, el detalle de sus fabricantes y otras especificaciones que el auditor considere conveniente incluir en la descripción del sistema.

- Observaciones detalladas y recomendaciones de auditoria.

- Respuestas de la gerencia a las observaciones con respecto a las acciones correctivas.

- Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

4. CONCLUCIONES Y RECOMENDACIONES

Después de realizada la investigación sobre la ausencia de lineamientos técnicos actualizados para el diseño de planeación de auditoria a los sistemas de información computarizados, se concluye y recomienda lo siguiente:

4.1. CONCLUCIONES

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

- La auditoria de sistemas de información computarizados es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

- Según los resultados de la investigación, la poca experiencia en el área y la falta de lineamientos técnicos actualizados, son las dificultades más influyentes al desarrollar una auditoria en un ambiente de sistemas de información computarizados, puesto que en esta área, se requiere la aplicación de conocimientos de

tecnología de información y comunicación, para desarrollar los procedimientos adecuados en el trabajo.

- De acuerdo con los resultados obtenidos de la investigación, los profesionales en auditoria consideran que la existencia de lineamientos técnicos actualizados dirigidos a la etapa de planeación para una auditoria a los SIC, permiten desarrollar auditorias más eficientes, gracias a que con estos, pueden realizarse procedimientos, planes, y programas de trabajo que consideren aspectos específicos en los sistemas, permitiendo una evaluación de forma integral.

- Los métodos que más se utilizan para la evaluación del control interno son las entrevistas, los cuestionarios, el análisis de los diagrama de flujo de proceso, la realización de pruebas de cumplimiento de las seguridades, revisión de procesos históricos (backups).

- En el desarrollo de una auditoria de sistemas, se hace muchas veces necesario auxiliarse de un experto en informática, sin embargo, quien le otorga el carácter propio de una auditoria aplicando criterios y lineamientos técnicos y normativos propios de su formación y capacidad profesional son los auditores.

4.2. RECOMENDACIONES

- Los contadores públicos y auditores deben considerar la necesidad de obtener conocimiento en el área tecnológica especialmente con los sistemas de información computarizada que están relacionados con la profesión contable, mediante un plan de educación continuada permitiendo de esta manera, diversificar sus servicios y cubrir los requerimientos necesarios en tecnología para un desarrollo más eficiente del trabajo.

- Los auditores deben considerar al efectuar una auditoria de sistemas, incluir una evaluación exhaustiva sobre la seguridad de la información que se maneja mediante medios computacionales, debido a la gran cantidad de información que se procesa, para obtener una mayor confiabilidad, oportunidad y eficiencia de los datos obtenidos, enfocándose principalmente a la seguridad física y lógica de los sistemas, con el fin de contribuir a minimizar riesgos que puedan presentarse en el desarrollo de las actividades relacionadas al procesamiento y divulgación de la información financiera.

- A las firmas de auditoria, que faciliten a su personal lineamientos apropiados para la planeación, tomando en cuenta los requerimientos en tecnología y normativa contable vigente aplicable.

- Para desarrollar una auditoria de sistemas más eficiente, el auditor si no posee la capacidad para desarrollar algún procedimiento debe auxiliarse de la ayuda de un experto, que posea los conocimientos necesarios sobre la tecnología de la información y comunicación.

- Para llevar a cabo una auditoria más eficiente los auditores deberían utilizar los siguientes métodos para la evaluación del control interno: las entrevistas, los cuestionarios, el análisis de los diagrama de flujo de proceso, la realización de pruebas de cumplimiento de las seguridades, revisión de procesos históricos (backups) y otros procedimientos que desarrolle el especialista.

- Que el presente documento se utilice como una herramienta de consulta tanto para los auditores independientes, como estudiantes que requieran información de una auditoria de sistemas enfocada al área de la seguridad informática.

BIBLIOGRAFÍA

- Comité Internacional de Practica de Auditoria, Normas Internacionales de Auditoria, Año 2007.

- Gómez Girón, José Alfredo; Velásquez Murío, Adán; Peña Dimas, Carlos Alberto. Año 1999, "Diseño de un Modelo de Evaluación de los Niveles de Riesgo en la Auditoria de Sistemas de Procesamiento Electrónico de Datos". Trabajo de graduación para optar a grado de Lic. En Contaduría Pública. Universidad de El Salvador.

- Fonseca, Jaime Alberto; Castro Calderón, Año 1998, "Guía de Lineamientos Técnicos para la Planeación de Auditoria de Estados Financieros de Empresas del Sector Comercial que Utilicen el Procesamiento Electrónico de Datos (PED)"

- Jovel Jovel, Roberto Carlos, Año 2008, "Guía Básica para la Redacción de Trabajos de Investigación Universidad de El Salvador".

- J, Emey, España 2004 "Sistemas de Planteamiento y Control de la Empresa", Edición Pirámide.

- MLeod JR. Año 2006, "Sistemas de Información General, Edición Pirámide". España.
- Escoto Rivas, Ricardo Iván; Alberto Martínez, Abjose Nilo, Año 2002 "Manual de Auditoria De Sistemas Operativos" San Salvador.
- Echenique García, José Antonio; Año 1995 "Auditoria en Informática", Editorial Mc Graw-Hill México.
- HL, David; Año 1992 "Auditoria en Centros de Computo" Editorial Trillos, México.
- http://www.monografia.com/trabajos55/analisis-sistemas-de-informacion/analisis -sistemas -de-informacion.shtml
- http://www.monografia.com/trabajos40/auditoria-informatica/auditoria-informatica-.shtml
- http://www.monografia.com/trabajos14/datos.shtml
- http://www.hugo-r-gonzalez-b-neurona.com
- http://www.bibliotec.bcv.org.ve/cgi-win/b-ales.exe

ANEXOS

Índice de los Anexos

.

Anexo 1: Encuesta dirigida a los auditores independiente

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONOMICAS
ESCUELA DE CONTADURIA PÚBLICA

CUESTIONARIO PARA AUDITORES

Estimados auditores, les solicitamos de su colaboración para brindar información relativa a su experiencia en el ejercicio de la Auditoria de Sistemas de información computarizados (SIC), la cual será utilizada con fines académicos, en la elaboración de trabajo de graduación de la carrera de Licenciatura en Contaduría Publica.

Objetivo: Lograr obtener información para diagnosticar la necesidad de elaborar lineamientos técnicos actualizados para el desarrollo de la planeación de auditoria de los sistemas de información computarizados (SIC).

Indicaciones: Se recomienda leer detenidamente cada interrogante, contestando de la manera mas adecuada posible. Si tiene dudas consulte con el encuestador. De antemano muchas gracias.

1. ¿Qué tipo de lineamientos técnicos utiliza para realizar la auditoria a los sistemas de información computarizados?
   a) Las NIAs ☐
   b) Lineamientos brindados por otros profesionales ☐
   c) Su experiencia ☐
   d) Otros (especifique)_____

2. ¿Cómo considera los lineamientos técnicos que utiliza?
   a) Adecuados ☐
   b) Pueden mejorarse ☐
   c) Limitados ☐

3. ¿A cuáles de los siguientes factores considera que obedece la poca existencia de lineamientos técnicos?
   a) No se encuentra fomentada la auditoria de sistemas en nuestro medio ☐
   b) Su elevado costo ☐
   c) Constantes cambios en las técnicas ☐
   d) Otros (especifique)_____

4. De que factores depende, según su opinión, que el auditor emita una conclusión errónea en la auditoria al funcionamiento de los SIC.
   a) Poca especialización ☐
   b) Falta de lineamientos teóricos actualizados ☐
   c) Procedimientos inadecuados ☐
   d) Otros (especifique)_____
   _____

5. ¿Cuál de las siguientes dificultades considera más influyentes, al desarrollar una auditoria a los sistemas de información computarizados?
   a) Falta de lineamientos técnicos actualizados ☐
   b) Poca experiencia en el área ☐
   c) Los constante cambios en los sistemas ☐
   d) Otros (especifique) _____

6. Para la realización de la auditoria de sistemas utiliza la ayuda de un experto
   a) Si ☐
   b) No ☐
   c) Por que_____

7. Si utiliza la ayuda de un experto, ¿cuál de los siguientes profesionales le es conveniente?
   a) Ingeniero en Sistemas ☐
   b) Técnico en Sistemas ☐
   c) Auditor especialista en Auditoria de Sistemas ☐
   d) Otros (especifique) _____

8. Mencione cuales procedimientos utiliza para desarrollar la auditoria a lo Sistemas de información computarizados (SIC).
   a) Revisión de la documentación de sistemas ☐
   b) Identificación de los controles existentes ☐
   c) Entrevistas con los especialistas técnicos a fin de conocer las técnicas y controles aplicados ☐
   d) Utilización de software de manejo de base de datos para examinar el contenido de los archivos de datos. ☐
   e) Otros (especifique)_____

9. ¿De qué manera evalúa el control interno en la auditoria de sistemas de información computarizados?
   a) Entrevistas ☐
   b) Cuestionarios ☐
   c) Análisis de los diagrama de flujo de proceso, ☐
   d) Realización de pruebas de cumplimiento de las seguridades, ☐
   e) Revisión de procesos históricos (backups) ☐
   f) Otros (especifique)_____
   _____

10. ¿De qué manera determina el riesgo en la auditoria a lo sistemas de información computarizados?

_____
_____

11. ¿De las siguientes áreas cuales considera usted que son las más criticas en los sistemas?
    a) Seguridad física ☐
    b) Seguridad lógica ☐
    c) Mantenimiento ☐
    d) Operaciones de procesamiento ☐
    e) Otros; _____

12. . ¿Ha tenido dificultades para realizar la auditoria a los sistemas de información computarizados? Menciónelas.

_____

13. En la firma de auditoria en donde usted labora, ¿cuenta con lineamientos propios para realizar la planeación de auditoria?; ¿En qué consisten?

_____

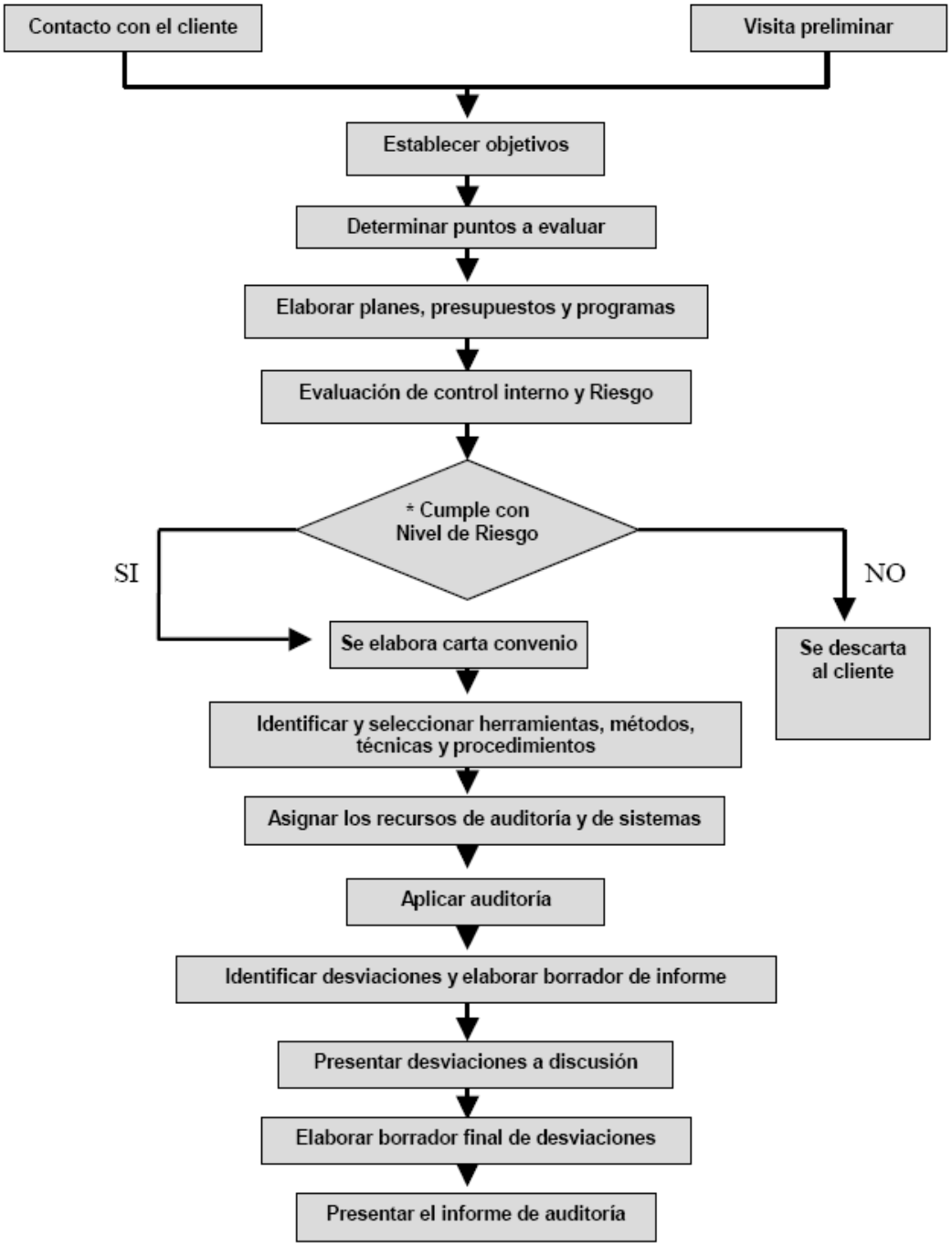
14. ¿Qué mecanismo considera que podría mejorar los procedimientos de auditoria?
    a) Modelo de auditoria de sistema ☐
    b) Lineamientos técnicos actualizados ☐
    c) Guía de procedimientos ☐
    d) Otros (especifique) _____

15. ¿Qué tipos de elementos debe contener una guía de lineamientos técnicos para el desarrollo de una auditoria?
    a) Formulación de Objetivos ☐
    b) Evaluación de Control Interno ☐
    c) Evaluación de riesgo ☐
    d) Procedimientos de auditoria ☐
    e) Papeles de trabajo. ☐
    f) Deficiencias de control interno. ☐
    g) Informe de auditoria.
    h) Otros; (especifique)_____

16. ¿Qué utilidad podría tener para usted la existencia de lineamientos técnicos actualizados para la planeación de auditoria de Sistemas de información computarizados?
    a) Mejora en los procedimientos ☐
    b) Facilidad en el desarrollo de la auditoria ☐
    c) Auditoria mas eficiente ☐

17. Usted utilizaría un documento que contenga lineamientos técnicos actualizados para elaborara la planeación de auditoria a los sistemas de información computarizados.
    a) Si ☐
    b) No ☐

Anexo 2: Flujograma del desarrollo de la auditoria de sistemas



Anexo 3: Esquema del proceso de planeación de auditoria de sistemas