UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"PROPUESTA DE UNA GUIA TECNICA EN EL ÁREA DE AUDITORIA DE SEGURIDAD INFORMÁTICA PARA VERIFICAR LA CONFIABILIDAD DE LA INFORMACION PROCESADA EN LOS SISTEMAS CONTABLES COMPUTARIZADOS"

TRABAJO DE INVESTIGACION PRESENTADO POR:

CARLOS MARIANO MORENO SALAMANCA

CARLOS ALBERTO PARADA BURUCA

ENRIQUE ALBERTO PEREZ RAMÍREZ

PARA OPTAR AL GRADO DE:

LICENCIADO EN CONTADURÍA PÚBLICA

SEPTIEMBRE 2005

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES UNIVERSITARIAS

Rector(a) : Dra. María Isabel Rodríguez

Secretaria General : Licda. Alicia Margarita Rivas de Recinos

Facultad de Ciencias Económica

Decano : Lic. Emilio Recinos Fuentes

Secretario(a) : Licda. Dilma Yolanda Vásquez de Del Cid

Docente Director : Lic. Héctor Alfredo Rivas Núñez

Coordinador de Seminario : Lic. Carlos Roberto Gómez Castaneda

Docente Observador : Lic. Álvaro Edgardo Calero Rodas

Septiembre de 2005

San Salvador El Salvador Centro América

DEDICATORIAS

Agradezco a **"DIOS"** todo poderoso porque siempre estuvo conmigo, a mi familia; especialmente a mi padre quien siempre me apoyo a mi madre, a mi hermana, a mi esposa y a mi hija que es un soplo de energía para seguir adelante. A mi asesor técnico que nos dio los lineamientos correctos para concluir nuestro trabajo de investigación. Y a mis compañeros de trabajo porque supimos seguir adelante.

Carlos Mariano Moreno Salamanca

Este triunfo académico se lo agradezco **"A DIOS TODO PODEROSO"** por permitirme haber logrado perseverar y culminar uno de mis más grandes retos; a mis padres, Carlos y Marta, quienes con su comprensión y acertada orientación me guiaron a lo largo de la carrera; a mis hermanos: Edgar Enrique y Claudia Judith, pues completaron el núcleo familiar más cercano a mi. Y a nuestro asesor: Lic. Héctor Alfredo Rivas Núñez por el empeño y disposición que mantuvo en el desarrollo de nuestro trabajo.

Carlos Alberto Parada Buruca

Gracias a **"Dios"** primeramente por regalarme vida e Iluminarme con sabiduría e inteligencia y permitirme haber logrado culminar uno de mis más grandes retos, a mis padres por haberme modelado con amor, sabiduría y apoyarme siempre, a mis hermanos por creer y confiar en mí, a mis compañeros por compartir buenos y difíciles momentos en el proceso de desarrollo del trabajo de graduación, a mis amigos por su aprecio, y en general, a todas las personas que de una u otra forma hicieron posible este sueño tan anhelado.

Enrique Alberto Pérez Ramírez

INDICE

RESUMEN

INTRODUCCIÓN

CAPITULO I

ASPECTOS GENERALES DE LA AUDITORIA DE SISTEMAS Y SEGURIDAD INFORMATICA

1. GENERALIDADES 1

1.1. ANTECEDENTES DE LA AUDITORIA DE SISTEMAS Y SEGURIDAD INFORMATICA 1

1.2. LA AUDITORIA DE SEGURIDAD INFORMATIVA 16

1.3. EVALUACION DE LA SEGURIDAD 19

1.4. EVALUACION DE RIESGOS EN UNA AUDITORIA DE SEGURIDAD INFORMATICA 21

1.5. HERRAMIENTAS Y TECNICAS PARA LA AUDITORIA DE SEGURIDAD INFORMATICA 24

1.6. LAS NORMAS INTERNACIONALES DE AUDITORIA (NIAS) EN EL AMBITO DE LA AUDITORIA INFORMATICA 31

1.6.1. ORIGEN Y EVOLUCION DE LAS NIA'S 31

1.6.2. RELACION DE LAS NIA'S CON LA AUDITORIA DE SISTEMAS 33

1.6.3. DIPAS 37

1.7. NORMAS GENERALES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN 59

1.7.1 NORMAS GENERALES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN 61

1.8. CONTROL INTERNO 66

1.8.1. DEFINICION 66

1.8.2. OBJETIVOS 67

1.8.3. AMBIENTE DE APLICACIÓN DEL CONTROL INTERNO 67

1.8.4. MEDIOS PARA LOGRAR EFECTIVIDAD DEL CONTROL INTERNO 68

1.8.5. TIPOS DE CONTROL 69

1.8.6. ENFOQUE CONTEMPORANEO DEL CONTROL INTERNO "INFORME COSO" 71

1.8.6.1. DEFINICIÓN 71

1.8.6.2. COMPONENTES 71

1.8.6.3. AMBIENTE DE CONTROL 71

1.8.6.4. EVALUACION DE RIESGO 72

1.8.6.5. ACTIVIDADES DE CONTROL 73

1.8.6.6. TIPOS DE CONTROL 74

CAPITULO II

DIAGNOSTICO SOBRE LA PROPUESTA DE UNA GUIA TECNICA EN EL ÁREA DE AUDITORIA DE SEGURIDAD INFORMÁTICA PARA VERIFICAR LA CONFIABILIDAD DE LA INFORMACION PROCESADA EN LOS SISTEMAS CONTABLES COMPUTARIZADOS

2. METODOLOGIA DE LA INVESTIGACION 76

2.1. TIPO DE INVESTIGACION 76

2.2. OBJETIVO DE LA INVESTIGACION 76

2.2.1. OBJETIVO GENERAL 76

2.2.2. OBJETIVOS ESPECIFICOS 76

2.3. POBLACION 77

2.4. MUESTRA 79

2.5 MÉTODOS E INSTRUMENTOS PARA RECOLECCION DE DATOS. 79

2.5.1. INVESTIGACIÓN BIBLIOGRÁFICA 79

2.5.2. INVESTIGACIÓN DE CAMPO 80

2.6 TABULACION DE DATOS 80

2.6.1. INTERPRETACIÓN DE LOS RESULTADOS 81

2.7. RESULTADOS DE LA INVESTIGACION 80

2.7.1. ANALISIS E INTERPRETACION DE LA INVESTIGACION DE CAMPO 81

2.8. DIAGNOSTICO DE LA INVESTIGACION 82

CAPITULO III

DISEÑO DE UNA GUÍA TÉCNICA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA VERIFICAR LA CONFIABILIDAD DE LA INFORMACIÓN PROCESADA EN LOS SISTEMAS CONTABLES COMPUTARIZADOS

3. GUÍA TÉCNICA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA VERIFICAR LA CONFIABILIDAD DE LA INFORMACIÓN PROCESADA EN LOS SISTEMAS CONTABLES COMPUTARIZADOS 87

3.1. DESCRIPCIÓN DE LA GUÍA 87

3.2. OBJETIVOS DE LA GUÍA 87

3.3. DESARROLLO DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA 88
3.3.1. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO 88
3.3.2. TÉRMINOS DE LOS TRABAJOS DE AUDITORÍA 118
3.3.3. PLANEACIÓN 119
3.3.3.1 PROCESOS A SEGUIR AL PLANIFICAR LA AUDITORÍA 120
3.3.4. EJECUCION 121
3.3.4.1 INSTRUMENTOS Y HERRAMIENTAS PARA LA AUDITORÍA 122
3.3.4.1.1. PROGRAMAS DE AUDITORÍA 122
3.3.4.1.2. CUESTIONARIOS 131
3.3.4.1.3. CHECKLIST 138
3.3.5. PAPELES DE TRABAJO 143
3.3.5.1. ARCHIVOS DE PAPELES DE TRABAJO 144
3.3.5.2 ÍNDICE DE REFERENCIACIÓN 144
3.3.5.3. MARCAS Y NOTAS DE AUDITORÍA 145
3.3.5.4 INFORME 145

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4. CONCLUSIONES Y RECOMENDACIONES 148
4.1 CONCLUSIONES 148
4.2 RECOMENDACIONES 149

GLOSARIO
BIBLIOGRAFÍA

ANEXOS

ANEXO N°1

TABULACION Y ANALISIS DE RESULTADOS

ANEXO N°2

ESQUEMA DEL PROCESO DE AUDITORÍA

ANEXO N°3

CÉDULA DE ANALISIS DE RIESGOS POR FACTORES Y ELEMENTOS

ANEXO N°4

HOJA DE PONDERACIÓN DE RIESGOS DE AUDITORÍA

ANEXO N°5

PRINCIPALES ACTIVIDADES AL EJECUTAR UNA AUDITORIA DE SISTEMAS.

ANEXO N°6

ARCHIVOS DE PAPELES DE TRABAJO.

ANEXO N°7

INDICES DE REFERENCIA.

ANEXO N°8

MARCAS Y NOTAS DE AUDITORÍA

ANEXO N°9

PROCEDIMIENTO PARA ELABORAR EL INFORME DE AUDITORÍA DE SISTEMAS COMPUTACIONALES.

RESUMEN EJECUTIVO

Es de considerar que la informática se ha extendido a todas las ramas de la sociedad en un crecimiento que permite seguir impulsando la investigación y actualización constante de la tecnología. Los sistemas informáticos se han convertido en las herramientas mas poderosas para materializar uno de los conceptos mas vitales y necesarios para cualquier organización empresarial las cuales se relacionan a los sistemas de información de la empresa, y que están orientados a la aplicación de controles, políticas y procedimientos que aseguran a los niveles mas altos de dirección que los recursos humanos, materiales y financieros estén protegidos adecuadamente, lo que satisfaga la obtención de la rentabilidad y competitividad del negocio.

El uso necesario de las computadoras para realizar tareas contables ha aumentado considerablemente, lo que obliga a obtener un conocimiento en detalle de los diversos sistemas de computación actuales y los distintos procedimientos aplicados a los niveles de control diseñados a cada entidad

Lo que resulta innegable es que la informática se convierte cada día en una herramienta permanente de los procesos principales que poseen los negocios.

Que es posible tenerlos si se implantan controles y esquemas de seguridad requeridos para su aprovechamiento.

Actualmente los contadores públicos carecen 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 lo que conlleve al desarrolla de la auditoria en forma eficiente, oportuna y profesional.

El objetivo principal de la guía técnica en el área de auditoria de seguridad informática es el de brindar al auditor una herramienta para verificar el nivel de confiabilidad de la información procesada en los sistemas contables computarizados.

El trabajo esta orientado a proporcionar una metodología especifica para que sirva de guía al profesional de la contaduría pública, a desarrollar en el área de auditoria informática una adecuada auditoria en cuanto a seguridad se refiere. Específicamente al manejo de la información financiera mediante sistemas computarizados, debido a que se manejan una gran cantidad de datos, y que permita obtener una mayor confiabilidad, oportunidad y eficiencias de la información procesada.

INTRODUCCIÓN

Habiendo realizado una investigación previa con los auditoras independientes que prestan servicios de Auditoria en Informática, se detectó la necesidad de una guía para verificar la confiabilidad de la información procesada en los sistemas contables computarizados, por lo anterior surge la necesidad de crear un documento que brinde lineamientos para la evaluación de la seguridad informática en forma sistemática y técnica cumpliendo con los requisitos normativos.

Es así como el presente trabajo está orientado a desarrollar una guía que proporcione al auditor independiente una herramienta para verificar la confiabilidad de la información procesada en los sistemas contables computarizados. Debido a que la alta dirección debe contar siempre con la certidumbre respecto de la integridad y disponibilidad de la información y los recursos de informática, es necesario formalizar un proceso de auditoria en informática en la organización.

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

Capitulo I Este comprende el desarrollo del marco teórico el cual contiene generalidades sobre la Auditoria en Informática que constituyen la base teórica del trabajo de investigación desarrollado y los conceptos concernientes al tema en estudio, los cuales serán aplicados en la ejecución y forman parte en el trabajo final; contiene la parte teórica referente a las bases para la evaluación de Seguridad Informática. Con la diversidad de conceptos incluidos en este capítulo el auditor independiente estará capacitado para abordar la parte operativa de informática, así como la administración de la misma sin importar su complejidad y la diversificación de servicios que presta a la empresa.

Capitulo II Presenta un panorama detallado de la metodología aplicada en el desarrollo de la investigación. Se determinan los objetivos en donde 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 Se presenta el desarrollo de una guía técnica que está diseñada para ser consultada por auditores independientes, la cual presenta las partes elementales para desarrollar una auditoria y evaluar la seguridad de los sistemas contables computarizados de donde emana la información financiera sujeta a revisión. 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 desde la óptica contable financiera.

Capítulo IV Se plantea 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.

CAPITULO I

ASPECTOS GENERALES DE LA AUDITORIA DE SISTEMAS Y SEGURIDAD INFORMATICA

1. GENERALIDADES

1.1. ANTECEDENTES DE LA AUDITORIA DE SISTEMAS Y SEGURIDAD INFORMATICA.

En los años cuarenta empezaron a darse resultados relevantes en el campo de la computación, con sistemas de apoyo para estrategias militares; posteriormente se incrementó el uso de las computadoras y sus aplicaciones y se diversificó el apoyo a otros sectores de la sociedad: educación, salud, industria, política, banca, aeronáutica, comercio, etc. En aquellos años la seguridad y control de ese medio se limitaba a dar custodia física a los equipos y a permitir el uso de los mismos a personal altamente calificado, ya que no existía gran número de usuarios, fueran estos técnicos o administrativos.

Esta rapidez en el crecimiento de la informática permite deducir que los beneficios se han incrementado con la misma velocidad, algunos con mediciones tangibles como reducción de costos e incremento porcentual de ventas y otros con aspectos intangibles como mejoría en la imagen o satisfacción del cliente, pero ambos con la misma importancia para seguir impulsando la investigación

y actualización constante de la tecnología. Con el paso de los años la informática y todos los elementos tecnológicos que la rodean han ido creando necesidades en cada sector social y se han vuelto un requerimiento permanente para el logro de soluciones.

Desde finales del siglo XX, los Sistemas Informáticos se han convertido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, la Informática hoy, está relacionada en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a las misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente a la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática. El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoría" como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas.

El concepto de auditoría es mucho más que esto. “Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.”

Según el autor Kell Ziegler auditoria se define como: "Un proceso sistemático para obtener y evaluar evidencia de una manera objetiva respecto de las afirmaciones concernientes a actos económicos y eventos para determinar el grado de correspondencia entre estas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados" En términos sencillos se concluye, que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo. Por otra parte los objetivos principales que constituyen a la auditoria en seguridad Informática son el control de la función informática, 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.

Auditoria de Sistemas Informáticos: Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones

ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas. [1] Los Sistemas Operativos engloban los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

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

[1] Benson, Chistopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft

El auditor debe conocer el número de “Tunning”, el cual consiste: En el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto así como sus resultados. Debe analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

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

La técnica de Sistemas se debe realizar mediante acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. El auditor de Base de Datos debería asegurarse de analizará los Sistemas de salvaguarda existentes, de igual forma revisará la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

La auditoria informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificultar las tareas fundamentales internas.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una auditoria en seguridad informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son tan empresas como una Sociedad Anónima o empresa Pública. Todos utilizan la informática para gestionar sus "negocios" de forma rápida y eficiente con el fin de obtener beneficios económicos y de costes. Por eso, al igual que los demás rubros de la empresa (Balances y Cuentas de Resultados, Tarifas, Sueldos, etc.), los Sistemas Informáticos están

sometidos al control correspondiente, o al menos debería estarlo. La importancia de llevar un control de esta herramienta se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoría Informática de Seguridad.[2]
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a aplicaciones independientes. En este caso interviene la Auditoría Informática de Datos.
- Un Sistema Informático mal diseñado puede convertirse en una herramienta peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modernización de la empresa está determinada por las computadoras que materializan los Sistemas de Información,

[2] Lucena López, Manuel José. Criptografía y Seguridad en Computadoras. Univ. De Jean. 3ª ed. España

la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

Estos se convierten en algunos de los inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la Auditoría de Seguridad en Sistemas.

Síntomas de Necesidad de una Auditoría de seguridad en Informática:

Las empresas acuden a las auditorias externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases: [3]

- Síntomas de descoordinación y desorganización:

  - No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.

  - Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

  - (Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante)

[3] Nombella, Juan José. Seguridad Informática. Editorial Paraninfo. España 2001

- Síntomas de mala imagen e insatisfacción de los usuarios:

  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, variación de los ficheros que deben ponerse diariamente a su disposición, etc.

  - No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

  - No se cumplen con los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

- Síntomas de debilidades económico-financiero:

  - Incremento desmesurado de costes.

  - Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).

  - Desviaciones Presupuestarias significativas.

- Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

- Síntomas de Inseguridad: Evaluación de nivel de riesgos

  - Seguridad Lógica

  - Seguridad Física

  - Confidencialidad (Los datos son propiedad inicialmente de la organización que los genera.)

  - Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia* Totales y Locales.

  - Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

*Planes de Contingencia:

Por ejemplo, la empresa sufre un corte total de energía, ¿Cómo se puede seguir operando en otro lugar? Lo que generalmente se pide es que se hagan Backups de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro afuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, es decir, si a la empresa principal le proveía teléfono (la empresa x), y a las oficinas paralelas, (la empresa Y). En este caso, si se produce la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas. Los Backups se pueden acumular durante dos meses, o el tiempo que estipule la empresa, y después se van reciclando.

Tipos y clases de Auditorias:

El departamento de Informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa. He aquí, la Auditoría Informática de Usuario. Se hace esta distinción para contraponerla a la informática interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una Auditoría Informática de Actividades Internas.

El control del funcionamiento del departamento de informática con el exterior, y con el usuario se realiza por medio de la Dirección. Su figura es importante, en cuanto es posible interpretar las necesidades de la Compañía. Una informática eficiente y eficaz requiere el apoyo continuado de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la Auditoría Informática de Dirección. Estas tres auditorias, mas la auditoría de Seguridad, son las cuatro Áreas Generales de la Auditoría Informática más importantes.

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos. Estas son las Áreas Especificas de la Auditoría Informática más importante.

Áreas Específicas	**Áreas Generales**			
	Interna	Dirección	Usuario	Seguridad
1- Explotación				
2- Desarrollo				
3- Sistemas				
4- Comunicaciones				
5- Seguridad				

Cada Área Especifica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.[4]

Objetivo fundamental de la auditoria de seguridad en informática:

Operatividad

La operatividad es una función que consistente básicamente en que la organización y las maquinas funcionen, siquiera mínimamente. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial. La operatividad de los Sistemas ha de constituir entonces la

[4] Ramos, Miguel Ángel. Auditoria de Seguridad. Universidad Carlos III de Madrid.España 2000

principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos

Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad.

Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados. Estos controles son importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de Software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del Software abonado. Puede ocurrir también con los productos de Software básico desarrollados por el personal de Sistemas Interno, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los

Centros de Proceso de Datos si no existen productos comunes y compatibles.

A continuación se mencionan algunas consideraciones que corresponden a una necesidad de realizar una Auditoria de Seguridad Informática:

- Todas las actividades de la sociedad buscan apoyarse de alguna forma en la tecnología de informática.
- Tanto los equipos de cómputo de diferentes marcas y capacidades como las bases de datos y los sistemas de información deben ser una solución integrada.
- La capacitación tiene que ser permanente en el uso de la tecnología de informática debido a su constante crecimiento y actualización.
- Hardware, software, telecomunicaciones y otros medios electrónicos han de estar interrelacionados para explotar al máximo sus capacidades y dar soluciones a todos los sectores de la sociedad.
- La gran penetración de la informática en todos los niveles del sector educativo así como en los sectores social y cultural.
- El control y seguridad sobre todos los recursos de informática es una necesidad.

- Se debe evaluar de manera formal y periódica la función de informática.
- El proceso de planeación de los negocios ha de integrar de manera permanente la función de informática. [5]

1.2. LA AUDITORIA DE SEGURIDAD INFORMATICA

La Auditoria de Seguridad Informática es uno de los tipos de auditoria que día con día esta tomando mucho mas fuerza, el surgimiento de esta auditoria se debe a la necesidad de evaluar los riesgos y el control interno del sistema de información computarizado ya que actualmente la tecnología ha tenido cambios extraordinarios y las empresas cada vez mas, intensifican el uso del computador para el procesamiento de la información.

Para poder desarrollar el proceso de una auditoria de seguridad informática es indispensable que el auditor tenga presente el objetivo y alcance de una auditoria y a la vez tener el conocimiento suficiente del sistema de información por computadora para poder evaluar el riesgo, y por lo cual deberá diseñar y desempeñar pruebas de control y procedimientos sustantivos apropiados en caso de necesitarse habilidades especializadas, el auditor buscara ayuda de un experto con conocimiento pleno en la materia.

[5] Ídem: [3]

Lo que resulta innegable es que la informática se convierte cada día en una herramienta permanente de los procesos principales de los negocios, en una fuerza estratégica, un aliado confiable y oportuno. Todo lo anterior es posible tenerlo en la empresa si se implantan controles y esquemas de seguridad requeridos para su aprovechamiento óptimo.

Se considera un trabajo novedoso por ser un área poco tratada en el ámbito nacional hasta la fecha la evaluación de la seguridad en la auditoria en informática, es tan importante como determinar los puntos débiles en el sistema y, por tanto, se ha de tener en cuenta en el alcance y extensión de los procedimientos que se van a aplicar en la auditoria.

Debido a que la alta dirección debe contar siempre con la certidumbre respecto de la integridad y disponibilidad de la información y los recursos de informática, es necesario formalizar un proceso de auditoria de seguridad informática en la organización. La orientación de dicha función es clara, eliminar o al menos minimizar en lo posible los riesgos y circunstancias dañinos.

Evaluación de la Seguridad Física:

Conocer si la empresa cuenta con la seguridad física necesaria para el resguardo del equipo de cómputo y su entorno; conocer

los controles existentes sobre la seguridad física del hardware, transmisión de datos, accesos físicos y seguridad en casos de emergencia.

Evaluación de Controles y Procedimientos:

Conocer la efectividad y eficacia de los controles y procedimientos aplicados para el resguardo del software y hardware; conocer los controles establecidos sobre el uso de programas y software, copia de respaldo, adquisición de paquetes y base de datos.

Evaluación de respaldo y recuperación:

Observar si los tipos de respaldo de la información aplicados por la empresa son efectivos, permitiendo en un momento determinado la recuperación de la información.

Evaluación del sistema de cómputo:

Conocer si el sistema contable cuenta con las características necesarias requeridas por la empresa en el procesamiento de datos.

Evaluación de Recursos Humanos:

Conocer la capacidad y eficiencia del personal del área, así como saber las necesidades existentes.

1.3. EVALUACION DE LA SEGURIDAD

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

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

fraudulentos. La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica:

-La seguridad física, se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

-La seguridad lógica, se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. [6]

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

[6] Rodríguez, Claudio. Seguridad Informática. Universidad de Concepción, facultad de Ingeniería. Chile mayo 1999.

Causas de realización de una Auditoría de Seguridad:

Esta constituye la fase inicial de la auditoría y el orden inicial de actividades de la misma. El auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad puede haber muchas causas:

- Reglas internas del cliente,
- Incrementos no previstos de costes,
- Obligaciones legales,
- Situación de ineficiencia global notoria, etc.

De esta manera el auditor conocerá el entorno inicial. y podrá elaborar un el Plan de Trabajo más adecuado.

1.4. EVALUACIÓN DE RIESGOS EN UNA AUDITORIA DE SEGURIDAD INFORMÁTICA.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

La seguridad informática se la puede dividir como Área General y como Área Especifica (seguridad de Explotación, seguridad de las

Aplicaciones, etc.). Así, se podrán efectuar auditorias de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorias de la Seguridad de un área informática determinada – Seguridad Especifica -.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocado, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.

- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Ejemplo:

Impacto	Amenaza				1: Improbable 2: Probable 3: Certeza 4:Despreciable
	Error	Incendio	Sabotaje	……..	
Destrucción de Hardware	-	1	1		
Borrado de Información	3	1	1		

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

1.5. HERRAMIENTAS Y TÉCNICAS PARA AUDITAR EL ÁREA DE SEGURIDAD DE LOS SISTEMAS

Cuestionarios:

Las auditorias de Seguridad informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias. Para esto, suele ser lo habitual comenzar solicitando la implementación de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables sobre las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de

modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

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

Entrevistas:

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. El auditor comienza a continuación las relaciones personales con el auditado realizándolo en tres posibles formas:

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

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

Listas de Chequeo o Checklist:

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

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria

o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

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

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la

función auditora se ejerce sobre bases de autoridad, prestigio y ética.

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

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

Trazas y/o Huellas:

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

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

Por lo que se refiere al análisis del Sistema, los auditores informáticos emplean productos que comprueban los valores asignados por Técnica de Sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante.

Software de Interrogación:

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de

generar programas para auditores escasamente cualificados desde el punto de vista informático. Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

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

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

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la Compañía. Efectivamente, conectados como terminales al "Host"(servidor), almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo

del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

1.6. LAS NORMAS INTERNACIONALES DE AUDITORIA (NIA'S) EN EL AMBITO DE LA AUDITORIA INFORMATICA

1.6.1. ORIGEN Y EVOLUCIÓN DE LAS NIA'S

Tal como se indica en el prefacio de las Normas Internacionales de Auditoria y Servicios relacionados (NIA's), la misión de la Federación Internacional de Contadores (IFAC) consiste en el desarrollo y enriquecimiento de una profesión contable que sea capaz de proporcionar servicios de una alta calidad para el interés publico, para lo cual establece el Comité Internacional de Practicas de Auditoria (IAPC), con el propósito de elaborar y emitir, a nombre del consejo, normas y declaraciones de auditoria y servicios relacionados. Con la emisión de dichas normas y declaraciones, el IAPC pretende mejorar el grado de uniformidad de las practicas de auditoria y servicios relacionados en todo el mundo. (NIA 100 párrafo 2) La aplicación de NIA's por parte de los profesionales en auditoria, se debe efectuar en aquellos estados financieros que estén preparados de

acuerdo con una o la combinación de: a) Normas Internacionales de Contabilidad (NIC); b) Normas Nacionales de Contabilidad (NCF en el caso de El Salvador); y c) Algún otro marco de referencia para informes financieros integral y con autoridad que haya sido diseñado para uso de informes financieros y que es identificado en los estados financieros. (NIA 120 párrafo 3). En El Salvador es una practica, aplicar para aquellas auditorias de estados financieros, las Normas y Procedimientos de Auditoria Generalmente Aceptadas (NAGA's), emitidas por el Comité Ejecutivo de Normas de Auditoria del Instituto Americano de Contadores Públicos.

(AICPA), y expedidas por el Comité de Auditoria de dicho instituto, habiendo sido adoptadas a partir de noviembre de 1972 a nivel internacional, y en El Salvador fueron adoptadas a partir se la I Convención Nacional de Contadores Públicos de El Salvador, la cual fue celebrada los días 4, 5 y 6 de abril de 1974, y en la IV Convención Nacional de Contadores de El Salvador, celebrada en San Salvador, los días 3,4 y 5 de julio de 1996, se analizaron nuevamente las NAGA's emitidas a esa fecha y se evaluaron las Declaraciones sobre Normas de

Auditoria (SAS) que no eran aplicables a El Salvador, y se adoptaron 72 SAS.[7]

Debido a la necesidad de aplicación de los estándares internacionales de auditoria y en base al acuerdo del Consejo de Vigilancia de la Contaduría Pública y Auditoría con fecha 10 de septiembre de 1999 se estableció que en la realización de auditorias a estados financieros, el auditor externo debe aplicar las Normas Internacionales de Auditoria dictadas por la Federación Internacional de Contadores (IFAC), ratificándose este pronunciamiento el 11 de diciembre de 2003, en el cual se afirmó la obligatoriedad de su aplicación.

1.6.2. RELACIÓN DE LAS NIA'S CON LAS AUDITORIA DE SISTEMAS

El uso creciente de la tecnología de la informática en la actividad económica ha dado lugar a un incremento sustancial en el número de puestos de trabajo informatizados. La Asociación de Auditoria y Control de Sistemas de Información ha determinado que la naturaleza especializada de las auditorias de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditoria requiere el desarrollo y la promulgación de normas generales para la auditoria de sistemas

[7] Melgar, O. Armando, Guardado Quintanilla, Glenda Azucena; Origen y evolución de la Contaduría Publica en El Salvador, Investigación 2001, Abril 2002.

de información. De acuerdo al IAPC, las NIA's aplicables a la auditoria de sistemas computacionales son las siguientes:

NIA 401- "Auditoria en un ambiente de sistemas de Información por computadoras"

El propósito de esta Norma Internacional de Auditoria es establecer normas y lineamientos sobre los procedimientos a seguir al realizar una auditoria de sistemas, sin embargo la NIA 401 y otras, han sido orientadas a la auditoria de estados financieros, pudiendo ser utilizada en una auditoria de sistemas mediante una adecuada adaptación por parte del auditor, el cual deberá de tener conocimientos suficientes del SIC (Sistema de Información Computarizado), al momento de plantear, dirigir, supervisar y revisar el trabajo que ha desarrollado.

Los recursos deben comprender también las habilidades con la que cuenta el grupo de trabajo de auditoria y el entrenamiento y experiencia que estos tengan considerando la disponibilidad del personal para la realización del trabajo de auditoria; y el entrenamiento y experiencia que estos tengan considerando la disponibilidad del personal para la realización del trabajo de auditoria; de no ser así, se necesitaría la ayuda de especialistas o profesionales que cuenten con las habilidades tomado en cuenta la asignación de recursos para el trabajo de auditoria en donde deberán considerarse las técnicas de

administración, desarrollando que deberá contener los pasos a seguir, para cada tarea y estimar de manera realista el tiempo, sin olvidar todas aquellas porciones de la auditoria que pueden ser afectadas por el ambiente del SIC al cliente.

Una planificación adecuada es sin duda alguna, uno de los primeros pasos necesarios para realizar una auditoria de sistemas eficaz, el auditor de sistemas debe comprender el ambiente del negocio en el que se ha de realizar la auditoria, así como los riesgos del negocio y el control asociado. La NIA en estudio establece que cuando el SIC es significativo el auditor deberá obtener una comprensión del ambiente del SIC, influyendo en la evaluación de los riesgos de auditoria que podemos definir como aquellos riesgos de que la información pueda tener errores materiales o que el auditor de sistemas no puede detectar un error que ha ocurrido.

De acuerdo con la NIA 400- "Evaluación del riesgo y control interno", el auditor deberá obtener una comprensión de los sistemas de contabilidad y de control interno, suficiente para planear la auditoria y desarrollar un enfoque de auditoria efectivo. El auditor deberá de usar juicio profesional para evaluar el riesgo de auditoria y diseñar los procedimientos de auditoria para asegurar que el riesgo se reduce a un nivel aceptable bajo.

"Riesgo de Auditoria" significa el riesgo de que el auditor de una opinión de auditoria inapropiada cuando los estados financieros están elaborados en forma errónea de una manera importante. El riesgo de auditoria tiene tres componentes:

"Riesgo Inherente", refleja la probabilidad de que pueda existir una pérdida material en alguna de las partes a auditar antes de que se considere la fiabilidad de los controles internos. En el caso de los sistemas contables computarizados tienen un alto riesgo inherente porque suelen tener un cierto grado de complejidad.

"Riesgo de Control", es el riesgo de que una representación errónea pudiera ocurrir en el saldo de cuenta o clase de transacción y que pudiera ser de importancia relativa individualmente o cuando se agrega con representaciones erróneas en otros saldos o clases que no han sido prevenidos, detectados y corregidos en su oportunidad por los sistemas de contabilidad y de control interno.

"Riesgo de Detección", es el riesgo de que los procedimientos sustantivos de un auditor no detecte una representación errónea que existe en un saldo de una cuenta o saldo de transacciones

que puede ser de importancia relativa individualmente o cuando se agrega con representaciones erróneas en otros saldos o clases. Tanto los riesgos como los controles introducidos como resultados dentro del SIC poseen un impacto potencial sobre la evaluación del auditor del riesgo y sobre la oportunidad y alcance de los procedimientos de la auditoria. La NIA hace mención que el surgimiento de nuevas tecnologías del SIC, por lo general son empleadas por los clientes para constituir sistemas computarizados cada vez mas complejos que puedan incluir enlaces, micro redes, bases de datos y sistemas de administración de negocios que alimentan información directa a los sistemas de contabilidad la cual tiende a incrementar el grado de complejidad en las diferentes operaciones que se deben realizar.

1.6.3 DIPAS

DIPA 1001- "Ambiente de SIC – Microcomputadoras Independientes"

El propósito de esta DIPA, es describir los sistemas de microcomputadoras que son usados como estación de trabajo, los efectos de esta en los sistemas de contabilidad, controles internos y los procedimientos de auditoria. Las microcomputadoras son herramientas comunes en todas las áreas, las cuales son usadas con el propósito de procesar transacciones

contables y poder proporcionar al final informes que serán utilizados para la preparación de los estados financieros; para poder realizar estas acciones deberán obtener los programas. Una microcomputadora debe ser concebida como parte de un sistema de información, la cual consta de cinco partes: Personas, procedimientos, software, hardware, y datos. Las microcomputadoras establecen enlaces a computadoras centrales y pueden usarse como parte de los sistemas, estas pueden actuar también como una terminal inteligente a causa de su lógica, transmisión almacenaje y capacidades básicas de computo.

Al referirse al software del sistema operativo, los programas de aplicación y datos deberán ser almacenados ya sean estos por medio de disquete, cartuchos y discos duros removibles los cuales están sujetos a borrarse, a daños físicos a perdidas o robos debido a sus tamaños pequeños ya que son portátiles para todos aquellos usuarios no autorizados. Por lo general el ambiente SIC, en el que se usan microcomputadoras es menos estructurado que en un ambiente SIC controlado en forma central. La operación de las microcomputadoras, dependerá de la administración la cual es la encargada de hacerla efectiva estableciendo y ejecutando políticas para un mejor control y un adecuado uso de estas. A esto agregaremos los efectos de las microcomputadoras en el sistema de contabilidad y los riesgos

asociados a los cuales dependerán del grado o el uso de la microcomputadora, para el procedimiento de aplicaciones contables, el tipo e importancia de las transacciones financieras que están siendo procesadas y desde luego la naturaleza de los archivos y programas utilizados en todas las aplicaciones. Es necesario mencionar algunas de las funciones que los usuarios desempeñan en un ambiente de microcomputadoras:

- Iniciar y autorizar documentos fuentes,
- Alimentar datos a los sistemas.
- Operar la computadora,
- Cambiar programas y archivos de datos,
- Usar o distribuir datos de salida y
- Modificar los sistemas operativos.

Mientras que en un ambiente de SIC, dichas funciones se segregaran normalmente por medio de controles generales de SIC apropiados, donde esta falla de segregación de funciones en un ambiente de microcomputadoras, pueden permitir que queden errores sin detectar y permitir que se cometa u oculte el fraude. Es necesario mencionar que dentro de un ambiente de microcomputadoras puede no ser factible para la administración implementar suficientes controles para reducir al mínimo los riesgos de errores no detectados. Así como el auditor puede a menudo a sumir que el riesgo de control es alto en dichos sistemas dichos riesgos son considerados en la NIA 400 y 401.

De acuerdo a esta situación el auditor deberá encontrar una forma más efectiva para una comprensión del ambiente de control y del flujo de transacciones, concentrar todos los esfuerzos de auditoria en pruebas sustantivas.

Los siguientes ejemplos de procedimientos de control son para que el auditor pueda considerar apoyarse en los controles internos de contabilidad, relacionados con Microcomputadoras independientes:

a. Segregación de obligaciones y controles de contrapartidas.
b. Sucesos a la microcomputadoras y sus archivos.
c. Uso de software de terceras partes.

DIPA 1002 "Ambiente de SIC — Sistemas de computadoras en línea"

El propósito de esta declaración es ayudar al auditor a implementar la NIA 400 "Evaluación del Riesgo y Control Interno" y la DIPA 1008 "Evaluación del Riesgo y Control interno - Características y Consideraciones de SIC", la cual describe los efectos de una computadora de sistemas en línea sobre el sistema de contabilidad y controles internos relacionados y sobre los procedimientos de auditoria. Cuando se hace mención de los sistemas de computadoras en línea, se dice que son aquellos que posibilitan a los usuarios el acceso a datos y programas directamente a través de aparatos terminales y que son conocidos corno sistemas de computadoras en línea, dichos sistemas pueden

estar basados en computadoras mainframen, mini computadoras o microcomputadoras estructuradas en un ambiente de red.

Las microcomputadoras también conocidas como computadoras de medio rango, son máquinas del tamaño de un escritorio, ocupan un lugar intermedio entre las microcomputadoras y las macrocomputadoras en cuanto a su velocidad para procesar y capacidad de almacenamiento de datos. Las pequeñas empresas suelen utilizar mini computadoras para sus necesidades generales de procesamiento de datos tales como contabilidad. Muchos tipos de aparatos terminales pueden usarse en los sistemas de computadoras en línea, las funciones desempeñadas por estos aparatos terminales varían ampliamente dependiendo de su lógica, transmisión, almacenamiento y capacidades básicas de computación.

Los sistemas de computadoras en línea pueden clasificarse de acuerdo a como se alimenta la información al sistema, como se procesa y cuando están disponibles los resultados para el usuario.

Las funciones de los sistemas de computadora en línea, se clasifican como:

- Procesamiento en línea/tiempo real.
- Procesamiento en línea/por lote.

- Actualización en línea / Memorandum
- Investigación en línea.
- Procesamiento de descarga/carga en línea.

La entrada y validación de los datos en línea, del acceso en línea a los sistemas por parte de los usuarios a la posible falta de un rastreo visible de la transacción y al acceso potencial del programador al sistema forma parte de las características más importantes en los sistemas de computadoras en línea, pues se encuentran diseñados de tal forma que este no facilite documentos de soporte para aquellas transacciones que deberán ser alimentadas al sistema. Uno de los párrafos de la declaración enfatiza que los programadores pueden tener un fácil acceso en línea al sistema lo que permitirá que estos desarrollen programas nuevos y a la vez sean modificados dependiendo de los requerimientos que posean los sistemas.

Dentro de un ambiente de SIC de Sistemas de Computadoras en Línea, no se puede olvidar el control interno donde son muchos los controles del SIC y de suma importancia para el procesamiento en línea. Esta declaración hace énfasis en los efectos de las microcomputadoras las cuales fueron mencionadas en su oportunidad encontrándose dentro del estudio de la DIPA 1002 — "Los Efectos de un Sistema de Computadora en Línea", sobre el sistema de contabilidad y los riesgos internos

relacionados que dependerán de:

- El grado al cual el sistema en línea está siendo usado para procesar aplicaciones contables.
- El tipo e importancia de las transacciones financieras que se procesan.
- La naturaleza de los archivos y programas utilizados en las aplicaciones.

La determinación preliminar durante el proceso de evaluación de riesgo del impacto del sistema sobre los procedimientos de auditoria generalmente en un sistema de computadora en línea bien diseñada y controlado, es probable que el auditor ponga mayor confianza en los controles internos en el sistema al determinar la naturaleza oportunidad y alcance de los procedimientos de auditoria.

Los procedimientos de auditoria llevados acabo concurrentemente con el procesamiento en línea pueden incluir pruebas de cumplimiento de los controles sobre aplicaciones en línea.

Después que el procesamiento ha tenido lugar los procedimientos deberán incluir:

-Pruebas de cumplimiento de los controles sobre las transacciones registradas por el sistema en línea para autorización, integridad y exactitud.

-Pruebas sustantivas de las transacciones y resultados del procesamiento en vez de pruebas de controles, donde las

primeras pueden ser más efectivas en costos o donde el sistema no está bien diseñado o controlado.

DIPA 1003 - "Ambiente de SIC — Sistemas de base de datos"

El propósito de esta declaración es ayudar al auditor a implementar la NIA 400 "Evaluación del Riesgo y del Control Interno", y la declaración internacional de auditoria 1008 "Características y consideraciones del SIC" por medio de la descripción de los sistemas de bases de datos. La declaración describe los efectos de un sistema de base de datos sobre el sistema de contabilidad y controles internos relacionados y sobre los procedimientos de auditoria.

Partiendo del concepto que una base de datos es una colección de datos que se comparten y se usan entre un número de diferentes usuarios para diferentes fines partiendo de que cada usuario puede no necesariamente estar enterado de todos los datos almacenados en la base de datos o de las maneras en que los datos pueden ser usados para múltiples fines.

Es de suma importancia mencionar que los sistemas de bases de datos comprenden dos componentes importantes:

- La base de datos.
- El sistema de administración de la base de datos.

Los sistemas de bases de datos se distinguen por dos importantes características que son:

- Datos compartidos e Independencia de Datos.

Una base de datos compartida está compuesta de datos que se instalan con relaciones definidas y se organizan de tal manera que permita a muchos usuarios usar los datos en diferentes programas de aplicación. En los sistemas que no son bases de datos se mantienen archivos de datos separados para cada aplicación y los datos similares que se usan en varias aplicaciones pueden estar repetidos en varios archivos diferentes. Las tareas de administración de la base de datos pueden también desempeñarse por individuos que no son parte de un grupo centralizado de administración de base de datos. Donde las tareas de administración de la base de datos no son centralizadas sino que están distribuidas en entidades organizacionales existentes, las diferentes tareas necesitarán aun ser coordinadas.

En algunas aplicaciones, pueden usarse más de una base de datos. En esta circunstancia, las tareas del grupo de administración de la base de datos necesitarán asegurarse que:

- Exista el enlazamiento adecuado entre la base de datos;
- Se mantenga la coordinación de funciones;
- Los datos contenidos en las diferentes bases de datos sean

consistentes.

- Control interno en un ambiente de base de datos.

Generalmente, el control interno en un ambiente de base de datos requiere controles efectivos sobre la base de datos, el SABS y las aplicaciones, la efectividad de los controles internos depende en un gran grado de la naturaleza de las tareas de administración de la base de datos.

Debido a los datos compartidos, a la independencia de los datos y otras características del sistema de bases de datos, los controles generales del SIC, normalmente tienen mayor influencia que los controles de aplicación del SIC sobre los sistemas de bases de datos. Los controles generales del SIC sobre la base de datos, el SABS y las actividades de la función de administración de la base de datos, tienen un efecto profundo sobre el procesamiento de las aplicaciones. Los controles generales del SIC de importancia particular en un ambiente de base de datos pueden clasificarse en los siguientes grupos:

- Enfoque estándar para el desarrollo y mantenimiento de programas de aplicación.
- Propiedad de los datos;
- Acceso a la base de datos; y
- Segregación de funciones.

- El efecto de la base de datos sobre el sistema de contabilidad y controles relacionados.

El efecto en un sistema de base de datos sobre los sistemas de contabilidad y los riesgos asociados generalmente dependerán de:

- El grado al cual las bases de datos se usen para las aplicaciones contables.
- El tipo e importancia de las transacciones financieras que se procesen.
- La naturaleza de la base de datos, el SABS (incluye el diccionario de datos), las tareas de administración de las bases de datos y las aplicaciones.
- Los controles generales del SIC que son particularmente importantes en un ambiente de bases de datos.

Los sistemas de bases de datos típicamente dan la oportunidad de mayor confiabilidad en los datos, que los sistemas que no son base de datos. Estos pueden dar como resultado un riesgo reducido de fraude o error en el sistema de contabilidad donde se usen base de datos. Los siguientes factores, combinados con controles adecuados, contribuyen a una mayor confiabilidad en los datos. Se logra mejorar consistencia de los datos por que estos son registrados y actualizados solo una vez, mejor en los sistemas que no son de base de datos, donde los mismos datos se almacenan en varios archivos y son actualizados en diferentes momentos y por diferentes programas.

La integridad de los datos se mejora con los usos efectivos de los recursos incluidos en el SABS, corno recuperación rutina de reinicio, rutinas generalizadas de edición y validación y características de seguridad de control. Otras funciones disponibles con el SABS pueden facilitar los procedimientos de control y de auditoria. Estas funciones incluyen generadores de informes, que pueden ser usadas para crear reportes de compensación, y lenguajes de consultas de dudas, que Pueden usarse para identificar inconsistencias en los datos.

Efectos de la base de datos sobre los procedimientos de auditoria. Los procedimientos de auditoria en un ambiente de base de datos serán afectados principalmente, por el grado al cual los datos en la base de datos sean usados por el sistema de contabilidad. Cuando aplicaciones contables de importancia usan una base de datos común, el auditor puede encontrar un costeo efectivo en utilizar algunos de los procedimientos.

Para obtener una comprensión del ambiente de control de base de datos y del flujo de transacciones, el auditor puede considerar el efecto de lo siguiente sobre el riesgo de auditoria al planear la auditoria:

- El SABS y las aplicaciones importantes que usan las bases de datos.
- Los estándares y procedimientos para desarrollo y mantenimiento de los programas de aplicación que usan la

base de datos.

- La función y administración de la base de datos.
- Descripciones de puestos, estándares y procedimientos para los individuos responsables del soporte técnico, diseño, administración y operación de la base de datos.
- Los procedimientos usados para asegurar la integridad y seguridad y que este completamente la información financiera contenida en la base de datos.
- La disponibilidad de los recursos para auditoria dentro del SAVBS.

DIPA 1008 - "Evaluación del riesgo y el control interno — Características y consideraciones de SIC"

Un entorno de sistema de información de cómputo (SIC) se define en la norma internacional de auditoria (NIA) 401 "Auditoria en un Entorno de Sistema de Información por Computadora".Para fines de las normas internacionales de auditoria, existe un entorno de GIS cuando hay implicada una computadora de cualquier tipo o tamaño en el procesamiento por parte de la entidad, de información financiera de importancia para la auditoria, ya sea que la computadora sea operada por la entidad o por un tercero.

Estructura organizacional

En un entorno de SIC, una entidad establecerá una estructura organizacional y procesamientos para administrar las actividades

de SIC. Las características de una estructura organizacional de SIC incluyen:

- Concentración de funciones ~ conocimientos.
- Concentración de programas y datos.

Naturaleza del procesamiento

El uso de computadoras puede dar como resultado el diseño de sistemas que proporcionen menos evidencia que aquellos que usen procedimientos manuales. Además, estos sistemas pueden ser accesibles a un mayor número de personas.

Las características del sistema que pueden ser resultado de la naturaleza del procesamiento SIC, incluyen:

- Ausencia de documentos de entrada.
- Falta de rastros visibles de transacciones.
- Falta de datos de salidas visibles.
- Facilidad de acceso a datos y programas de computadora.

Controles generales de SIC

El propósito de los controles generales de SIC es establecer un marco de referencia de control global sobre las actividades de SIC y proporcionar un nivel razonable de certeza de que se logren los objetivos globales del control interno.

Los controles generales de SIC pueden incluir:

a. Controles de administración y organización; diseñados para establecer un marco de referencia organizacional sobre las actividades de SIC, incluyendo:
   - Políticas y procedimientos relativos a funciones de control.
   - Segregación apropiada de funciones incompatibles.

b. Desarrollo de sistemas de aplicación y controles de mantenimiento, diseñado para proporcionar certeza razonable que los sistemas se desarrollan y mantienen de manera eficiente y autorizada. También están diseñados típicamente para establecer control:
   - Pruebas, conversión, implementación y documentación de sistemas nuevos o revisados.
   - Cambios a sistemas de aplicación.
   - Acceso a documentación de sistemas.
   - Adquisición de sistemas con aplicación de terceros.

c. Controles de operación de computadoras, diseñados para controlar la operación de los sistemas y proporcionar certeza razonable que:
   - Los sistemas son usados para propósitos autorizados únicamente.

- El acceso a las operaciones de la computadora es restringido a personal autorizado.
- Solo se usan programas autorizados.
- Los errores de procesamientos son detectados y corregidos.

d. Controles de software de sistemas, diseñados para proporcionar razonable certeza de que el software del sistema se adquiere o desarrolla de manera autorizada y eficiente, incluyendo:
    - Autorización, aprobación, pruebas, implementación de documentación de software de sistemas nuevos y modificaciones de software de sistemas.
    - Restricción de acceso al software y documentación de sistemas al personal autorizado.

e. Controles de entradas de datos y de programas, diseñados para proporcionar razonable certeza de que:

    - Hay establecida una estructura de organización sobre las transacciones que se alimentan al sistema
    - El acceso a los datos y programas están restringidos al personal autorizado.

DIPA 1009 — "Técnicas de auditoria con ayuda de computadora"

El propósito de esta norma es proporcionar lineamientos en el uso de TAACs Técnicas de Auditoria con Ayuda de Computadoras, aplicables a todos los usos de TAACs que impliquen una computadora de cualquier tipo o tamaño. El alcance de una auditoria no cambia cuando una auditoria se conduce en un entorno de SIC de acuerdo a la (NIA 401) "Auditoria en un Entorno de Sistemas de información por Computadoras". Donde la aplicación de procedimientos de auditoria puede requerir que el auditor considere técnicas que usen las computadoras.

De acuerdo a la NIA 401 enfatiza algunos de los usos de TAACs como los siguientes:

La ausencia de documentos de entrada o la falta de un rastro visible de auditoria pueden requerir el uso de TAACs en la aplicación de procedimientos sustantivos y de cumplimiento.
La efectividad y eficiencia de los procedimientos de auditoria pueden ser mejoradas mediante el uso de TAACs. Descripción de Técnicas de Auditoria con Ayuda de Computadora (TAACs).
Dentro de esta norma se describe los dos tipos más comunes de TAACs, siendo estos:

Software de Auditoria

Consiste en programas de computadora usados por el auditor como parte de sus procedimientos de auditoria para procesar datos de

importancia de auditoria del sistema de contabilidad de la entidad. Pueden consistir en programas de paquete, programas escritos para un propósito, programas de utilería. Independientemente de la fuente de los programas, el auditor deberá verificar su validez para fines de auditoria antes de su uso.

Datos de pruebas

Las técnicas y datos de prueba se usan para conducir procedimientos de auditoria alimentando datos, al sistema de computadora de una entidad, y comparando los resultados obtenidos con resultados predeterminados.

Uso de TAACs

Pueden ser usados para realizar diversos procedimientos de auditoria incluyendo:

- Pruebas de detalles de transacciones y saldos.
- Procedimientos de revisión analítica.
- Pruebas de cumplimiento de controles generales de SIC.
- Pruebas de cumplimiento de control de aplicación de SIC.

Consideraciones en el uso de TAACs

Al planear la auditoria el auditor deberá considerar una combinación apropiada de técnicas de auditoria manuales y con ayuda de computadora. Al determinar si se usan TAACs. Los factores a considerar incluyen:

Conocimiento, pericia y experiencia del auditor en computadoras

La DIPA "Auditoria en un entorno de Sistemas de Información por Computadora" trata del nivel de habilidades y competencia que el auditor deberá tener cuando conduzca una auditoria en un entorno de SIC y da lineamientos para cuando se delega el trabajo a asistentes con habilidades de SIC, o cuando se usa el trabajo por otros auditores o expertos con dichas habilidades.

Disponibilidad de TAACs e instalaciones adecuadas de computación

El auditor deberá considerar la disponibilidad de TAACs, instalaciones adecuadas de computación. El auditor puede planear usar otras instalaciones de computación cuando el uso de TAACs en la computadora de la entidad no es económico o no es factible.

No factibilidad de pruebas manuales

Muchos sistemas de contabilidad computarizados realizan tareas para las que no hay evidencia visible disponible y, en estas circunstancias, puede no ser factible para el auditor realizar pruebas en forma manual. La falta de evidencia visible puede ocurrir en diferentes etapas del proceso contable.

Efectividad y eficiencia

La efectividad y eficiencia de los procedimientos de auditoria puede mejorarse mediante el uso de TAACs al obtener y evaluar evidencia de auditoria.

El uso de TAACs puede ser más eficiente los procedimientos sustantivos adicionales que apoyarse en los controles y en los relativos procedimientos de cumplimiento.

Los asuntos que se refieren a eficiencia que pueden necesitar ser considerados para el auditor incluyen:

- El tiempo para planear, diseñar, ejecutar y evaluar TAACs.
- Revisión técnica y horas de asistencia.
- Diseño e impresión de formas.
- Tecleo y verificación de datos de entrada.
- Tiempo de computadora.

Oportunidad

Ciertos archivos de computadora, como los archivos de transacciones detalladas a menudo se conservan por solo un tiempo corto y pueden no estar disponibles en forma legible por la máquina cuando el auditor lo requiere. Así el auditor necesitara hacer arreglos para la conservación de datos que él requiera o pueda hacer alterar la programación de su trabajo que requiera de estos datos. Cuando el tiempo disponible para llevar a cabo una auditoria es limitado, el auditor puede planear usar una TAAC por satisfacer sus requerimientos de tiempo mejor que otros procedimientos.

Documentación

El estándar de papeles de trabajo y de procedimientos de retención para una TAAC deberá ser consistente con el de la auditoria. Puede ser conveniente mantener los técnicos que se refieren al uso de la TAC separados de otros papeles de trabajo de la auditoria. Los papeles de trabajo deberán contener suficiente documentación para describir la aplicación de la TAAC, tal como:

a) Planeación

- Objetivos de la TAAC.
- TAAC específica que se va a usar.
- Controles que se van a ejercer.
- Personal, tiempo y costo.

b) Ejecución

- Preparación de la TAAC y procedimiento de pruebas y controles.
- Detalle de las pruebas ejecutadas por la TAAC.
- Detalle de datos de entrada, procesamiento y datos de salidas.
- Información técnica relevante sobre el sistema de contabilidad de la entidad, tal como compaginación de archivos de computadora.

c) Evidencia de Auditoria

- Datos de salida proporcionados.
- Descripción de trabajo de auditoria realizado en los datos de salida.
- Conclusiones de auditoria.

d) Otros

Recomendaciones a la administración de la entidad.

Otras NIA's y DIPA's que deben ser consideradas por el auditor en una auditoria de sistemas son las siguientes:

- NIA 220 "Control de calidad para el trabajo de auditoria".
- NIA 230 "Documentación"
- NIA 240 "Fraude y error"
- NIA's 300/399 "Planeación"
- NIA 400 "Evaluación de riesgos y control interno".
- NIA 402 "Consideraciones de auditoria relativas a entidades que utilizan organizaciones de servicios".
- NIA 500/599 "Evidencia de auditoria"
- NIA's 600/699 "Uso del trabajo de otros"
- NIA 910 "Trabajos para revisar estados financieros"
- DIPA 1005 "Consideraciones especiales en la auditoria de entidades pequeñas".
- DIPA 1007 "Comunicaciones con la administración.

1.7. NORMAS GENERALES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Dichas normas han sido propuestas por ISACA (Information Systems Audit and Control Foundation) Es la asociación líder en Auditoría de Sistemas, con 23.000 miembros en 100 países alrededor del mundo. La naturaleza especial de la Auditoría de Sistemas de Información, y las capacidades necesarias para la realización de dichas auditorías, requieren estándares de aplicación específica a la auditoría de sistemas. Uno de los objetivos de la Asociación de Auditoría y Control de Sistemas de Información (ADACSI), miembro de ISACA, es avanzar en la generación de estándares globalmente aplicables que satisfagan esta necesidad. El desarrollo y distribución de estándares es la piedra angular de la contribución profesional que realiza ISACA a la comunidad de auditores.

Objetivos:

El objetivo de los Estándares de Auditoría de Sistemas de ISACA es informar:

A los auditores de sistemas el mínimo nivel aceptado para resolver las responsabilidades profesionales precisadas en el código de ética profesional de ISACA para auditores de sistemas de información. A las gerencias y otras partes interesadas sobre

las expectativas de la profesión concernientes a quienes la practican.

El objetivo de las Guías de Auditoría de Sistemas es proveer información sobre el cómo cumplir con los estándares de la Auditoría de Sistemas.

Alcance y Autoridad de los Estándares de Auditoría de Sistemas

El esquema de estándares de Auditoría de Sistemas de ISACA provee múltiples niveles de estándares:

Estándares: Definen los requerimientos obligatorios para la auditoría de sistemas y la generación de informes.

Guías: Proveen una guía para la aplicación de los estándares de Auditoría de Sistemas. El Auditor de Sistemas debería tenerlos en consideración al implementar los estándares, usar su criterio profesional para aplicarlos y estar preparado para justificar cualquier diferencia.

Procedimientos: Provee ejemplos de procedimientos que el Auditor de Sistemas puede utilizar en una revisión. Los procedimientos ofrecen información de cómo cumplir con los estándares al realizar una auditoría de sistemas pero no especifican requerimientos.

A continuación se presentan las normas generales para auditar los sistemas de información:

1.7.1. NORMAS GENERALES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

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

Introducción: La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

La auditoria de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Las normas promulgadas por la Asociación de Auditoria y Control de Sistemas de Información son aplicables al trabajo de auditoria realizado por miembros de la Asociación de Auditoria y Control de Sistemas de Información y por las personas que han

recibido la designación de Auditor Certificado de Sistemas de Información.

Objetivos: Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

010 Título de auditoría

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

020 Independencia

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

- 020.020 Relación organizativa: La función de auditoria de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoria.

030 Ética y normas profesionales

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

- 030.020 Atención profesional correspondiente: En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional. 040 Idoneidad

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

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

050 Planificación

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

060 Ejecución del trabajo de auditoría

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

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

070 Informes

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

080 Actividades de seguimiento

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

Fecha de vigencia: 25 de julio de 1997, Publicado en: 2004-06-09 (607 Lecturas)

1.8. CONTROL INTERNO

1.8.1. DEFINICIÓN

El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y confiabilidad de su información financiera, promover eficiencia operacional y provocar adherencia a las políticas prescritas por la administración. Una definición mas completa del control interno es: "El control contable comprende el plan de organización y los procedimientos y registros relacionados con la salvaguarda de activos y la confiabilidad de los registros financieros y, consecuentemente, el diseño de éstos para proveer una razonable seguridad de que las transacciones son ejecutadas de acuerdo con autorizaciones generales o específicas por parte de la administración.

Que las transacciones son registradas atendiendo la necesidad de permitir la preparación de estados financieros de conformidad con principios de contabilidades generalmente aceptadas o cualquier otro criterio aplicable a tales estados y mantener la Contabilización de activos.

- Que el acceso a los activos sólo sea permitido de acuerdo con autorización general o específica de la administración.
- Que los registros contables de los activos sean comparados, por períodos razonables con los activos existentes y que se

tomen acciones apropiadas con respecto a cualquier diferencia" [8]

1.8.2. OBJETIVOS

Son objetivos del control interno:

- Promover la eficiencia en las operaciones y la capacitación y uso de los recursos.
- Mejorar la utilidad, oportunidad, confiabilidad y razonabilidad de la información que se genera sobre el manejo de los recursos.
- Optimizar los procedimientos para que todo ejecutivo logre informar oportunamente acerca de los resultados de su gestión dentro de la organización.
- Mejorar la capacidad administrativa para impedir, identificar y comprobar el manejo inadecuado de los recursos.

1.8.3. AMBIENTE DE APLICACIÓN DEL CONTROL INTERNO

La función del control interno debe diseñar e implementarse en la empresa en forma sistematizada, y que se le dote de los elementos necesarios para su funcionamiento, de tal forma que sus resultados sean óptimos. Uno de los elementos más

[8] Boletín E-02 de la Comisión de Normas y Procedimientos de Auditoria del Instituto Mexicano de Contadores Públicos

importantes para el buen funcionamiento del control interno es el ambiente dentro del cual será implementado. Las características del ambiente que más influye en el funcionamiento del control interno son:

- Estructura organizacional.
- Naturaleza de los procesos.
- Diseño y aspectos relativos a los procesos.

1.8.4. MEDIOS PARA LOGRAR EFECTIVIDAD DEL CONTROL INTERNO

Cada empresa posee diferentes condiciones de operación de acuerdo a su naturaleza magnitud y localización. No es posible prefabricar un sistema estándar de control interno que llene las necesidades de todas ellas. Existe, sin embargo, ciertos factores que puedan ser considerados como esenciales para lograr una función de control interno satisfactoria para la mayoría de las organizaciones de gran tamaño, estos son un plan de organización y su función será de proporcionar una separación de responsabilidades apropiadas y funcionales. Más explícitamente, se refiere a la definición de la estructura organizacional de la empresa en la cual se define la relación jerárquica entre los diferentes puestos y las responsabilidades inherentes a cada uno de ellos de tal forma que no existe dualidad de mando ni de operaciones.

Un sistema de autorización y registro: su objetivo será el promover un control financiero y administrativo sobre los recursos, obligaciones, ingresos y gastos. Este incluye técnicas presupuéstales de costos, un catalogo e instructivo de cuentas, manuales de procedimientos y graficas descriptivas del flujo de transacciones.

Un conjunto de normas a las cuales deberán ceñirse cada una de las unidades y miembros de la organización.

El grado de idoneidad del personal que deberá ser proporcional a las responsabilidades del puesto que desempeña.

1.8.5. TIPOS DE CONTROL

Los controles internos pueden ser clasificados a través de diferentes criterios. El criterio mas general es el de clasificarlos de acuerdo al área de la empresa en que estos son aplicados. Se pueden mencionar tres tipos básicos:

Controles contables: Son aquellos diseñados para ser aplicados en el departamento de contabilidad y tienen como función asegurar los activos de la empresa, asegurar la exactitud y veracidad de la información contable. Algunos controles contables son:

- Manual de procedimientos contables.
- Separaciones de responsabilidades en el departamento de contabilidad.
- Sistemas de vaucher.
- Diseño de formato.
- Programas de retención de documentos.
- Controles por lotes.

Controles administrativos: Tienen por objetivo incrementar y asegurar la eficiencia operacional de la empresa, algunos de estos controles son:

- Definición de las amortizaciones generales y específicas de las transacciones.
- Políticas de precios.
- Control de calidad.
- Control de mando de la empresa.

Controles internos varios: Son aquellos cuya área de aplicación no la construyen departamentos definidos, sino más bien se aplican a toda la empresa. Entre estos se pueden mencionar:

- Políticas de personal.
- Comité de auditoria.
- Procedimientos generales de la empresa.

1.8.6. ENFOQUE CONTEMPORANEO DEL CONTROL INTERNO "INFORME COSO"

1.8.6.1. DEFINICIÓN.

Es un proceso, ejecutado por el directorio, la gerencia y otro personal de la entidad, diseñado para proveer un aseguramiento razonable en relación al logro de los objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de los reportes financieros
- Cumplimiento con las leyes y regulaciones aplicables.

1.8.6.2. COMPONENTES:

El sistema de control interno consiste en cinco componentes interrelacionados:

(1) Ambiente de control,

(2) Evaluación de riesgos,

(3) Actividades de control,

(4) Información y comunicación, y

(5) Monitoreo.

1.8.6.3. AMBIENTE DE CONTROL

El ambiente de control consiste en el establecimiento de un entorno que estimule e influencie la actividad del personal con respecto al control de sus actividades. El mismo abarca factores tales como filosofía y estilo operativo de la gerencia, políticas y prácticas de recursos humanos, la integridad y valores éticos de los empleados, la estructura organizacional, y la atención y dirección del directorio. El informe COSO brinda una guía para evaluar cada uno de estos factores. Por ejemplo, la filosofía gerencial y el estilo operativo pueden ser evaluados examinando la naturaleza de los riesgos del negocio que acepta la gerencia, la frecuencia de su interacción con los subordinados, y su actitud hacia los informes financieros.

1.8.6.4. EVALUACIÓN DE RIESGOS.

Consiste en la identificación y análisis de riesgos relevantes para el logro de los objetivos y la base para determinar la forma en que tales riesgos deben ser manejados.

La identificación del riesgo incluye examinar factores externos tales como los desarrollos tecnológicos, la competencia y los cambios económicos, y factores internos tales como calidad del personal, la naturaleza de las actividades de la entidad, y las características de procesamiento del sistema de información. El análisis de riesgo involucra estimar la significación del

riesgo, evaluar la probabilidad de que ocurra y considerar cómo administrarlo.

1.8.6.5 ACTIVIDADES DE CONTROL.

Son aquellas que realiza la gerencia y demás personal de la organización para cumplir diariamente con las actividades asignadas. Estas actividades están expresadas en las políticas y procedimientos.

Las actividades de control incluyen revisiones del sistema de control, los controles físicos, la segregación de tareas y los controles de los sistemas de información.

Las actividades de control son políticas y procedimientos que se desarrollan a través de toda la organización y garantizan que las directrices de la gerencia se lleven a cabo y los riesgos se administren de manera que se cumpla los objetivos.

Incluyen actividades preventivas, detectivas y correctivas tales como:

- Aprobaciones y autorizaciones
- Análisis de registro de información
- Reconciliaciones
- Verificaciones
- Segregación de funciones
- Revisión de desempeños operacionales
- Salvaguarda de activos
- Seguridades físicas
- Indicadores de desempeño
- Revisiones de informes de actividades y desempeño
- Fianzas y seguros
- Controles sobre procesamiento de información

Las actividades de control son importantes no solo porque en si implican la forma correcta de hacer las cosas, sino debido a que son el medio idóneo de asegurar en mayor grado el logro de los objetivos.

1.8.6.6 TIPOS DE CONTROL

Básicamente existen tres diferentes tipos de control: detectivos, preventivos y correctivos, los cuales tienen propósitos y características especificas para cada uno de ellos, según se observa en el siguiente cuadro:

Detectivos		Preventivos		Correctivos	
PROPOSITO	**CARACTERÍSTICAS**	**PROPOSITO**	**CARACTERÍSTICAS**	**PROPOSITO**	**CARACTERÍSTICAS**
Diseñado para detectar hechos Indeseables. Detectan la manifestación ocurrencia de un hecho.	Detiene el proceso o aíslan las causas del riesgo o las registran Ejerce una función de Vigilancia Actúan cuando se evaden los controles preventivos No evitan las causas, las personas involucradas. Consientes y obvios mide efectividad de Controles preventivos Más costosos- pueden Implicar correcciones	Diseñado para prevenir resultados indeseables Reducen la posibilidad de que se detecte	Están incorporados en los procesos de forma imperceptible Guías que evitan que exista las causas, hechos imprevistos Impedimento a que algo suceda mal Más barato evita costo de correcciones	Diseñado para corregir efectos de un hecho indeseable Corrigen las causas del riesgo que se detectan	Es el complemento del Control detectivo al originar una acción luego de la alarma Corrigen la evasión o falta de lo preventivo ayuda a la investigación y corrección de causas Permite que la alarma se escuche y se remedie el problema Mucho mas costoso Implican correcciones y reprocesos.

CAPITULO II

METODOLOGIA Y DIAGNOSTICO DE LA INVESTIGACION

2. METODOLOGIA DE LA INVESTIGACION

2.1 TIPO DE INVESTIGACION

La investigación desarrollada fue de tipo descriptiva y analítica debido a que primero se seleccionaron las características fundamentales del objeto de la investigación y la descripción detalladas de sus partes, para posteriormente presentar una solución del problema. El trabajo se realizo estructurando una investigación de campo apoyada en otra de tipo documental.

2.2 OBJETIVOS DE LA INVESTIGACION

2.2.1 OBJETIVO GENERAL

Proporcionar una guía técnica enmarcada en la Auditoria de Seguridad Informática, que cuente con los lineamientos necesarios para comprobar el nivel de confiabilidad de la información procesada en los sistemas contables computarizados.

2.2.2 OBJETIVOS ESPECIFICOS

Desarrollar programas, procedimientos y manuales, entre otras herramientas y técnicas en cuanto a las áreas:

- Área de Seguridad Física, referente al resguardo del equipo de cómputo y su entorno; conocer los controles existentes

sobre la seguridad del hardware, transmisión de datos, accesos físicos y seguridad en casos de emergencia.

- Área de Controles y Procedimientos, en cuanto a la verificación de la efectividad y eficacia de los controles y procedimientos aplicados para el resguardo del software y hardware, así como los controles establecidos sobre el uso de programas y software, copia de respaldo, adquisición de paquetes y base de datos.
- Área de Respaldo y Recuperación, dentro de la cual se establece si los tipos de respaldo de la información aplicados por la empresa son efectivos, permitiendo en un momento determinado la recuperación de la información.
- Área del Sistema de Cómputo, se verifica si el sistema contable cuenta con las características necesarias requeridas por la empresa en el procesamiento de datos
- Área de Recursos Humanos, define la capacidad y eficiencia del personal del área, así como saber las necesidades existentes.

2.3 POBLACION

Según datos proporcionados por el diario oficial N° 42 tomo 362 de fecha 2 de marzo de 2004, el total de auditores independientes inscritos en el Consejo de Vigilancia de la Contaduría Pública y Auditoria de El Salvador (2,813)

2.4 MUESTRA

La muestra poblacional examinada fue de 80 Auditores Independientes, obtenida por medio de la fórmula siguiente:

$$n = \frac{Z^2 . P . Q . N .}{(N-1)E^2 + Z^2 . P . Q .}$$

En la cual:

n = Muestra a obtenerse al sustituir valores y efectuar las operaciones respectivas.

Z = Valor crítico que corresponde a un coeficiente de confianza del 90%, donde Z es 1.96, de acuerdo al área bajo la curva normal.

P = Probabilidad de Éxito (70 %)

Q = Probabilidad de Fracaso (30 %)

N = Total de auditores independientes inscritos en el Consejo de Vigilancia de la Contaduría Publica y Auditoria de El Salvador (2,813)

E = Error muestral (0.07%)

Sustituyendo Valores en fórmula:

$$n = \frac{(1.96)^2 \ (0.70) \ (0.30) \ (2813)}{(2813 -1)(0.07)^2 + (1.96)^2(0.7)(0.3)}$$

Desarrollando el resultado, se obtiene:

n = 80 Auditores Independientes.

2.5 MÉTODOS E INSTRUMENTOS PARA RECOLECCION DE DATOS.

2.5.1. INVESTIGACIÓN BIBLIOGRÁFICA

La técnica documental sirvió para conocer los aspectos generales y específicos del tema, basados en los conocimientos y experiencias relacionadas a la Auditoria en Informática; los datos recolectados a través de esta técnica son el punto inicial de la investigación y es determinante para completar el trabajo de campo. Lectura o investigación documental de libros, revistas, tesis, diccionarios y literatura que tenga relación con los diferentes tipos de Herramientas relacionadas con la Evaluación de la Seguridad en Informática, especialmente aquellos que se refieran a la evaluación del riesgo y control en la Auditoria en informática y sistemas de información.

Sobre la base de esta fuente de información se pudo ampliar los conocimientos, conceptos y otros aspectos que tienen relación con el tema a desarrollar, a fin de concretizar resultados positivos.

2.5.2. INVESTIGACIÓN DE CAMPO

La investigación bibliográfica se complementó con la investigación de campo, para determinar la aplicación de la Auditoria en Informática, la investigación se efectuó por medio de un cuestionario para los auditores independientes sujetos de estudio. Siendo esta la forma tradicional mas utilizada en la recolección de dato, en la cual cada pregunta fue contestada por el sujeto investigado. El instrumento principal utilizado en la recolección de la información, fue el cuestionario, el cual estuvo estructurado en preguntas tanto abiertas, cerradas y de selección múltiple, que se relacionaron con los aspectos generales de la auditoria en informática y su relación con la seguridad, utilizando en este un lenguaje claro y sencillo, que permitió alcanzar los objetivos planteados.

2.6. TABULACION DE DATOS

La información obtenida de cada cuestionario, se tabuló agrupando la cantidad de respuestas por cada pregunta tanto en el caso de las respuestas abiertas, cerradas y de selección múltiple, obteniendo de esa manera las frecuencias en términos absolutos y luego convirtiéndolas en términos relativos (porcentajes), posteriormente se elaboró un cuadro para cada una de ellas.

2.6.1. INTERPRETACIÓN DE LOS RESULTADOS

Una vez tabuladas las respuestas en sus cuadros correspondientes, se desarrolla la interpretación de las frecuencias absolutas y relativas establecidas por cada pregunta, considerando adicionalmente los comentarios expresados por los auditores independientes, sobre los cuales se llevó a cabo la investigación. (Ver anexo No.1)

2.7. RESULTADOS DE LA INVESTIGACION

2.7.1. ANALISIS E INTERPRETACION DE LA INVESTIGACION DE CAMPO

De una población total de 2,813 auditores independientes inscritos en el Consejo de Vigilancia de la Contaduría Publica y Auditoria de El Salvador, la muestra poblacional estimada fue de 80 unidades (M = 80); Considerando que la cantidad de preguntas incluidas en el cuestionario no era extensa, la clasificación y la tabulación de datos se efectuó en forma manual. A continuación se presenta cada uno de los cuadros con sus preguntas, análisis e interpretación respectivos:

2.8. DIAGNOSTICO DE LA INVESTIGACION

Nivel de demanda y participación en auditorias informáticas.

En lo que se refiere a principales servicios que los clientes demandan de los auditores independientes, se obtuvo que los más significativos son Auditaría Financiera con 54% en promedio, Auditoria Fiscal con 26%, servicios contables con 19% en promedio y la Auditoria en Informática con 1% en promedio, constituyéndose los primeros tres servicios en los más importantes, ya que suman el 99% del total y significan los ejes principales del quehacer de los auditores independientes. Muy distantes de los servicios anteriores se coloca la Auditoria en Informática con el 1% en promedio del total. Los resultados son razonables respecto a los servicios tradicionales que brindan los auditores independientes pequeños, sin embargo, es necesario incorporar otros servicios que estén acordes a las exigencias de la época entre los que destaca la Auditoria en Informática.

Por otra parte el 53 % de los encuestados consideraron que la Auditoria en Informática presenta un nivel de poca demanda y el 6 %, manifiestan que el este servicio no presenta ningún nivel de demanda. Lo anterior evidencia que la auditoria en informática en el presente no ha tenido mayor demanda, pero la importancia de ésta radica en que con los avances tecnológicos de la época, los sistemas mecanizados cada vez van adquiriendo un mayor nivel de participación en el quehacer de las empresas,

por lo que es imprescindible que los auditores independientes tengan como parte de su oferta de servicios la realización de auditorias informáticas, lo que les daría la posibilidad de mejorar la calidad y prestación de sus servicios.

En cuanto a la participación en el desarrollo de una Auditoria en Informática, por parte de los auditores independientes el 61% de de la muestra manifestó que no ha tenido la oportunidad de participar en una auditoria informática y el 39% del total contestaron afirmativamente, por lo que se denota que ha existido un cierto nivel de participación en este tipo de auditoria. Dentro de los auditores independientes que no han tenido la oportunidad de participar en una auditoria informática, un 58% opina que el motivo de no haber realizado alguna vez dentro de su campo profesional una auditoria informática es a causa de que la demanda de este tipo de servicio es mínimo, mientras que un 24% manifiesta que la causal principal de no haber efectuado es te tipo de auditoria es por falta de conocimiento y la capacitación suficiente del auditor, con lo cual se demuestra que existe un conocimiento insuficiente para llevar a cabo este tipo de auditoria.

Experiencia adquirida en una auditoria informática.

Los auditores independientes que han participado en una auditoria informática, consideran un 32% de estos, que la

experiencia adquirida al realizar dicha auditoria es media, en segundo lugar un 26% manifiesta no haber obtenido ningún tipo de experiencia, por lo que efectuar una auditoria informática no es suficiente como para adquirir todos los conocimientos básicos que demanda este tipo de auditoria, por lo que es necesario buscar otros elementos didácticos bibliográficos que sirvan de herramientas, así como también la participación en eventos nacionales y regionales de la profesión que se desarrollan y que les permita obtener una actualización continua de conocimientos para ofertar este tipo de servicios.

En la realización de una Auditoria en Informática los auditores independientes toman como diferencias más significativas respecto al resto de auditorias la especialización de las pruebas que se deben de efectuar en una auditoria informática con un 18%, la naturaleza de las operaciones con un 14%, y un 12% a la naturaleza de las evidencias obtenidas.

Importancia de la realización de una auditoria informática.

La importancia que conlleva realizar una auditoria de sistemas en una empresa que procesa su información financiera mediante un sistema contable computarizado es de vital importancia, por lo cual casi el cien por ciento (97%) de los auditores independientes manifiesta que es una necesidad imperante realizar una auditoria de los sistemas contables computarizados.

El principal factor que influye para que la información procesada en los sistemas contables computarizados sea lo suficientemente confiable depende, según los encuestados de que el recurso humano tenga la experiencia y capacidad necesaria en el manejo de los sistemas (31%). Otra variante que es de vital importancia para obtener información confiable lo constituye el conjunto de controles adecuados encaminados a minimizar riesgos en la seguridad física y lógica de los sistemas contables computarizados y su entorno (28%). Finalmente en tercer factor para lograr una información confiable depende, según encuestados, de la calidad de software y hardware utilizado (22%).

La auditoria de seguridad informática.

Dentro de la auditoria informática, se debe evaluar la seguridad de los sistemas, y uno de los principales motivos por los cuales es necesaria la evaluación de la seguridad de los sistemas contables computarizados, es con el fin principal de detectar las deficiencias de los sistemas contables (71%), para que posteriormente se puedan subsanar dichas deficiencias, con el objetivo de que la información generada por los sistemas sea íntegra, confiable y oportuna (26%).

La Auditoria de Seguridad Informática contribuye a determinar el grado de confiabilidad de la información procesada en un sistema

contable computarizado, según lo manifiesta el 100% de auditores independientes encuestados, ya que mediante ésta se pueden detectar deficiencias en los sistemas contables computarizados en cuanto a los niveles de seguridad lógica y física, lo cual constituye una pauta para determinar si la información financiera ha sido procesada a través de mecanismos que tengan por objetivo conservar su integridad, para que ésta cumpla finalmente con las características de íntegra, confiable y oportuna.

El total de los encuestados (100%) considera que sería de utilidad la propuesta de creación de una guía que facilite la evaluación de la Seguridad Informática en cuanto a la información procesada en los sistemas contables computarizados como mecanismo de consulta para auditores que efectúen una auditoria informática.

CAPITULO III

PROPUESTA DE UNA GUÍA TÉCNICA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA VERIFICAR LA CONFIABILIDAD DE LA INFORMACIÓN PROCESADA EN LOS SISTEMAS CONTABLES COMPUTARIZADOS

3. GUÍA TÉCNICA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA VERIFICAR LA CONFIABILIDAD DE LA INFORMACIÓN PROCESADA EN LOS SISTEMAS CONTABLES COMPUTARIZADOS

3.1. DESCRIPCIÓN DE LA GUÍA

Esta guía está diseñada para ser consultada por auditores independientes con las partes elementales para desarrollar la auditoría y evaluación de la seguridad de los sistemas contables computarizados de donde emana la información financiera sujeta a revisión. Por lo tanto es, 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 desde la óptica contable financiera.

3.2. OBJETIVOS DE LA GUÍA

- Dar cumplimiento a la normativa técnica que exigen las normas internacionales de auditoría, en una auditoría de estados financieros en un ambiente de sistema de información computarizado.
- Que los auditores independientes hagan uso de ésta guía de aplicación, que posee los elementos esenciales y específicos para desarrollar una auditoría de estados financieros, en un ambiente de sistema de información computarizado.

- Ser una herramienta que minimiza los riesgos existentes en una auditoría de estados financieros, en un ambiente de sistema de información computarizado

3.3 DESARROLLO DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA.

3.3.1. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO

De acuerdo con NIAS para la "Evaluación del riesgo y control interno" el auditor debería considerar el ambiente de sistema de información computarizada al diseñar los procedimientos de auditoría para reducir el riesgo de auditoría a un nivel aceptablemente bajo. Al obtener una comprensión del sistema de información de contabilidad del cliente y las actividades del control relacionadas, generalmente los auditores encuentran útil dividir el sistema global en sus ciclos de transacciones más importantes. El término ciclo de transacciones se refiere a las políticas y las secuencias de procedimientos para procesar un tipo particular de transacciones. Si los datos de contabilidad se procesan manualmente o por computadora, los objetivos específicos de la auditoría no cambian, sin embargo los métodos de aplicación de procedimiento de auditoría para reunir evidencia pueden ser influenciados por los métodos de procesamiento por computadora.

El auditor puede usar procedimientos de auditoria manuales, técnicas de auditoría con ayuda de computadora, o una combinación de ambos para obtener suficiente material de evidencia. En algunos sistemas de contabilidad que se usa una computadora para procesar aplicaciones significativas, puede ser difícil o imposible para el auditor obtener ciertos datos para inspección, investigación, o confirmación.

A la vez que se obtiene una comprensión de los componentes del control interno (el ambiente de control, la evaluación del riesgo, actividades de control, el sistema de información contable y, de comunicación y monitoreo), los auditores generalmente obtienen conocimiento sobre las actividades del cliente. Tiene que comprenderse los controles y roles de cada componente del sistema de control interno. Dentro de la estructura organizativa de la compañía sujeta a la auditoría, se deberá observar:

a) Control interno sobre el análisis, desarrollo e implementación de sistemas.
   - Estandarización de metodología para el desarrollo de proyectos.
   - Asegurar que el beneficio de los sistemas sea óptimo.
   - Elaborar estudios de factibilidad del sistema.
   - Garantizar la eficiencia y eficacia en el análisis y diseño de sistemas.

- Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema.
- Optimizar el uso del sistema por medio de su documentación.

b) Controles internos sobre la operación del sistema:
   - Prevenir y corregir los errores de operación.
   - Prevenir y evitar la manipulación fraude de la información.
   - Implementar y mantener la seguridad en la operación.
   - Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la institución.

c) Controles internos sobre los procedimientos de entradas de datos, el procesamiento de la información y la emisión de los resultados:
   - Verificar la existencia y funcionamiento de los procedimientos de capturas de datos.
   - Comprobar que todos los datos sean debidamente procesados.
   - Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
   - Comparar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información.

d) Controles internos sobre la seguridad del área de sistemas:

- Controles para prevenir y evitar las amenazas, riesgos y contingencias que inciden en las áreas de sistematización.
- Controles sobre la seguridad física del área de sistemas.
- Controles sobre la seguridad lógica de los sistemas.
- Controles sobre la seguridad de las bases de datos.
- Controles sobre la operación de los sistemas computacionales.
- Controles sobre la seguridad del personal de informática.
- Controles sobre la seguridad de telecomunicación de datos.
- Controles sobre la seguridad de redes y sistemas multiusuarios.

METODOLOGÍA

La primera metodología es conocida como la Ponderación

Es una técnica especial de evaluación, mediante la cual se procura darle un peso específico a cada una de las partes que serán evaluadas; su objetivo es tratar de compensar el valor que se le asigne a las actividades o tópicos que tienen poca importancia en la evaluación, en relación con los que tienen mayor importancia.

Permite equilibrar las posibles descompensaciones que existen entre las áreas o sistemas computacionales que tienen mayor peso e importancia y las áreas o sistemas que tienen poco peso e importancia en la evaluación, respetando en cada caso el peso e importancias representativas que tienen para el sistema computacional o para todo centro de cómputo.

Ejemplo gráfico de una evaluación de sistemas.

Cuadro 1

Columna 1	**Columna 2**	**Columna 3**
Factores primarios que serán ponderados	**Peso por factor**	**Valor % específico**
Evaluación de la gestión informática del centro de cómputo		**100 %**
1. Objetivos del centro de cómputo **(cuadro 2)**	10%	
2. Estructura de organización	10%	
3. Funciones y actividades	15%	
4. Sistemas de información	20%	
5. Personal y usuarios	15%	
6. Documentación de los sistemas	2%	
7. Actividades y operación del sistema	14%	
8. Configuración del sistema	4%	
9. Instalaciones del centro de cómputo	10%	
Peso total de la ponderación	**100 %**	

Primer paso:

En la columna 1 se anotan las áreas o aspectos de sistemas que serán evaluados, y en la columna 2 se establece un peso porcentual específico para cada factor; el auditor establece ese peso según su juicio profesional.

En éste primer paso se eligen los factores más importantes que se van a evaluar (los de mayor jerarquía o los que pueden ser representativos de un grupo o sector), a fin de darle a cada uno de esos factores un valor porcentual (peso específico), el cual representará la importancia de ese factor en la evaluación. La suma total de los factores primarios siempre debe ser 100% (columna 3).

Cuadro 2

Columna 1	**Columna 2**	**Columna 3**	**Columna 4**
Actividades que van a ser evaluadas y ponderadas	**Peso por Actividad**	**Peso por factor ponderado**	**Valor de ponderación**
1. Objetivos del centro de cómputo			**10.0 %**
Establecimiento del objetivo general	25%	2.5%	
Cumplimiento del objetivo general	30%	3.0%	
Difusión del objetivo general	20%	2.0%	
Derivación de objetivos secundarios	15%	1.5%	
Seguimiento y control de objetivos	10%	1.0%	
Total del factor a ponderar	**100 %**	**10.0 %**	

Segundo paso:

A cada uno de los factores elegidos como primarios se le designan actividades específicas que contribuyan a su evaluación total; en el ejemplo (cuadro2), al factor primario 1 (Objetivos del centro de cómputo) se le agregan las actividades que pueden ayudar a evaluarlo (columna 1). De la misma manera, a cada una de las actividades señaladas se le da un peso específico (porcentual), el cual representará la importancia que tiene esa actividad dentro del factor primario (columna 2). El total de

esas actividades también deben sumar 100%, pero sólo dentro del grupo al cual pertenecen. (**Objetivos del centro de cómputo**)

También se le asignaran valores específicos (columna 2) a cada una de las actividades del factor primario indicado como número 1, el cual tiene un valor específico de 10% (columna 4).

Además, estos porcentajes se pueden hacer comparativos y asignar a cada actividad un peso ponderado (columna 3), el cual es el valor porcentual que la representa, en relación con el peso específico del factor primario. En éste caso, ya que al factor primario se le asignó el valor de 10%, entonces cada uno de sus componentes representará un peso ponderado.

Siguiendo el mismo ejemplo tenemos lo siguiente: a la difusión del objetivo general se le asignó 20% y esto representa un valor ponderado de 2% (columna 3) en relación con el valor total de ese punto (columna 4). Tomando en cuenta los factores primarios indicados en el primer paso. Notemos que la suma de las actividades de cada factor siempre resultará 100% (columna 2) y que el valor ponderado (columna 3) representará el valor total de cada punto (columna 4). Los valores porcentuales que presentamos aquí son arbitrarios, elegidos por preferencia y sólo como un ejemplo. En la práctica, el auditor responsable de la auditoría deberá asignar tanto los factores primarios que va a evaluar, como el valor que le asignará a cada factor. Además,

también debe elegir las actividades y asignarles el valor que represente para cada uno de esos factores primarios.

Cuadro 3

Columna 1	Columna 2	Columna 3	Columna 4
Actividades que van a ser evaluadas y ponderadas	**Peso por Actividad**	**Peso por factor ponderado**	**Valor de ponderación**
1. Objetivos del centro de cómputo			**10.0%**
Establecimiento del objetivo general	25%	2.50%	
Cumplimiento del objetivo general	30%	3.00%	
Difusión del objetivo general	20%	2.00%	
Derivación de objetivos secundarios	15%	1.50%	
Seguimiento y control de objetivos	10%	1.00%	
Total del factor a ponderar	**100%**	**10.00%**	
2. Estructura de organización			**10.0%**
Definición de estructura de organización	25%	2.50%	
Definición de funciones	25%	2.50%	
Descripción de puestos	20%	2.00%	
Definición de canales de comunicación	10%	1.00%	
Definición de niveles de autoridad	10%	1.00%	
Actualización de estructuras y puestos	5%	0.50%	
Evaluación periódica de funciones	5%	0.50%	
Total del factor a ponderar	**100%**	**10.00%**	
3. Funciones y actividades			**15.0%**
Definición de funciones	20%	3.00%	
Cumplimiento de las funciones	30%	4.50%	
Manuales e instructivos	10%	1.50%	
Métodos y procedimientos	15%	2.25%	
Cumplimiento de actividades	20%	3.00%	
Seguimiento de actividades	5%	0.75%	
Total del factor a ponderar	**100%**	**15.00%**	
Columna 1	**Columna 2**	**Columna 3**	**Columna 4**
Actividades que van a ser evaluadas y ponderadas	**Peso por Actividad**	**Peso por factor ponderado**	**Valor de ponderación**
4. Sistemas de información			**20%**
Definición del sistema (software)	30%	6.00%	

Definición del equipo (hardware)	30%	6.00%	
Definición de instalaciones	15%	3.00%	
Evaluación de adquisiciones	10%	2.00%	
Interrelación de funciones	15%	3.00%	
Total del factor a ponderar	**100%**	**20.00%**	
5. Personal y usuarios			**15%**
Manejo del sistema	25%	3.75%	
Aprovechamiento del sistema	15%	2.25%	
Oportunidad en la información	10%	1.50%	
Asesoría interna a usuarios y personal	15%	2.25%	
Asesoría externa a personal del área	15%	2.25%	
Capacitación y desarrollo del personal	10%	1.50%	
Administración de prestaciones	10%	1.50%	
Total del factor a ponderar	**100%**	**15.00%**	
6. Documentación de los sistemas			**2%**
Manual de usuarios	30%	0.60%	
Manual técnico del sistema	40%	0.80%	
Manuales de capacitación	20%	0.40%	
Actualización de manuales	10%	0.20%	
Total del factor a ponderar	**100%**	**2.00%**	
7. Actividades y operación del sistema			**14%**
Definición del equipo (hardware)	30%	4.20%	
Definición de instalaciones	30%	4.20%	
Evaluación de adquisiciones	20%	2.80%	
Interrelación de funciones	20%	2.80%	
Total del factor a ponderar	**100%**	**14.00%**	
8. Configuración del sistema			**4%**
Definición del equipo (hardware)	25%	1.00%	
Definición del equipo (software)	25%	1.00%	
Adaptación de instalaciones	15%	0.60%	
Adaptación del medio ambiente	15%	0.60%	
Planes contra contingencias	20%	0.80%	
Total del factor a ponderar	**100%**	**4.00%**	

Columna 1	Columna 2	Columna 3	Columna 4
Actividades que van a ser evaluadas y ponderadas	**Peso por Actividad**	**Peso por factor ponderado**	**Valor de ponderación**

9. Instalaciones del centro de cómputo			**10%**
Adaptación de instalaciones	30%	3.00%	
Adaptación de medidas de seguridad	30%	3.00%	
Adaptación del medio ambiente	10%	1.00%	
Adaptación de las comunicaciones	20%	2.00%	
Mantenimiento del sistema	10%	1.00%	
Total del factor a ponderar	**100%**	**10.00%**	
Total del factor a ponderar			**100%**

En el punto número 6, Documentación de los sistemas, el valor ponderado del factor es 2.0% y los valores para cada una de sus actividades son: 30%, 40%, 20% y 10%, lo cual nos da un total de 100% (columna 2); mientras que el porcentaje del valor ponderado del factor es: 0.6%, 0.8%, 0.4% y 0.2%, respectivamente (columna 3). Para el cálculo se aplica una regla de tres simple: si 2 es igual a 100%, ¿cuánto representará 30%? Se aplica la fórmula: (2.0 * 0.30)/100 = 0.60, lo cual equivale a 0.6% del valor total de éste factor.

Tercer paso:

Se aplica ésta guía de evaluación y se registran calificaciones adjudicadas para cada una de las actividades propuestas (columna 5). Después, con esos resultados se obtienen los puntos alcanzados para cada actividad y para el total por cada factor primario (columna 6). Esto permite comparar los resultados con los valores establecidos inicialmente para cada actividad y emitir un juicio sobre el cumplimiento.

Veamos el ejemplo del cuadro 4 para el punto 6, Documentación de los sistemas.

Cuadro 4

Columna 1	Columna 2	Columna 3	Columna 4	Columna 5	Columna 6
Actividades que van a ser evaluadas y ponderadas	**Peso por actividad**	**Peso por ponderar**	**Valor de ponderación**	**Calificación**	**Porcentaje de puntos obtenidos**
6. Documentación de los sistemas			**2.0%**		
Manual de usuarios	30%	0.60%		0.60	0.36%
Manual técnico del sistema	40%	0.80%		0.85	0.68%
Manuales de capacitación	20%	0.40%		1.00	0.40%
Actualización de manuales	10%	0.20%		0.85	0.17%
Total del factor a ponderar	**100%**	**2.00%**		**0.825**	**1.61%**

Como podemos observar en el cuadro 4, el auditor asigna una calificación a cada actividad (columna 5), y con ella emite un criterio (cualitativo o cuantitativo) para evaluar el grado de cumplimiento de dicha actividad. Este es un valor numérico, el cual representa la calificación que el auditor le otorga a cada uno de esos puntos de acuerdo con su desempeño. El total del factor a ponderar, se calcula sumando los valores y el resultado se divide entre el número de líneas.

El auditor debe establecer el criterio para evaluar el cumplimiento de cada uno de los puntos de ésta guía de ponderación, según las herramientas, técnicas y demás procedimientos de auditoría que utilice. El valor más alto se otorga cuando no existen fallas o cuando el punto evaluado no

cumple totalmente con lo establecido, y entre menos cumpla, más desciende. Después de asentar esas calificaciones, el auditor hace el cálculo del porcentaje de puntos obtenidos por cada actividad (columna 6), el cual será el resultado de multiplicar el valor de peso ponderado (columna 3) por la calificación obtenida (columna 5). El resultado, en decimales, es el valor porcentual del grado de cumplimiento de cada actividad. Al final, el auditor obtiene el promedio aritmético de esa columna y lo anota.

Algunas veces, por los resultados de las multiplicaciones, se pueden obtener resultados que no coinciden aritméticamente, como en el caso de éste ejemplo, en donde la suma de la columna 6 nos da por resultado 1.61. Mientras que, si multiplicamos el valor total ponderado de la columna 5 (2.0 por 8.25) el resultado es 1.65; la diferencia 0.04 no es significativa y se puede anotar el valor que más crea conveniente el auditor. Lo importante es la evaluación que se debe hacer de ese valor. Como se indica en el cuarto pasó.

Cuarto paso:

Después de haber obtenido las calificaciones y los valores de toda la guía de ponderación (columna 5), así como el porcentaje de los puntos obtenidos (columna 6), el responsable de la auditoría debe realizar un análisis profundo sobre cada uno de

los resultados y valorar el grado de cumplimiento de cada una de las actividades. Es recomendable adoptar un criterio uniforme para calificar de la misma manera todos los puntos evaluados.

Para explicar esto utilizaremos resultados hipotéticos en el punto 8, Configuración del sistema; así encontraremos los siguientes valores para la calificación (columna 5) y el cálculo del porcentaje de los puntos obtenidos (columna 6). El criterio de calificación que utilizaremos es el siguiente:

Calificación	Desde	Hasta	Comentario
Excelente	81%	100%	(para el cumplimiento más alto)
Bueno	61%	80%	(para un cumplimiento bueno sin llegar a ser excelente)
Regular	41%	60%	(para un cumplimiento mínimamente aceptable)
Deficiente	21%	40%	(para un cumplimiento malo y peor de lo esperado)
Pésimo	0%	20%	(para un "incumplimiento" francamente desastroso)

Una vez obtenidas las calificaciones, promedios y sumas de cada uno de los factores, se comparan los resultados de cada factor con su peso específico. El propósito es que el auditor tenga un criterio numérico mediante el cual pueda tener los parámetros para comprar el grado de cumplimiento alcanzado por cada factor con el grado de cumplimiento esperado.

Cuadro 5

Columna 1	Columna 2	Columna 3	Columna 4	Columna 5	Columna 6
Actividades que van a ser evaluadas y ponderadas	**Peso por actividad**	**Peso por ponderar**	**Valor de ponderación**	**Calificación**	**Porcentaje de puntos obtenidos**
8.Configuración del sistema			**4.0%**		
Definición del equipo (hardware)	25%	1.00%		95	0.95

Definición del equipo (software)	25%	1.00%		95	0.95
Adaptación de instalaciones	15%	0.60%		80	0.48
Adaptación del medio ambiente	15%	0.60%		50	0.30
Planes contra contingencias	20%	0.80%		10	0.08
Total del factor a ponderar	**100%**	**4.00%**		**66%**	**2.64**

Como podemos observar, el total es un poco más que regular, 2.64% alcanzado en comparación con 4.00% del total esperado de éste factor (apenas se obtuvo 66% en comparación con 100% del esperado); esto nos haría juzgar que el cumplimiento de la configuración del sistema es mínimamente aceptable. Sin embargo, esto no es lo real ni tampoco lo más justo. Sería muy arbitrario e injusto calificar el cumplimiento del 95% de los dos primeros puntos (definición del hardware y definición del software) con 66% (cada uno de ellos casi alcanza el más alto cumplimiento); tampoco es nada equitativo "premiar" 10% del último; se esperaba 0.80% y sólo alcanzó 0.08% (éste no alcanza ni el cumplimiento mínimo señalado en la tabla).

En el ejemplo vemos que al factor Planes contra contingencias se le concede nulo o muy poco valor. Por eso es muy útil ésta guía de ponderación, ya que permite evaluar, lo más objetivamente posible, los resultados obtenidos en una auditoría, elegir los factores primarios que serán evaluados, las actividades que serán evaluadas en cada uno de ellos, así como darles un peso

específico equitativo a todos esos factores. También permite hacer una verdadera valoración del grado de cumplimiento de cada factor y cada actividad.

Conviene indicar que ésta técnica se puede aplicar en todo el ámbito de sistemas o en cada uno de los aspectos de sistemas que deban ser evaluados. Dicha aplicación se hará de acuerdo con las necesidades de la evaluación.

La segunda metodología es la identificación y evaluación de riesgos

Esta herramienta es una base técnica para la identificación y evaluación de riesgos, sobre la cual el auditor (contador público) define las actividades a desarrollar asignando los recursos a las áreas de sistemas de mayor riesgo de sus clientes, que haya identificado. Está tiene como objetivos:

a) Identificar a través de una evaluación técnica y sistemática las áreas que representan mayor riesgo de los clientes.
b) Asignar el recurso humano según los resultados de la evaluación técnica, a las áreas de mayor riesgo.
c) Definir el plan de auditoría considerando el resultado de la evaluación de los riesgos de cada área de sistemas.

Los factores de riesgos son los criterios utilizados para identificar la importancia relativa y probabilidad de que condiciones y/o eventos pueden ocurrir que afecten adversamente los sistemas informáticos y de información del cliente. La

cantidad de factores de riesgo a ser utilizados puede ser limitado, pero suficiente para proveer al auditor la confianza de que la evaluación de riesgo de las áreas de sistemas será completa. Entre los factores a considerar como base técnica y sistemática para la evaluación de las áreas de mayor riesgo del cliente, se consideran cinco, es importante mencionar que el número de factores queda a criterio del auditor, y a los cuales se le asignará a cada uno una ponderación igual en orden de importancia, con la finalidad de que sean medibles sobre la misma base, tal como se describe a continuación:

FACTOR DE EVALUACIÓN	**PONDERACIÓN**
Control interno de sistemas	20%
Materialidad de las operaciones	20%
Entorno del área de sistemas	20%
Sistemas y organización	20%
Leyes y regulaciones aplicables	20%
Total	**100%**

La ponderación asignada en igual porcentaje se hace con el propósito de darles la misma oportunidad a todos los factores en la evaluación de las áreas o procesos a examinar, y la suma de todas las ponderaciones no importando el número de factores siempre tendrá que ser igual al cien por ciento. El socio o gerente de auditoría pueden decidir conjuntamente con el especialista asignar valores numéricos a los factores de riesgo para representar su importancia relativa y frecuencia de

ocurrencia en las áreas de sistemas de sus clientes. La asignación de un valor numérico a un factor de riesgo refleja el juicio del auditor acerca del impacto relativo que el factor puede tener en la selección de una actividad para la auditoría dentro de las actividades u operaciones del cliente.

La evaluación se hace por medio de puntos para cada área, que están en el rango de 100 a 500, esto permite establecer las prioridades para la evaluación de las áreas seleccionadas. El rango varía según el número de factores seleccionados. Los criterios que se tomarán en cuenta para la determinación de la frecuencia y la prioridad de la cobertura dirigida a cada área a ser auditada, queda a discreción del auditor ya que depende de la ponderación de los elementos identificados en cada factor, así como del conocimiento y experiencias que el auditor tenga sobre las diferentes áreas de sistemas del cliente.

A continuación se detallan los rangos de puntaje a ser considerados por el auditor para determinar la frecuencia de las evaluaciones:

a) Las áreas de sistemas identificadas según ésta metodología, con un rango entre 401 a 500 puntos, deben ser consideradas de bajo riesgo pueden ser cubiertas por requerimiento específico.

b) Las áreas con puntajes con un rango entre 301 a 400 puntos, se considerarán de un riesgo aceptable y pueden ser auditadas una vez al año.
c) Las áreas identificadas con puntajes de 201 a 300 puntos, serán auditadas cada seis meses, por considerarse con riesgo moderado.
d) Las áreas con puntaje de 101 a 200 puntos, serán consideradas con riesgo alto moderado, requiriendo que la frecuencia de la revisión sea trimestral.
e) Las áreas identificadas con menos de 100 puntos, representan un riesgo alto, tanto para el cliente como para el auditor, lo recomendable es no aceptar clientes que se encuentren en éste rango, sin embargo, el auditor puede aceptarlo, indicándole al cliente que la auditoría a ser practicada requerirá mayor presencia en forma mensual, hasta que el nivel de riesgo sea aceptable para el auditor.

Los factores a ser evaluados deben ser disgregados en elementos para una mejor comprensión y análisis, considerando aquellos que tienen mayor incidencia en las operaciones del cliente, y dentro de estos elementos se pueden incluir los siguientes:

a) La competencia y suficiencia del personal.
b) El ambiente ético.
c) El tamaño de los activos, liquidez, o volumen de transacciones.

d) Las condiciones competitivas.

e) La complejidad o volatilidad de las actividades.

f) Clientes, proveedores, y entes reguladores del estado.

g) El tipo de sistemas de información computarizado.

h) La dispersión geográfica de las operaciones.

i) La suficiencia y efectividad del sistema de control interno.

j) Los cambios tecnológicos o económicos.

k) Los juicios de la administración y las proyecciones contables.

l) La aceptación de los hallazgos de auditoría y las acciones correctivas adoptadas.

Para el desarrollo de ésta metodología, se considerarán diferentes elementos para cada factor de acuerdo a los de mayor incidencia dentro de las operaciones que realizan los clientes, a estos elementos se les aplicará puntajes del uno al cinco de cuerdo al nivel de riesgo que representan, indicando con el número uno que representa malo o deficiente hasta el número cinco que representa satisfactorio, estos puntajes se establecen con base a criterios definidos por el auditor, los cuales son detallados a continuación:

CRITERIO	**PUNTAJE**
MALO (DEFICIENTE)	1
DÉBIL	2
REGULAR	3
ACEPTABLE	4
SATISFACTORIO	5

A continuación se mencionan, los elementos considerados para cada uno de los cinco factores identificados dentro de las áreas de sistemas, para medir el nivel de riesgo existente, así como los criterios de ponderación a ser aplicados.

CONTROL INTERNO DE LOS SISTEMAS

Este factor está relacionado con el nivel esperado de efectividad de los sistemas de control interno de los sistemas computarizados establecidos por el cliente, así como los cambios significativos y de identificación de los sistemas sobre los cuales se va a tomar confianza.

Entre los principales elementos a ser considerados dentro del factor de control interno se pueden mencionar:

1. La experiencia en el cumplimiento de las normas y políticas establecidas.
2. La historia de pérdidas y fraudes.
3. El resultado de auditorías anteriores.
4. La confianza de la administración en el área.
5. La existencia de registros auxiliares.
6. La automatización de registros y transacciones, los sistemas de programación, así como el acceso de la información.
7. Prácticas de supervisión y protección física de documentos, archivos e información de alto riesgo.

Los puntajes de ponderación en éste factor se asignan con base a los siguientes criterios:

Nivel de Riesgo Descripción del Criterio

1. Deficiente: El sistema de control interno de sistemas no cuenta con controles mínimos requeridos, ya sea por que los procedimientos, normas o manuales no existen o no son utilizados.
2. Débil: El ambiente de control interno en el área de sistemas no cuenta con los controles necesarios para salvaguardar adecuadamente los activos del cliente y/o las omisiones de aplicación pueden comprometer el desarrollo normal de las operaciones.
3. Regular: El sistema carece de ciertos controles, que de ser implementados se controlaría con los elementos para ejercer un buen control sobre el área, además de observarse algunas omisiones de aplicación.
4. Aceptable: El sistema cuenta con los elementos necesarios, pero se observan algunas omisiones en su aplicación, las que no comprometen el desarrollo normal de las operaciones del cliente.
5. Satisfactorio: El sistema de control interno cuenta con los elementos adecuados (manuales de procedimientos, normas

y políticas y las pautas de control) que permiten salvaguardar adecuadamente los activos del cliente

- **Materialidad de las operaciones:**

Este factor considera la importancia relativa de los elementos de los estados financieros del cliente, así como la exposición a errores e irregularidades de importancia.

Los principales elementos que se consideran dentro del factor de materialidad se mencionan a continuación:

1. Los saldos de las cuentas, según los estados financieros con relación a los rubros y cuentas de detalle de estos.
2. El volumen periódico de las transacciones en valores y cantidades.
3. Las exigencias presupuestarias.
4. La cantidad de personal involucrado en el área de sistemas.
5. La rotación de los activos.

Los puntajes de ponderación en éste factor se asignan con base a los siguientes criterios:

Nivel de Riesgo Descripción del Criterio

1. Deficiente: Las transacciones que son manejadas en el área de sistemas representan montos significativos y de fácil pérdida o daño.

2. Débil: Las transacciones que son manejadas en el área de sistemas son susceptibles a pérdida o daño aún cuando los montos de éstas no son muy importantes.
3. Regular: Las transacciones manejadas por el área de sistemas son susceptibles a pérdida o daño, sin embargo sus montos requieren un adecuado tratamiento de control.
4. Aceptable: El monto de las transacciones es bajo, así como también el número que son manejadas en el área de sistemas.
5. Satisfactorio: Los montos de las transacciones manejados por el área de sistemas, son irrelevantes y su manejo resulta fácil.

- **Entorno del área de sistemas:**

Este se relaciona con los factores del medio, tales como: los fenómenos y tendencias para derivar riesgos, amenazas y oportunidades, etc. Dentro de los elementos a considerar en el factor entorno del área de sistemas, se pueden mencionar los siguientes:

1. Adecuados sistemas computacionales.
2. Manuales, procedimientos e instructivos actualizados.
3. Documentación suficiente.
4. Adecuados registros.
5. La oportunidad de los reportes e informes.
6. La capacidad del personal del área.

7. Los cambios en la tecnología.

Los puntajes de ponderación en éste factor se asignan con base a los siguientes criterios:

Nivel de Riesgo Descripción del Criterio

1. Deficiente: Existen problemas serios para determinar cuan confiable es la información generada en el área de sistemas.
2. Débil: La confiabilidad de la información es dudosa, debido a que los elementos con que se cuenta para realizar las actividades son insuficientes.
3. Regular: La inexistencia de adecuados elementos de apoyo afectan la confiabilidad de la información que genera el área de sistemas, no obstante lo anterior, es factible desarrollar con algún esfuerzo las actividades que son requeridas.
4. Aceptable: Si bien no existen todos los elementos de apoyo que serían necesarios, esto no afecta la confiabilidad ni la oportunidad con que es generada la información.
5. Satisfactorio: La información procesada y mantenida en el área de sistemas es totalmente confiable y oportuna.

- **Sistemas y organización:**

Este factor se considera que es parte de la administración del cliente que implica el establecer una estructura de funciones.

Entre los principales elementos a considerar en el factor sistemas y organización, se mencionan:

1. La frecuencia de los cambios en los sistemas.
2. La complejidad de los sistemas.
3. La estandarización.
4. La definición de funciones y objetivos.
5. La carga de trabajo y segregación de funciones.

Los puntajes de ponderación se asignan con base a los siguientes criterios:

Nivel de Riesgo Descripción del Criterio

1. Mala: Los sistemas son desorganizados o no hay documentación y existen serias fallas en la organización que desvíen constantemente los resultados.
2. Débil: Los sistemas son complejos y no están documentados, existe centralización de funciones y la organización no está definida claramente.
3. Regular: Los sistemas existentes son relativamente complejos, existen ciertas debilidades en el aspecto organizativo que podría causar atrasos o falla en los resultados propuestos.
4. Aceptable: Los sistemas son adecuados aunque falta alguna estandarización, la organización es apropiada y el personal tiene alguna experiencia en los puestos.

5. Satisfactorio: Los sistemas del cliente son sencillos, fáciles de entender y están documentados, la organización es adecuada, el personal está capacitado y conoce sus tareas a fondo, existe una adecuada segregación de funciones y distribución de tareas.

- **Leyes y regulaciones aplicables:**

Este factor se refiere al cumplimiento a las regulaciones a la que se encuentra sometido el cliente, la revisión de la base legal y los aspectos jurídicos relacionados con el giro del negocio del cliente.

Se relaciona con aquellos elementos que de no ser considerados pueden hacer que el cliente llegue a incumplimiento a regulaciones, normas y procedimientos legales y en consecuencia a penalidades económicas.

Dentro de los elementos a considerar en el factor leyes y regulaciones aplicables, se pueden mencionar los siguientes:

1. Asuntos legales involucrados.
2. Conocimiento y aplicación de leyes, instructivos, políticas, normas y decretos.
3. Regulaciones fiscales.
4. Regulaciones específicas del negocio del cliente.

Los puntajes de ponderación en éste factor se asignan con base a los siguientes criterios:

Nivel de Riesgo Descripción del Criterio

1. Mala: Existen leyes, regulaciones y lineamientos de mucha importancia del área de sistemas que deben ser cumplidos con exactitud y en los plazos señalados, de no ser así el cliente estaría ante un riesgo legal considerable.
2. Débil: El área está sujeta a normas de ética, leyes y demás regulaciones importantes que requieren atención constante y los controles existentes para garantizar su aplicación son relativamente débiles.
3. Regular: Los lineamientos y leyes que norman el área son flexibles, y el área tiene los controles suficientes para garantizar su cumplimiento.
4. Aceptable: Existen muy pocas leyes, normas y reglamentos relacionados con el área, y existe buena experiencia en su cumplimiento.
5. Satisfactorio: No existen leyes o lineamientos importantes a que está sujeta el área de sistemas.

El cuadro 6 permite obtener el nivel de riesgo por factor con base al promedio resultante del puntaje asignado a cada uno de los elementos definidos. El puntaje para cada elemento es discrecionalidad del auditor, para éste caso el número uno es malo o deficiente, el dos débil, el tres regular, el cuatro aceptable y el cinco excelente. (Ver cuadro 6 en anexo No.3)

Para proceder a la ponderación de riesgos según los niveles establecidos anteriormente, se utiliza una cédula en la que se detallan los cinco factores a evaluar, los diferentes niveles de riesgo asignados que van del uno al cinco, según criterios ya definidos con su respectivo puntaje. El número del puntaje asignado a cada elemento de acuerdo al criterio y experiencia del auditor, se multiplica por el porcentaje de ponderación de cada factor, que en éste caso es del veinte por ciento (20%) para cada uno, obteniendo al final una ponderación total calculada la cual sirve para ubicar el área evaluada en el nivel de riesgo previamente establecido, que para éste caso comienzan con 100 y terminan con 500, por el número de factores considerados. (Ver cuadro 7 en anexo No.4).

Es importante mencionar que los valores contenidos en la columna promedio se obtiene de la cédula anterior, que de éste valor multiplicado por el factor de peso definido previamente (20%) resulta la ponderación para cada factor y que al final la suma obtenida es la ponderación total calculada. De acuerdo a la ponderación de riesgos obtenida en éste ejemplo, ésta presenta un total de 363.0 puntos, que se considera aceptable. Como resultado de la ponderación de riesgos realizada, se obtienen las áreas o procesos con puntajes altos, medios y bajos, lo que

representa el nivel de riesgo correspondiente, permitiendo al auditor establecer prioridades en la evaluación.

Cuadro 8

EMPRESA XYZ, S.A. DE C.V.
ANALISIS Y EVALUACIÓN DE RIESGOS
ÁREA:_____

CEDULA DE PRIORIDADES DE EVALUACIÓN DE RIESGOS DE AUDITORÍA

PONDERACIÓN	NIVEL DE RIESGO	PRIORIDAD DE EVALUACIÓN
de 001 a 100 puntos	Alto	Mensual
de 101 a 200 puntos	Alto Moderado	Trimestral
de 201 a 300 puntos	Moderado	Semestral
de 301 a 400 puntos	Aceptable	Una vez al año
de 401 a 500 puntos	Bajo	Por requerimiento específico

La asignación de tiempo para cada actividad a evaluar en los clientes se realiza con base a la priorización de las áreas.

Las áreas que representen mayor nivel de riesgo se les asigna mayor número de horas hombre para la evaluación, así como la frecuencia de realización también es mayor. Las horas hombre a asignar para cada área o proceso a evaluar resultará de la distribución proporcional del tiempo total calculado con base al número de auditores dependiendo del nivel de riesgo que presenta el área.

Cuadro 9

EMPRESA XYZ, S.A. DE C.V.
PLAN DE ACCIÓN

HOJA DE ASIGNACIÓN DE TIEMPO POR RIESGO

ÁREAS	RIESGO PONDERADO	% DE RIESGO	TIEMPO ASIGNADO	% DE TIEMPO
CONTROLES GENERALES:				
De Organización y Operación				
De los Sistemas de Desarrollo y Documentación				
De Equipo y Sistema Software				
De Acceso				
De Datos y de Procedimiento				
CONTROLES DE APLICACIÓN:				
De Acceso				
De Procesamiento				
De Resultados				
TOTALES		**100%**		**100%**

NOTA: Esta cédula muestra a manera de ejemplo algunas de las áreas de sistemas computarizados. El contador público también debe considerar, poder adquirir un software de auditoría, conocidos como programas de auditoría, los cuales consisten en la utilización de lenguajes de interrogación de ficheros, lo cual le permite al auditor informático lo siguiente:

- En el marco de una auditoría de aplicación, el controlar el contenido de los ficheros y detectar anomalías eventuales en estos.
- En el marco de asistencia de la revisión contable, el poder validar los resultados de algunos de los procesos, o también

poder poner en evidencia las informaciones anómalas o erróneas.

3.3.2 TÉRMINOS DE LOS TRABAJOS DE AUDITORÍA

Debe determinarse los objetivos, responsabilidades y alcance de la auditoría para evitar malos entendidos respecto del trabajo. Conviene a los intereses tanto del cliente como al del auditor, que éste envíe una carta compromiso preferiblemente antes del inicio del trabajo como para ayudar a evitar malos entendidos respecto del trabajo. La carta compromiso documenta y confirma la aceptación del nombramiento por parte del auditor, el objetivo y alcance de la auditoría el grado de responsabilidades del auditor hacia el cliente y la forma de cualquier informe. El auditor deberá incluir como mínimo dentro del cuerpo de la carta compromiso los siguientes puntos:

- El objetivo de la auditoría de estados financieros.
- Responsabilidad de la administración por los estados financieros.
- Alcance de la auditoría, incluyendo referencias a la legislación aplicable, reglamentos o pronunciamientos de organismos profesionales, a los cuales se adhiere el auditor.
- La forma de cualquier informe u otra comunicación del resultado del trabajo.

- La evaluación de la estructura del control interno, así como la evaluación de los sistemas contables.
- Acceso sin restricción a cualquier registro, documentación y otra información solicitada en conexión con la auditoria.

Adicionalmente el auditor, podrá incluir en la carta compromiso todos aquellos aspectos que a su juicio sean relevantes para el desarrollo de una auditoría de los sistemas de información.

3.3.3 PLANEACIÓN

Significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperados de la auditoria. El auditor planea desempeñar la auditoría de manera eficiente y oportuna. El auditor deberá planear el trabajo de auditoría de modo que la auditoría sea desempeñada en una manera efectiva. La planeación adecuada del trabajo de auditoría ayuda a asegurar que se presta atención adecuada a áreas importantes de la auditoría, que los problemas potenciales son identificados y que el trabajo es completado en forma expedita. La planeación también ayuda para la apropiada asignación de trabajo a los auxiliares y para la coordinación del trabajo hecho por otros auditores y/o expertos en sistemas.
El plan preliminar que comprende el estudio y evaluación del control interno y la evaluación operativa de gestión y de cumplimiento; así mismo el memorándum de planeación, en el cual

se presenta el contenido básico de la misma, ésta guía plasma los aspectos generales que se refieren a la entidad, como son:

- Sus antecedentes relacionados con su creación, los objetivos de la entidad, objetivos de la auditoría, políticas contables, alcance de la auditoría, limitación al alcance, componentes del control interno entre otros.
- También contiene la estrategia de la auditoría que se va a desarrollar, es decir, que está comprende los aspectos tales como: áreas a auditar, determinación de los componentes de auditoría, naturaleza de los componentes, determinación de los factores de riesgo de auditoría, estimación de riesgo de auditoría, enfoque de la auditoría por componentes, finalmente la administración de trabajo de auditoría, la cual está conformada por: personal clave de la institución, personal clave, del personal de auditoria en sistemas, presupuesto de tiempo y cronología de actividades.

3.3.3.1 PROCESOS A SEGUIR AL PLANIFICAR LA AUDITORÍA

El plan global de auditoría

El auditor debería desarrollar y documentar un plan global de auditoría describiendo el alcance y conducción esperada de la auditoría. Mientras que el plan global de auditoría necesitará estar suficientemente detallado para guiar el desarrollo del programa de auditoría, su forma y contenido precisos variarán de

acuerdo al tamaño de la entidad, a la complejidad de la auditoría y a la metodología específica usada por el auditor.

Las etapas o procesos que se consideran al desarrollar el plan global de auditoría incluyen:

- Conocimiento del negocio.
- Comprensión de los sistemas.
- Riesgo e importancia relativa.
- Naturaleza, tiempos, y Alcance de los procedimientos.
- Coordinación, dirección, supervisión y revisión.
- Otros asuntos.

3.3.4 EJECUCIÓN

En ésta etapa el auditor desarrollará una serie de actividades lógicas en el desarrollo de la auditoría, tales como la evaluación del sistema de control interno del área de sistemas, por medio de entrevistas o narrativas, cuestionarios y flujograma, remitiendo posteriormente carta a la gerencia o administración de las deficiencias encontradas en dicha evaluación, asimismo elaborará el memorándum de planeación de la auditoría, diseñará y ejecutará los programas de auditoría, pudiendo ser estos estándares o a la medida de cada cliente, y finalmente emitirá un informe de auditoría correspondiente a las áreas o componentes de los estados financieros examinados. Todo lo anterior se representará por medio de los papeles de trabajo

que constituyen la documentación de soporte y evidencia del examen realizado por al auditor. (Ver anexo No.5).

3.3.4.1 INSTRUMENTOS Y HERRAMIENTAS PARA LA AUDITORÍA

3.3.4.1.1 PROGRAMAS DE AUDITORÍA

En éste punto el auditor diseñará los programas de auditoría, los cuales comprenden un conjunto de procedimientos determinados durante la etapa de planeación, así como los objetivos general y específicos de las áreas o componentes definidos, con el propósito de verificar las operaciones efectuadas por la administración del cliente. Los programas de auditoría normalmente están divididos en tres partes: pruebas de controles, pruebas sustantivas de las operaciones y pruebas detalladas de transacciones y saldos. Los programas de auditoría para auditorias de estados financieros se estructuran de la siguiente forma: el nombre del cliente, área o componente a auditar, fecha del examen, objetivos que se persiguen con la auditoría, los procedimientos a ser realizados, referencia a los papeles de trabajo, firma de quién ejecutó la auditoría, firma y fecha de revisión, autorización de la ejecución de la auditoria. A continuación se presenta un modelo de Programa de auditoría de sistemas o guía de evaluación:

PROGRAMA DE: ORGANIZACIONAL Y DE GESTIÓN

EMPRESA: _____

Elaborado por:		
Revisado por:		

Objetivos:

1. Verificar que la estructura organizativa este adecuada a las necesidades existentes.
2. Verificar si las responsabilidades han sido delimitadas adecuadamente dentro de la organización.
3. Verificar el cumplimiento de objetivos y metas establecidas.
4. Verificar si se cumplen los lineamientos organizacionales.
5. Verificar la existencia de la documentación de las actividades, funciones y responsabilidades.

No	Procedimiento	Hecho por	Ref. Pt´s
1	Obtener el manual de organización y funciones.		
2	Obtener el organigrama de la industria y evaluar la ubicación de la unidad dentro de la organización.		
3	Evaluar la estructura orgánica, respecto del personal existente.		
4	Verificar que la actual estructura orgánica del área de informática cumple con la estructura general de la industria		
5	Verificar el cumplimiento de funciones y responsabilidades establecidas en el Manual de Puestos.		
6	Verificar el cumplimiento de los objetivos y metas establecidos.		
7	Verificar la existencia de una segregación adecuada de funciones dentro del área de Informática.		
8	Indagar con el personal del área de informática las razones por las cuales no se estén cumpliendo determinados objetivos.		
9	Verificar e indagar que las funciones realizadas en el área de Informática estén encaminadas a la operatividad del negocio.		
10	Verificar que los procedimientos y aplicaciones llevados a cabo en el área de Informática estén debidamente documentados.		
11	Verificar que el área de Informática cuenta con el equipo adecuado que permita el cumplimiento de los objetivos de la organización.		
12	Indagar sobre limitaciones de recursos materiales y económicos que el área de Informática posea.		

13	Indagar las razones de cambios que se den en el área de Informática.		
14	Verificar que el área de Informática cuenta con estrategias para minimizar los resultados negativos que se generen producto de cambios en la misma.		

PROGRAMA DE: FUNCIONAMIENTO

EMPRESA: _____

Elaborado por:		
Revisado por:		

Objetivos:

1. Asegurar la existencia de un proceso adecuado de información en los programas de funcionamiento.
2. Verificar que los programas en funcionamiento actuales de la empresa estén en función de los requerimientos de información de la misma.
3. Verificar la existencia de un plan de contingencias relacionando con los programas en funcionamiento.
4. Evaluar el nivel de conocimiento de los empleados de la Industria en relación a los programas de funcionamiento.
5. Verificar que los programas en funcionamiento utilizados sean de costo/benéfico para la empresa y el mantenimiento de los mismos estén en función de los requerimientos hechos por los usuarios.
6. Exponer las recomendaciones pertinentes para que dicha metodología satisfaga las necesidades de desarrollo e implantación de sistemas.

No	Procedimiento	Hecho por	Ref Pt´s
1	Verifique que los programas en funcionamiento cumplan lo siguiente: Que hayan sido autorizados por el área de Informática para poder ser operados al interior de la empresa.		
2	Verifique si el área de Informática tiene identificada la siguiente información: -Usuarios. -Registros y Niveles de acceso. -Equipos donde se encuentra instalado cada tipo de Software. -Periféricos conectados a dichos equipos. -Software original y pirata instalado en equipos. -Otros.		
3	Verifique los controles implementados en los sistemas en funcionamiento contemplan al menos: • Protección de archivos		

	• Protección a programas fuentes de las aplicaciones que están en los equipos. • Protección a otro Software alojado en los equipos. • Métodos para prevenir el monitoreo no autorizado del equipo y sistemas. • Detección inmediata y automatizada de acceso no automatizados a los sistemas y equipos. • Contraseñas que autoricen el acceso a los equipos y eviten el acceso a archivos no autorizados. • Otros.		
4	Evalué si las políticas y procedimientos relativos al uso y protección del Software son adecuados e implementados.		
5	Obtenga un detalle de los programas en funcionamiento por el periodo de _____ y asegurase que las mismas satisfagan los requerimientos específicos del negocio.		
6	Efectué inspección física de los equipos de acuerdo a la ubicación dada por el Departamento de Informática.		
7	Verifique que la ubicación física del inventario requerido esta en función de la asignación de los mismos y que estos no se encuentran en un lugar diferente al que se esta mencionando.		
8	Indague con el personal de la Industria acerca del conocimiento que estos tienen en relación a los programas en funcionamiento utilizados por la Industria.		
9	Obtenga las políticas de capacitación del personal de nuevo ingreso a la Industria y verifique que estos, hayan sido capacitados formalmente en el uso de los programas en funcionamientote tal forma que sean de costo benéfico para las operaciones que estos realicen.		
10	Obtenga los manuales de los programas en funcionamiento y verifique lo siguiente: Que se encuentren autorizados por el funcionario respectivo. Que estén actualizados. Que están de acuerdo a los requerimientos de información de los usuarios. Que se haya revisado periódicamente su contenido.		
11	Obtenga un detalle de las mejoras a los programas en funcionamiento y verifique que los mismos han sido autorizados por el funcionario respectivo.		
12	Verifique que los cambios y las mejoras en los programas en funcionamiento se encuentre documentada		
13	Compruebe si existen parámetros de medición del desempeño del equipo (bitácoras, graficas, estadísticas).		
14	Compruebe mediante pruebas sustantivas la suficiencia de controles y procedimientos de seguridad en el Software existente.		
15	Asegurese por medio de un chequeo físico de documentación a las licencias que el Software		

	existente se encuentra legalizado.		
16	Realice una evaluación del Software actual de la siguiente forma: • Análisis y diagnostico del Software instalado en los equipos de computo como, procesadores, etc. • Bases de datos. • Lenguajes de programación, sistemas operativos, etc.		

PROGRAMA DE: DESARROLLO

EMPRESA:_____

Elaborado por:		
Revisado por:		

Objetivos:

1. Asegurar que exista un proceso metodológico para ejecutar el ciclo de vida de desarrollo e implantación de sistemas de información formal y estandarizada en la organización.
2. Confirmar que el personal de desarrollo de sistemas de información conozca dicha metodología, con el fin que se asegure la calidad y productividad durante el desarrollo de los sistemas de información.
3. Exponer las recomendaciones pertinentes para que dicha metodología satisfaga las necesidades de desarrollo e implantación de sistemas.

No	Procedimiento	Hecho por	Ref Pt´s
1	Verifique con el área de Informática acerca del tipo de metodología existente en la evaluación de sistemas en desarrollo por medio de entrevistas.		
2	Obtenga la metodología formal de desarrollo de sistemas, y verifique lo siguiente: • Que se encuentren por escrito • Que se encuentre autorizada por el funcionario responsable. • Que se encuentre vigente a la fecha de nuestra revisión.		
3	Obtenga un detalle de la metodología de implantación comprada o rentada a externos por el periodo de _____del año en curso y asegúrese que las mismas satisfagan los requerimientos específicos del negocio.		
4	Compruebe con el personal de Informática acerca del conocimiento que estos tienen en relación a la metodología utilizada en el desarrollo de sistemas informáticos y concluya al respecto.		
5	Obtenga las políticas de capacitación del personal de nuevo ingreso a la Industria en el área de Informática y verifique que estos, hayan		

	sido capacitados formalmente en el uso de la metodología de desarrollo de sistemas.		
6	Verifique que la política de capacitación se encuentre vigente y autorizada.		
7	Obtenga un detalle de las mejoras de la metodología de ciclo de desarrollote implantación de sistemas de Informática y verifique que los mismos han sido autorizados por el funcionario respectivo.		
8	Verifique que los cambios y mejoras a la metodología se encuentren documentadas.		
9	Redacte un resumen de los Hallazgos.		

PROGRAMA DE: HARDWARE/SOFTWARE

EMPRESA:_____

Elaborado por:		
Revisado por:		

Objetivos:

1. Garantizar la integridad de los sistemas operativos de la Industria.
2. Garantizar que los programas del sistema se protejan adecuadamente.
3. Asegurarnos que la adquisición de tecnología fue aprobada por la Junta Directiva.
4. Asegurarnos del cumplimiento de las políticas de adquisición de tecnología de información establecidas por la Gerencia.
5. Asegurarnos que la adquisición de tecnología esta en función de las necesidades de la Industria.
6. Asegurarnos de la adecuada documentación y garantía de la tecnología adquirida

No	Procedimiento	Hecho por	Ref Pt´s
1	Mediante cuestionario de control interno indague con el área de informática lo adecuado de la adquisición de equipo, considerando el Hardware y Software.		
2	Verifique que la empresa cuente con manuales de procedimientos y de control para la adquisición de Hardware y Software y su mantenimiento.		
	HARDWARE		
3	Evalué el método realizado de costo y beneficio por la empresa en la adquisición de Hardware y Software.		
4	Verifique que existe un plan formal de adquisición del Hardware que contenga lo siguiente: • Evaluación del Hardware actual. • Análisis y evaluación del Hardware a		

	adquirir. • Análisis y diagnostico del numero de equipo. • Análisis y diagnostico de periféricos.		
5	Compruebe que las instalaciones de los equipos sean oportunas conforme a contratos y compras formales de los mismos.		
6	Evalué las actividades realizadas durante la instalación de la tecnología adquirida, en cuanto al tiempo y costo de la industria.		
7	Solicite un listado del equipo de cómputo que la empresa posee y con ello realice un inventario físico.		
8	Verifique el estado(s) de la computadora(s) y su capacidad de memoria(s).		
9	Verifique que todos los usuarios del sistema cuenten con el equipo necesario.		
10	Prepare una cedula donde describa Usuario, equipo, nivel de autorización, ubicación, etc.		
11	Investigue si se tiene un plan de sustitución de equipos		
12	Investigar y documentar el plan de contingencias por si falla el Hardware.		
13	Realice pruebas que lo lleven a probar si la empresa le da mantenimiento tanto preventivo como correctivo a los equipos		
14	Verifique que todos los equipos tengan su respectivo antivirus.		
15	Asegurese que todos los equipos tengan sus respectivos documentos que aseguren la propiedad de los mismos.		
SOFTWARE			
16	Solicite las evaluaciones y plantación para la compra de software. Y si no han sido planeado formalmente como lo justifican. Verifique que sean bien documentados.		
17	Verifique que el software sea instalado en los equipos correspondientes y que tengan sus licencias, es decir que sean legales.		
18	Realice un análisis del proceso e instalación de los componentes de la tecnología adquirida, y Asegurese que la instalación de los mismos esté de acuerdo a las necesidades básicas expuestas por la empresa.		
19	Investigue si el sistema de información cuenta con un software desarrollado en la empresa o se a adquirido ya desarrollado.		
20	Asegurese de la legalidad del software y prepare una cedula con generalidades del sistema.		
21	Investigue quien es el proveedor del sistema y que otras empresas lo utilizan.		
22	Investigue si existe certificación por un consultor independiente del buen funcionamiento del sistema.		
23	Analizar y dejar prueba documental de la		

	evidencia de los cambios que se le realicen al sistema y cuestionar entre otras cosas: a) Quien solicita el cambio. b) Quien autoriza. c) Quien ejecuta.		
24	Revisar el funcionamiento del sistema y verificar si el programa esta en línea dentro de la empresa o se trabaja con computadoras independientes.		
25	Investigue y prepare evidencia sobre los niveles de seguridad que se tienen para la protección del software.		
26	Realice pruebas selectivas con los empleados sobre el conocimiento y el uso adecuado del software.		
27	Realice una verificación del sistema sobre los reportes que el sistema puede emitir.		
28	Asegurese del buen uso de los reportes.		
29	Revise sino están imprimiendo reportes sin utilidad.		
30	Ingrese al sistema y pruebe si existe la posibilidad de que la información sea manipulada por un intruso.		
31	Verifique la integridad de la base de datos.		
32	Evalué cada uno de los menús del programa y cerciorase de que funcionan como lo establece su respectivo manual.		
33	Documente cada uno de los procesos que se hacen para la obtención de la información.		
34	Investigue el proceso de actualización de la información procesada.		
35	Realice investigación sobre el adecuado almacenamiento de los respaldos (backup) y su uso no indebido.		

PROGRAMA DE: PROCESAMIENTO ELECTRONICO

EMPRESA: _____

Elaborado por:		
Revisado por:		

Objetivo:

Determinar si la gerencia ha establecido los suficientes controles para el procesamiento electrónico de datos con el fin de salvaguardar la protección de los archivos de datos.

No	**Procedimiento**	**Hecho por**	**Ref Pt´s**
Manual de Procedimientos y Asignación de Puestos			
1	Solicite el manual de procedimientos, asignación de funciones y distribución de actividades del área de informática y compruebe lo siguiente:		

	a) Se cumplen los estándares de calidad de dichos manuales. b) Se mantienen estos manuales actualizados y se le entregan a todos los empleados del área de informática. c) Se realiza una inducción adecuada al personal nuevo en cuanto a las prácticas y normas contenidas en dicho manual.		
2	Realice una revisión de funciones vinculadas a la aplicación critica, relativa a: a) Incompatibilidad de funciones. b) Calidad del soporte técnico. c) Políticas relevantes sobre evacuación de aplicaciones de programa.		
3	Solicite el manual de usuarios y verifique lo siguiente: a) Niveles de acceso bien identificados. b) Autorización de cambios de aplicación en programas computarizados, fecha y quien autoriza el proceso de cambio de aplicación.		
Manual de Políticas, Procedimientos y Asignación de Funciones.			
4	Obtenga las políticas sobre la confidencialidad de los datos y verifique lo siguiente: a) Están documentadas las políticas en los manuales de procedimiento. b) Las políticas están vigentes y actualizadas acorde a las necesidades del área de informática.		
Descripción de Software			
5	Elabore un detalle que contenga los Software instalados y verifique lo siguiente: a) Que todos los Software instalados en cada computadora posea su respectiva licencia para su utilización. b) Que cada uno de los Software instalados posea su documentación de respaldo en cuanto a su adquisición.		
Controles de Acceso			
6	Verifique si existen controles de los passwords, sobre el servidor y terminales de la red, con el objetivo que se tenga control de entrada y salida de cada equipo.		
Capacitación			
7	Obtenga el programa de capacitación del personal del área de informática y verifique lo siguiente: a) Si el personal a sido capacitado en los últimos 6 meses en cuanto a diseño y operatividad de nuevos Software y Hardware. b) Se capacita constantemente al personal a través de seminarios, charlas informáticas, etc.		
Programa de Mantenimiento			
8	Solicite los programas de mantenimiento preventivo del equipo de computo y verifique lo		

	siguiente: a) Fecha de vigencia de contrato b) Cada cuanto tiempo se reanuda el contrato c) Monto de contrato de mantenimiento d) Cumplimiento del contrato		
Análisis de Eficiencia de Gestión			
9	Desarrolle los siguientes parámetros de gestión para el área de informática: a) Total de hojas de datos procesados en el mes/total de hora hombre ocupadas en el mes. b) Total de programas utilizados por los usuarios/ total de seminarios de capacitación recibidos por los empleados de informática.		

3.3.4.1.2. CUESTIONARIOS

MANTENIMIENTO DE HARDWARE

EMPRESA:	**FECHA:**
ENTREVISTADO:	**PUESTO:**
REALIZADO POR:	

PREGUNTA	**SI**	**NO**	**N/A**	**Observaciones**	**REF.**
¿Cuentan con un inventario total del hardware de la empresa (actualizado)?					
¿Existen contratos de mantenimiento preventivo y correctivo para el hardware de la empresa con alguna empresa externa?					
¿Están definidos los procedimientos que debe llevar a cabo la empresa externa al efectuar el mantenimiento preventivo?					
¿El servicio que les han brindado es satisfactorio?					
¿Se tiene previsto seguir con esa empresa?					
¿Los términos del contrato son adecuados?					
¿Existe un cronograma para los mantenimientos preventivos?					
¿Alguien valida que los mantenimientos se realicen oportuna y correctamente de acuerdo con los términos del contrato?					
¿De no existir contratos externos, informática se encarga de estos procesos? ¿Quién está a cargo?					
¿Existen procedimientos y cronogramas					

para realizar los mantenimientos preventivos?					
¿Alguien se encarga de validar que este trabajo se efectúe oportuna y correctamente?					
¿Existe un procedimiento a seguir cuando se debe reparar un equipo?					
¿Se cuenta con algún stock para repuestos de equipos?					
¿Se ha designado a una persona como autorizada para hacer uso de este stock?					
¿Cuentan con procedimientos escritos que indique qué hacer con las piezas dañadas o deterioradas y con el equipo catalogado como irreparable?					

SEGURIDAD FÍSICA

EMPRESA:	**FECHA:**
ENTREVISTADO:	**PUESTO:**
REALIZADO POR:	

PREGUNTA	**SI**	**NO**	**N / A**	**Observaciones**	**REF.**
¿Existe una persona asignada formalmente (por escrito) como responsable de la seguridad física de los equipos de cómputo en las distintas áreas de cómputo?					
¿Existe algún tipo de responsabilidad para los usuarios que cuentan con alguna computadora? ¿Cuál y cómo se controla?					
¿Existe algún lugar establecido para resguardar el servidor (equipo principal) de la organización?					
Este lugar cumple con los requerimientos mínimos para estos casos:					
• Control de acceso.					
• Aire acondicionado.					
• Alarmas contra robo e incendio.					
• Detectores de humo.					
¿La temperatura ambiente del lugar donde se ubica el servidor es adecuada y se mantiene regulada?					
¿Cuenta el servidor con alguna unidad de poder ininterrumpida (UPS) con regulador de voltaje que lo soporte el tiempo que sea necesario en caso de falta de fluido eléctrico?					

¿Existe restricción adecuada para controlar el ingreso del personal al área donde se encuentra el servidor de datos?					
¿Existe algún tipo de vigilancia constante sobre el área donde se ubica el servidor?					
¿Existe algún equipo de respaldo para el servidor de datos?					
¿Cada cuánto se actualizan los datos en el equipo de respaldo?					
¿El equipo de respaldo se encuentra ubicado en el mismo lugar del servidor principal?					
¿Se encuentra la instalación eléctrica del servidor y de los equipos de cómputo en general, aparte de la del resto del edificio y debidamente polarizada e identificada?					
¿Se cuenta como mínimo con un extintor en las distintas áreas de cómputo, principalmente donde está ubicado el servidor?					
¿Estos extintores son los apropiados para los tipos de incendios que se puedan producir en estas áreas?					
¿Se ha brindado la capacitación necesaria en el uso de los extintores al personal de cómputo?					
¿Los extintores son revisados y recargados periódicamente por personas o empresas especializadas?					
¿Los equipos que no están bajo garantía de compra, se encuentran incluidos dentro de alguna póliza de seguros ya sea de incendios, robos, desastres naturales, etc.?					
¿Se tiene asignada una persona como responsable de controlar y actualizar las pólizas de equipo electrónico?					
¿Existe algún inventario actualizado de los equipos que están bajo las pólizas?					
¿Está accesible a cualquier persona la caja de breaker que controla la corriente eléctrica del servidor de datos?					
¿Existen salidas de emergencia en el centro de cómputo o en áreas cercanas?					
¿Existen señalizaciones que indiquen las salidas de emergencia y las zonas de seguridad sísmica?					
¿Existe un diagrama de conexiones y comunicación actualizado, que incluya las sucursales si existen?					

SEGURIDAD LÓGICA

EMPRESA:	**FECHA:**
ENTREVISTADO:	**PUESTO:**
REALIZADO POR:	

PREGUNTA	SI	NO	N/A	Observaciones	REF.
¿Existe una persona asignada formalmente (por escrito) como responsable de la seguridad lógica de los equipos de cómputo principales (servidores) de la institución?					
¿Existen procedimientos escritos para la asignación, modificación y eliminación de claves de los usuarios?					
¿Se ha establecido un estándar en cuanto a la longitud y combinación de caracteres de las claves de usuario?					
¿El sistema operativo permite el ingreso sólo a usuarios autorizados?					
¿Los sistemas obligan a cambiar las claves de usuario periódicamente?					
¿La seguridad de los datos es controlada por el sistema operativo?					
¿La seguridad de los datos es controlada por el sistema de aplicaciones?					
¿Se restringe el uso de terminales o estaciones de trabajo a través de la clave del usuario?					
¿Las claves de usuario puedan ser cargadas en la red una sola vez?					
¿Se desactiva o paraliza la terminal del usuario, en caso de estar cierto tiempo sin uso?					
¿Son encriptadas las claves de usuario tanto para acceder la red como a las aplicaciones?					
¿Existen controles para bloquear las terminales o estaciones de trabajo, luego de cierta cantidad de intentos fallidos en el momento de ingresar la clave?					
¿Existe una bitácora de acceso a la red, donde se pueda observar fecha y hora de ingreso de los usuarios?					
¿Existe restricción de acceso a la red y a las aplicaciones de acuerdo con horarios predeterminados?					
¿Existe un inventario total del software instalado en los equipos de la empresa?					
¿Cuenta la empresa con todas las licencias del software instalado?					

¿Alguien está a cargo de revisar que no se instale software ilegal o que no es de importancia para el desarrollo de las actividades de la empresa?					
¿Existe algún procedimiento por si se encuentra software no autorizado en los equipos?					
¿Se ha realizado algún estudio del por qué existe software no autorizado instalado?					
¿Cuentan los equipos con algún software antivirus?					
¿Las unidades de disquete y CD instalados en los equipos están habilitadas? ¿Es necesario?					
¿Existe algún procedimiento para revisar los diskettes contra virus antes de bajar la información al disco duro o a la red?					
¿Existen procedimientos que aseguren que el antivirus se encuentra actualizado?					
¿Existen pistas de auditoría sobre la información crítica o sensible de la empresa, que permita la reconstrucción de transacciones y donde se pueda observar el tipo de movimiento realizado, la fecha, hora y usuario, como mínimo?					
¿Se revisan periódicamente estas pistas de auditoría?					
¿Existen tablas de autorización que restrinjan el acceso a un nivel determinado del sistema?					
¿Existen procedimientos contra la alteración no autorizada de información con fines propios?					
¿Se cuenta con acceso a Internet?					
¿Existen políticas sobre el uso de Internet por parte de los empleados?					
¿Existen controles para resguardar la información de la organización, en caso de utilizarse acceso a Internet?					
¿Se restringe el acceso a diferentes sitios de ocio en Internet?					

CONTINGENCIAS

EMPRESA:	**FECHA:**
ENTREVISTADO:	**PUESTO:**
REALIZADO POR:	

PREGUNTA	SI	NO	N / A	Observaciones	REF.
¿Cuenta la empresa con un plan de contingencias?					
¿Se le han realizado pruebas del plan de contingencias?					
¿Fue corregido el plan de contingencias después de las pruebas?					
¿El plan de contingencias es conocido por todo el personal y puede ser puesto en práctica?					
¿Existen procedimientos formales (por escrito y con visto bueno) para la realización de respaldos de información y para la recuperación de los datos de ser necesario?					
¿Se hacen pruebas de recuperación de datos con regularidad y se documentan?					
¿Se han identificado los datos que deben ser respaldados y la periodicidad con que deben respaldarse?					
¿Los medios usados para respaldar datos se encuentran identificados adecuadamente?					
¿Existe un lugar definido para guardar los respaldos, que cumpla con las medidas de seguridad mínimas (control de acceso, temperatura ambiente, etc)?					
¿Existe un inventario de los medios de respaldo el cual tenga como mínimo número del medio, fecha de compra, estado?					
¿Cuentan con una bitácora manual o electrónica que contenga entre otros elementos de control: número de medio de respaldo, tipo de medio, ruta de los datos, tipo de datos, resultado del respaldo, fecha, hora, hecho por y período de retensión.					
¿Existe algún contrato para resguardar la información de la empresa fuera de ella, como por ejemplo con algún banco?					
¿Existe algún procedimiento formal para el traslado de respaldos fuera de la empresa?					

¿Se ha establecido algún lugar, que pueda servir como centro de cómputo alterno?					

DESARROLLO DE SISTEMAS

EMPRESA:	**FECHA:**
ENTREVISTADO:	**PUESTO:**
REALIZADO POR:	

PREGUNTA	SI	NO	N / A	Observaciones	REF.
¿Se han establecido políticas para el desarrollo de sistemas?					
¿Existen procedimientos formales para la solicitud de nuevos sistemas?					
¿Existe documentación de sistemas?					
• Estudios de factibilidad.					
• Estudios de Costo – Beneficio.					
• Diagramas de flujos de datos.					
• Diagramas de Entidad – Relación.					
• Manuales técnicos.					
• Manuales de usuario.					
• Manual de operación.					
• Códigos fuentes.					
¿Existen procedimientos para el control de modificaciones de las aplicaciones?					
¿Existen parámetros definidos para las pruebas de sistemas (parámetros de entrada, valores mínimos y máximos, etc)?					
¿Las planificación de pruebas es formal y existe documentación de los resultados de éstas?					
¿En la aceptación de las pruebas participa el usuario y el comité de sistemas?					
¿Todos los sistemas que se desarrollan cuentan con ayuda en línea?					
¿Se establecen en el desarrollo de sistemas pistas de auditoría y bitácoras de acceso?					
¿Existen políticas para el mantenimiento de sistemas?					
¿Se cuenta con planes para capacitar al personal usuario?					

¿Se tiene establecido algún lugar y equipo para capacitar a los usuarios?					
¿Se definen con anterioridad los períodos para mantener un paralelo entre el sistema actual y el nuevo?					
¿Existe documentación de los resultados de las pruebas en paralelo?					
¿Existe algún estudio posterior para valorar los costos y beneficios estimados contra los reales?					

3.3.4.1.3 CHECKLIST

PARA IDENTIFICAR LAS NECESIDADES DE SERVICIOS EN SEGURIDAD Y AUDITORIA DE SISTEMAS

Nombre del Cliente (Empresa): _____

1. TALENTO HUMANO ASIGNADO A LA FUNCIÓN DE SISTEMAS DE INFORMACIÓN.

1.1 CANTIDAD DE PERSONAS EN EL ÁREA DE SISTEMAS: _____

1.2 PERFIL DEL PERSONAL DE SISTEMAS.

PERFIL	CANTIDAD
TECNÓLOGOS EN SISTEMAS	
INGENIEROS DE SISTEMAS	
ESPECIALISTAS EN TELECOMUNICACIONES.	
OTROS (INDIQUE)	

2. PLATAFORMAS DE HARDWARE Y SOFTWARE UTILIZADAS.

PLATAFORMA	DESCRIPCIÓN
SISTEMAS OPERACIONALES	
MOTORES DE BASES DE DATOS	
OTRAS HERRAMIENTAS DE DESARROLLO	
SOFTWARE DE RED.	
EQUIPOS ACTIVOS DE LA RED	
INTERNET	
INTRANET	
EXTRANET	

SERVIDORES DE CORREO ELECTRÓNICO	
FIREWALLS	
SERVIDORES DE ARCHIVO	
MAINFRAMES	
MINICOMPUTARES	
MICROCOMPUTADORES	
E-BUSINESS	
BUSINESS INTELLIGENCE	
DATA WAREHOUSE	
OTRAS (INDIQUE)	

3. SISTEMAS DE INFORMACIÓN ERPS (ENTERPRISE RESOURCE PLANNING) QUE UTILIZA LA EMPRESA.

NO	NOMBRE DEL ERP	MÓDULOS COMPONENTES

4. PORTAFOLIO DE APLICACIONES O MÓDULOS DE SISTEMAS DE INFORMACIÓN ERPS QUE ESTÁN EN DESARROLLO O IMPLANTACIÓN Y SU IMPORTANCIA PARA LA EMPRESA.

NO	NOMBRE DE LA APLICACIÓN	IMPORTANCIA PARA LA EMPRESA (1)	HERRAMIENTA DE DESARROLLO UTILIZADA	POSEEN PROGRAMAS FUENTES ? (2)

(1) IMPORTANCIA PARA LOS OBJETIVOS DE LA EMPRESA. UTILICE UN NUMERO ENTRE 1 Y 5 (1: LA MENOR IMPORTANCIA; 5: LA MAYOR IMPORTANCIA).

(2) CONTESTE SI O NO.

5. LAS ACTIVIDADES DE PROCESAMIENTO DE DATOS QUE SE REALIZAN EN LA EMPRESA.

No	Descripción	Marque con X
1	Grabación (captura de Datos)	
2	Control de Entradas y Salidas.	
3	Producción de información (Procesamiento y actualización de archivos).	
4	Help Desk.	
5	Soporte a usuarios de microcomputadores y LANs.	
6	Mantenimiento de hardware.	
7	Administración de bases de datos (DBA)	
8	Administración de la Seguridad lógica (controles de acceso)	
9	Planeación estratégica de sistemas.	
10	Administración de contratos de terceras partes.	
11	Definición e implementación de políticas de seguridad corporativas.	2 ( )
12	Análisis y Diseño de Sistemas.	2 ( )
13	Construcción de Programas (Elaboración de programas de computador).	2 ( )
14	Mantenimiento de Software Aplicativo	2 ( )
15	Administración de Telecomunicaciones.	2 ( )
16	Quality Assurance.	2 ( )
17	Otras.	2 ( )

7 SERVICIOS DE PROCESAMIENTO DE DATOS QUE SON CONTRATADOS CON TERCEROS.

No	Descripción	Marque con X
1	Mantenimiento de hardware.	
2	Administración de los Centros de Procesamiento de Datos	
3	Grabación de Datos	
4	Planeación estratégica de sistemas.	
5	Interventoría de proyectos de sistemas.	
6	Planeación de Contingencias en Sistemas de Información.	
7	Análisis y Diseño de Sistemas.	
8	Programación de aplicaciones.	
9	Mantenimiento de Software Aplicativo	
10	Administración y soporte técnico en Telecomunicaciones.	
11	Quality Assurance (Aseguramiento de calidad).	
12	Seguridad en Sistemas de Información.	
13	Otras (indíquelas).	

8. MÓDULOS COMPONENTES DEL SISTEMA DE INFORMACIÓN COMERCIAL (DILIGENCIAR ÚNICAMENTE EN EMPRESAS DE SERVICIOS PÚBLICOS)

No	Descripción	Marque con X
1	Facturación.	
2	Recaudos	
3	Solicitudes de Servicios	
4	Atención al Suscriptor	
5	Medidores	
6	Financiación de servicios y de deuda	
7	Control de Perdidas y Fraudes	
8	Cartera	
9	Enlace Financiero	
10	Seguridad y Administración del sistema	
11	Estadísticas	
12	Auditoria de Sistemas	
13	Administración de Parámetros Generales	
14	Facturación en sitio	
15	Otros (especifique)	

9. SERVICIOS DE CONTROL INTERNO Y SEGURIDAD DE SISTEMAS QUE UD. SOLICITA (QUE SON DE SU INTERÉS.)

No	Descripción	Marque con X
1	Asesoría para implantación de estándar COBIT (Control Objectives for Information and Related Technology).	
2	Diseño e implantación de Controles en operaciones de negocio que se soportan en Sistemas de Información (Aplicaciones de Computador).	
3	Diseño e implantación del Plan de Acción de Prevención y Mitigación de Riesgos (Mapas de Riesgo).	
4	Diseño e implantación de controles en el Desarrollo de Sistemas (especifique)	
5	Aseguramiento de Calidad del Software	
6	Aseguramiento de Calidad de Bases de Datos	
7	Elaboración e Implantación del Plan de Continuidad (Contingencias) en Sistemas de Información.	
8	Ejecución de pruebas de software	
9	Asesoría para implantar AUDICONTROL (Metodología Asistida por computador para Diseño de Controles y Administración de Riesgos en Sistemas de Información).	
10	Capacitación en Controles y Seguridad en Sistemas de Información.	
11	Definición de Políticas, Estándares y Procedimientos de Seguridad en Tecnología de Información	
12	Otros (Especifique)	

10. SERVICIOS DE AUDITORIA DE SISTEMAS QUE UD. SOLICITA (QUE SON DE SU INTERÉS).

No	*Descripción*	Marque con X
1	Auditoria a la Organización y Funcionamiento de la Informática de la Empresa (Auditoria de Controles Generales de Sistemas de Información)	
2	Auditoría de Sistemas ERPs y Aplicaciones en Producción	
3	Auditoria al Sistema de Información Comercial (Únicamente para empresas de Servicios Públicos)	
4	Auditoría al Desarrollo de Sistemas (especifique)	
5	Auditoria al Plan de Contingencias de Sistemas de Información (Continuidad del Negocio)	
6	Desarrollo de Software de Auditoria (Especifique)	
7	Organización e Implantación de la Auditoría de Sistemas.	
8	Asesoría para la adquisición de Software de Auditoría	
9	Capacitación en Auditoría de Sistemas.	
10	Asesoría para implantar el enfoque de Auditoría de Sistemas Orientada al Riesgo.	
12	Asesoría para implantar AUDAP (Metodología Asistida por Computador para auditoría orientada al riesgo en Operaciones de Negocio Automatizadas).	
13	Asesoría para implantar el software IDEA (Interactive Data Extraction and Analysis).	
14	Otros – Especifique	

11. PERIODICIDAD DE LOS SERVICIOS DE AUDITORIA DE SISTEMAS SOLICITADOS.

No	*Descripción*	Marque con X
1	Por una sola vez (trabajo puntual).	
2	Por periodos Anuales	
3	Asesoría Permanente	
4	Otro – Especifique	

3.3.5. PAPELES DE TRABAJO

En éste punto el auditor registrará los procedimientos aplicados, pruebas desarrolladas, información obtenida y las conclusiones relacionadas con el trabajo de auditoría, también obtendrá información por medio de cintas, videos, backup de bases de datos u otros instrumentos que le sirvan de evidencia suficiente y competente para sustentar el informe de auditoría que contiene los hallazgos encontrados en la ejecución del trabajo. Los papeles de trabajo se elaborarán de acuerdo al tamaño, complejidad y circunstancias de cada auditoría, asimismo los resguardará el tiempo que sea necesario. Los papeles de trabajo se estructuran de la forma siguiente: nombre del cliente, nombre de la cédula, período cubierto, descripción del contenido, firma de quien lo preparó, la fecha de preparación, el código del índice, fecha y firma de quién los revisó y el número de columnas que sean necesarias en los mismos. Se debe establecer un índice de papeles de trabajo asignándoles una codificación numérica, alfabética o alfanumérica. Los papeles de trabajo se deben referencias en forma cruzada enviando información por la derecha y recibiendo información por la izquierda, indicando con claridad el trabajo de auditoría realizado, es decir, que éstos incluyan suficiente información para cumplir con los objetivos para los cuales fueron diseñados. Las anotaciones que se realicen en los papeles de trabajo serán

por medio de marcas que son símbolos escrito adyacentes a los detalles en el cuerpo de las cédulas. También se deben expresar en forma clara las conclusiones que el auditor llega a establecer sobre el área o componente de auditoría que éste realice.

3.3.5.1. ARCHIVOS DE PAPELES DE TRABAJO

El contenido de los papeles de trabajo varía de un auditor a otro, lo mismo sucede con la forma de concentrar los papeles de trabajo, sin embargo estos deben ser integrados siguiendo los lineamientos establecidos por el socio de la firma de auditoria. (Ver anexo 6).

3.3.5.2. ÍNDICE DE REFERENCIACIÓN

En éste ítem el auditor formulará la referenciación relacionado con las áreas examinadas, a fin de identificar los papeles de trabajo, facilitar su búsqueda y en caso de ejecutar la auditoría en forma manual referenciarlos a lápiz y de color rojo. El índice de referenciación en la práctica comúnmente se realiza en forma alfanumérica, asignando una letra o doble letra, números y números y letras. Esto dependerá de las necesidades o preferencias de la firma de auditoría o del auditor responsable de la misma. La única condición es que sea una presentación ordenada y que se identifiquen claramente las páginas y contenido. (Ver ejemplo de éste tipo de índices

aplicado a una auditoría en un ambiente de sistemas computacionales en anexo 7)

3.3.5.3. MARCAS Y NOTAS DE AUDITORÍA

En éste punto el auditor formulará las marcas de revisión que considere convenientes, con el propósito de dejar constancia de los procedimientos ejecutados en los papeles de trabajo. Las marcas son símbolos y distintivos que hace el auditor para señalar el tipo de trabajo o prueba efectuada. Estas marcas se encuentran en los papeles de trabajo. Además, cada firma de auditoría, crea las marcas a su gusto y conveniencia, dándoles el significado apropiado para su comprensión. Las notas del auditor sirven para registrar la información suficiente de ciertos asuntos que debe recordar para beneficio propio y del examen realizado.(Ver anexo No.8).

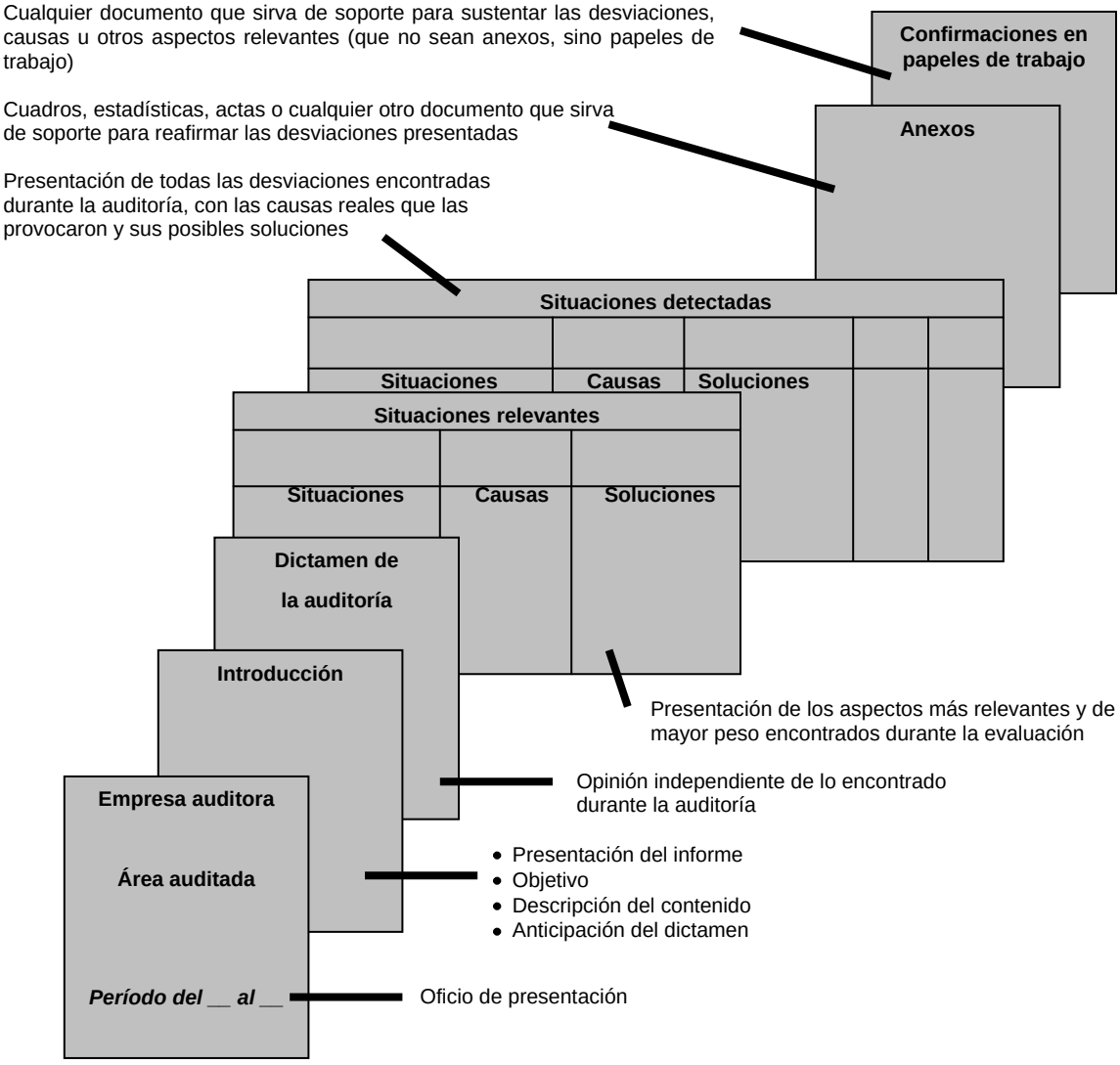
3.3.5.4. INFORME

En ésta etapa el auditor elaborará el informe de auditoría siendo el producto final de su trabajo, el cual contendrá el desarrollo de los hallazgos sobre aspectos de seguridad , de control interno del área de sistemas y aspectos relacionados, que resulten como producto de la aplicación de los procedimientos de auditoría, asimismo presentará conclusiones y recomendaciones para subsanar las deficiencias obtenidas.

El auditor del área de sistemas generalmente prepara el informe de auditoría con la estructura siguiente: portada, índice, introducción, encabezado, objetivos de la auditoría, áreas a auditar, alcance y limitaciones del trabajo, desarrollo de hallazgos, comentarios de la administración, conclusiones, recomendaciones, fecha, firma del auditor y anexos.

Este es un documento formal que utiliza el auditor de sistemas para informar por escrito y de manera oportuna, precisa, completa, sencilla y clara, sobre los resultados que obtuvo después de haber aplicado las técnicas, métodos y procedimientos apropiados al tipo de revisión que realizó, para fundamentar con ellos su opinión respecto a la auditoría realizada y estar en condiciones de poder emitir un dictamen correcto sobre el comportamiento del sistema, sobre los empleados del área de sistemas y sobre los resultados obtenidos de su operación normal, a fin de que el alto funcionario del cliente que reciba el informe conozca la situación real del área de sistemas auditada.

CONTENIDO DEL INFORME DE AUDITORÍA DE SISTEMAS COMPUTACIONALES:



CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Las auditorias financieras y fiscales son las principales áreas en el que generalmente se desenvuelven los auditores independientes, esto debido a la obligatoriedad legal y normativa de su aplicación. Por otra parte la auditoria informática o de sistemas es un tipo de auditoria especial que no esta legalmente regularizada para las empresas en general, lo que implica poco interés por parte de éstas, debido a lo anterior, ésta presenta un nivel mínimo de demanda.

- Para el desarrollo de una auditoria de sistemas, generalmente las empresas utilizan o emplean a un experto en informática para que lleve a cabo una evaluación de tipo operativa de los sistemas, el cual, en la mayoría de los casos no posee los lineamientos técnicos y normativos propios de los auditores.

- La auditoria en informática por su complejidad es realizada en su mayoría por las grandes firmas y consultoras, lo que no le permite que el auditor independiente tenga la posibilidad de desenvolverse en esta área con facilidad, debido a que no posee los recursos y especializaciones necesarias que tienen las grandes firmas de auditoria.

- La importancia que conlleva realizar una auditoria de sistemas en una empresa que procesa su información financiera mediante un sistema contable computarizado es

vital para su buen funcionamiento, ya que se pretende detectar posibles debilidades de los sistemas, con el objetivo de ayudar a minimizar riesgos en cuanto al manejo de la información y lograr finalmente que la información generada por los sistemas contables sea integra, confiable y oportuna.

- La confiabilidad de los sistemas contables computarizados depende principalmente del recurso humano capacitado y de los controles adecuados encaminados a minimizar riesgos de la seguridad física y lógica, controles que se evalúan mediante la realización de una auditoria de seguridad informática, la cual contribuye a verificar el grado de confiabilidad que tiene la información que se procesa en un sistema contable computarizado.

4.2. RECOMENDACIONES

- Los auditores independientes deben considerar como parte de su plan de educación continuada, el mantener actualizados los conocimientos técnicos en el área de sistemas, lo que les permitiría ser mas competitivos en el mercado de servicios de auditoria de sistemas contables computarizados.

- Los auditores independientes 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.

- 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 auditoría aplicando criterios y lineamientos técnicos y normativos propios de su formación y capacidad profesional son los auditores.

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

GLOSARIO

Alcance:

Se refiere a los procedimientos de auditoria considerados necesarios en las circunstancias para lograr el objetivo de la auditoria.

Ambiente de control:

El entorno de control comprende la actitud total, la conciencia y acciones de los directores y administración respecto del sistema de control interno y su importancia en al entidad.

Auditoria de Sistemas:

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes.

Antivirus:

Programa encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca.

Archivo:

Conjunto de Bytes relacionados y tratados como una unidad. Un programa puede contener programas, datos o ambas cosas.

Bases de Datos:

Una colección de datos que se comparte y usa por un número de diferentes usuarios para diferentes propósitos.

Backup:

Copia de seguridad que se realiza con el fin de mantener los datos en forma segura.

Bit:

En informática, unidad mínima de información

Bug:

Un error en un programa o equipo. Se habla de bug si es un error de diseño cuando la falta es provocada por otro motivo.

Byte:

Combinación de Bits. En la representación más común 8 bits forman un byte

Certeza (Seguridad):

Se refiere a la satisfacción del auditor respecto de la confiabilidad de una aseveración hecha por una de las partes, para ser usada por otra de las partes.

Cookie:

Es un pequeño trozo de información enviado por un servidor de Web al sistema de un usuario.

Correo electrónico:

Aplicación que permite enviar mensajes a otro usuario de la red sobre la que este instalado. También denominado **E-Mail.**

Cortafuegos:

Ver Firewall

Cracker:

Persona que quita la protección a programas con sistemas anticopia. Hacker maligno, que se dedica a destruir información.

Conocimiento del negocio:

Conocimiento general del auditor de la economía y la industria dentro de la cual opera la entidad y un conocimiento más particular de cómo opera la entidad.

Controles de aplicación en sistemas de información por computadora:

Los controles específicos sobre las aplicaciones contables relevantes mantenidas por la computadora. El propósito de los controles de aplicación es establecer procedimientos específicos de control sobre las aplicaciones contables para brindar una seguridad razonable de que todas las transacciones se autorizan, y se procesan por completo, con precisión y oportunidad.

Criptografia:

Ciencia que consiste en transformar un mensaje inteligente en otro que no lo es, mediante la utilización de **claves**, que solo el emisor y receptor conocen.

Controles de calidad:

Las políticas y procedimientos adoptados por una firma para proporcionar razonable seguridad de que todas las auditorias hechas por la firma se llevan a cabo de acuerdo a los objetivos

y principios básicos que gobiernan una auditoría, según se expone en las NIAS.

Controles generales en los sistemas de información por computadora:

El establecimiento de un marco de referencia para un control global sobre las actividades de los sistemas de información por computadora, para proporcionar un nivel razonable de seguridad de que los objetivos globales del control interno se logren.

Dictamen:

El dictamen del auditor contiene una clara expresión de opinión escrita sobre los resultados obtenidos al evaluar la seguridad de los sistemas contables computarizados como un todo.

Documentación:

Es el material (papeles de trabajo) preparado por y para, u obtenido o retenido por el auditor en conexión con el desempeño de la auditoría.

Experto:

Es una persona o firma que posee la habilidad, conocimiento y experiencia especiales en un campo particular distinto al de la contabilidad y auditoría.

Fake Mail:

Envía correos falseando el remitente.

Firma de auditoría:

Se considera firma de auditoría a toda entidad, "ya sean los socios de una firma (sociedad o persona jurídica) que proporciona servicios de auditoría o un auditor independiente que proporciona servicios de auditoría, según sea apropiado".

Firewall:

Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los limites entre dos o mas redes y restringe la entrada y salida de la información.

Fraude:

Se refiere a un acto intencional por uno o más individuos dentro de la administración, empleados, o terceras partes, el cual da como resultado una representación errónea de los estados financieros.

Guía:

Libro, folleto con datos, explicaciones o normas de una determinada materia, para información del usuario.

Gusano:

Programa ilegitimo que es capaz de reproducirse a si mismo infinitas veces hasta colapsar el sistema, en el que se esta ejecutando.

Hacker:

Una persona que disfruta explotando los detalles de las computadoras y de cómo extender sus capacidades.

Hardware:

Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

Incumplimiento:

Se usa para referirse a actos de omisión o comisión por parte de la entidad que está siendo auditada, ya sea en forma intencional o no intencional, y que son contrarios a las leyes y reglamentos vigentes.

Inspección:

Consiste en examinar registros, documentos o activos tangibles.

Internet:

Sistema de redes de computación ligadas entre si, con alcance mundial, que facilita servicios de comunicación de datos como registros remotos, transferencia de archivos, correos electrónicos y grupos de noticias.

Intruso:

Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

Investigación:

Consiste en buscar información de personas conocedoras dentro o fuera de la entidad.

Limitación sobre alcance:

A veces puede imponerse por parte de la entidad una limitación al alcance del trabajo del auditor. Las circunstancias pueden imponer una limitación al alcance. También puede darse cuando, según opinión del auditor, los registros contables de la entidad son inadecuados o cuando el auditor no puede llevar a cabo un procedimiento de auditoría considerado deseable.

Login:

Nombre de acceso de un usuario a una red o sistemas multiusuarios. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password) para tener acceso al sistema.

Normas:

Reglas que se deben seguir: "normas de corrección". Modelo a que se ajusta un trabajo

Normas nacionales (de auditoría):

Conjunto de normas de auditoria definidas por leyes gubernamentales o por un organismo con autoridad a nivel del país, cuya aplicación es obligatoria en la conducción de una auditoria o servicio relacionado y que deberían ser cumplidas en la conducción de una auditoria o servicios relacionados.

Observación:

Consiste en estar presente durante todo o parte de un proceso desempeñado por otros.

Papeles de trabajo:

Pueden ser en forma de datos almacenados en papel, película, medios electrónicos u otros medios.

Password:

(Clave), Contraseña

Planeación:

Significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperados de la auditoria. El auditor planea desempeñar la auditoría en manera eficiente y oportuna.

Población:

Es todo el conjunto de datos sobre los cuales desea el auditor hacer el muestreo para alcanzar una conclusión.

Procedimientos de control:

Son aquellas políticas y procedimientos además del ambiente de control que la administración ha establecido para lograr los objetivos específicos de la entidad.

Procedimientos sustantivos:

Son pruebas realizadas para obtener evidencia de auditoría para detectar representaciones erróneas sustanciales en los sistemas contables.

Programa de auditoría:

Expone la naturaleza, tiempo y grado de los procedimientos de auditoría planeados que se requieren para implementar el plan de auditoría global. Sirve como un conjunto de instrucciones para los auxiliares involucrados en la auditoría y como un medio para controlar la ejecución apropiada del trabajo.

Prueba de rastreo:

Implica seguir la pista a algunas transacciones dentro del sistema contable

Pruebas de control:

Se realizan para obtener evidencia de auditoría sobre la efectividad del diseño de los sistemas de contabilidad y de control interno, o sea, si están diseñados apropiadamente para prevenir o detectar y corregir representaciones erróneas sustanciales; y operación de los controles internos a lo largo del período.

Riesgo de auditoría:

Es el riesgo que el auditor atribuye a una opinión de auditoría inapropiada

Riesgo de control:

Es el riesgo de que una representación errónea que pudiera ocurrir, no sea prevenido o detectado y corregido oportunamente por los sistemas de contabilidad y de control interno.

Riesgo de detección:

Es el riesgo de que los procedimientos sustantivos de un auditor no detecten una representación errónea y que pudieran ser de relativa importancia.

Riesgo inherente:

Refleja la probabilidad de que pueda existir una pérdida material en alguna de las partes a auditar antes de que se considere la fiabilidad de los controles internos. En el caso de los sistemas contables computarizados tienen un alto riesgo inherente porque suelen tener un cierto grado de complejidad.

Sistema de contabilidad:

Es la serie de tareas y registros de una entidad por medio de los cuales se procesan las transacciones como un medio para mantener los registros financieros. Dichos sistemas identifican, agrupan, analizan, calculan, clasifican, registran, resumen y reportan las transacciones y otros eventos.

Sistema de control interno:

Consiste en todas las políticas y procedimientos (controles internos) adoptados por la administración con el fin asegurar hasta donde sea posible, la conducción ordenada y eficiente de su negocio, incluyendo adhesión a las políticas de la administración, la conservación de los activos, la prevención y detección de fraude y error

Sistema de información por computadora (SIC):

Existe un entorno de sistemas de información por computadora (SIC), cuando está involucrada una computadora de cualquier tipo o tamaño, en el procesamiento por parte de la entidad de la información financiera de importancia para el auditor, ya sea que la computadora sea operada por la entidad o por terceras partes.

Software:

Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de maquinas

Unidad de muestreo:

Las partidas individuales que componen la población.

UNIX:

Sistema operativo utilizado por la gran mayoría de maquinas de Internet.

BIBLIOGRAFIA

LIBROS DE CONSULTA

BERNAL T. CESAR AUGUSTO
METODOLOGIA DE LA INVESTIGACION PARA ADMINISTRACION Y ECONOMIA
EDITORIAL NOMOS, S. A,
Colombia, 2000.

BENSON, CHRISTOPHER
ESTRATEGIAS DE LA SEGURIDAD
INOBIS CONSULTING Pty Ltd. Microsoft
Noviembre 2000

HERNANDEZ SAMPIERI, ROBERTO
METODOLOGIA DE LA INVESTIGACION
EDITORIAL MacGRAW-HILL, Segunda edición
Colombia, 2001.

INSTITUTO MEXICANO DE CONTADORES PÚBLICOS
NORMAS INTERNACIONALES DE AUDITORIA
México, 2003.

LUCENA LOPEZ, MANUEL JOSE
CRIPTOGRAFIA Y SEGURIDAD EN COMPUTADORAS
UNIVERSIDAD DE JAEN. TERCERA EDICION.
España, 2001.

MELGAR, O. ARMANDO, GUARDADO QUINTANILLA
ORIGEN Y EVOLUCIÓN DE LA CONTADURÍA PÚBLICA EN EL SALVADOR
Investigación 2001, Abril 2002.

MUÑOZ RAZO, CARLOS
AUDITORIA EN SISTEMAS COMPUTACIONALES
PEARSON EDUCATION.
México, 2002.

NOMBELLA, JUAN JOSE
SEGURIDAD INFORMATICA
EDITORIAL PARANINFO.
España, 2001.

RAMOS, MIGUEL ANGEL
AUDITORIA DE LA SEGURIDAD
UNIVERSIDAD CARLOS III de MADRID.
España, 2000.

ROJAS SORIANO, RAUL
GUIA PARA REALIZAR INVESTIGACIONES SOCIALES
PLAZA Y VALDES EDITORES, 30ª Edición
México, 1998.

RODRIGUEZ, CLAUDIO
SEGURIDAD INFORMATICA. MECANISMO DE CONTROL Y AUDITORIA ORIENTADOS A GARANTIZAR LA SEGURIDAD DE LOS PROCESOS Y DE DATOS.
EDICION VIRTUAL
Chile, 1999.

PÁGINAS EN INTERNET CONSULTADAS

http://www.geocities.com/Isialer/NotasInteresantes.htm

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

http://www.monografias.com/trabajos/maudisist/maudisist.shtml

http://www.seguridata.com

http://www.kriptopolis.com

http://www.seguridadcorporativa.org

ANEXOS

ANEXO N°1

TABULACION Y ANALISIS DE RESULTADOS

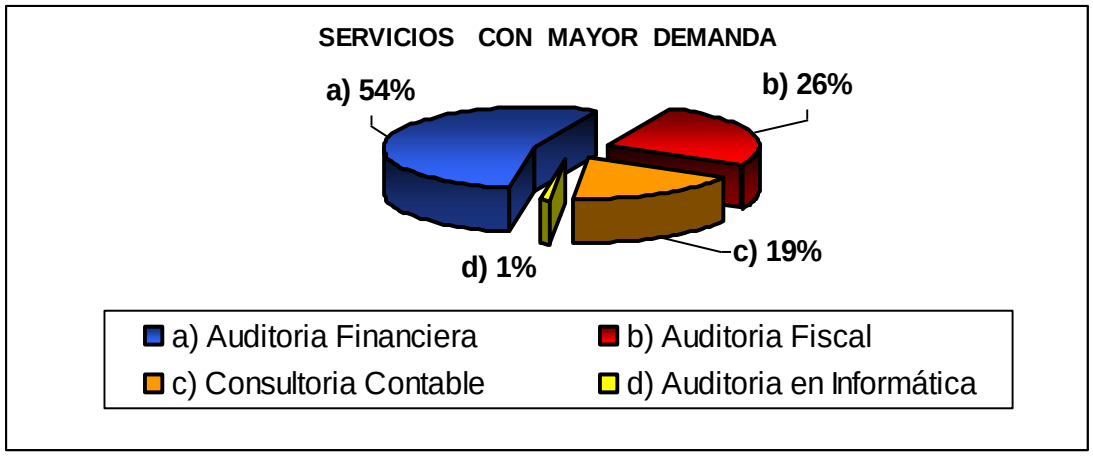
PREGUNTA N° 1

En orden de importancia por la demanda, ¿Cuáles de los siguientes servicios tiene mayor demanda en el mercado?

Objetivo de la pregunta:

Conocer por su importancia, que tipo de auditorias tiene mayor demanda en el mercado.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Auditoria financiera	43	54 %
b) Auditoria fiscal	21	26 %
c) Consultoría Contable	15	19 %
d) Auditoria en informática	1	1%
TOTAL	**80**	**100%**



Análisis:

En lo que se refiere a principales servicios que los clientes demandan de los auditores independientes, se obtuvo que los más significativos son Auditaría Financiera con 54% en promedio, Auditoria Fiscal con 26%, servicios contables con 19% en promedio y la Auditoria en Informática con 1% en promedio, constituyéndose los primeros tres servicios en los más importantes, ya que suman el 99% del total y significan los ejes principales del quehacer de los auditores independientes. Muy distantes de los servicios anteriores se coloca la Auditoria en Informática con el 1% en promedio del total. Los resultados son normales respecto a los servicios tradicionales que brindan los auditores independientes pequeños, sin embargo, es necesario incorporar otros servicios que estén acordes a las exigencias de la época entre los que destaca la Auditoria en Informática.

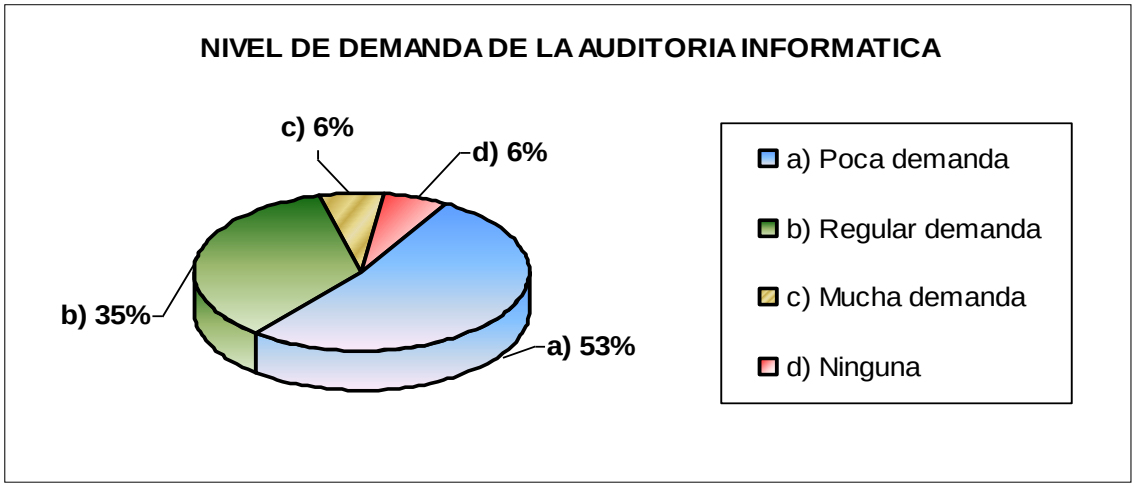
PREGUNTA N° 2

¿Qué nivel de demanda considera usted que tiene la Auditoria en Informática?

Objetivo de la pregunta:

Determinar el grado de demanda que tiene la Auditoria en Informática.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Poca demanda	42	53 %
b) Regular demanda	28	35 %
c) Mucha demanda	5	6%
d) Ninguna	5	6%
TOTAL	**80**	**100%**



Análisis:

Según el cuadro anterior, los resultados obtenidos indican que del total de 80 auditores independientes encuestados 42 de ellos equivalentes al 53%, consideraron que la Auditoria en Informática presenta poca demanda y 5 de ellos equivalentes al 6 %, manifiestan que el este servicio no presenta ningún nivel de demanda. Lo anterior evidencia la importancia de apoyar con investigación académica que se encuentre enfocada en el desarrollo de herramientas técnicas para la Evaluación de la

Seguridad, en una Auditoria en Informática lo que les daría la posibilidad de mejorar la calidad y prestación de sus servicios.

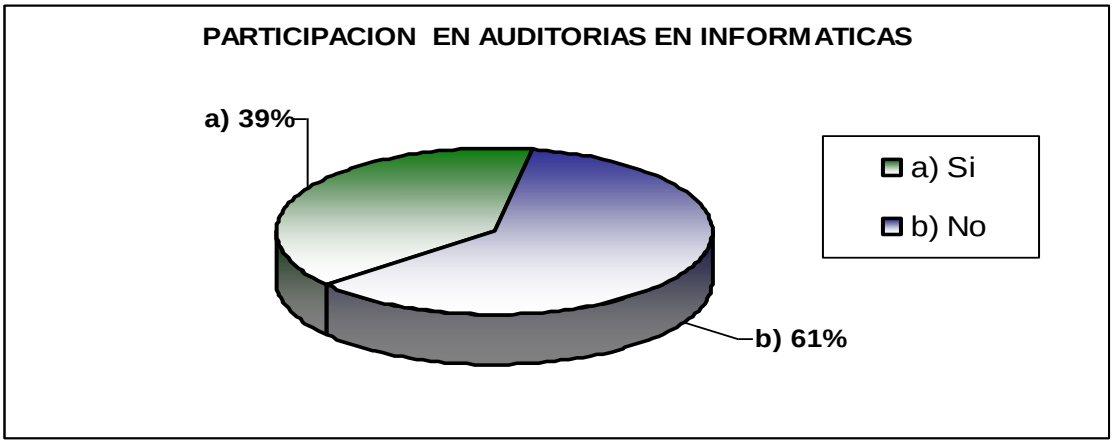
PREGUNTA N° 3

¿Cómo auditor ha participada en la realización de una Auditoria en Informática alguna vez?

Objetivo de la pregunta:

Conocer si el auditor ha tenido la iniciativa propia de participar en la realización de una Auditoria Informática.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Si	31	39 %
b) No	49	61%
TOTAL	**80**	**100%**



Análisis:

En cuanto a la participación en el desarrollo de una Auditoria en Informática, por parte de los auditores independientes un total de 49 personas equivalente al 61% del total respondió que no la han desarrollado y 31 personas equivalentes al 39% del total contestaron afirmativamente. Demostrando de esta forma que se le esta dando mayor importancia a la auditoria en informática.

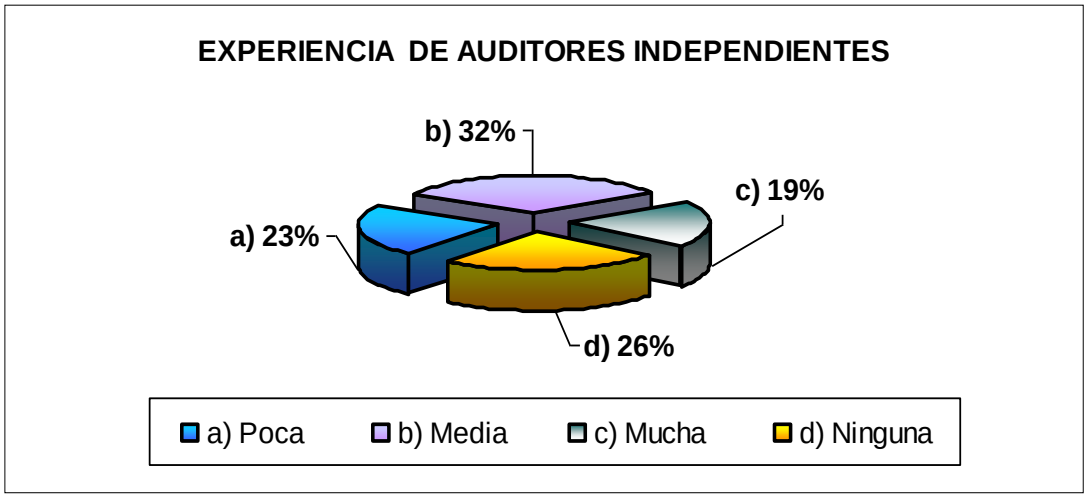
PREGUNTA N° 4

Si su respuesta a la pregunta anterior es afirmativa ¿Qué nivel de experiencia ha adquirido en la realización de dicha auditoria?

Objetivo de la pregunta:

Determinar el nivel de experiencia que ha adquirido un auditor, si ha participado en la realización de una Auditoria en Informática.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Poca	7	23 %
b) Media	10	32 %
c) Mucha	6	19 %
d) Ninguna	8	26%
TOTAL	**31**	**100%**



Análisis:

De los 80 auditores independientes encuestados, 10 de 31 respondieron que la experiencia adquirida al realizar dicha auditoria es media, conformando un 32%; en segundo lugar con el 26%, los auditores manifiestan no haber obtenido ningún tipo de experiencia. En cuanto a este tipo de Auditoria, de que manera han adquirido esos conocimientos afirmaron haberlos obtenido al involucrarse en los distintos eventos nacionales y regionales de la profesión que se desarrollan y que les ha permitido obtener una actualización continua de conocimientos para ofertar este tipo de servicios, además de estar incorporados a Asociaciones Profesionales de Contadores Públicos.

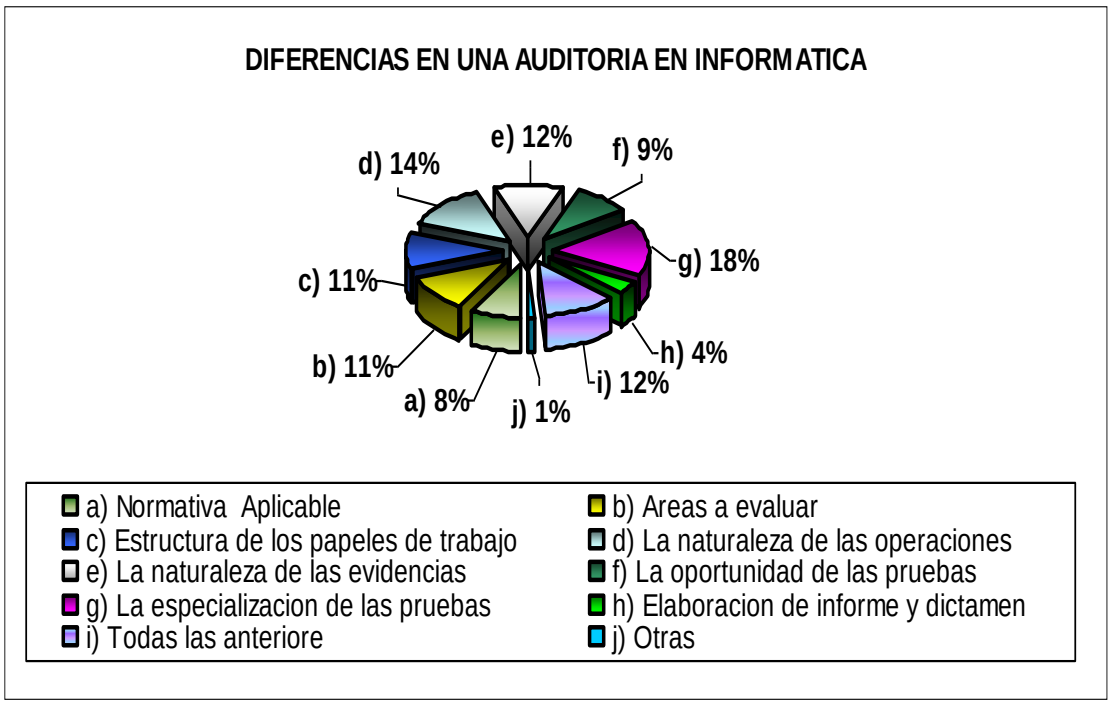
PREGUNTA N° 5

¿Qué diferencia piensa usted conlleva la realización de una auditoria en informática con respecto al resto de auditorias.

Objetivo de la pregunta:

Obtener el punto de vista del auditor independiente, que al ejecutar una auditoria en Informática de las posibles diferencias que se encuentran en dicha auditoria con relación a las demás.

CATEGORIA	FRECUENCIA					
	ABSOLUTA			RELATIVA		
a) Normativa Aplicable	14	66	80	8%	92%	100%
b) Áreas a Evaluar	19	61	80	11%	89%	100%
c) Estructura de los papeles de trabajo	19	61	80	11%	89%	100%
d) La naturaleza de las operaciones	23	57	80	14%	86%	100%
e) La naturaleza de las evidencias	20	60	80	12%	88%	100%
f) La oportunidad de las pruebas	16	64	80	9%	91%	100%
g) La especialización de las pruebas	28	52	80	18%	82%	100%
h) Elaboración de informe y dictamen	7	73	80	4%	96%	100%
i) Todas las anteriores	21	59	80	12%	88%	100%
j) Otras	2	78	80	1%	99%	100%
TOTAL	**169**	**631**	**800**	**100%**	**900%**	**1000%**



Análisis:

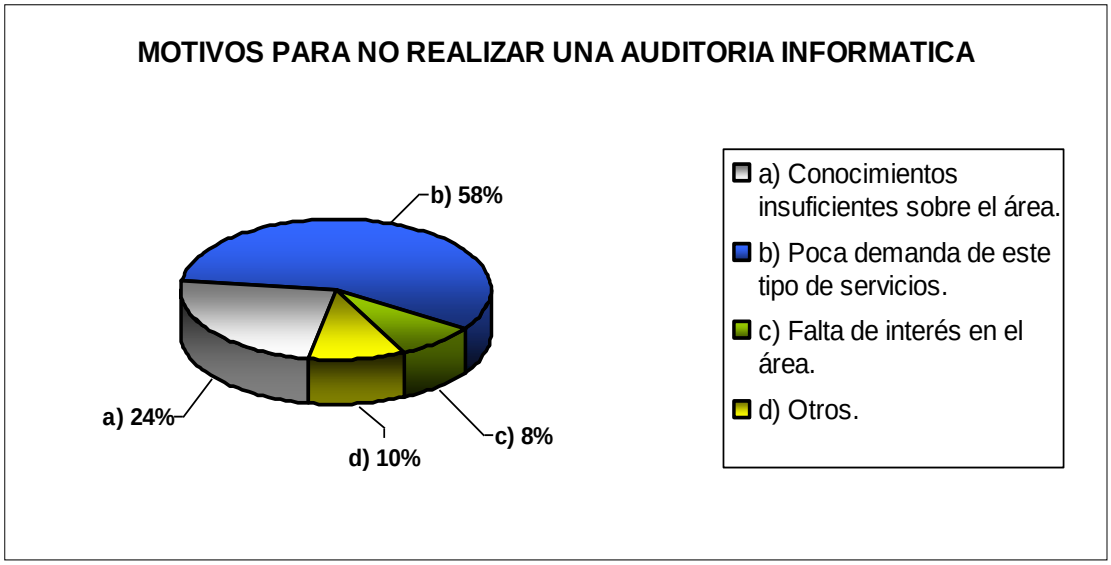
Es notorio que en la ejecución de una Auditoria en Informática los auditores independientes toman como diferencias más significativas la especialización de las pruebas, la naturaleza de las operaciones, la naturaleza de las evidencias y todas las anteriores., ya que un total de 18% y 14% respectivamente contestaron dar mayor énfasis a estas diferencias; en segundo lugar la naturaleza de las evidencias y todas las anteriores conformando un total de un 24%; Quedando el 44% que considera otro tipo de diferencias distintas a las anteriormente mencionadas.

PREGUNTA No.6

Si su respuesta a la pregunta No.3 es negativa, ¿Por que motivo no ha participado en una auditoría informática?

Objetivo de la pregunta:
Indagar sobre las posibles razones por las cuales el auditor independiente no ha efectuado alguna vez una auditoria informática.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Conocimientos insuficientes sobre el área.	12	24%
b) Poca demanda de este tipo de servicios.	28	58%
c) Falta de interés en el área.	4	8 %
d) Otros.	5	10 %
TOTAL	**49**	**100%**



Análisis:

La gran mayoría de auditores independientes (58%)opina que el motivo de no haber realizado alguna vez dentro de su campo profesional una auditoría informática es a causa de que la demanda de este tipo de servicio es mínimo, mientras que en segundo lugar (24%), la causal principal de no haber realizado es te tipo de auditoría es por falta de conocimiento y la capacitación suficiente del auditor, con lo cual se demuestra que existe un conocimiento insuficiente para efectuar este tipo de auditoría.

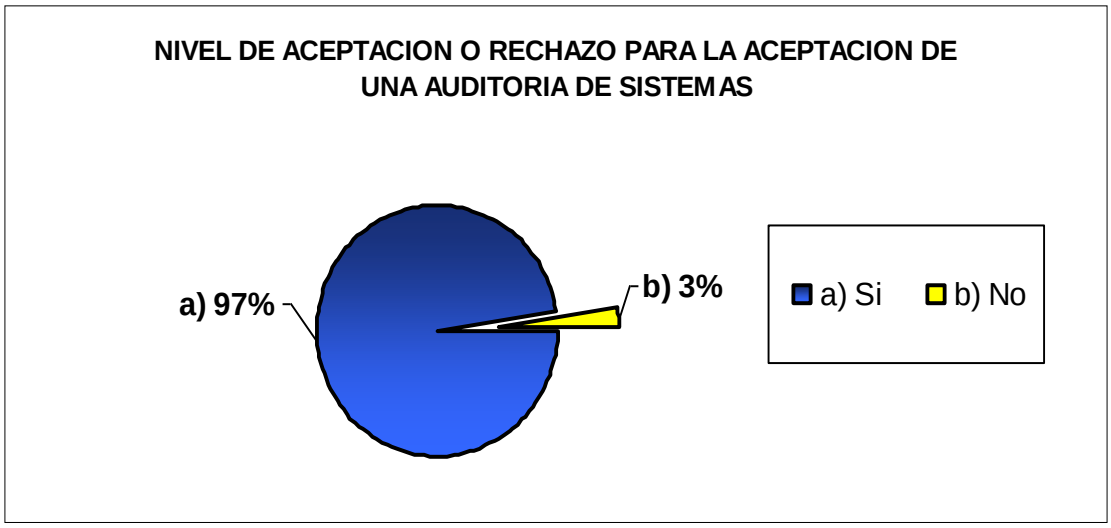
PREGUNTA No.7

¿Considera indispensable y de utilidad efectuar una auditoría de sistemas en aquellas empresas que procesan su información financiera mediante un sistema contable computarizado?

Objetivo de la pregunta:

Conocer el grado de importancia que tiene la realización de una auditoria de sistemas contables computarizados en las empresas que procesan su información financiera mediante un sistema contable mecanizado.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Si	78	97 %
b) No	2	3%
TOTAL	**80**	**100%**



Análisis:

La importancia que conlleva realizar una auditoria de sistemas en una empresa que procesa su información financiera mediante un sistema contable computarizado es de vital importancia, por lo cual casi el cien por ciento de los encuestados manifiesta que es una necesidad imperante realizar una auditoria de los sistemas contables computarizados.

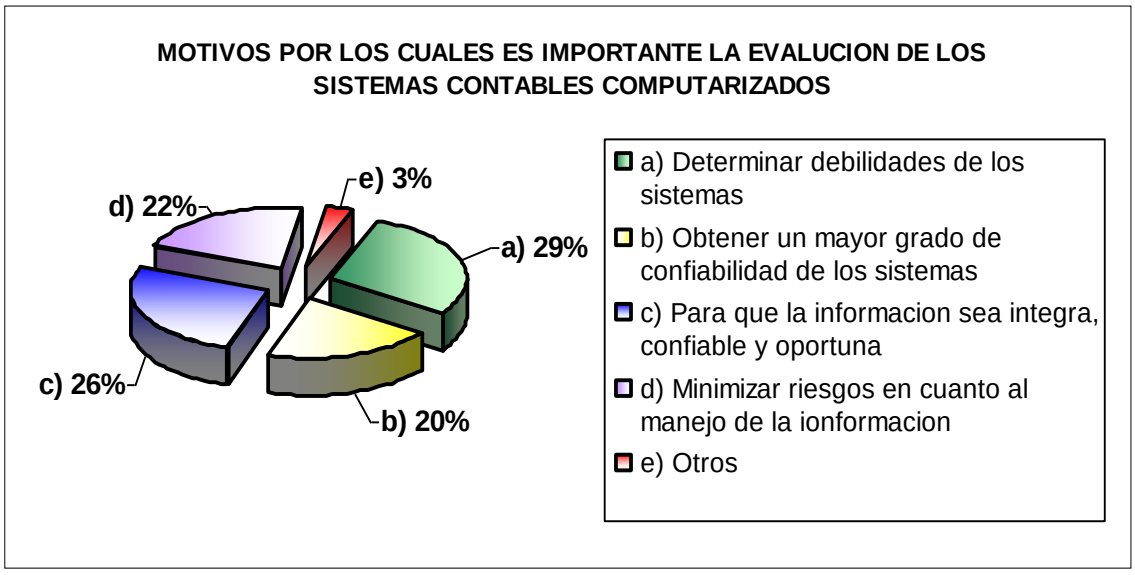
PREGUNTA No.8.

¿Por cual de los siguientes motivos consideraría Ud. que es importante la evaluación de la seguridad de los sistemas en una Auditoria en Informática?

Objetivo de la pregunta:

Conocer los principales motivos y el respectivo grado de importancia que consideran los auditores independientes debe considerarse en la evaluación de la seguridad en una auditoria informática.

CATEGORIA	FRECUENCIA					
	ABSOLUTA			RELATIVA		
a) Detectar debilidades de los sistemas	50	30	80	29 %	71%	100%
b) Obtener un mayor grado de confiabilidad de los sistemas.	34	46	80	20 %	80%	100%
c) Para que la información generada por los sistemas sea íntegra, confiable y oportuna.	45	35	80	26%	74%	100%
d) Minimizar riesgos en cuanto al manejo de la información	37	43	80	22%	78%	100%
e) Otros.	5	75	80	3%	97%	100%
TOTAL	**171**	**229**	**400**	**100%**	**400%**	**500%**



Análisis:

Uno de los principales motivos por los cuales se efectúa la evaluación de la seguridad de los sistemas contables computarizados, es con el fin principal de detectar las deficiencias de los sistemas contables y posteriormente se puedan subsanar dichas deficiencias, con el objetivo de que la información generada por los sistemas sea íntegra, confiable y oportuna.

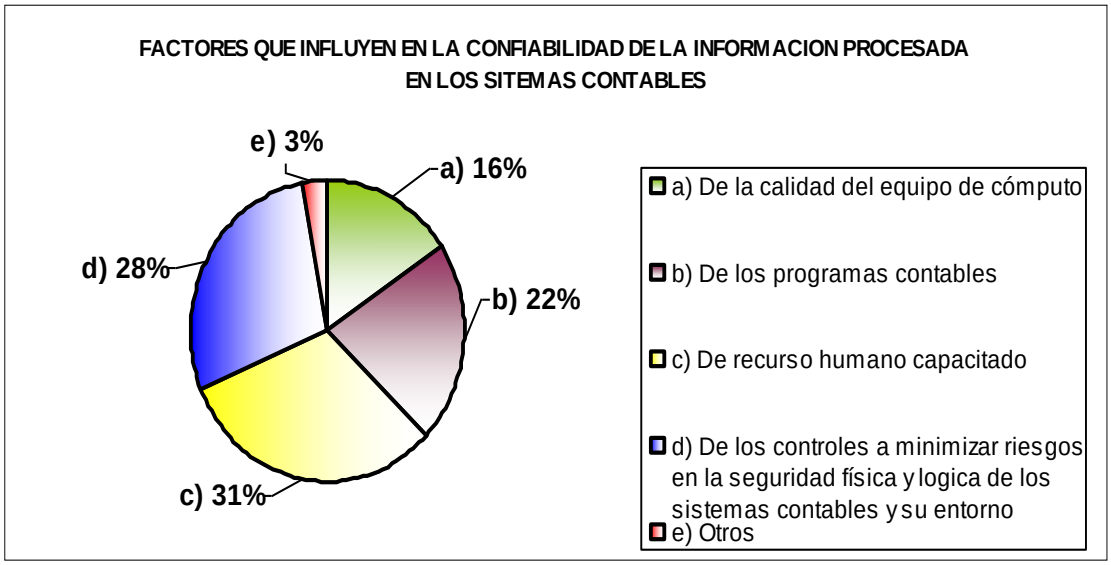
PREGUNTA No.9

¿De que factores considera Ud. depende la confiabilidad de la información procesada en los Sistemas Contables Computarizados?

Objetivo de la pregunta:

Verificar que factores tienen mayor relevancia para que la información procesada en los sistemas contables computarizados sea lo mas confiable posible.

CATEGORIA	**FRECUENCIA**					
	ABSOLUTA			**RELATIVA**		
a) De la calidad del equipo de cómputo	26	54	80	16 %	84%	100%
b) De los programas contables.	36	44	80	22 %	78%	100%
c) De recurso humano capacitado	52	28	80	31%	69%	100%
d) Controles adecuados encaminados a minimizar riesgos en la seguridad física y lógica de los sistemas contables computarizados y su entorno	47	33	80	28 %	72%	100%
e) Otros.	5	75	80	3%	97%	100%
TOTAL	**166**	**234**	**400**	**100%**	**400%**	**500%**



Análisis:

El principal factor que influye para que la información procesada en los sistemas contables computarizados sea lo suficientemente confiable depende, según los encuestados de que el recurso humano tenga la experiencia y capacidad necesaria en el manejo de los sistemas. Otra variante que es de vital importancia para obtener información confiable lo constituye el conjunto de controles adecuados encaminados a minimizar riesgos en la seguridad física y lógica de los sistemas contables computarizados y su entorno. Finalmente en tercer factor para lograr una información confiable depende, según encuestados, de la calidad de software y hardware utilizado.

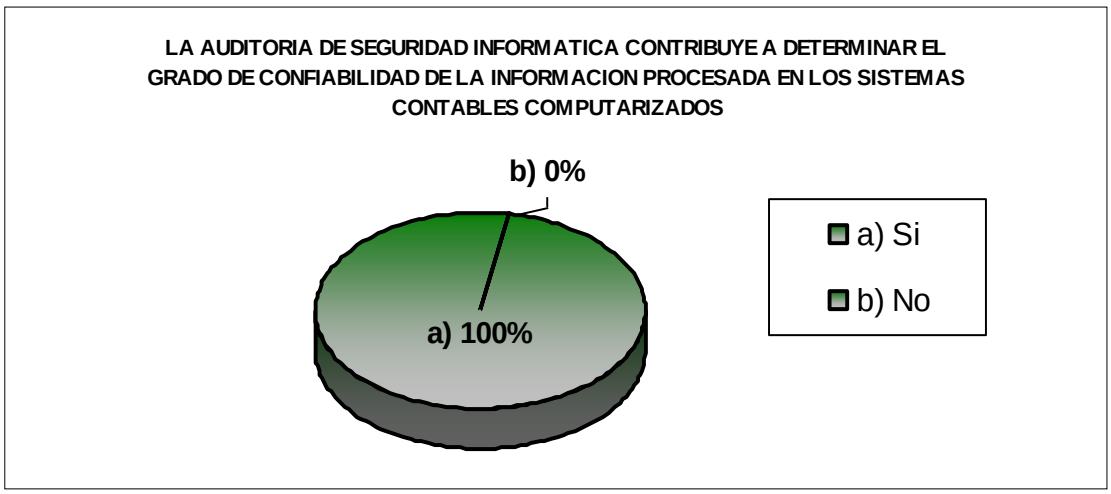
PREGUNTA No.10

¿Cree Ud. que la realización de una Auditoria de Sistemas encaminada dentro del área de la Seguridad Informática contribuiría a determinar el grado de confiabilidad que tiene la información que se procesa en un sistema contable computarizado?

Objetivo de la pregunta:

Conocer si la Auditoría de Seguridad informática influye para determinar el grado de confiabilidad que tiene la información procesada en un sistema contable computarizado.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Si	80	**100 %**
b) No	0	**0%**
TOTAL	**80**	**100%**



Análisis:

Según los resultados anteriores la Auditoria de Seguridad Informática contribuye a determinar el grado de confiabilidad de la información procesada en un sistema contable computarizado, ya que mediante ésta se pueden detectar deficiencias en los sistemas contables computarizados en cuanto a los niveles de seguridad lógica y física, lo cual constituye una pauta para determinar si la información financiera ha sido procesada a través de mecanismos que tengan por objetivo conservar su integridad, para que ésta cumpla finalmente con las características de íntegra, confiable y oportuna.

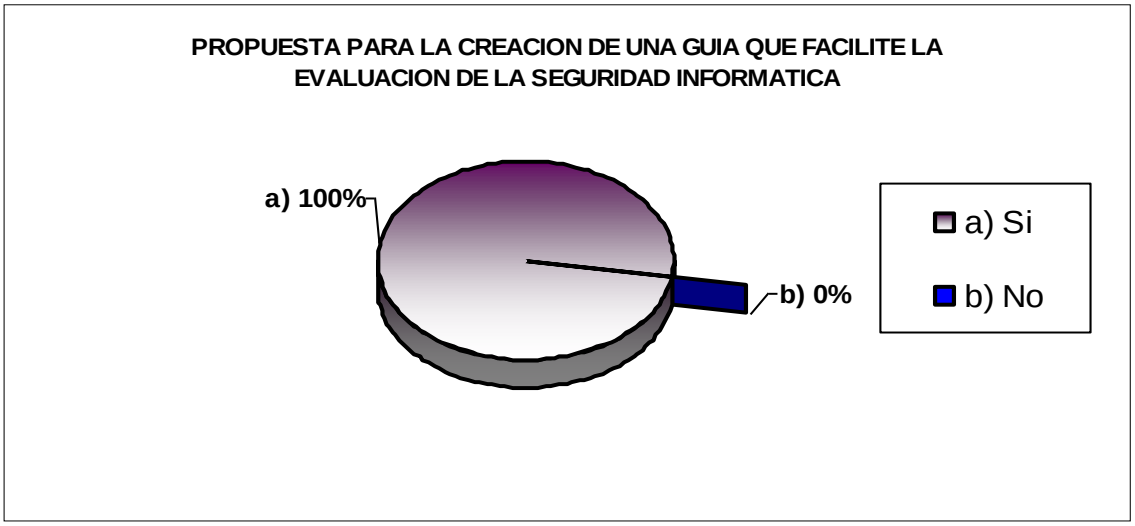
PREGUNTA No.11

¿Considera Ud. idónea la creación de una guía práctica que facilite la evaluación de la Seguridad Informática en cuanto a la información procesada en los sistemas contables computarizados como mecanismo de consulta para auditores que efectúen este tipo de auditoría?

Objetivo de la pregunta:

Verificar el grado de aceptación de la propuesta de creación de una guía que facilite la evaluación de la Seguridad Informática en cuanto a la información procesada en los sistemas contables computarizados como mecanismo de consulta para auditores que efectúen este tipo de auditoria.

CATEGORIA	FRECUENCIA	
	ABSOLUTA	RELATIVA
a) Si	80	100 %
b) No	0	0%
TOTAL	**80**	**100%**

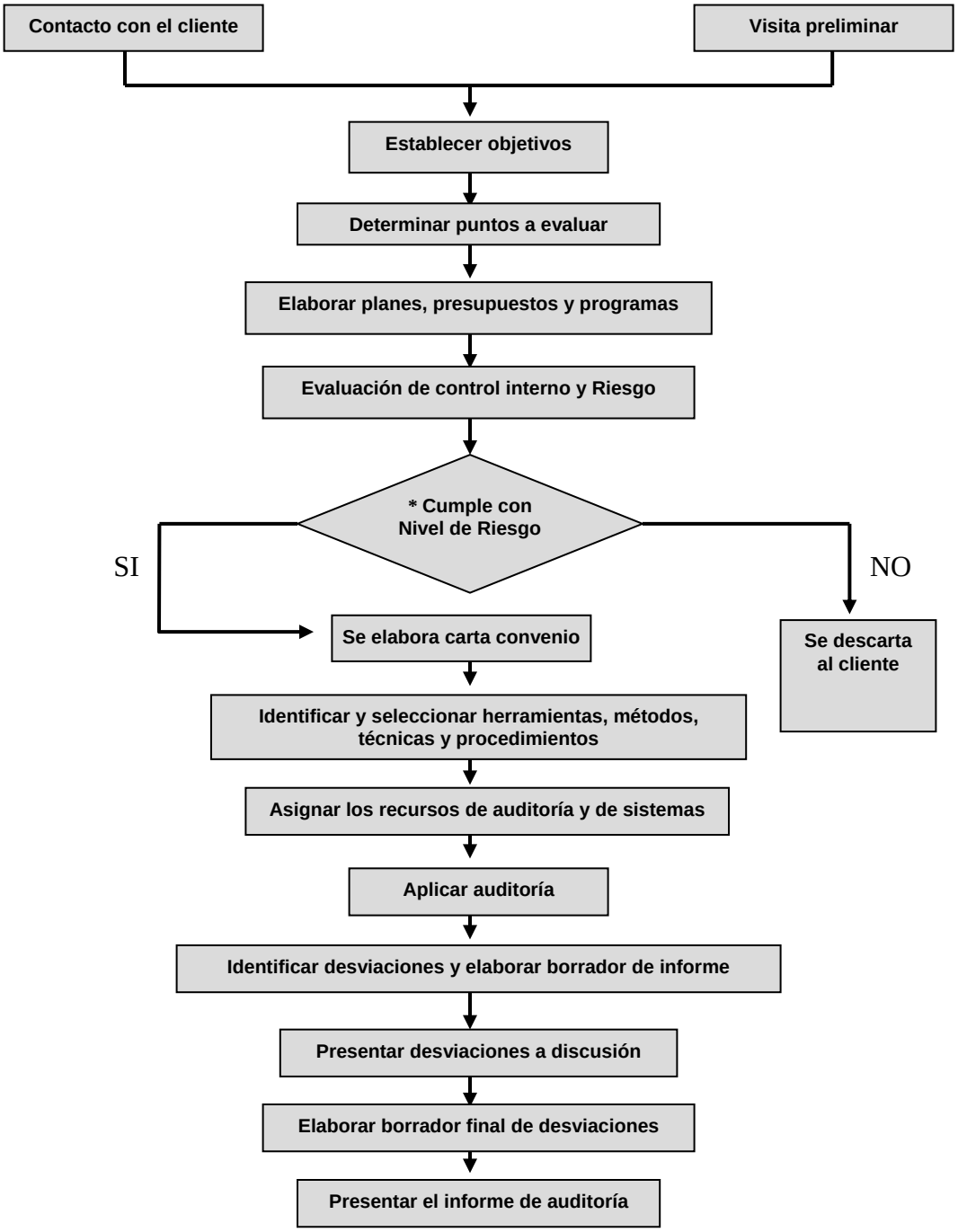


Análisis:

El total de los encuestados considera que sería de utilidad la propuesta de creación de una guía que facilite la evaluación de la Seguridad Informática en cuanto a la información procesada en los sistemas contables computarizados como mecanismo de consulta para auditores que efectúen una auditoria informática.

ANEXO N° 2

ESQUEMA DEL PROCESO DE AUDITORÍA



ANEXO N° 3

Cuadro 6

EMPRESA XYZ, S.A. DE C.V.
ANALISIS Y EVALUACIÓN DE RIESGOS
ÁREA:_____
CÉDULA DE ANALISIS DE RIESGOS POR FACTORES Y ELEMENTOS

FACTORES	ELEMENTOS	NIVELES DE RIESGO					Promedio
		S	A	R	D	M	
		5	4	3	2	1	
CONTROL INTERNO DE SISTEMAS	1. La experiencia en el cumplimiento de las normas y políticas establecidas.			X			3.57
	2. La historia de pérdidas y fraudes.		X				
	3. El resultado de auditorías anteriores.		X				
	4. La confianza de la administración en el área.			X			
	5. La existencia de registros auxiliares.		X				
	6. La automatización de registros y transacciones, los sistemas de programación, así como el acceso de la información.			X			
	7. Prácticas de supervisión y protección física de documentos, archivos e información de alto riesgo.		X				
MATERIALIDAD DE LAS OPERACIONES	1. Los saldos de las cuentas, según los estados financieros con relación a los rubros y cuentas de detalle de estos.	X					4.20
	2. El volumen periódico de las transacciones en valores y cantidades.	X					
	3. Las exigencias presupuestarias.		X				
	4. La cantidad de personal involucrado en el área de sistemas.			X			
	5. La rotación de los activos.		X				
ENTORNO DEL ÁREA DE SISTEMAS	1. Adecuados sistemas computacionales.			X			3.43
	2. Manuales, procedimientos e instructivos actualizados.	X					
	3. Documentación suficiente.			X			
	4. Adecuados registros.			X			
	5. La oportunidad de los reportes e informes.			X			
	6. La capacidad del personal del área.			X			
	7. Los cambios en la tecnología.		X				
SISTEMAS Y ORGANIZACIÓN	1. La frecuencia de los cambios en los sistemas.			X			3.20
	2. La complejidad de los sistemas.			X			
	3. La estandarización.			X			
	4. La definición de funciones y objetivos.			X			
	5. La carga de trabajo y segregación de funciones.		X				
LEYES Y REGULACIONES APLICABLES	1. Asuntos legales involucrados.		X				3.75
	2. Conocimiento y aplicación de leyes, instructivos, políticas, normas y decretos.		X				
	3. Regulaciones fiscales.			X			
	4. Regulaciones específicas del negocio del cliente.		X				

ANEXO N° 4

Cuadro 7

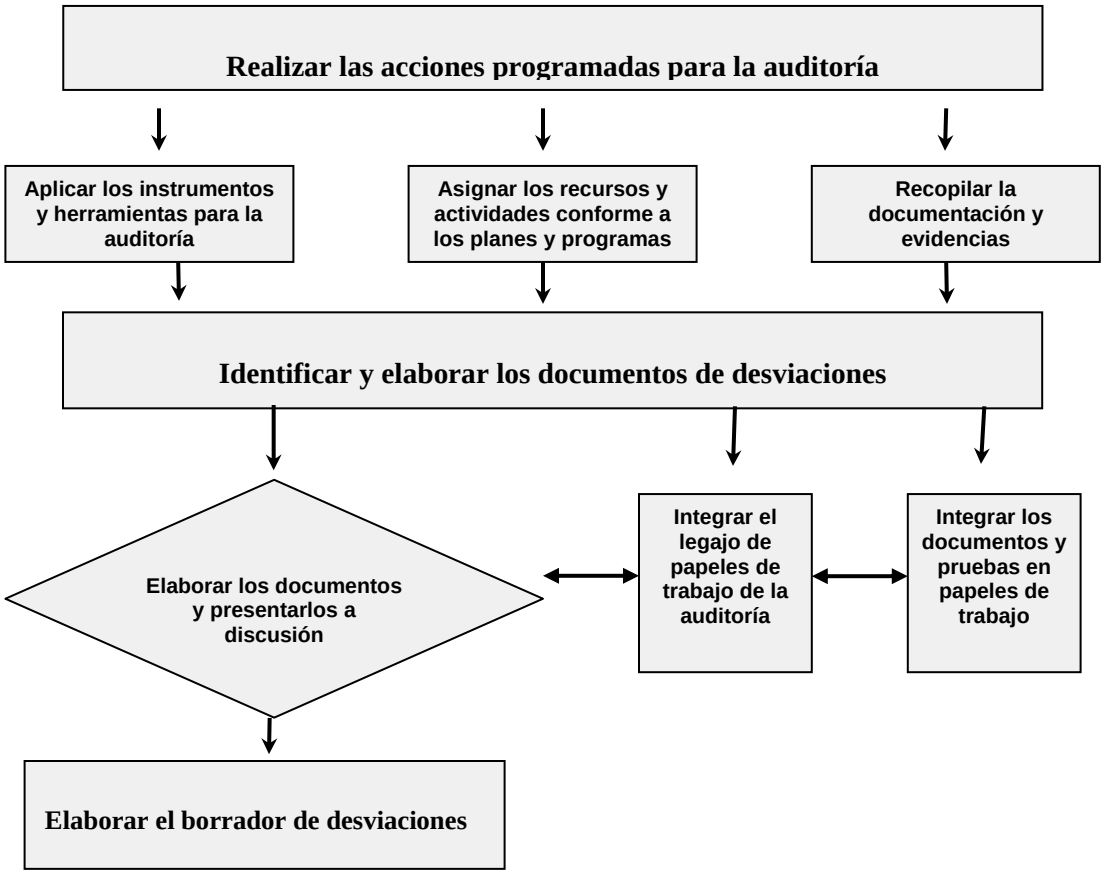
EMPRESA XYZ, S.A. DE C.V.
ANALISIS Y EVALUACIÓN DE RIESGOS
ÁREA:_____

HOJA DE PONDERACIÓN DE RIESGOS DE AUDITORÍA

FACTORES A EVALUAR	Promedio (Cuadro 1)	Factor de peso %	Ponderación Total
Control interno de sistemas 5 4 3 2 1 Satisfactorio aceptable regular débil mala	**3.57**	**20**	**71.4**
Materialidad de las operaciones 5 4 3 2 1 Satisfactorio aceptable regular débil mala	**4.20**	**20**	**84.0**
Entorno del área de sistemas 5 4 3 2 1 Satisfactorio aceptable regular débil mala	**3.43**	**20**	**68.6**
Sistemas y organización 5 4 3 2 1 Satisfactorio aceptable regular débil mala	**3.20**	**20**	**64.0**
Leyes y regulaciones aplicables 5 4 3 2 1 Satisfactorio aceptable regular débil mala	**3.75**	**20**	**75.0**
PONDERACIÓN TOTAL CALCULADA		**100%**	**363.0**
PONDERACIÓN FINAL (A JUICIO DEL AUDITOR)	**363.0**		

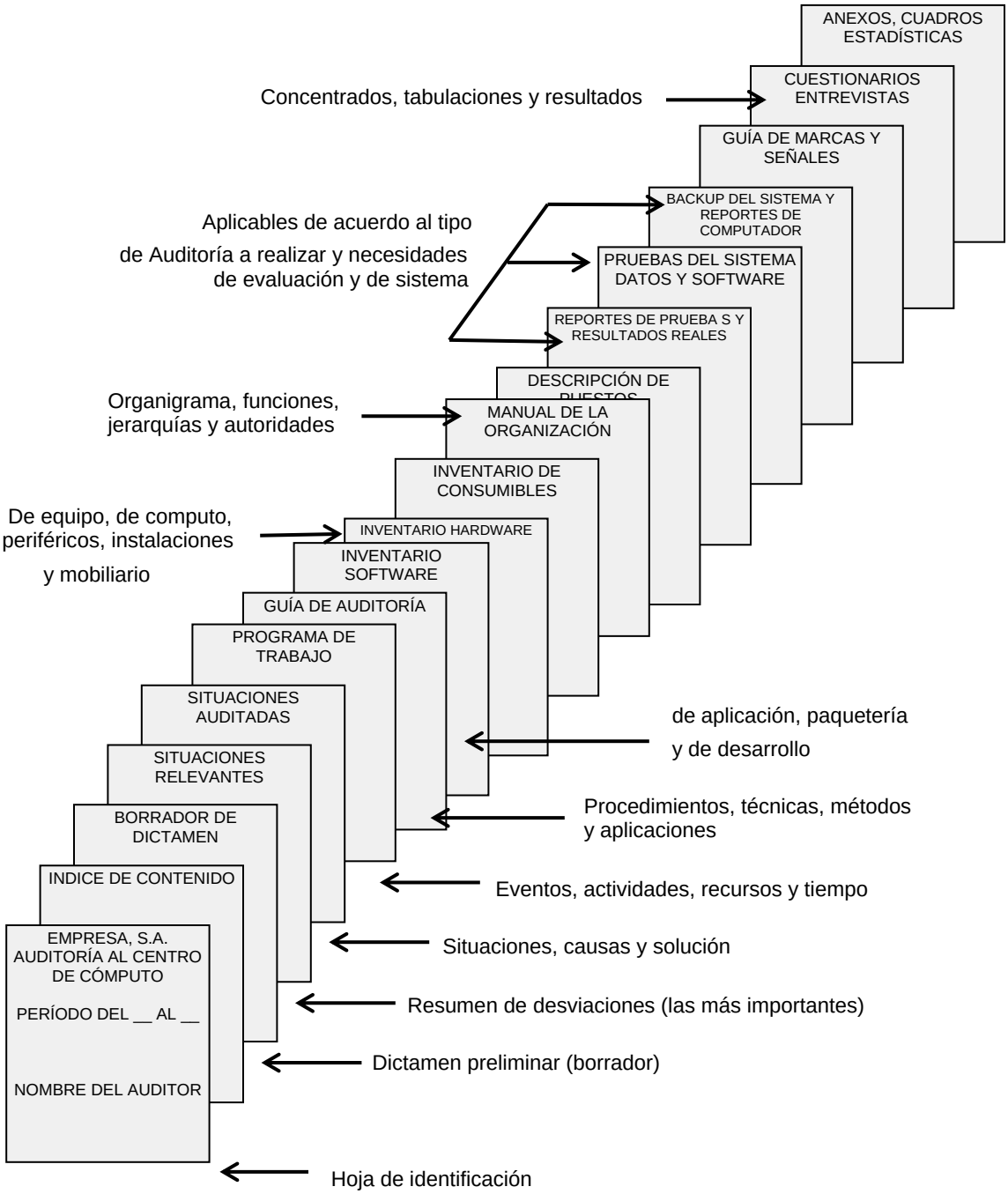
ANEXO N° 5

PRINCIPALES ACTIVIDADES AL EJECUTAR UNA AUDITORIA DE SISTEMAS.



ANEXO N° 6

ARCHIVOS DE PAPELES DE TRABAJO.



ANEXO N° 7

INDICES DE REFERENCIA.

BD Para la documentación relacionada con las bases de datos, información y demás archivos de datos.

CC Para la documentación relacionada con el centro de cómputo.

CM Para la documentación relacionada con los consumibles del área de sistemas.

DS Para la documentación relacionada con el análisis, diseño y desarrollo de sistemas.

GA Para la documentación relacionada con la gestión administrativa del centro de cómputo.

HW Para la documentación relacionada con el equipo físico, periféricos y demás equipos de sistemas.

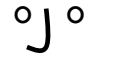
IS Para la documentación relacionada con las instalaciones del área de sistemas.

SG Para la documentación relacionada con la seguridad general de informática.

SW Para la documentación relacionada con el software y paqueterías.

ANEXO N° 8

MARCAS Y NOTAS DE AUDITORÍA

SIMBOLO	SIGNIFICADO O INTERPRETACIÓN
	Verificado una vez.
	Verificado dos veces.
	Dato correcto.
	Dato con error.
	Pendiente de chequear.
	Chequeado y corroborado.
	Desviación pendiente de comprobar.
	Desviación comprobada.
¿?	Confirmar preguntas.
!!	Observación importante.
ERR	No coinciden datos.
VIR	Virus informático Disco contaminado.
ENT	Entrevista.
	Archivo verificado.
	Archivo con errores.
	Listado de resultados.
	Verificado en pantalla.
	Errores en resultados.
	Transmisión interrumpida.
COM	Comentario especial.
OBS	Observación.
EE	Entrevista a empleado.
EF	Entrevista a funcionario
EU	Entrevista a usuario.
EP	Entrevista al personal
CUES	Cuestionario

ANEXO N° 9

PROCEDIMIENTO PARA ELABORAR EL INFORME DE AUDITORÍA DE SISTEMAS COMPUTACIONALES.