UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONOMICAS

ESCUELA DE CONTADURIA PÚBLICA

"Modelo de Planeación de Auditoria Financiera bajo el enfoque de la presunción de los Delitos Informáticos "

Trabajo de graduación presentado por

Acosta Ventura Simón

De Jesús López Carlos Alfredo

Para optar al grado de

LICENCIATURA EN CONTADURIA PÚBLICA

Julio 2008.

San Salvador El Salvador Centro América

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

RECTORA	: Máster Rufino Antonio Quezada Sánchez
Secretaria General	:Licenciado Douglas Vladimir Alfaro Chávez
Decano de la facultad de Ciencias Económicas	:Máster Roger Armando Arias Alvarado
Asesor	: Lic. Juan Vicente Alvarado Rodríguez
Tribunal Examinador	: Lic. Juan Vicente Alvarado Rodríguez Roberto Carlos Jovel Jovel

.

Julio de 2008.

San Salvador, El Salvador Centro América

AGRADECIMIENTOS

A Dios Todopoderoso: Por regalarnos el Don de la vida, por iluminarnos y guiarnos por el camino correcto, permitiendo culminar con éxito esta carrera.

A mis padres: Inocente Acosta Sánchez (Q.D.G) y Maria Josefina vida de Acosta (Q.D.G), a mis Hermanos y Hermanas y junto a ellos a mis sobrinos y sobrinas. Por brindarme su apoyo moral de manera incondicional en todo momento y que confiaron siempre.

A Mi esposa, por haberme dado mis dos hijos, Eduardo Acosta y Gabriela Acosta.

A nuestros Maestros, por dedicarnos su tiempo y proporcionar sus conocimientos, cuales facilitaron el desarrollo y formación en nuestra carrera profesional.

Simón Acosta

Al solo sabio Dios, y a nuestro Señor Jesucristo, por ser el iluminador y dador de la sabiduría para lograr la meta hoy alcanzada.

A mis seres queridos: mamá Sarita y papá Lorenzo (QDDG), a mi esposa Rosa Delmy e hijos, por apoyarme en los momentos más difíciles.

A todos los catedráticos y asesores que a través de los años de estudio nos dieron los insumos necesarios para forjar en nosotros los profesionales que representemos a nuestra querida UES.

Carlos Alfredo De Jesús López

INDICE

CAPITULO III

RESUMEN

Los constantes avances tecnológicos en las comunicaciones, que en la actualidad podemos contemplar, obligan a las empresas a involucrarse al mismo ritmo en que estas se van desarrollando; todo esto, con la finalidad de estar en igualdad de condiciones, para poder competir en el mundo globalizado.

Estos avances, que bien aprovechados producirán beneficios a las empresas; pero a la par de estos avances, surgen también, nuevas formas de cometer actos fraudulentos.

Es normal que las empresas, ante estas situaciones. Deberán establecer y evaluar en forma periódica, el sistema de control interno, que les permitan disminuir este riesgo asociado a los avances tecnológicos.

Conociendo estos antecedentes, se lleva a cabo esta investigación, que tiene como finalidad hacer un conocer si los despachos de auditoría, consideran la presunción de los delitos informáticos, en la etapa de planeación de auditoría; comprobar la hipótesis planteada, indagar sobre la situación planteada y establecer criterios, que permitan elaborar un modelo de planeación de auditoría financiera, bajo el enfoque de la presunción de los delitos informáticos, que ayude a disminuir,

el riesgo de estos delitos en los sistemas de información de las empresas, con la finalidad de tener una seguridad razonable, que los Estados Financiero, están libre de errores importantes.

La investigación, se realizo, mediante el enfoque HIPOTETICO DEDUCTIVO, y se estudio el fenómeno, bajo el tipo, ANALITICO DESCRIPTIVO, se termino la población, mediante el listado inscritos en el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditaría. Tomando para ello, una muestra de 50 Auditores.

Al realizar la investigación, se confirmo que en su mayoría los despachos de auditoría no consideran los delitos informáticos, en la etapa de planeación, por carecer de conocimientos necesarios para su detección; dado a que, no reciben capacitación en esta área especifica.

Se plantea un modelo seguir bajo la consideración de los delitos informáticos. Buscando con ellos, tener una certeza razonable, por parte del audítor, que los Estados Financieros, están libres de errores importantes.

Se concluyo, que la mayoría de despachos un 74%, no consideran la presunción de los delitos informáticos.

Se recomienda, que los despachos contables, capaciten al personal, para hacerle frente a este nuevo desafío que tienen

todos los auditores, con la tecnología de la información y el avance de los sistemas informáticos.

INTRODUCCION

A nadie escapa la enorme influencia que ha alcanzado la Informática, en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo del país, las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la Contabilidad, la Auditoría, etc., son algunas áreas que dependen cada día de un adecuado desarrollo de la tecnología informática.

Junto al avance y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica "Delitos Informáticos". Debido a lo anterior, se desarrolla el presente trabajo que contiene una investigación sobre la temática en estudio de manera que, al final pueda establecerse una relación con Auditoria de Estados Financieros.

El trabajo se ha abordado en cuatro capítulos de la siguiente manera:

Capitulo I

Comprende el marco teórico de la investigación realizada con una conceptualización, de los tipos de delitos informáticos, para conocer la influencia de estos en las diferentes áreas

informáticas de las empresas, se dan a conocer las normativas técnicas de auditoría.

Se describen los diferentes tipos de auditoría, el nuevo rol del audítor, con los avances tecnológicos.

Finalmente, se clasifican los diferentes tipos de delitos.

Capitulo II

Se refiere a la metodología utilizada para llevar a cabo la investigación, la determinación de la muestra que es el objeto de la investigación y por último, se diagnostico la situación real en los despachos de auditoría observados.

Capitulo III

Comprende la propuesta del modelo, que se espera ayudara a preparar una planeación de auditoría, que disminuirá el riesgo de la incidencia de los delitos informáticos, y como resultado final un informe de calidad de trabajo del auditor al ser aplicado adecuadamente.

Capitulo IV

Son las conclusiones y recomendaciones, aportadas sobre la base de la investigación realizada.

Finalmente, se presenta la bibliografía utilizada para poder llevar a cabo la investigación.

CAPITULO I

1.1 ANTECEDENTES DE LOS DELITOS INFORMÁTICOS.

Los constantes avances tecnológicos en el entorno mundial junto con la globalización mueven a las empresas a una nueva economía; el comercio electrónico y el desarrollo del área de informática. En este nuevo orden, surge un factor de nueva generación.

La información y el conocimiento han originado los elementos determinantes que han producido los cambios en la tecnología de la información y la comunicación.

En un principio, estos avances comenzaron como herramientas poco refinadas, pero con la intervención cada vez más del trabajo intelectual, ha traído como consecuencia el perfeccionamiento de la tecnología de la información, no como al inicio, que era para un número limitado de usuarios, debido al costo elevado que representaba el tener acceso; hoy se puede decir que hay facilidades de acceder a cualquier tipo de información y tecnología(texto, voz, imágenes, genéricos, video) en el momento deseado, sin importar donde se encuentre el usuario, la importancia de adaptarse a estos cambios tecnológicos, que

proporcionan información, soportada por sistemas ágiles, oportunos, eficientes, confiables y costeables.

Este increíble avance en el complejo universo de las nuevas tecnologías informáticas, tuvo como consecuencia un nuevo instrumento y medio para cometer delitos, estafas y defraudaciones, que antes eran impensables.

Igualmente trajo consigo la vulneración de los sistemas de seguridad y consecuentemente, la invasión de la intimidad de las personas (acceso a bases de datos, intromisiones ilegitimas, etc.).

Todo esto coloca ante un nuevo reto y cuestionamiento, ante la situación de la vulneración de los sistemas, se hace necesario que se regulen los tipos de transacciones, para evitar una situación de violación, consideradas como delitos a la propiedad intelectual, la piratería y el fraude electrónico; son estos, los delitos que de forma más frecuente se cometen en un medio tan ilimitado como Internet, y es precisamente su extensión, lo que dificulta en gran medida, no solo el descubrimiento del delito sino la prueba de la implicación de los responsables de cometerlo.

Evidentemente, lo que resulta atractivo para robar es el dinero o bienes de valor, por lo tanto, los sistemas que pueden estar

más expuestos a fraude, son los que tratan en controlar bienes de valor, como las planillas, ventas, compras, inventarios.

1.1.1 Conceptos de delito informático

Etimológicamente, proviene de la voz latina " Delictum" doctrinariamente hay varias acepciones, siendo la mas aceptada la que la conceptualiza como un acto típico, antijurídico culpable, sancionado con una pena o una medida de seguridad y conforme a condiciones objetivas de punibilidad.

El diccionario enciclopédico océano, define al delito "Es una acción u omisión voluntaria, castigada por la ley con pena grave".

"Toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma".[1]

---

[1] JIJEMA LEIVA, Reinaldo Javier, La protección Penal de la intimidad y el delito informático. Editorial Jurídico de Chile. Santiago de Chile. Pagina 88.

”En forma típica y atípica, entendido por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumentos o fin”. Y por las segundas, “actitudes ilícitas en que se tienen a las computadoras como instrumentos o fin”.[2]

“Los delitos electrónicos o informáticos en un sentido amplio como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin”.[3]

---

[2] TÉLLEZ VALDEZ, Julio. Op. Cito. Pág.82

[3] DE LA LUZ LIMA, María. Delitos Electrónicos. México. Academia Mexicana de Ciencias Penales. Editorial Porrua 1984. Pág.100

1.1.2 Características de los delitos informáticos[4]

Los delitos informáticos presentan las características siguientes:

a- Conductas criminales, en tanto que solo un determinado número de personas con ciertos conocimientos (técnicos) pueden llegar a cometerlo.

b- Acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto esta trabajando.

c- Acciones de oportunidad, ya que se aprovecha una ocasión o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d- Producen serias pérdidas económicas.

e- Ofrecen posibilidad de tiempo y espacio, ya que en milésimas de segundos, pueden llegar a consumarse.

f- Presentan dificultades para su comprobación, esto por su mismo carácter técnico.

g- Tienden a proliferar cada vez más; por lo que, se requiere una urgente regulación.

---

[4] Legislación sobre delitos informáticos Ien lineal Disponible en <http//monografías .com/trabajos/legisdelinf/legisdelinf.shtml> (consulta: 25 de junio 2007)

1.1.3 Tipos de delitos informáticos

El descubrimiento y revelación de secretos o la vulneración de la intimidad de las personas y empresas, invadiendo por ejemplo los correos electrónicos o interceptando el envío de documentos.

La alteración, destrucción o los daños en datos, programas o documentos electrónicos ajenos. En este tipo de delito se incluirían conductas como, por ejemplo, los actos de sabotaje contra soportes electrónicos, o la introducción de virus electrónicos para causar daños.

El espionaje industrial informático, previsto con el fin de conocer los secretos empresariales.

Las estafas informáticas, en las que se utiliza internet como medio de comunicación anónimo: es un lugar ideal para cometer este tipo de delitos.

Delitos contra la propiedad industrial e intelectual; él internet se muestra como un medio de lo más propicio para

vulnerar los derechos de autor, por ejemplo, la reproducción sin permiso de los contenidos que configuran una página Web.
Son estos, a grandes rasgos, los delitos que de forma más frecuente se cometen en un medio tan ilimitado como es Internet y es precisamente su extensión lo que dificulta en gran medida, no sólo el descubrimiento del delito, sino la prueba de la implicación de los responsables del mismo.

1.1.4 Causas que inciden en la perdida o fraude de la información en los sistemas informáticos.

Estas causas son muy variadas, pero se pueden destacar las siguientes:

1. Tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.

2. Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.

3. A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un período de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.

4. Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y no comprenden, o no les afecta, el significado de los datos que manipulan.

5. En el diseño de un sistema es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir. Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de agujeros.

7. En el centro de cómputo hay un personal altamente capacitado, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar controles y supervisión de cada uno de ellos.

8. El Error y Fraude son difíciles de equiparar. A menudo, los errores no son iguales al fraude. Cuando surgen discrepancias, no se imagina que se ha producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla esta operación, se buscan fallos técnicos y operativos. Sólo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude.

1.1.5 Delitos cometidos en los sistemas informáticos[5].

Sabotaje Informático

El término sabotaje informático, comprende todas aquellas conductas dirigidas a causar daños en el Hardware ó en el Software de un Sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos, son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

---

[5] FERNÁNDEZ IGLESIAS, Manuel José. Algunos softwares malignos Ien lineal Disponible en <http//monografías .com/trabajos34/softwares-malignos/softwares-malignos. Shtml· virus > (consulta: 25 de junio 2007)

Conductas dirigidas a causar daños físicos.

Conductas destinadas a la destrucción física del Hardware y el Software de un sistema, por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

Conductas dirigidas a causar daños lógicos

Este segundo grupo, esta más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos lógicos, o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema, se puede alcanzar de diversas formas, desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se esta trabajando con él borrado de documentos o datos de un archivo,

hasta la utilización de los más complejos programas lógicos destructivos, sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

Bombas lógicas (time bombs): En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo, por ejemplo, a los dos meses o en una fecha o a una hora determinada, o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

Engañando al ordenador.

Pesca u olfateo de claves secretas: Los delincuentes suelen engañar a los usuarios nuevos e incautos de Internet, para que, revelen sus claves personales haciéndose pasar por agentes de la ley ó empleados del proveedor del servicio. Los sabuesos, utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

Estratagemas: los estafadores utilizan diversas técnicas para ocultar computadoras que se «parecen» electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos.

1.1.6 Fraudes cometidos mediante manipulación de las computadoras

a) Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático mas común, ya que, es fácil de cometer y difícil de describir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b) Manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida, debido a que el delincuente, debe tener conocimientos técnicos concretos de informática. Este delito, consiste en modificar los programas existentes en el sistema de computadoras ó insertar nuevos programas o nuevas rutinas. Un medio común utilizado por las personas que tienen conocimientos especializados en programación e informática es el denominado, "caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para

que pueda realizar una función no autorizada, al mismo tiempo que su función normal.

c) Manipulación de los datos de salida. Se efectúa fijando un objeto al funcionamiento del sistema informático, el ejemplo más común, es el fraude de que se hace a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente, esos fraudes se hacían basándose en tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

1.1.7 Clasificación de los delitos informáticos.

Los delitos informáticos, se clasifican de acuerdo a dos criterios:

Como Objeto: En esta categoría se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física. Ejemplos como fin u objeto:

1. Programación de instrucciones que producen un bloqueo total al instante.
2. Destrucción de programas por cualquier método.
3. Daño a la memoria.
4. Atentado físico contra la maquina o sus accesorios.
5. Secuestro de soportes magnéticos entre los que figura información valiosa con fines de chantaje (pago de rescate).

Como instrumentos o medio: En esta categoría se encuentran las conductas criminales, que se valen de las computadoras, como método medio o símbolo de comisión del ilícito.

Ejemplo como Instrumento:

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.
2. Variación de los Activos y Pasivos en la situación contable de las empresas.
3. Planeamiento y simulación de delitos convencionales (robos, fraudes, etc.).
4. Lectura, sustracción o copiado de información confidencial.

5. Modificación de datos, tanto en la entrada como en la salida.
6. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
7. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria.
8. Uso no autorizado de programas de cómputo.
9. Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas.
10. Alteración en el funcionamiento de los sistemas a través de los virus informáticos.
11. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
12. Acceso a áreas informatizadas en forma no autorizada.
13. Intervención en las líneas de comunicación de datos o teleproceso.

1.1.8 Daños ó modificaciones de programas y datos computarizados.

Sabotaje informática. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. La técnica que permiten cometer sabotajes informáticos son: virus, bomba lógica, etc.

Acceso no autorizado a servicios y sistemas informáticos. Por motivos diversos, desde la simple curiosidad, como en el caso de muchos piratas informáticos, conocidos como Hackers hasta el sabotaje o espionaje informático.

1.1.9 Leyes que penalizan los delitos informáticos

En el contexto nacional se pueden encontrar legislaturas que castiguen algunos de los tipos de delitos informáticos, para lo cual se deben citar:

a) Del código procesal penal.

b) Ley de Fomento y Protección de la Propiedad Intelectual.

c) Código Penal.

Dentro de este cuerpo de leyes, se contemplan algunos artículos que guardan relación con los delitos informáticos, específicamente con los siguientes:

a) La difusión, exhibición, explotación de pornografía infantil por medios informáticos.[6]
b) Estafa agravada, realizar manipulación que interfiera el resultado de un procesamiento o transmisión de datos (Art. 216 Num.5 del código Penal Salvadoreño).

Delitos relativos a la propiedad intelectual (Art. 226 y 227 del Código Penal Salvadoreño); además, en dicho código se establece que la realización de estos delitos puede significar para los delincuentes penas de prisión que van desde los 6 meses hasta los 8 años (dependiendo del tipo de delito)

- **Ley de fomento y protección de la propiedad intelectual.**

Al revisar el contenido de esta ley, y relacionarlo con la informática, haciendo mayor énfasis en la protección contra los delitos informáticos, se pueden establecer dos áreas de alcance:

[6] Decreto Legislativo No.1030, Código. Penal Salvadoreño. Diario Oficial No.105. Tomo No.335.26 abril 1996. Arts. No.172 y 173

1. La protección de la propiedad intelectual.

La propiedad intelectual, comprende las siguientes áreas: literaria, artística, industrial y científica (donde se sitúa la informática). El derecho de propiedad exclusivo, se conoce como 'derecho de autor'; en ese sentido, cualquier tipo de violación dará lugar a reparación del daño e indemnización de perjuicios. Dentro de las categorías de obras científicas protegidas por esta ley se pueden mencionar los programas de ordenador según el artículo 32 de la referida ley, y en general cualquier obra con carácter de creación intelectual o personal, según el artículo 10, de la misma ley.

2. La sustracción de información clasificada.

La sustracción de información clasificada, se considera secreto industrial o comercial, articulo · 604 "Ley de fomento a la protección a la propiedad intelectual "toda información que guarde una persona con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros, en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas razonables para

preservar su confidencialidad y el acceso restringido a la misma.

Para la protección de la información secreta, la ley establece que toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios; tenga acceso a un secreto industrial o comercial del cual se le haya prevenido sobre su confidencialidad; deberá, abstenerse de utilizarlo para fines comerciales propios ó de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado, en caso contrario será responsable de los daños y perjuicios ocasionados.

También, será responsable el que por medio ilícito, obtenga información que contemple un secreto industrial ó comercial.

Efectos de la inexistencia de legislatura informática.

Ante la inexistencia de una ley informática, imposibilita a que la persecución y castigo de los autores de delitos informáticos sea efectiva. Aunado a esto, las autoridades (PNC, fiscalía, corte de cuentas, órgano judicial) no poseen el nivel de experticia requerido, en estas áreas, ni la capacidad instalada para desarrollar actividades de investigación, persecución y recopilación de pruebas digitales y electrónicas. Por lo que,

todo tipo de acción contra los delincuentes informáticos quedaría prácticamente en las manos de la organización que descubre un delito y el tipo de penalización sería *más* administrativa que de otro tipo (si para el caso el delito proviene de fuentes internas de la entidad).

Los esfuerzos encaminados en la legislación informática, en nuestro país, como consecuencia del comercio electrónico a nivel mundial, y la aprobación de la firma digital 76 en EE.UU. La cual comprende lo siguiente, "El sistema utilizado por la firma digital es la criptografía asimétrica o de clave pública; que genera, a través de algoritmos, dos claves: una pública y otra privada que son complementarias (una para cifrar y la otra para descifrar), es decir, que si se firma con una de ellas se necesitará la otra para desencriptarla". En tal sentido, se esta trabajando en nuestro país de establecer una estructura de leyes que le brinde un marco legal a las prácticas del comercio electrónico (las transacciones por Internet).

1.2 Bases de Datos

1.2.1 Concepto:

Una base de datos, es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su uso posterior.

También se define como una colección de datos relacionados que se refieren a un asunto ó propósito particular y las herramientas utilizadas para manipular esos datos.

Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos, que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

En general, las bases de datos, consisten en información que están claramente estructuradas. Según como sea, haya sido estructura, será de un tipo ú otro.

1.2.2 Tipos de bases de datos

Se clasifica de acuerdo a varios criterios:

Según la variabilidad de los datos almacenados:

a) Bases de datos estáticas: Son de solo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar, para estudiar, el comportamiento de un conjunto de datos, a través del tiempo, realizar proyecciones y tomar decisiones.

b) Bases de datos dinámicas: Son aquellas, donde la información almacenada se modifica con el tiempo, permitiendo operaciones como actualización y adición de datos, además de las operaciones fundamentales de consulta.

Según el contenido:

a) Bases de datos bibliográficas: Contienen un representante de la fuente primaria, que permite localizarla. Un registro típico de una base de datos bibliográfica, es la que contiene información sobre el autor, fecha de publicación, editorial, titulo, edición; de una determinada publicación, etc.

b) Base de datos numéricas: Como su nombre lo indica, contiene cifras o números; por ejemplo, una colección de resultados de análisis de laboratorio.

c) Base de datos de texto completo: Almacenan las fuentes primarias, como por ejemplo, todo el contenido de las ediciones de una colección de revistas científicas.

d) Banco de imágenes: audio, video, multimedia, etc. Como su nombre lo indica, almacenan información en distintos formatos.

e) Bases de datos o bibliotecas de información: Son bases de datos, que almacenan diferentes tipos de información provenientes de la ciencia médica, se pueden considerar varios tipos:

1) Bases de datos de rutas metabólicas.
2) Base de datos de estructura.
3) Bases de datos bibliográficas.

1.3 Procesamiento electrónico de datos

1.3.1 Concepto de datos.

Datos son los hechos que describen sucesos y entidades."Datos" es una palabra en plural que se refiere a más de un hecho. A un hecho simple se le denomina "data-ítem" o elemento de dato. Los datos son comunicados por varios tipos de símbolos tales como las letras del alfabeto, números, movimientos de labios, puntos y rayas, señales con la mano, dibujo, etc. Estos símbolos se pueden ordenar y reordenar de forma utilizable y se les denomina información. Los datos son símbolos, que describen condiciones, hechos, situaciones o valores. Estos se caracterizan por no contener ninguna información. Un dato puede significar un número, una letra, un signo ortográfico o cualquier símbolo que represente una cantidad, una medida, una palabra o una descripción.

La importancia de los datos, está en su capacidad de asociarse dentro de un contexto para convertirse en información. Por si mismos, los datos no tienen capacidad de comunicar un significado y por tanto no pueden afectar el comportamiento de

quien los recibe. Para ser útiles, los datos deben convertirse en información para ofrecer un significado ó conocimiento.

1.3.2 Concepto de información.

La información, una colección de hechos significativos y pertinentes, para el organismo o entidad que los percibe.

Para ser significativos, los datos deben constar de símbolos reconocibles, estar completos y expresar una idea no ambigua. Los símbolos de los datos son reconocibles cuando pueden ser correctamente interpretados. Muchos tipos diferentes de símbolos comprensibles se usan para transmitir datos. La integridad significa que todos los datos requeridos para responder a una pregunta específica están disponibles.

Conoceremos el contexto de estos símbolos antes de poder conocer su significado. Otro ejemplo de la necesidad del contexto es el uso de términos especiales en diferentes campos especializados, tales como la contabilidad. Los Contadores utilizan muchos términos de forma diferente al público en general, y una parte de un aprendizaje de contabilidad, es aprender el lenguaje de

Contabilidad. Así, los términos Debe y Haber, pueden significar para un contador no más que "derecha" e "izquierda" en una contabilidad en T, pero pueden sugerir muchos tipos de ideas diferentes a los no contadores.

Datos Permanentes. Datos pertinentes (relevantes), pueden ser utilizados para responder a preguntas propuestas.

Solo los hechos relacionados con las necesidades de información son pertinentes. La organización selecciona hechos entre sucesos y entidades particulares para satisfacer sus necesidades de información.

1.3.3 Diferencia entre dato e información.

TABLA CONCEPTOS DE DATOS E INFORMACION.

DATO	INFORMACIÓN
Los datos a diferencia de la información, son utilizados como diversos métodos para comprimir la información; a fin de, permitir una transmisión o almacenamiento más eficaz.	1.-En su concepto más elemental, la información es un mensaje con un contenido determinado emitido por una persona hacia otra y, como tal, representa un papel primordial en el proceso de la comunicación.
Poema de amor, las cuentas del banco o instrucciones para un amigo. Es lo mismo que la memoria de la computadora Sólo el procesador reconoce la diferencia entre datos e información de cualquier programa Para la memoria de la computadora , y también para los dispositivo de entrada y salida (E/S) y almacenamiento en disco, un programa es solamente más datos, más información que debe ser almacenada, movida o manipulada.	

1.3.4 Elementos del sistema procesamiento electrónico de datos (PED).

Un sistema de procesamiento electrónico de datos comprende de los siguientes elementos:

1) Un procesador electrónico de datos unidad central de procesamiento. El equipo periférico asociado, formado por dispositivo de preparación de datos, de entrada y salida.

2) El equipo periférico asociado, formado por dispositivos de preparación de datos, de su entrada y salida, etc. Este elemento central ejecuta funciones de lógica, aritmética, almacenamiento de los datos durante el proceso, y control de los mismos.

3) Procesamiento para indicar que datos se necesitan, cuando y donde obtenerlos y en que forma utilizarlo.

4) Rutinas de instrucción para el procesador.

5) Persona para operar, conservar y mantener el equipo, para analizar y establecer procedimientos, para preparar instrucciones, proporcionar datos de entrada, utilizar informes, revisar resultados y supervisar la operación en su totalidad.

1.3.5 Diferencia entre PED y procesamiento manual.

1 El sistema procesamiento electrónico de datos (PED) puede producir una pista o huella de transacciones que tan solo sea aplicable por un breve período, ventas por teléfono).

2 Con frecuencia existe menos evidencia documental de los procedimientos del control del sistema computarizado que en sistemas manuales.

3 La información dentro de los sistemas manuales es visible.

1.4 El Audítor y el sistema de procesamiento electrónico de datos.

Muchos de los atributos de un sistema PED afectan al audítor y al trabajo que este desempeña. El cambio en los rastreos de Auditoría, la velocidad y exactitud de la computadora, así como sus capacidades de revisión, exigen al Audítor examinar los procedimientos tradicionales y efectivos para los sistemas electrónicos.

La concentración del procesamiento en sistemas PED y la complejidad de dichos sistemas requieren que el Audítor se familiarice con la planeación, programación y la documentación necesaria de las actividades de PED. La comprensión del procesamiento electrónico de datos y de los tipos de control factibles en los sistemas electrónicos, es de gran importancia para la evaluación que el Auditor pueda hacer de los controles internos, así como, para utilizar las computadoras en Auditoría.
El proceso secuencial es necesario puesto que el acceso a los registros conservados en un archivo tiene que ser secuencial. Un registro es un acervo de información sobre un determinado sector. La característica principal del procesamiento secuencial

es la necesidad de leer todo el archivo cada vez que una transacción va a procesarse y compararse contra él.

En los archivos de acceso aleatorio, las transacciones que los afectan se alimentan a la computadora de manera aleatoria, a medida que se presentan. Esto ha demostrado ser mucho más exacta que las personas y que los dispositivos mecánicos anteriores para efectuar cálculos y para registrar y recorrer los datos.

La computadora, cuando se programa debidamente, puede desempeñar funciones de revisión similares a las realizadas por personas.

En algunos aspectos, la complejidad de un sistema PED ayuda al audítor. Un sistema electrónico, exige anunciar los procedimientos en forma excepcionalmente detallada, precisa y completa. Como parte de la documentación de los sistemas, es muy posible que el Audítor encuentre diagramas de recorrido de sistemas, diagramas de recorrido de programa, relaciones de programa, y descripciones narrativas. Los diagramas de recorrido son un medio de presentar la información y las operaciones de tal manera que resulten fáciles de visualizar y seguir. Existen dos tipos de diagramas de recorrido:

1. Diagramas de recorrido del sistema y,
2. Diagramas de recorrido de programa.

Un diagrama de recorrido del sistema muestra la corriente de los datos a lo largo de todas las partes del sistema.

Se emplean diversos símbolos para describir el recorrido que siguen los datos y las relaciones entre estos, para representar el equipo, las operaciones de equipo y las operaciones manuales.

Un diagrama de recorrido de programas describe lo que sucede en un programa almacenado o lo que esta representado por un solo símbolo de procesamiento en el diagrama de recorrido del sistema. El diagrama de recorrido muestra operaciones y decisiones especificas e indica la secuencia u orden en que deben realizarse las operaciones lógicas y de aritmética.

La relación del programa, muestra las instrucciones en el lenguaje del programa tal y como las ha escrito el programador; y las instrucciones en el lenguaje de maquina a la que aquellas han sido traducidas. Las instrucciones en el lenguaje fuente se traduce al lenguaje de maquina con programas especiales de computadora denominados programas de ensamblado y copiladores.

El lenguaje de maquina obtenido como resultado de una rutina de ensamblado o de copilador consiste en instrucciones escritas en un sistema de clave (codificado) de números y letras anteriores o de los datos fuente original. El muestreo sistemático de

renglones individuales procesados proporciona otro control de salida. Además de los controles de organización y de procedimientos, todo sistema PED necesita controles administrativos. Estos controles pueden asociarse con la formulación, documentación y administración de los métodos y practicas de operación en el diseño de sistemas, la programación y las operaciones de la computadora.

Diseño de sistemas La complejidad de los sistemas electrónicos requieren programaciones y diseños de sistemas detallados. Estos detalles deben estar debidamente documentados, a fin de evaluar y modificar el sistema.

1.5 Generalidades de Auditoría

1.5.1 Concepto básico de Auditoría

. La Auditoría en su amplio sentido, puede ser definida como una investigación sobre la contabilidad de los aspectos financieros y de operación de una organización económica.[7]

---

[7] Grimaker, Robert L y Ben B. Barr, " Auditoria Examen de los Estados Financieros, P.15

. Auditoría es la acumulación y evolución de las evidencias basadas en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La Auditoría, debe realizarla una persona independiente y competente.[8]

. Auditoría, es la supervisión de las cuentas de una empresa, hecha por decisión de un tribunal o instancia de particular.[9]

El diccionario pequeño Larauce ilustrado lo enuncia: como el examen de las operaciones financieras, administrativas y de otro tipo de una entidad pública o de una empresa por especialistas ajenos a ella y con el objeto de evaluar la situación de los mismos.[10]

Es la revisión independiente de algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de auditoría, con el propósito de evaluar su correcta realización y con base en ese análisis, poder emitir una opinión autorizada sobre la

---

[8] Alvin A Arens Randal J Elder –Mark S. Bealey "Auditoría un enfoque integral "Pág.14

9 Gran Diccionario del Saber Humano, varios auditores Director Gonzalo Ang. Editorial Selecciones del Reader's Digest, México, 1992 volumen I Pág.190.

10 García Pelayo, Ramón y Cross" diccionario pequeño Laraoucce " ilustrado Pág.78

razonabilidad de sus resultados y el cumplimiento de sus operaciones.[11]

1.5.2 Importancia

A medida que las sociedades han evolucionado, las empresas también han aumentado sus actividades económicas-financieras, y con el auge de internet y nuevas formas de dirigir los negocios de manera electrónica (e-commerce), comercio electrónico, han aumentado el volumen de información en tiempo real, se necesita un aseguramiento mayor que los proteja de fraudes.

El nuevo rol de la Auditoría, es el servicio de aseguramiento, para mejorar la calidad de la información para la toma de decisiones.

La necesidad de aseguramiento, no es nueva los auditores han prestado esto servicios, para asegurar la información histórica de los Estados Financieros.

Servicio de aseguramiento, es la tecnología de la información, Que responder a la creciente necesidad de aseguramiento de los negocios que hacen transacciones por Internet, el AICPA (Instituto Estadounidense de contadores Públicos), formo el

---

[11] YANEZ, Reynaldo de Jesús, Glosario de Términos Jurídicos, Pág. 8

Special Comité on Assurance Services (SCAS), comité especial de servicios de aseguramiento.

Las firmas de Auditoría están autorizadas para que presten el servicio de proporcionar seguridad a los usuarios de sitios de red a través del sello electrónico Wed Trust. Este sello le asegura al usuario que el dueño ha cumplido con el criterio de prácticas empresariales integridad de transacciones y procedimientos de información.

1.5.3 Objetivos generales de la auditoría.

Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.

Hacer una revisión especializada, desde el punto de vista profesional y autónomo del aspecto contable, financiero y operacional de las áreas de una empresa.

Evaluar el cumplimiento de planes, programas, políticas, normas y lineamientos que regulen la actuación de los empleados

y funcionarios de una institución, así como evaluar las actividades que desarrollan en sus áreas y unidades administrativas.

Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, así como el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones.

1.5.4 Clasificación de la Auditoría.

En términos generales, las auditorias se pueden clasificar en tres grupos: auditoría operacional, auditorias de cumplimiento, y auditoría estados financieros.[12]

Auditoría Operacional: Evalúa la eficiencia y eficacia de cualquier parte de los procedimientos y métodos de operación de una organización; cuando se completa una Auditoría operacional, por lo general, la administración, espera recomendación.

---

[12] MICHAEL E. Rudy. Manual de Finanzas. Contabilidad. Informe y Auditoria. Enero 1995. Pág.5

Auditoría de cumplimiento: Se realiza para determinar si la entidad auditada aplica correctamente los procedimientos, reglas o reglamentos que una autoridad superior ha establecido.

Auditoría de Estados Financieros: Se realiza para determinar si los Estados Financieros, en general han sido elaborados de acuerdo con el criterio establecido en las normas internacionales de Contabilidad.[13]

TIPOS DE AUDITORIA	**EJEMPLOS**	**INFORMACION**	**CRITERIOS ESTABLECIDOS**	**EVIDENCIA DISPONIBLE**
Auditoría Operacional	Evaluar si el procedimiento de nominas computarizadas subsidia operación de manera eficiente y	Números de registros de nomina procesados en un mes, costo del departamento y número de	Estándares de la compañía para lograr eficiencia y eficacia en el departamento	Reportes de errores registros de nomina y costos de procesamiento de nómina

[13] ALVIN. Arens, RANDAL J.Hederle .MARK S. Beasley. Auditoria Integral

	eficaz	errores	de nóminas	
Auditoría de cumplimiento	Determinar si se han cumplidos los requerimientos del banco para continuación de un préstamo	Registro de compañía	Depósitos del contrato de préstamos.	Estados Financieros y cálculo del auditor.
Auditoría de Estados Financieros	Auditoría anual de Estados Financieros	Estados Financieros	Normas de información financiera aplicables	Documentos registros fuentes externos de evidencia

1.5.4.1 Por su lugar de origen[14]

Auditoría externa: Es la revisión independiente, que realiza un profesional de auditoría, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de las actividades, operaciones y funciones, que se realizan en la empresa que lo contrata; así como, la razonabilidad en la emisión de sus resultados financieros. La relación de trabajo del auditor es ajena a la institución donde se aplicara la auditoría y esto le permite emitir un dictamen libre e independiente.[15]

Auditoría interna: Es la revisión que realiza, un profesional de auditoría, cuya relación de trabajo es directa y subordinada a la institución, donde se aplicara la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de sus resultados financieros.

---

[14] MUÑOZ RAZO, CARLOS. Auditoría en sistemas Computacionales, México. Primera Edición, 2002. Pág.14

[15] Ibid 14, Pág. 13

1.5.4.2 Por su área de aplicación.

Auditoria Financiera: Es la revisión sistemática, explorativa y critica que realiza un profesional de contabilidad a los libros y documentos contables, a los controles y registros de las operaciones financieras. Y a la emisión de los estados financieros de una empresa; con el fin, de avaluar y opinar sobre la razonabilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros, obtenidos durante un período específico o un ejercicio fiscal.

El propósito final es emitir un dictamen contable, sobre la correcta presentación de los resultados financieros a los accionistas, clientes, autoridades fiscales, y terceros interesados, en relación con las utilidades, pagos de impuestos, y situación financiera y económica de la institución.[16]

Auditoría Informática: Es la revisión técnica, especializada y exhaustiva, que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos o de redes; así como, a sus

---

[16] Ibid.14, Pág. 15

instalaciones, telecomunicaciones, mobiliario, equipo periférico y demás componentes.

Dicha revisión, se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.

El propósito fundamental, es avaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades, operaciones de funcionarios y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.[17]

1.6.- Auditoría de sistemas computacionales (Auditoría Informática).

Auditoría alrededor de la computadora: Es la revisión especifica, que se realiza a todo lo que esta alrededor de la

---

[17] Ibid.14, Pág. 19

actividad de los sistemas de computo, sus actividades y funcionamiento, haciendo una evaluación de sus métodos, procedimientos y procesamiento de datos, su emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del propio centro de computo, los aspectos operacionales y financieros, gestión administrativa de accesos al sistema, la atención a los usuarios y el desarrollo de nuevos sistemas, las comunicaciones internas y externas y todos aquellos aspectos que contribuyen al buen funcionamientos de un área de sistematización.[18]

Auditoría de la seguridad de los sistemas computacionales: Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de computo, sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de equipos computacionales.[19]

---

[18] Ibid.14, Pág. 26
[19] Ibid.14, Pág. 26

1.6.1 Objetivos de auditoría en sistemas computacionales.[20]

Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de sus operaciones de sistema y la gestión administrativa del área de informática.

Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información; así como, del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

Evaluar el uso y aprovechamiento de los equipos de computo, sus periféricos, las instalaciones y mobiliario del centro de computo, así como el sus de sus recursos técnicos y materiales para el procesamiento de información.

Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paquetes de aplicación y desarrollo así como el desarrollo e instalación de nuevos sistemas.

---

[20] Ibid.14, Pág. 39

Evaluar el cumplimiento de planes, programas, estándares, políticas, normas de procesamiento de información, así como de su personal y de los usuarios del centro de información.

Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio de la computadora.

1.6.2 Etapas de Auditoría.[21]

Planeación: Es la primera etapa de toda auditoría, es donde se plasman los procedimientos a utilizar, aquí se define el valor que afectar la razonabilidad de cada uno de los aspectos importantes, los métodos a utilizar en la evaluación preliminar del control interno, que sirve para determinar el alcance de los procedimientos.

---

[21] INSTITUTO Mexicano de Contadores Públicos. NIA 300. Planeación. Normas Internacionales de Auditoria, México, 2004, Pág.81

Ejecución: Es la etapa donde se realiza el trabajo, se revisa la calendarización que se hizo en la planeación, la obtención de evidencia, para evaluar si cumple con lo planeado, obtener pruebas, hacer una evaluación de los procedimientos de control interno, para obtener evidencia, si estos influyen en el dictamen que se va a emitir.

Finalización: Es la emisión del informe del auditor, es el documento que el contador público, emite a su cliente de acuerdo a Normas de Auditoría Generalmente Aceptadas, Normas Técnicas de la profesión y de acuerdo al alcance y resultados del examen realizado.

1.6.3. Métodos, Técnicas, Herramientas y procedimientos de Auditoría

Son las principales herramientas que utiliza el auditor para llevar a cabo su trabajo, los cuales se ubican en tres grandes grupos, entre ellos los tradicionales y herramientas especificas, aplicables a los sistemas computacionales.

1.6.4. Instrumentos de recopilación de datos aplicables en la auditoría de sistemas.

Entrevistas,

Cuestionarios,

Encuestas,

Observaciones,

Inventarios,

Muestreo,

Experimentación.

1.6.5. Técnicas de evaluación aplicables en la auditoría de Sistemas.

Examen,

Inspección,

Confirmación,

Comparación,

Revisión Documenta.

1.6.6. Técnicas especiales para la auditoría de Sistemas Computacionales.

Guías de Evaluación,

Ponderación,

Simulación,

Evaluación,

Diagrama del círculo de sistemas,

Matriz de evaluación,

Programas de verificación,

Seguimiento de programación.

1.7 NORMAS DE AUDITORIA GENERALMENTE ACEPTADAS.

1.7.1. **Normas Generales.**

Entrenamiento técnico y capacidad profesional del Auditor independiente: El examen deberá llevarse a cabo, por una o varias personas que tengan entrenamiento técnico y la capacidad profesional como auditores.

Independencia: En todos los asuntos relacionados con el trabajo encomendado, él o los auditores mantendrán una actitud mental independiente.

Cuidado y diligencia profesionales: Se ejercitara el cuidado profesional, en la ejecución del examen y en preparación del informe.

1.7.2. Normas relativas a la ejecución del trabajo.

La planeación adecuada y la oportunidad de ejecución del trabajo: El trabajo debe planearse adecuadamente y los ayudantes, si los hay, deben ser supervisados apropiadamente.

Evaluación de la estructura del Control Interno en una auditoría de Estados Financieros: Un suficiente entendimiento del control interno, tendrá al planear la auditoría y para determinar la naturaleza, tiempo y extensión de las pruebas a ser desarrolladas.

Evidencia: Se obtendrá material de prueba suficiente y adecuada, por medio de la inspección, observación, investigación indagación y confirmación, para lograr una base razonable y así poder expresar una opinión en relación con los Estados Financieros que se examinan.

1.7.3. Normas relativas al informe.

Cumpliendo con los principios de contabilidad Generalmente Aceptados: El informe indicara si los estados financieros se presentan de acuerdo a principios de contabilidad generalmente aceptados.

Uniformidad en la aplicación de las normas internacionales de contabilidad.

En el caso que los Estados Financieros, no muestren uniformidad en el periodo actual en relación con el período precedente, dicha situación deberá revelarse en el informe.

1.8 CONCEPTO DE PLANEACIÓN

Según el autor: Héctor Sánchez, en el libro "la planeación de la auditoría dice que: planear el trabajo de auditoría, será decidir previamente cuales son los procedimientos más convenientes que han de emplearse y que extensión se les dará a las pruebas, la oportunidad para su aplicación, que papeles de trabajo se emplearan para registrar los resultados, que personal intervendrá en el trabajo así como la calidad profesional del mismo. Pero en el momento de la planeación, se debe tener presente las condiciones y características propias de lo que se esta realizando; así como, las limitaciones que puedan presentarse en el desarrollo del trabajo, considerando que lo planeado inicialmente esta sujeto a modificaciones de acuerdo al desarrollo del propio trabajo.[22]

Según la NIA 300, párrafo 3, Planeación, significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperados de la auditoría.[23]

---

[22] Ibid 21, Pág.
[23] Ibid 21, Pág. 10

1.9 CONCEPTO DE PROGRAMA DE AUDITORÍA.

Según la NIA 300, párrafo 10, Es el conjunto de intrusiones a los auxiliares involucrados en la auditoría y sirve como un medio para el control y registró de la ejecución apropiada del trabajo. Puede contener los objetivos de la auditoría para cada área y un presupuesto de tiempos en el que son presupuestadas las horas para las diversas áreas o procedimientos de auditoría.[24]

1.9.1 Concepto de Plan Global de Auditoría.

Es un detalle General del desarrollo de la auditoría describiendo el alcance y conducción esperados. Según la NIA 300, párrafo 8

1.9.2 Determinación de las áreas de riesgos.

El audítor deberá obtener una comprensión de los sistemas de contabilidad y de control interno, suficiente para planear la auditoría y desarrollar un enfoque de auditoría efectivo. El auditor deberá usar juicio profesional para evaluar el riesgo de

---

[24] Ibid 21, Pág. 2

Auditoria, y diseñar los procedimientos para asegurar que el riesgo se reduce a un nivel de aceptación.[25]

1.9.2.1 Concepto de Riesgo de Auditoría:

Significa el riesgo de que el auditor de una opinión de auditoría, inapropiada cuando los estados Financieros están elaborados en forma errónea de una manera importante.[26]

1.9.2.2 Componentes del Riesgo de Auditoría.

Riesgo Inherente,

Riesgo de Control,

Riesgo de Detección.

Riesgo Inherente: Es la susceptibilidad del saldo de una cuenta o clase de transacciones a una representación errónea que pudiera ser de importancia relativa, individualmente o cuando se

---

[25] INSTITUTO Mexicano de Contadores Públicos. NIA 400. Evaluaciones de Riesgo y de Control Interno. Normas Internacionales de Auditoria, México, 2004, Pág.2

[26] Ibid 25, Pág.2

agrega con representaciones erróneas en otras cuentas o clases, asumiendo que no hubo controles internos relacionados.[27]

Riesgo de Control: Es el riesgo de una representación errónea que pudiera ocurrir en el saldo de cuenta o clase de transacciones y que pudiera ser de importancia relativa individualmente o cuando se agrega con representaciones erróneas en otros saldos o clases, no sea prevenido o detectado y corregido con oportunidad por los sistemas contables y de control interno.[28]

Riesgo de Detección: Es el riesgo de que los procedimientos sustantivos de un auditor no detecten una representación errónea que existe en un saldo de una cuenta o clase de transacciones que podría ser de importancia relativa, individualmente o cuando se agrega con representaciones erróneas en otros saldos o clases.[29]

---

[27] Ibid 25, Pág. 4
[28] Ibid 25, Pág. 5
[29] Ibid 25, Pág. 6

CAPITULO II

2.1 DISEÑO METODOLOGICO

2.1.1 TIPO DE INVESTIGACION

El problema relacionado con los delitos informáticos, en la etapa de planeación de Auditoría de los Estados Financieros, se investigó mediante el enfoque HIPOTETICO DEDUCTIVO, se analizó así: desde una perspectiva global los diferentes aspectos que pudiesen ser la causa fundamental en el surgimiento de la problemática, con la intención de descubrir realidades o elementos específicos de comprobación que permitieron plantear una alternativa de solución.

2.1.2 TIPO DE ESTUDIO

La investigación se basó en un estudio de tipo ANALÍTICO DESCRIPTIVO, que analizó y describió la problemática relacionada con la incidencia de los Delitos Informáticos en la Etapa de la Planeación de la Auditoria de los Estados Financieros; el grado de inferencia que tienen estos en la etapa de la Ejecución del trabajo a desarrollar.

2.1.3 DETERMINACION DE LA POBLACION

La población para esta investigación, estuvo constituida por un universo finito de 3300 Auditores inscritos en el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría, inscritos hasta el 31 de diciembre del año 2006, sobre la base de listado publicado, por dicho Consejo.

2.1.4 DETERMINACION DE LA MUESTRA.

2.1.4.1 PRUEBA PILOTO.

Se realizo con el objeto de determinar el valor de la probabilidad de éxito (p) y de fracaso (q), y de esa manera se evaluó el grado de comprensión de las interrogantes formuladas.

Para determinar "**p**" y "**q** se realizo una prueba piloto con 10 encuestas que fueron contestadas por los Auditores legalmente autorizados por el consejo de Vigilancia de la Contaduría Pública, y del municipio de San Salvador, cuyo resultado fue: **p** =90% y **q** = 10%

2.1.4.2 MUESTRA.

Para efecto de la investigación, se tomó la muestra en el área metropolitana de San Salvador a los Auditores legalmente autorizados, y se procedió a calcular de ésta con la siguiente formula bajo el método Aleatorio Simple, y por tratarse de una población finita que presenta Fisher y Navarro (1996), se determinó con la siguiente formula.[30]

$$n = (r^2 N p q) / e^2(N-1) + r^2 p q$$

Donde:

n = Tamaño de la muestra

N = Tamaño del Universo

p = Probabilidad de éxito

q = Probabilidad de Fracaso

r = Nivel de Confianza

e^2 = Margen de error al cuadrado.

---

[30] HERNÁNDEZ, Sampiere Roberto. "Metodología de la investigación "Editorial Mc Graw Hill. México, 2003. Tercera Edición. Pág. 3

DESARRLLO

q = 0.90

p = 0.10

e = 0.08

e = 0.05

Sustituyendo

$$\mathbf{n} = \frac{(1.90)^2\ (3300)(0.9)(.10)}{(0.08)^2\ (3300-1)+(1.90)^2(0.90)(0.10)}$$

$$\mathbf{n} = \frac{1072.17}{21.4385}$$

Resultando una muestra de **50** Auditores encuestados

2.1.5 UNIDAD DE ANÁLISIS

La Unidad de análisis estuvo constituida por los Auditores legalmente acreditados ante el Consejo de Vigilancia de la Contaduría Pública.

2.1.6 INSTRUMENTOS Y TÉCNICAS DE INVESTIGACION.

Para la recolección de Datos de la investigación que se llevó a cabo, se utilizó el instrumento del **cuestionario**, elaborado con preguntas cerradas, incluyó los diferentes indicadores que se exploraron y se dirigió a Socios, Gerentes o Auditor Operativo de los despachos; dicho instrumento se distribuyó entre todos los despachos que fueron seleccionados en la muestra.

La información recopilada fue compilada y ordenada y se emplearon diversos análisis, cuantitativos y cualitativos con el fin de demostrar la magnitud de la problemática planteada en el anteproyecto, y su incidencia en la opinión del Audítor.

2.1.6.1 ENCUESTA.

Se realizo con finalidad de analizar los hechos, opiniones y actitudes, mediante el instrumento de un cuestionario; los agentes en estudio, de la información que se obtuvo directamente de las personas, para conocer sus puntos de vista.

2.2 TABULACION Y ANÁLISIS DE DATOS.

El cuestionario fue diseñado en su mayoría con preguntas cerradas de posible respuestas SI o NO, a excepción de las preguntas número 3 que su posible respuesta puede ser: Gerente de auditoría, Supervisor de Auditoría, y Asistente de Auditoría; la pregunta 13 su posible respuesta puede ser: Riesgo Alto, Riesgo Medio, y Riesgo Bajo; la pregunta 16, su posible respuesta puede ser: Realiza prueba aleatoria de documentos soporte del sistema examinado, Entrevista al usuario del sistema y verifica su limite de acceso, comprobar si las transacciones se autorizan apropiadamente antes de ser procesadas por la computadora, revisa transacciones incorrectas, rechazadas, corregidas, modificadas y reclasificadas; examinar si transacciones autorizadas se registran completas y no están perdidas/ añadidas/ duplicadas/ o se cambiaron inapropiadamente.

2.2.1 Análisis de datos de la investigación efectuada a los Auditores legalmente autorizados.

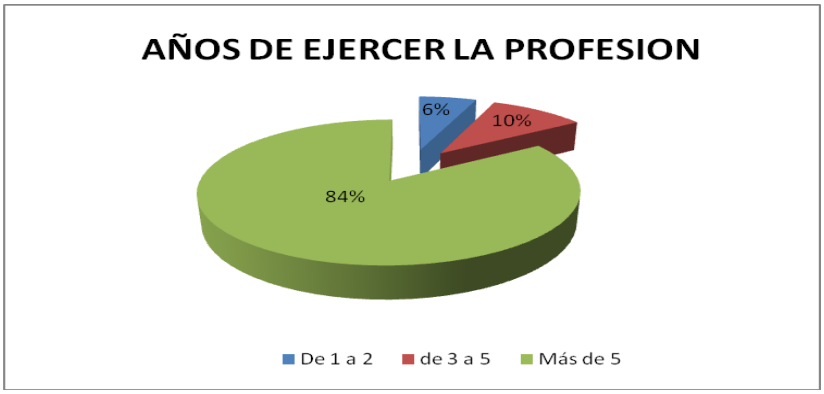
Pregunta No.1.

¿Cuántos años tiene de ejercer la auditoría?

Objetivo:

Determinar el tiempo promedio que tienen los despachos de auditoría de ejercer su profesión, para compararlo con el tiempo que tiene de ejercer auditoría bajo la presunción de los delitos informáticos.

AÑOS	CANTIDAD	PORCENTAJE
De 1 a 2	3	6.00%
de 3 a 5	5	10.00%
Más de 5	42	84.00%
TOTAL	50	100.00%



Análisis:

De la población estudiada, el 84% tienen mas de 5 años de ejercer la auditoría, mientras que el 10%, tiene de 3 a 5 años y los restantes 6%, tienen de 1 a 3 años.

La experiencia y la capacitación constante en el ejercicio de la auditoría, es muy importante, para la preparación de una buena planeación de la auditoría, ya que permitirá obtener los mejores resultados.

Pregunta No.2

¿Elabora el memorando de planeación de la Auditoría de Estados Financieros?

Objetivo:

Conocer si los auditores le dan cumplimiento a la normativa técnica.

ELABORAN	CANTIDAD	PORCENTAJE
SI	47	94.00%
NO	3	6.00%
TOTAL	50	100.00%

Análisis:

De la muestra del universo, el 94% opinaron que si elaboran el memorando de planeación, mientras que los 6% restantes opinaron que no lo elaboran.

Esta situación deja de manifiesto, que la mayoría, si tiene el debido cuidado en la preparación del memorando de planeación.

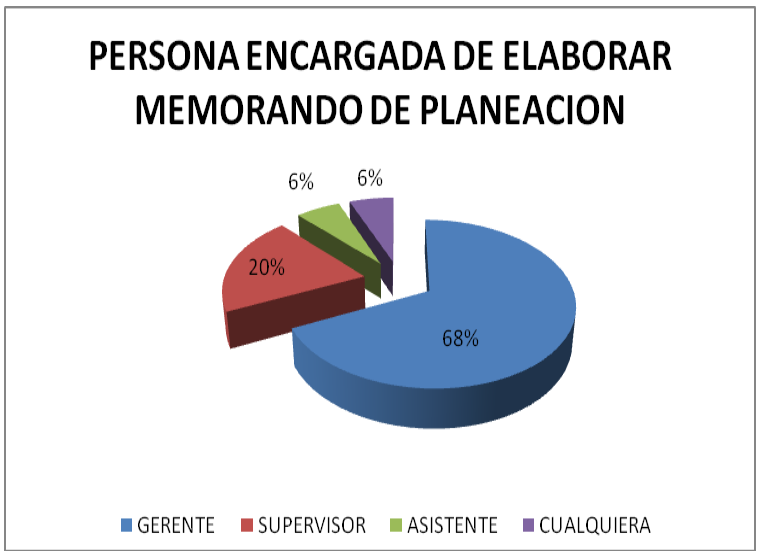
Pregunta No.3

¿Quién elabora el memorando de Planeación de la auditoría de Estados Financieros?.

Objetivo:

Indagar sobre el personal a cargo y las responsabilidades que se podrían delegar para la consideración de los delitos informáticos.

ENCARGADO DE ELABORACION	CANTIDAD	PORCENTAJE
GERENTE	34	68.00%
SUPERVISOR	10	20.00%
ASISTENTE	3	6.00%
CUALQUIERA	3	6.00%
TOTAL	50	100.00%



Análisis:

Del universo analizado, el 68% opinaron que es el Gerente quien elabora el memorando de Planeación, el 20% opinaron que el Supervisor, el 6% es el Asistente de Auditoría; y por último, el 6% que lo elabora cualquiera de los anteriores.

Al igual que en la pregunta No.2, es de suma importancia la preparación del memorando de planeación de auditoría, para garantizar que se emitirá una buena opinión de las cifras de los Estados Financieros.

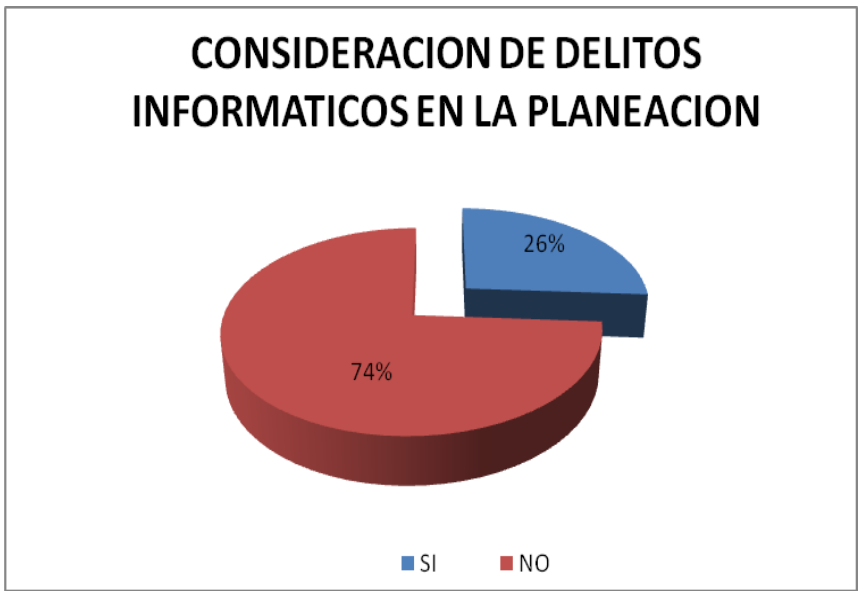
Pregunta No.4

¿Considera los delitos informáticos en la Planeación de la auditoría de Estados Financieros?

Objetivo:

Conocer si se toma en cuenta los delitos, que pueden afectar la opinión del auditor.

CONSIDERACION DELITOS	CANTIDAD	PORCENTAJE
SI	13	26.00%
NO	37	74.00%
TOTAL	50	100.00%



Análisis:

De los encuestados, 74% opinaron que no consideran los delitos informáticos en la Planeación de la auditoría, y el 13% restantes, opinaron que si los consideran.

Aquí se ve una limitación para el desarrollo de la auditoría, ya que, no se considerando la presunción de los delitos informáticos que inciden en la preparación de los Estados Financieros.

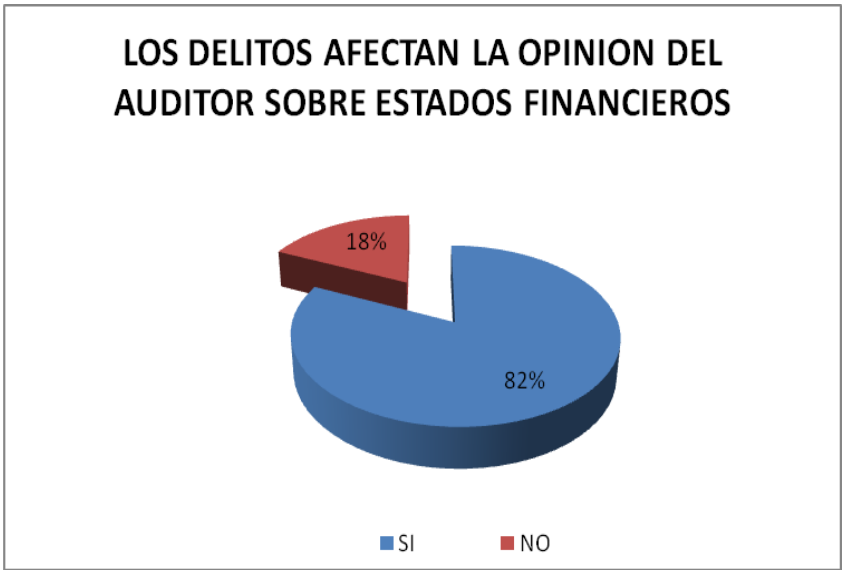
Pregunta No.5

¿Considera que los delitos informáticos afectan la opinión que dan los Auditores externos sobre los Estados Financieros?

Objetivo:

Conocer si el auditor toma en cuenta la presunción de los delitos informáticos en la razonabilidad de las cifras de los Estados Financieros.

DELITOS AFECTAN OPINION	CANTIDAD	PORCENTAJE
SI	41	82.00%
NO	9	18.00%
TOTAL	50	100.00%



Análisis:

De la población encuestada, el 82% dijeron: consideran que los delitos informáticos afectan la opinión del auditor, y el 10% dijeron que no afectan.

Se considera que los delitos informáticos, afectan directamente la opinión del audítor; dada la facilidad, que se pueden manifestar en estos tiempos de avances tecnológicos por el uso de sistemas de informáticos.

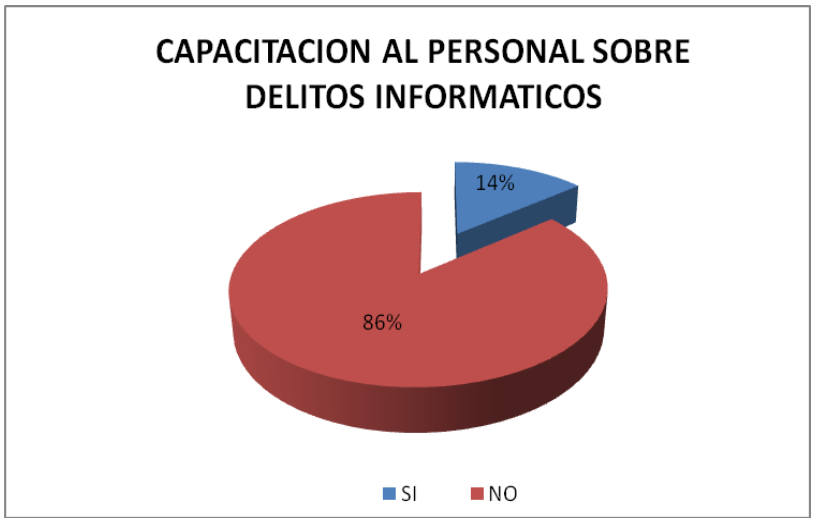
Pregunta No.6

¿Capacita a su personal el despacho de auditoria, en el área de los delitos informáticos?

Objetivo:

Indagar si los auditores capacitan a sus subalternos constantemente

CAPACITACION	CANTIDAD	PORCENTAJE
SI	7	14.00%
NO	43	86.00%
TOTAL	50	100.00%



Análisis:

Del total de la población encuestada, el 86% manifestaron que el personal no es capacitado para la detección de delitos informáticos, y el 14% dijeron que si se capacitan.

Existe una limitación para que el personal encargado de la Ejecución del trabajo de auditoría, lo desarrolle con un enfoque mas especifico. Como lo es, la detección de delitos informáticos, por lo que se debe capacitar en esta área de gran importancia.

Pregunta No.7

¿Evalúa el nivel de riesgo de los delitos informáticos en la planeación de la auditoría de Estados Financieros?

Objetivo:

Indagar si el auditor evalúa el nivel de riesgo al que pueden ser sometidos, mediante la presunción de los delitos informáticos.

ESTUDIO DELITOS INFORMATICOS	CANTIDAD	PORCENTAJE
SI	11	22.00%
NO	39	78.00%
TOTAL	50	100.00%

Análisis:

Aquí del total de los encuestados, el 78% manifestaron que no evalúan el nivel de riesgo de los delitos informáticos en la planeación, y el 22% respondió que si evalúan el nivel de riesgo.

La falta de consideración de los delitos informáticos en la planeación de la auditoría, hacen que el nivel de riesgo sea alto, dado que se desconoce el grado de incidencia de estos.

Pregunta No.8

¿El despacho de Auditoría, representa a una firma internacional?

Objetivo:

Conocer el prestigio del despacho y evaluar si le da importancia a los delitos informáticos.

REPRESENTACION INTERNACIONAL	CANTIDAD	PORCENTAJE
SI	7	14.00%
NO	43	86.00%
TOTAL	50	100.00%

Análisis:

De los auditores encuestados, el 86% respondió que no representan una firma internacional y los restantes 14% dijo que si.

Se puede observar la representación de firmas internacionales es poca, pero al igual trabajan con responsabilidad para empresas locales.

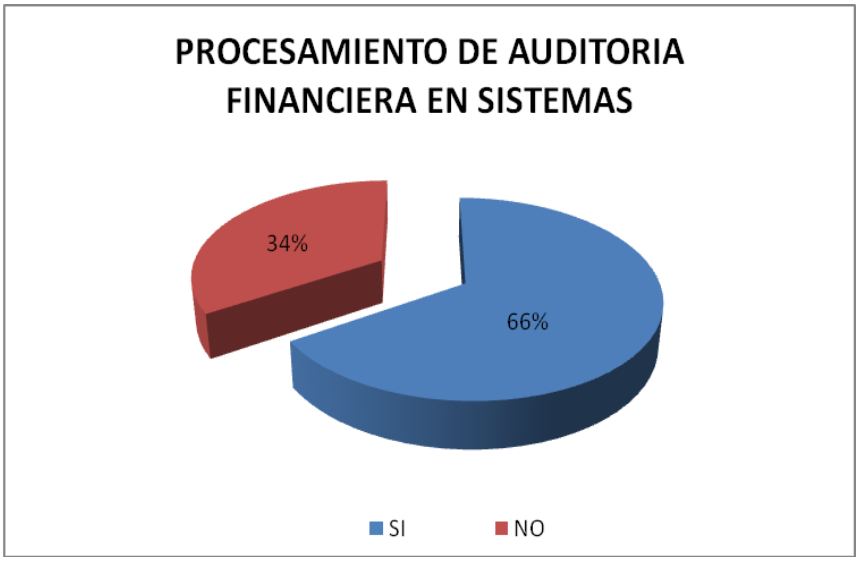
Pregunta No.9

¿Considera que los delitos informáticos afectan la opinión que da los auditores externos en los estados financieros?

Objetivo:

Conocer el grado de afectación de la opinión del auditor

PROCESO AUDITORIA EN SISTEMA	CANTIDAD	PORCENTAJE
SI	33	66.00%
NO	17	34.00%
TOTAL	50	100.00%



Análisis:

De la población encuestada, el 66% realizo auditoria de Estados Financieros generados por sistemas contables computarizados, y el 34% dijo que audito los Estados Financieros generados por medios manuales.

Se puede observar como se va incrementado el uso de sistemas contables computarizados para la generación de información necesaria en la elaboración de los Estados Financieros.

Pregunta No.10

¿Cuántos de los clientes, utilizan un sistema de Contabilidad computarizado?

Objetivo:

Determinar el nivel de riesgo de los delitos informáticos al que esta expuesto el auditor por todos los clientes que utilizan sistema de contabilidad computarizado.

UTILIZACION DE SISTEMAS	CANTIDAD	PORCENTAJE
SI	47	94.00%
NO	3	6.00%
TOTAL	50	100.00%

Análisis:

Del universo encuestado, el 94% opinaron que tienen clientes que utilizan sistema contable computarizado, y los restantes 6% dijeron que lo hacen por medios manuales.

Se puede determinar que existe un riesgo alto por el procesamiento de la información en los sistemas contable computarizados, esto debido a la presencia de los delitos informáticos, y que el auditor debe disminuirlos.

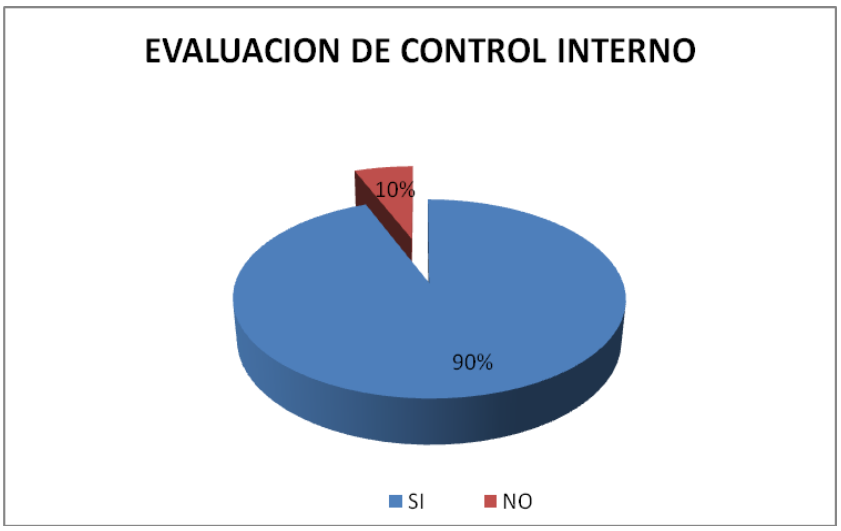
Pregunta No.11

¿En la planeación de la auditoria, realiza una evaluación del control interno, ejercido por la empresa que le de una certeza razonable para confiar en la información que genera?

Objetivo:

Conocer el grado de confianza que pueda tener el auditor para limitar las pruebas.

EVALUA CONTROL INTERNO	CANTIDAD	PORCENTAJE
SI	45	90.00%
NO	5	10.00%
TOTAL	50	100.00%



Análisis:

A esta pregunta el 90% de la población encuestada, respondió que realiza evaluación del control interno de las entidades que auditan para tener seguridad de la información que deberá analizar, y el 10% restante dijo que no hace evaluación del control interno.

El auditor busca tener seguridad razonable de la efectividad, de los controles internos establecidos, mediante la comprobación del cumplimiento de estos.

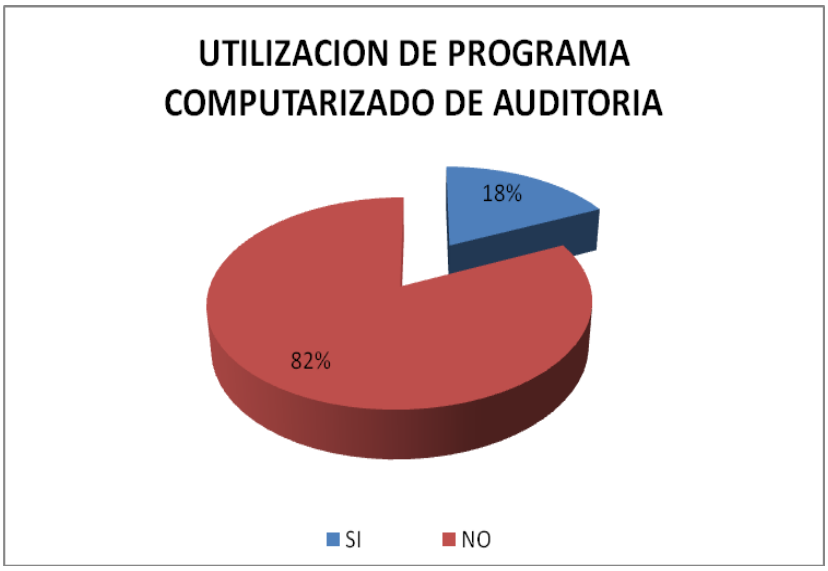
Pregunta No.12

¿Tiene un programa computarizado de auditoria para evaluar los Estados Financieros?

Objetivo:

Conocer si trabajan bajo un mismo sistema de evaluación.

UTILIZACION DE SISTEMA	CANTIDAD	PORCENTAJE
SI	9	18.00%
NO	41	82.00%
TOTAL	50	100.00%



Análisis:

El 82% de encuestados, dicen no disponer de un programa de auditoria para evaluar los Estados Financieros, y el 18% restante dijeron que si tienen

Se observa que los auditores no disponen en su mayoría de programa de auditoria para la evaluación de los Estados Financieros, haciendo pruebas selectivas de toda la información financiera y contable presentada para su análisis.

Pregunta No.13

¿Qué nivel de riesgo, representa para la entidad auditada, la utilización de sistemas Informáticos?

Objetivo:

Determinar si el despacho valora el nivel de riesgo de los sistemas informáticos en la planeación de la auditoria.

NIVEL DE RIESGO	CANTIDAD	PORCENTAJE
ALTO	28	56.00%
MEDIO	16	32.00%
BAJO	6	12.00%
TOTAL	50	100.00%

Análisis:

Aquí el 56% opinaron que el riesgo de las empresas auditadas es alto, el 32% dijeron que es riesgo medio, y 12% restantes dijo que el riesgo es bajo.

Si el riesgo es alto, el auditor tiene la tarea de disminuirlo, para que no se vea afectada la opinión que dará sobre las cifras examinadas de los Estados Financieros.

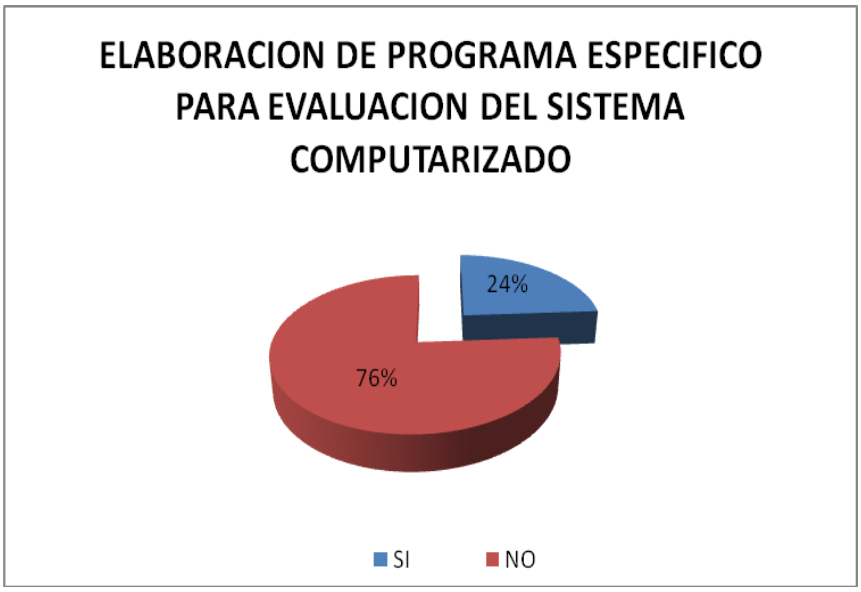
Pregunta No.14

¿En una planeación de auditoria, se toma en cuenta el hacer un programa específico para evaluación del sistema computarizado?

Objetivo:

Conocer si en la planeación de la auditoria, se es minucioso el estudio que se le hace al sistema.

ELABORA PROGRAMA	CANTIDAD	PORCENTAJE
SI	12	24.00%
NO	38	76.00%
TOTAL	50	100.00%



Análisis:

El 76% de los encuestados opinaron que No planean la evaluación de sistemas computarizados, y el restante 24% dijeron que Si planean hacer una evaluación.

No estante que los auditores realizan evaluaciones en ciertas áreas a examinar, no se esta elaborando un programa especifico para evaluar el área de sistemas computarizados, dada la facilidad con que se puede manipular, amerita se le de atención oportuna.

Pregunta No.15

¿En el programa, se toma en cuenta realizar una evaluación de entrada y salida de los sistemas computarizados?

Objetivo:

Conocer si se toma en cuenta realizar una evaluación de los aspectos importantes para la detección de los delitos informáticos.

CONSIDERACION ACCESO	CANTIDAD	PORCENTAJE
SI	12	24.00%
NO	38	76.00%
TOTAL	50	100.00 %

Análisis:

El 76% de los encuestados, opino que en el programa de auditoria no se considera el hacer una evaluación de entradas y salidas del sistema computarizado, el 24% opino que si considera la evaluación.

El no considerar en el programa la evaluación de las entradas y salidas del sistema, esta descuidando aspectos importantes como la detección oportuna de delitos informáticos.

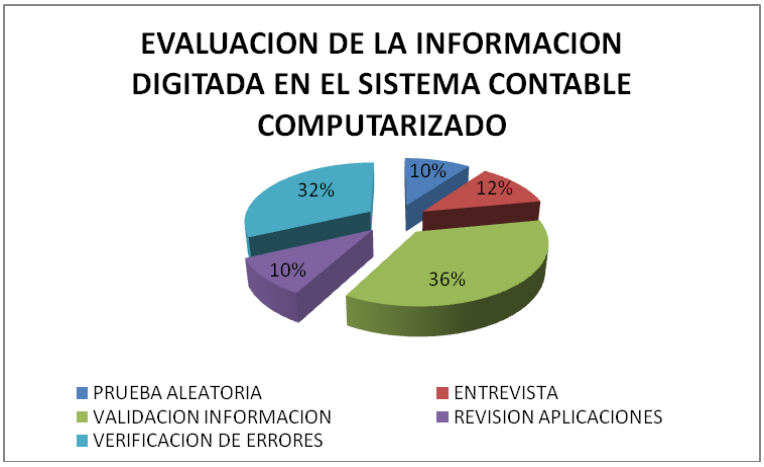
Pregunta No.16

¿Qué tipo de evaluación hace, para las entradas y salidas del sistema computarizado?

Objetivo:

Conocer que tipo de evaluaciones realizan para la detección de delitos informáticos.

VERIFICACION DE INFORMACION	CANTIDAD	PORCENTAJE
PRUEBA ALEATORIA	5	10.00%
ENTREVISTA	6	12.00%
VALIDACION INFORMACION	18	36.00%
REVISION APLICACIONES	5	10.00%
VERIFICACION DE ERRORES	16	32.00%
	50	100.00%



Análisis:

El 36% respondió que validan la información autorizada antes de ser presentada, el 32% respondió que hace una verificación de errores y si estos no han sido cambiado inapropiadamente, el 12% dijo que examina los accesos restringidos para hacer modificaciones, anulaciones y generación de datos, por ultimo el 10% respondió que revisa las transacciones incorrectas, las que fueron rechazadas, corregidas, modificadas y reclasificadas.

Los auditores deben estar en la plena capacidad para detectar la presencia de los delitos informáticos, que le aseguren emitir una buena opinión, y sobre la base de la evidencia recopilados.

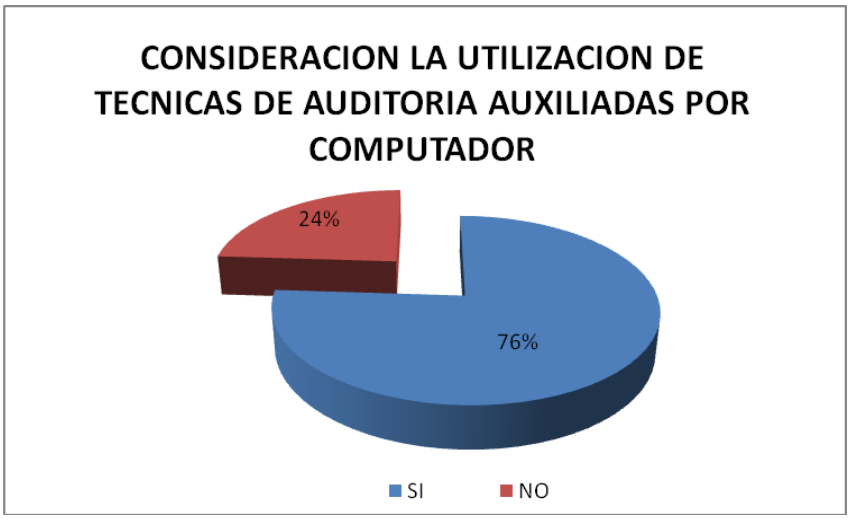
Pregunta No.17

¿En el programa se toma en cuenta, el hacer uso de las técnicas de auditoría auxiliadas por el computador?

Objetivo:

Conocer el tipo de herramientas que se utilizan para la evaluación del Sistema

USO DE PROGRAMA AUDITORIA	CANTIDAD	PORCENTAJE
SI	38	24.00%
NO	12	76.00%
TOTAL	50	100.00%



Análisis:

De la totalidad de la población encuestada, el 76% No utiliza técnicas de auditoría auxiliadas por computador, y 24% dijo que Si las utiliza.

Se puede apreciar que la utilización de esta herramienta para la realización de auditoría, se vuelven parte indispensable para desarrollar un buen trabajo.

2.3 DIAGNOSTICO DE LA INFORMACIÓN

- Del total de auditores entrevistados su mayoría no consideran los delitos informáticos en la etapa de planeación de auditoria de estados financieros.
- La mayoría de auditores consideran que los delitos informáticos afectaran la opinión sobre los estados financieros.
- El personal encargado de ejecutar el trabajo de auditoria casi en su totalidad no reciben capacitación sobre delitos informáticos.
- Los auditores en su mayoría no consideran en la planeación evaluar el nivel de riesgos de los delitos informáticos, aunque si evalúan otras aéreas.
- De las empresas que se auditan, se considera que el uso de sistemas informáticos, en un 56% es alto, lo que implica que los sistemas son vulnerables a manipulación o fraudes.
- No se consideran evaluar los sistemas informáticos en la planeación.
- En su mayoría, los auditores no consideran hacer una evaluación de control interno de entrada y salida(PED)

- Los auditores entrevistados en el caso de que evalúen el control interno, referente a las entradas y salidas de información de los sistemas informáticos, consideran en su mayoría: hacer una evaluación consistente en entrevistar al usuario del sistema y verificar el limite de accesibilidad y su verificación si los datos son autorizados antes de ser procesados en el computador dejando abierta la posibilidad de transacciones perdidas añadidas, duplicadas o cambiadas en forma inapropiada.

2.4 CONCLUSION GENERAL DE LA EXISTENCIA DEL PROBLEMA.

Los auditores necesitan conocer las incidencias de los delitos informáticos y aplicar las medidas que permitan controlar el riesgo de dar una mala opinión, debido a que no se están considerando su incidencia directa en la etapa de planeación de la auditoría de estados financieros; ya que, para el auditor la planeación es la base, para lograr la efectividad de todas las actividades que va a realizar en su examen. Se necesita capacitar a los auditores en lo relativo a las formas en que los delitos informáticos puedan incidir en la opinión. Sobre la base

de la información generada por los programas contables y de información financiera, ya que son frágiles y susceptibles a ser manipulados; ya sea por, el propio responsable de manejar el sistema o por terceras personas.

CAPÍTULO III

MODELO DE PLANEACION DE AUDITORIA DE ESTADOS FINANCIEROS BAJO EL ENFOQUE DE LOS DELITOS INFORMÁTICOS.

3.1. DESCRIPCIÓN DE LOS COMPONENTES QUE FORMAN UN MEMORANDUM DE PLANEACIÓN DE AUDITORÍA EXTERNA.

Una de las fases más importantes dentro del proceso de la auditoría de Estados Financieros, es la planeación del trabajo a desarrollar; en esta face, se describe el alcance, se establece los procedimientos de conducción de la auditoría.

La NIA 300 requiere que el auditor desarrolle y documente un plan global del trabajo; donde, describirá el alcance esperado, identificará los eventos y transacciones que puedan tener un efecto importante, en los Estados Financieros. Esta norma considera ciertos elementos o componentes importantes que debe contener la etapa de planeación de la auditoría, entre los cuales están:

a) Objetivos de la auditoria.

b) Conocimiento del Negocio.

c) Riesgo e Importancia Relativa.

d) Programas de Auditoria.

El módelo de planeación de Estados Financieros, que se plantea bajo el enfoque de los delitos informáticos, pretende ser de especial utilidad; ya que actualmente, con los constantes avances de la tecnología de la información se abren nuevos tipos de fraudes, que afectan las cifras de los Estados Financieros. Este módelo va enfocado a evaluar las áreas tradicionales de la auditoría externa, así como también, el control Interno del procesamiento electrónico de dato (PED).Tal como lo abordamos en el capitulo I, apartado 1.3, el PED esta compuesto por tres elementos principales:

a) entradas de datos al sistema.

b) Procesamiento de datos.

c) Emisión de resultados útiles para la toma de decisiones.

3.2. MEMORADUM DE PLANEACIÓN DE AUDITORÍA DE ESTADOS FINANCIEROS, BAJO EL ENFOQUE DE LOS DELITOS INFORMÁTICOS.

3.2.1. Términos de referencia del contrato.

Objetivo de la contratación.

El despacho ha sido contratado por la Empresa Servicios Integrados, S.A. de C.V., para realizar la Auditoría Externa de las operaciones contables, bajo el enfoque de los delitos informáticos, para el ejercicio fiscal del 200X.

3.2.2 expectativas del cliente.

Que la Firma, lleve a cabo su labor de la mejor manera posible, analizando en forma adecuada la situación financiera y controles internos , de tal forma que pueda dar fe de la razonabilidad de las cifras mostradas en los estados financieros; así como, del cumplimiento del control interno, leyes y regulaciones aplicables, emanadas de los diferentes entes fiscalizadores relacionados.

3.2.3 Alcance y oportunidad de los procedimientos de auditoría.

A) Alcance General.

El alcance general de la auditoría externa comprenderá la realización del trabajo siguiente:

1. Pruebas sobre los sistemas contables.
2. Pruebas sobre procedimiento de control Interno.
3. Pruebas sobre la información producida por los sistemas contables.
4. Pruebas de control sobre el procesamiento electrónico de datos (PED).
5. Pruebas de cumplimientos de políticas y procedimientos.

B. Alcance Específico.

El alcance de las técnicas y procedimientos a aplicar en el examen, se basara en las normas Internacionales de auditoría; se realizará de tal forma que su aplicación cubra al menos lo siguiente:

1.- Fases Generales.

Conocer las afirmaciones de la administración agrupadas de la siguiente manera:

Existencia u ocurrencia,

Integridad,

Valuación o asignación,

Derechos y obligaciones,

Presentación y revelación,

b. Fases Específicas.

Estudio y evaluación del control interno contable.

Pruebas de cumplimiento para confirmar la información obtenida.

Confirmación de saldos de cuentas por cobrar.

Verificación de costos financieros, análisis de adiciones al activo fijo financiero.

Examen de hechos ocurridos después de efectuado el cierre de cuentas Contables o período subsecuentes al cierre del ejercicio, tales como:

Exámenes del pasivo por operaciones financieras y relacionados con provisiones o estimaciones Contables, etc.

Salvaguarda de los respaldos después del cierre contable.

Evaluar el control en la fase del procesamiento electrónico de Datos (PED).

Evaluar el control interno para la seguridad del sistema contable.

3.2.4. Conocimiento del negocio.

La empresa Servicios Integrales, S.A. de C.V., esta constituida bajo el régimen de "Sociedad Anónima"; bajo las leyes mercantiles de El Salvador; el capital inicial de fundación de la empresa fue de Cuatro Mil dólares Americanos ($ 4,000.00), dividido en acciones por un valor de $ 11.43 cada una.

La administración de la sociedad en el año 200X; estará a cargo del Administrador Único Propietario, quien es el encargado de tomar las decisiones y la Gerencia Administrativa, la encargada de ejecutar las decisiones y delegar funciones.

La finalidad principal de la Sociedad, es la prestación de Servicios de Asesoramientos Administrativos y Financieros.

Sistema de información contable y de control.

El sistema de contabilidad MAGIC 7.1, se maneja separadamente los módulos contables, IVA, planillas, cuentas por pagar. Por lo que, hay un trafico de información al modulo de contabilidad.

La red esta compuesta por un servidor central y 9 terminales de donde se alimenta la información.

3.2.5 Riesgo e importancia relativa.

El procesamiento electrónico de datos permite concentrar numerosas etapas en un solo departamento, eliminando así el tradicional control interno, logrado mediante la separación de funciones en la etapa de registro de operaciones.

Por tal motivo, se debe considerar la importancia de los principales atributos de información, como la confiabilidad, oportunidad, veracidad y la suficiencia, estos como pilares fundamentales para evaluar el control interno, en la etapa de captura, procesamiento de datos y emisión de resultados.

3.2.6 Estudio y evaluación del control interno del PED:

Verificar y evaluar el registro y control contable efectuado mediante el procesamiento electrónico de datos.

Inspeccionar el control y acceso a los archivos que contengan las contraseñas de los usuarios.

Verificar el mantenimiento de registros de transacciones y control de lote por departamento, usuario y entrada en línea.

La firma efectuará el estudio, comprensión y evaluación del control interno existente, para determinar el alcance de los procedimientos de auditoría a aplicar. Como parte, de esta evaluación se efectuará el trabajo siguiente:

Revisión y evaluación del control interno, establecido por la Administración de la empresa.

Se obtendrá un entendimiento suficiente del control interno para planear la auditoría y determinar la naturaleza, oportunidad y extensión de las pruebas a ser desarrolladas.

Enfocaremos la evaluación hacia el ambiente de control del sistema de información y comunicación, las actividades de control, la valoración del riesgo y la vigilancia.

3.2.7. Sistemas de contabilidad y control interno

Es necesario conocer la forma en que la información contable es producida y procesada por la empresa; para lo cual, debe entenderse los sistemas y procedimientos contables, incluyendo el efecto que sobre ellos tienen los sistemas computarizados.

Se verificaran aquellos controles del PED (dentro o fuera de los sistemas de contabilidad y de control interno) que sean considerados relevantes para la auditoría de los estados financieros.

3.2.8 Ambiente de control.

Se obtendrá una comprensión del ambiente de control, suficiente para evaluar las actitudes, conciencia, y acciones de directores y administración respecto a los controles interno y su importancia en la entidad. (NIA 400, párrafo 19).

Los factores para obtener una comprensión del ambiente de control con respecto al PED pueden incluir:

1. Filosofía y estilo de operación de la administración y su enfoque en el PED, tales como cualesquier esfuerzo para mejorar el desempeño.

2. La estructura organizacional de la entidad y métodos de asignar autoridad y responsabilidad para manejar las funciones operativas del PED.
3. El sistema de control de la administración, incluyendo la función de auditoría interna, el desempeño, política de personal.
4. Procedimientos y apropiada segregación de funciones.
5. Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.
6. Establecer como prioridad la seguridad y protección de la información.

3.2.9 Procedimientos de control.

Verificación y comprensión de los controles del PED. Tales como:

1. Las políticas para Monitorear el procesamiento electrónico de datos.
2. Control interno sobre la organización del área de informática.
3. Control interno sobre los procedimientos de entradas de datos, procesamiento de información y la emisión de resultados.
4. Control interno sobre la seguridad del área de sistemas.

3.2.10. Evaluación del ríesgo de auditoría de los Estados Financieros.

Basados en los resultados de la revisión analítica preliminar, el entendimiento de los principales ciclos del negocio, relacionados con el hecho generador y las pruebas de doble propósito, se ha concluido que las áreas criticas sujetas a ser evaluadas, son:

3 Efectivo y Equivalente.

4 Cuentas por cobrar clientes- empleados y funcionarios.

5 Recursos Humanos.

6 Procesamiento electrónico de datos.

7 Ingresos.

El ríesgo de detección y ríesgo de control, se ha evaluado cualitativamente y cuantitativamente, de la siguiente manera:

Ríesgo Inherente	
Alto	Mayor de 60%
Medio	Entre 40% y el 60%
Bajo	Menor de 40%

Ríesgo de Control	
Alto	Mayor de 40%
Medio	Entre el 20 y 40%
Bajo	Menor de 20%

El ríesgo de detención se ha obtenido utilizando la formula de ríesgo de auditoría, despejando la formula y previa cuantificación de los componentes, se procede de la siguiente manera:

Donde:
RA = 5%
RI = 50%
RC = 30%
RD = ?

$$0.05 = 0.5 \times 0.30 \times rd$$

Por tanto.

$$RD = \frac{0.05}{(0.5 \times 0.30)} = 33\%$$

3.3 CONSIDERACIÓN DE LEYES Y REGLAMENTOS EN UNA AUDITORÍA DE ESTADOS FINANCIEROS

Es responsabilidad de la administración, asegurar que las operaciones de la entidad sean conducidas de acuerdo con leyes y reglamentos. La prevención y detección de incumplimiento descansa en la administración (NIA 250, párrafo 9). En este contexto, se verificara:

La compañía Servicios Integrales, S.A. de C.V., esta regulada principalmente por las siguientes leyes salvadoreñas:

a) Código Tributario y su reglamento.
b) Ley de Impuesto sobre la renta y su reglamento.
c) Ley de impuesto a la transferencia de Bienes Muebles y la prestación de servicios.
d) Código de Comercio.
e) Ley de registro de comercio.
f) Ley del seguro social.
g) Código de Trabajo.
h) Código Municipal.
i) Ley de Vialidad.
j) Ley de Tributaria Municipal.

k) Ley de Administración de Fondos para pensiones.

l) Ley de la Superintendencia de Obligaciones Mercantiles.

a) Ley Orgánica del Servicio Estadístico Nacional.

3.4. PROGRAMAS DE AUDITORÍA.

En las páginas siguientes se presentan los Programas de Auditoría a ejecutar en el examen de los Estados Financieros, bajo el enfoque de la presunción de los delitos informáticos. Se evalúa controles claves asociados al procesamiento electrónico.

CUESTIONARIO DE EVALUACIÓN SOBRE CONTROLES CLAVES ASOCIADOS AL AMBIENTE DE COTROL DEL PED

CLIENTE

PREPARADO POR

PERIODO AUDITADO

Ref

Fecha

Iniciales

Formulario P-1

No	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿ Existen descripciones del trabajo adecuadas para el personal de contabilidad ?				
2	¿Se aplican las politicas generales de PED y de seguridad de datos en forma de normas de acceso y de desarrollo de sistemas?				
3	¿ Existe una supervision adecuada de los empleados de procesamiento de dato?				
4	Esta bajo control y/o supervision del departamento del PED las siguientes actividades, acceso estándar, metodoligia de desarrollo y cambio de datos?				
5	¿ Existe un plan para el desarrollo futuro de nuevos sistemas y adquisicion de equipo, autorizadas por la gerencia?				
6	¿ Realiza la gerencia análisis de riesgo respecto a los sistemas de PED para poder llegar a opiniones informadas sobre el nivel de seguridad requerido?				
7	Existe un metodo establecido y eficaz para comunicar al personal las politicas contables procedimientos, controles internos, requi sitos o instrucciones escritas?				
8	¿ Asegura la gerencia que los sistemas contables(incluyento los aspectos del PED) y de control interno estan debidamente diseñadas se han realizado pruebas de aceptacion sobre estos y y han sido previamente autorizados?				
9	¿Vigila y supervisa la gerencia los sistemas de contabilidad (incluyendo los aspectos del PED) y los controles internos				
10	¿Existe una politica uniforme de desarrollo de sistemas, incluyendo pruebas de aceptacion que se utilizan en todos los programas ?				
11	¿Existe una politica uniforme que se sigue para todos los cambios de los programas existentes, incluyendo pruebas de aceptacion?				
12	¿ Requieren estas politicas la participacion activa de los usuarios en las fases importantes de desarrollo o de cambios incluyendo una aprobacion final?				
13	¿Requieren los estandares de PED una documentacion uniforme para cada una de las siguienes aplicaciones del PED a) Documentacion de Sistemas b) Instrucciones de operación c) Documentacion para el usuario e) Pruebas de aceptacion				
14	¿Permite la carga de trabajo del siguiente personal que realicen sus responsbilidades de control interno? Contabildiad PED				
15	¿ Se mantiene la segregacion de funciones durante la ausencia del personal(vacaciones, enfermedades, renuncias)?				
16	¿ Autorizan o realizan las siguientes funciones usuarios que no pertenezcan al departamento de PED?				
17	¿ Parece adecuada la estructura de la organización para proveer una debida segregacion de funciones?				

	CUESTIONARIO DE EVALUACIÓN SOBRE CONTROLES CLAVES ASOCIADOS AL AMBIENTE DE COTROL DEL PED CLIENTE PREPARADO POR PERIODO AUDITADO				Ref Fecha Iniciales Formulario P-1
No	PREGUNTA	SI	NO	N/A	OBSERVACIONES
18	¿ Estan segregadas las siguientes funciones? programacion de sistemas programacion de aplicaciones operaciones de los computadores administracion de bases de datos administrcion de seguridad de datos				
19	¿ Los metodos empleados para supervisar al personal orientados a conseguir que sean competentes en las posiones de contabilidad?				
20	¿ Estan los metodos empleados para supervisar al personal orientados a conseguir que sean competentes en las posiciones de Contabilidad? Contabilidad PED Otros con responsabilidad de control interno				
21	¿ Es probable que los metodos de evaluación y remuneracion del personal aseguren que las personas en las siguientes posiciones sean competentes de cumplir sus responsabilidades				
22	¿ Es relativamente estable la fuerza gerencial (es decir, rotacion) en: Gerencia Departamento de Cotabilidad Departemento de PED				
23	¿Indica los siguientes factores la competencia del personal? Baja frecuencia en los ajustes contables internos Pocos errores que requieran atencion por el personal de PED Bajo Nivel de quejas por los dapartementos de usuarios de las aplicaciones de PED. Baja frecuencia de ajustes de auditoría en años anteriores				
24	¿ La segregacion de funciones impide el acceso directo de los programas a loas bibliotecas de produccion.				
25	¿ Los cambio de Emergencia se vuelven a someter como cambios de programas normales proco despues del cambio				
26	¿ Usa la instalacion, extensamente, los controles preventivos tales como ediciones, limites de cheques, etc.?				
27	¿ Hay procedimientos para detectar situaciones en las que el procesamiento por lotes termina anormalmente?				
28	¿ Hay procedimientos para detectar situaciones en las que el procesamiento en linea termina anormalmente?				
29	¿ Son satisfactorios los controles de seguimientos manuales?				

CUESTIONARIO DE EVALUACIÓN SOBRE CONTROLES CLAVES ASOCIADOS AL DISEÑO DE SISTEMAS CLIENTE PREPARADO POR PERIODO AUDITADO				Ref Fecha Iniciales Formulario P-1
PREGUNTA	SI	NO	N/A	OBSERVACIONES
¿ Quienes intervienen al diseñar un sistema? Usuarios Analistas Programadores Operadores Gerente de Departamento				
¿Los Analistas son tambien programadores?				
¿Qué lenguaje conocen los analistas?				
¿ Que lenguaje conoce los programadores?				
¿Indique que pasos siguen los programadores para el desarrollo de un programa? Diagrama de Flujo Tablas de decisiones codificacion				
¿ Que documentacion acompaña al programa, cuando se recibe? Manual de Usuario Manual de operación Flujograma de procesos				
¿Existen normas minimas relacionadas con la documentacion de modificaciones realizadas a los programas ?				
¿ Se lleva un registro de cambios a los programas establecidos para cada aplicación que incluya detalle de cuando, por que y por quien fue realizado?				
¿ Cada vez que se modifica un programa se genera nueva documentacion de soporte?				

CUESTIONARIO DE EVALUACIÓN SOBRE CONTROLES CLAVES ASOCIADOS AL PROCESAMIENTO DE INFORMACION CLIENTE PREPARADO POR PERIODO AUDITADO			Ref Fecha Iniciales Formulario P-1	
PREGUNTA	SI	NO	N/A	OBSERVACIONES
¿ Existen normas que definan el contenido de los instructivos de captacion de datos?				
¿ Indique cuales controles internos existen en el área de capta cion de datos ? a) Firma de Autorizacion b) Recepcion de Trabajo C) Revision de Documentos e) Verificacion f) Errores de Trabajo g) produccion de trabajo				
¿Quien controla las entradas las entradas de documentos fuentes?				

EVALUACION DEL CONTROL INTERNO GENERAL					
Nª	Preguntas	Respuestas			
		N/A	SI	NO	OBSERVACIONES
1	¿Se tiene una grafica de organización?				
2	¿Las funciones de Contabilidad estan separadas y definidas?				
3	¿Los auditores internos son razonablemente independientes de las personas o departamantos sujetos a sus auditorias				
4	¿El alcance de la auditoria interna es razonablemente correcto?				
5	¿Los auditores internos se guian por programas escritos?				
6	¿Rinden reportes escritos los auditores internos sobre todo el trabajo desarrollado?				
7	¿Todo el personal que tiene puesto de responsabilidad esta convenientemente afianzado?				
8	¿ La empresa sigue la practica de registrar todos los ingresos, costos y gastos por medio de cuentas deudoras y acreedoras de modo que la contra -cuenta de una partida de caja sea siempre cuenta de balance?				
9	¿El personal que disfruta de vacacioenes es sustituido por alguien durante su ausencia?				
10	¿Las acciones y certificados de aportacion estan controlados convenientemente?				
11	¿ Son todos los asientos de diario aprobados por un funcionario autorizado?				
12	¿Se hace una revision periodica de los seguros en vigor por algun funcionario autorizado?				
13	¿ Se preparan los Estados Financiros a intervalos suficientemente frecuentes en forma tal que atraigan la atencion de la gerencia sobre: Fluctuaciones en costos, ingresos, cuentas por cobrar, inventarios, etc.				
14	¿ Se exige a los empleados que desempeñen funciones de contabilidad y tesoreria que tomen vacaciones y sus tareas son desempeñadas por otros?				
15	¿ Estan todos los asientos de diario debidamente explicados y adecuadamente respaldados por los comprobantes relativos?				
16	¿ La empresa tiene fondo de caja chica o fondo de caja variable?				
17	¿ Son los encargados de fondos de caja independientes del empleado que es encargado de cobrol?				
18	¿ Recae la responsabilidad principal de cada fondo de caja sobre una sola persona?				
19	¿ Se hace corte de los fondos en efectivo por las personas encargadas de sus custodia? ¿ Con que frecuencia?				
20	¿ Estan los fondos de caja chica debidamente respaldados por comprobantes?				
21	¿ Estan autorizadas por el consejo de administracion todas las cuentas bancarias asi como las combinaciones de firmas que se requieren?				

EVALUACION DEL CONTROL INTERNO GENERAL					
Nª	Preguntas	Respuestas			
		N/A	SI	NO	OBSERVACIONES
22	¿ Estan registradas en libros todas las cuentas bancarias que existen a nombre de la compañía?				
23	¿ Se registran en libros un asiento para cada una de las transferencias de una cuenta bancaria a otra?				
24	¿ Liste a continuacion las personas que estan autorizadas para firmar cheques?				
25	¿ Se controlan todos los talonarios o formas de cheques que no estan en uso en forma tal que se impida su utilizacion indebida?				
26	¿ Se mutilan los cheques anulados (para evitar su uso posterior) y se archivan a fin de controlar que la secuencia numerica este completa?				
27	¿ Esta prohibida la firma de cheques en blanco?				
28	¿ Se hacne los pagos unicamente contra comprobantes aprobados?				
29	¿ Se depositan las cobranzas intactas y diariamente?				
30	¿ Se prepara y archivan duplicados de las fichas de deposito selladas por el banco?				
31	¿ Se concilian las cuentas bancarias en forma regular?				
32	¿ Formula las conciliaciones un empleado que no interviene en la preparacion aprobacion o firma de los cheques o maneja cobros?				
33	¿ Revisa las conciliaciones un funcionario responsable?				
34	¿ Que clase de registros de pagos se llevan y quien lo lleva?				
35	¿ Necisitan dos firmas todos los cheques que representan desembolsos de fondos en general?				
36	¿ Esta el departamento de facturacion completamente separado del departamento de cuentas por cobrar?				
37	¿ Cuales son las condiciones de pago concedidas a los clientes?				
38	¿ Se proporcionan a los clientes estados de cuentas periodicos?				
39	¿ Quien autoriza la extencion de credito o aprueba los descuentos, las devoluciones o las rebajas a los clientes?				
40	¿ Se toman normalmente los precios de facturacion de listas de ellos debidamente aprobados?				
41	¿ Se autoriza por el departamento de ventas las excepciones a los precios de lista?				
42	¿ Se verifica los precios y calculos de las facturas por otra persona que no sea el mismo facturador?				
43	¿ Recibe el departemento de cobros directamente del departamento de facturacion, copias de todas las facturas?				
44	¿ Se concerva todos los ejemplares de las facturas canceladas y se autoriza su cancelacion por un supervisor adecuado?				
45	¿ Se aseguran las mercancias enviadas estableciendo oportunamente reclamos por daños a transporte?				
46	¿ Tienen prohibido los empleados de los departamentos de facturacion y de ventas manejar fondos de la compañía?				

EVALUACION DEL CONTROL INTERNO GENERAL					
Nª	Preguntas	Respuestas			
		N/A	SI	NO	OBSERVACIONES
47	¿ Se ha centralizado la funcion de compras en un departemento separado de los departamentos de contabilidad y bodega?				
48	¿ Se hacen todas las compras sobre la base de requisiciones o solicitudes escritas o se caso en cedulas progrmas, relaciones en orden de produccion preparados por el departamento de producion ?				
49	¿ En las compras de importancias se piden dos o mas cotizaciones a los proveedores?				
50	¿ Se hace por escrito las ordenes de compras a los proveedores, indicando calidades, precios, fechas de entrega, etc.?				
51	¿ Se firman las ordenes de compras por personas autorizadas ?				
52	¿ se requiere que las ordenes de compras que excedan de ciertos limites importes sean aprobadas y firmadas por algun funcionario superior?				
53	¿ Estan prenumeras por la imprenta las ordenes de compra ?				
54	¿ Se mandan copias de las ordenes de compra a los departamentos de contabilidad y de recibo de mercancias?				
55	¿ Se hacen notas de cargo para: mecancias devueltas, faltantes, reclamaciones a los transportistas?				
56	¿ Conserva el departamento de Bodega un registro permanente y cronologico de todas las entradas?				
57	¿ Existen controles adecuados para el registro del impuesto al valor agregado?				
58	¿ Existe un departamento de personal que mantenga un regristro completo del personal, que incluya los datos sobre cuotas de salarios, etc.?				
59	¿ Se pagan los salarios minimos aprobados por el consejo del salario minimo?				
60	¿ Se procura que haya rotancion de los puestos ?				
61	¿ Se les obliga a que tomen vaciones anuales, según lo estipula la ley?				
62	¿ Se autorizan por escrito los cambios de sueldos y salarios, ya sea por el departamento de personal o por ejecutivos facultados para ello?				
63	¿ Se incorpora todo el personal al regimen de seguro social?				
64	¿ Dan por escrito los empleados aquellos descuentos que son diferente a los obligados por ley?				
65	¿ Existen procedimientos adecuados para asegurar informes correctos sobre el tiempo trabajado ?				
66	¿ Se requiere autorizacion por escrito para pagar ausencias por enfermedad o permisos?				
67	¿ Se controlan adeacuadamente los salarios y sueldos no pagados para evitar mal uso de ellos?				
68	¿ Se hacen distribucion contables de sueldos y salarios?				
69	¿ Se hacen periodicamente auditoria internas de nominas y listas de personal?				
70	¿ Se llevan cuentas de control apropiadas para la ubicación de los acitvos fijos de la empresa?				

EVALUACION DEL CONTROL INTERNO GENERAL					
Nª	Preguntas	Respuestas			
		N/A	SI	NO	OBSERVACIONES
71	¿ Se lleva un control sobre las adiciones al activo fijo a traves de un sistema mecanizado?				
72	¿ Concuerdan los registros detallados con los controles y con el mayor auxiliar?				
73	¿ Que normas rigen en lo que respecta los bienes totalmente depreciado?				
74	¿ Cual es la politica de la compañía en cuanto asegurar los bienes ?				
75	¿ Autoriza la administracion las peticiones de prestamos personales?				
76	¿ Existen compias de actas conrespectos a prestamos adquiridos por la compañía?				
77	¿ Emplea la compañía agentes independientes para el registro y traspaso de las acciones?				
78	¿ Quien esta acargo de la custodia de los certificados no emitidos ?				
79	¿ Se lleva un libro de aumento y disminucion de capital?				
80	¿ Exite acta de acuerdo de amortizacion de perdidas y de ganancias acumuladas?				
81	¿Se ha protocolizado ante un notario tanto el capital original dela empresa, como los aumentos posteriores?				
82	¿ Se distinguen debidamente en la contabilidad las diferentes clases de acciones emitidas por la empresa?				
83	¿ Se contabilizado debidamente los dividendos decretados?				
84	¿ Existen unicamente acciones nominativas?				
85	¿ Se requieren pedidos escritos de los clientes en todos los casos?				
86	¿ Se revisan los pedidos por el departemento de ventas o por el departamento de bodega , antes de ser aceptados ?				

CAPITULO IV

4. CONCLUCIONES Y RECOMENDACIONES

Sobre la base de la investigación realizada en los despachos de Auditoria legalmente autorizados para ejercer en el área de San Salvador, por medio de encuesta a gerentes, y encargados de elaborar el Memorando de Planeación de Auditoría de Estados Financieros, se ha preparado el presente capitulo titulado **MODELO DE PLANEACION DE AUDITORIA FINANCIERA BAJO EL ENFOQUE DE LA PRESUNCIÓN DE LOS DELITOS INFORMATICOS,** con el cual damos por finalizado el trabajo de graduación

4.1 Conclusiones

. En los despachos de auditoría, a pesar de que en la mayoría los gerentes elaboran el memorando de planeación, no se está considerando la incidencia de los delitos informáticos en la etapa de planeación.

. El Personal encargado de elaborar el memorando de planeación, esta conciente de que los delitos informáticos afectan la opinión del audítor sobre los Estados Financieros; más sin embargo el resultado

de nuestra investigación, revela que el 74% de los despachos que ejercen la auditoría, no consideran evaluar la parte de controles interno de los sistemas.

La investigación revela, que un 86% de la población encuestada no capacita al personal encargado de ejecutar el trabajo de auditoría para que detecten los delitos informáticos.

. Sobre la base de la experiencia los despachos, los auditores evalúan el Control Interno que las empresas. Determinan que el Riesgo es alto, pero no consideran evaluar áreas de riesgo como el procesamiento electrónico de datos (PED).

La carencia de controles específicos del área de sistemas informáticos computarizados, tienen riesgo alto; ya que, se ejerce poco control en la evaluación en esta área, por parte de los auditores.

4.2 Recomendaciones

. Es indispensable considerar en la etapa de la planeación de la auditoría los delitos informáticos, ya que estos, inciden directamente en la opinión de los auditores sobre la razonabilidad de las cifras en los estados financieros.

. En virtud de la existencia de los delitos informáticos, es necesaria la implementación de planes que incluyan la capacitación del personal de auditoría en el área de detección y control de las incidencias de los delitos informáticos; dado, los constantes cambios y crecientes modificaciones en los sistemas, nuevos software, nuevos niveles de acceso a los sistemas para procesar los datos.

. El auditor debe sugerir a la administración, que se busquen los mecanismos que permitan la reducción de riesgo, mediante la implementación de controles en el área operativa de los sistemas

. Los auditores al planear, deben incluir evaluaciones en el área del PED, que les permitan verificar la eficiencia y eficacia en el resultado de la información, con la finalidad de vigilar el adecuado

cumplimiento de la captura de los datos, procesamiento y emisión de resultados, prevenir y disminuir posibles errores, deficiencias de operación, el uso fraudulento de la información que se procesa, robos; alteraciones, modificaciones de la información, sistemas, programas de la empresa auditada; así como, el mantenimiento y seguridad de equipos y sistemas.

X. BIBLIOGRAFIA

LIBROS

ARENS, A. Arens, RANDAL J. Elder, MARK S. Beasley, año 2007, Décimo primera Edición Auditoria un enfoque integral.

GRINAKER R.L. y BARR, Ben B., Auditoria. El examen de los Estados Financieros.

HERNÁNDEZ SAMPIERE, Roberto y Otros, Metodología de la Investigación, Segunda Edición.

MUÑOZ RAZO, CARLOS. Año 2002, Primera Edición. Auditoria en sistemas Computacionales, Primera Edición, México.

PERDOMO MORENO, Antonio, Cuarta Edición "Guia de Auditoria" Mc Graw Hill
Fundamentos de Control Interno, Cuarta edición, A. Perdomo Moreno.

GONZALEZ CASTELLANOS, Herbin Amory. Año 1978 "Fraudes en Sistemas de Procesamiento Electrónico de Dados. Guatemala.

BENAVIDES SALAMANCA, Leo Bladimir. Año 2005, La Penalización de los Delitos Informáticos en El Salvador. Trabajo de Graduación para optar al grado de Licenciado en Ciencias Jurídicas, Universidad de El Salvador. Facultad de Jurisprudencia y Ciencias Sociales.

DIRECCIONES ELECTRONICAS

www.monrafias.com/trabajos/legisdelinf/legisdelinf.shtml

www.monografias.com/trabajos34/softwares-malignos/softwares-malignos.shtml#virus

NORMAS LEGISLATIVAS

Decreto Legislativo No.1030, Código. Penal Salvadoreño. Diario Oficial No.105. Tomo No.335.26 abril 1996. Arts. No.172 y 173

NORMAS TÉCNICAS, CONTABLES Y DE AUDITORIA

Instituto Mexicano de Contadores Públicos. NIA 300: Planeación, Normas de Auditoria, México 2004

Instituto Mexicano de Contadores Públicos. NIA 400: Planeación, Normas de Auditoria, México 2004

ANEXO

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

CUESTIONARIO DE INVESTIGACION

ESTUDIANTES UNIVERSITARIOS, PARA OBTAR AL GRADO DE LICENCIATURA EN CONTADURIA PÚBLICA.

N° _____

FECHA:_____

DIRIGIDO A LOS DESPACHOS DE AUDITORIA

TEMA DE INVESTIGACION Consideran los despachos de auditoria los delitos informáticos en la etapa de planeación de la auditoria de los estados financieros.

Objetivo:

1. indagar si los despachos de auditoria, le dan cumplimiento a las normas de auditoria, en cuanto planear el trabajo del auditor
2. Obtener información necesaria y actualizada acerca de la consideración de los delitos informáticos en la etapa de planeación de la auditoria de Estados Financieros.

INDICACIONES: lea cuidadosamente cada pregunta para su mejor comprensión, y luego responda en forma objetiva a cada una de ellas, o selecciones la alternativa que a su juicio considere la mas indicada.

CONOCIMIENTOS GENERALES

1) ¿Cuantos años tiene de ejercer la auditoria Externa?

1 a 2 ☐

3 a 5 ☐

Más de 5 años ☐

Objetivo: Determinar el tiempo promedio que tienen los despachos de auditoria de ejercer su profesión, para compararlo con el tiempo que tienen ejercer auditoria bajo la presunción de los delitos informáticos.

2) ¿Elabora el memorandum de planeación de la auditoria de estados financieros?

Objetivo: conocer si los auditores, le dan cumplimiento a la normativa técnica.

SI ☐ NO ☐

3) ¿quien elabora el memorandum de planeación de la auditoria de estados financieros?

Gerente de Auditoria ☐

Supervisor de Auditoria ☐

Asistente de Auditoria ☐

Objetivo: indagar sobre el personal a cargo y las responsabilidades que se podían delegar para la consideración de los delitos informáticos

4) ¿considera los Delitos informáticos en la planeación de la auditoria de estados financieros?

Objetivo: conocer si toma en cuenta los delitos que puedan afectar la opinión del auditor.

SI ☐ NO ☐

5) ¿Considera que los delitos informáticos afectan la opinión que da los auditores externos en los estados financieros?

.Objetivos: conocer si el auditor toma en cuenta la presunción de los delitos informáticos en la razonabilidad de las cifras de los estados financieros.

SI ☐ NO ☐

6) ¿Capacita a su personal el despacho en el área de los delitos informáticos?

Objetivo: indagar si los auditores capacitan a sus subalternos constantemente.

SI ☐ NO ☐

7) ¿Evalúa el nivel de riego de los delitos informáticos en la planeación de la auditoria de estados financieros?

Objetivo: indagar si el auditor evalúa el nivel de riesgo al que pueden ser sometidos, mediante la presunción de los delitos informáticos

SI ☐ NO ☐

8) ¿El despacho de auditoria representa a una firma internacional?

Objetivo: Conocer el prestigio del despacho y evaluar si le da importancia a los delitos informáticos.

SI ☐ NO ☐

9) ¿En el Ejercicio recién pasado realizo auditoria de Estados Financieros, que fueron preparados por un sistema de Contabilidad?

Objetivo: Conocer si el auditor a trabajado con estados financieros preparados con sistema.

SI ☐ NO ☐

10) ¿Cuántos de sus clientes usan un sistema de contabilidad computarizado?

Objetivo: Detectar el nivel de riesgo de delitos informáticos al que esta expuesto el auditor por todos los clientes que utilizan un sistema de contabilidad computarizado.

de 1 a 10 ☐

De 10 a 25 ☐

De 25 en adelante ☐

11) ¿En la planeación realiza una evaluación del control interno ejercido por la empresa que le de una certeza razonable para confiar en la información que este genera?
Objetivo: conocer el grado de confianza que pueda tener el auditor para limitar sus pruebas.

SI ☐ NO ☐

12) ¿Tiene un programa computarizado de auditoria para evaluar los estados financieros?
Objetivo: Conocer si trabajan bajo un mismo sistema de evaluación.

SI ☐ NO ☐

13) ¿En el programa computarizado de auditoria existe un formato de los programas que utilizan en la ejecución del trabajo?
Objetivo: detectar si utilizan estándares en los programas o utilizan alternativas para ampliar las pruebas.

SI ☐ NO ☐

14) ¿En la planeación toma en cuenta hacer un programa específico para evaluación del sistema computarizado?
Objetivo: Conocer si en la plantación de la auditoria, se es minucioso el estudio que se le hace al sistema.

SI ☐ NO ☐

15) ¿En el programa se toma en cuenta realizar una evaluación de las entradas y salidas del sistema computarizado?
Objetivo: Conocer si considero uno de los aspectos importantes para la detección de los delitos informáticos

SI ☐ NO ☐

16) ¿Qué tipo de Evaluaciones hace para las entradas y salidas del sistema computarizado?

Realiza pruebas aleatorias de la documentación soporte del sistema, examinando la fuente de los mismos.

☐ • Se entrevista al usuario del sistema y se verifica su limite de acceso.

☐ • Se examina y se verifica si existe el acceso restringido del personal autorizado para las modificaciones, anulaciones y salidas de datos.

☐ • Se comprueba si las transacciones son autorizadas en forma apropiada antes de ser procesadas por la computadora.

☐ • Revisa las transacciones incorrectas, las que fueron rechazadas, corregidas, modificadas, reclasificaciones.

☐ • Examina si las transacciones que están autorizadas son registradas completamente y no están perdidas, añadidas, duplicadas o han sido cambiado en forma no apropiada.

Objetivo: conocer que tipo de evaluaciones realizan para la detección de delitos informáticos.

17) ¿En el programa se toma en cuenta hacer uso de las Técnicas de Auditoria Auxiliadas por el Computador?
Objetivo: para conocer el tipo de herramientas que se utilizan para la evaluación del sistema.

SI ☐ NO ☐