# UNIVERSIDAD DE EL SALVADOR

## FACULTAD DE CIENCIAS ECONÓMICAS

## ESCUELA DE CONTADURÍA PÚBLICA


# "PROGRAMAS DE TRABAJO PARA LA OBTENCION DE EVIDENCIA SOBRE LAS OPERACIONES VIRTUALES". CASO. AUDITORIA REALIZADA A EMPRESAS SALVADOREÑAS QUE SE DEDICAN AL COMERCIO ELECTRÓNICO.

**TRABAJO DE INVESTIGACION PRESENTADO POR:**

PEDRO RIGOBERTO GIRON LIEVANOS
LIZETH GUADALUPE PALACIOS MENDEZ
MARIA JOSÉ ZELAYANDIA CASTILLO

**PARA OPTAR AL GRADO DE**

**LICENCIADO(A) EN CONTADURÍA PÚBLICA**

**SEPTIEMBRE 2007**

**SAN SALVADOR EL SALVADOR CENTROAMERICA**

## AUTORIDADES UNIVERSITARIAS

| | |
|---|---|
| Rector(a) | : Dra. Maria Isabel Rodríguez |
| Secretario(a) General | : Licda. Alicia Margarita Rivas de Recinos |

Facultad de Ciencias Económicas:

| | |
|---|---|
| Decano | : Lic. Emilio Recinos Fuentes |
| Secretario(a) | : Licda. Vilma Yolanda Vasquez de Del Cid |
| Docente Director | : Lic. Juan Vicente Alvarado |
| Coordinador de Seminario | : Lic. Héctor Alfredo Rivas Núñez |
| Docente Observador | : Lic. Eddie Gamaliel Castellanos |

Septiembre de 2007

San Salvador El Salvador Centro América

## AGRADECIMIENTOS

Agradezco a Dios todo poderoso por darme la fortaleza de culminar mi carrera, a mi padre quien en gloria este, a mi madre que con amor y esfuerzo a cuidado a mis dos tesoros Katya y Miguelito, a mi esposo por su amor y comprensión, a mis suegros y a mi hermana que de una u otra forma me brindaron su apoyo.

LIZETH GUADALUPE PALACIOS MENDEZ

Agradezco a Dios todo Poderoso, a mis padres por su comprensión y apoyo en el transcurso de mi carrera. Agradezco también a mi familia y demás personas que de alguno u otra forma me ayudaron a dar este paso.

PEDRO RIGOBERTO GIRON LIEVANOS

Agradezco primeramente a Dios todo poderoso y a la Santísima Virgen María por permitirme lograr uno de mis objetivos, a mis padres: Antonia Castillo y José Zelayandia que siempre me han brindado su ayuda, amor y comprensión, a mis hermanos Esmeralda y Gustavo por su apoyo incondicional y a todas las personas que de alguna manera han contribuido a lograr este triunfo.

MARIA JOSE ZELAYANDIA CASTILLO

# INDICE

**CONTENIDO** **PAG.**

**CONTENIDO** **PAG.**

**CONTENIDO** **PAG.**

**CONTENIDO** **PAG.**

**CONTENIDO** **PAG.**

10. LISTADO DE DESPACHOS CONTABLES Y DE AUDITORIA CONSTITUIDOS COMO SOCIEDADES COLECTIVAS DE CAPITAL FIJO QUE HAN ACTUALIZADO INFORMACIÓN DEL REGISTRO, SEGÚN ARTÍCULO 7 DE LA LEY REGULADORA DEL EJERCICIO DE LA CONTADURIA PÚBLICA (ACTUALIZADO A FEBRERO 2007)
11. LISTADO DE EMPRESAS SQUE REALIZAN COMERCIO ELECTRÓNICO EN EL SALVADOR
12. ENCUESTA DIRIGIDA A FIRMAS DE AUDITORIA AUTORIZADAS POR EL CONSEJO DE VIGILANCIA DE LA PROFESIÓN DE LA CONTADURÍA PÚBLICA Y AUDITORIA
13. ENCUESTA DIRIGIDA A EMPRESAS QUE REALIZAN COMERCIO ELECTRÓNICO EN EL SALVADOR
14. PRINCIPALES PUNTOS EN LA AUDITORIA DE SISTEMAS
15. METODOLOGIA PARA REALIZAR AUDITORIAS DE SISTEMAS COMPUTACIONALES
16. ESQUEMA DE CONTROL INTERNO EN EL AREA DE INFORMÁTICA

16-A CUADRO DE CONTROL INTERNO EN EL AREA DE INFORMÁTICA

17. CICLO DE VIDA DE LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL
18. PROCEDIMIENTOS PARA ELABORAR EL INFORME DE AUDITORIA

# RESUMEN EJECUTIVO

Los avances tecnológicos en el mundo actual han impulsado el uso del comercio electrónico como herramienta de comercialización de productos o servicios, por lo que las empresas han optado por la utilización de este medio para realizar sus transacciones, al mismo tiempo se han visto en la necesidad de contar con personal que evalué la veracidad de todas las operaciones, es aquí donde surge la auditoría de los sistemas de información en la que el auditor se encarga de la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad de la información. En este tipo de auditorías habrá que evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, y obtención de información.

Se requieren varios pasos para realizar una auditoría, el auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos, alcance y procedimientos que le permitan obtener evidencia para sustentar los hallazgos

encontrados y poder emitir así su opinión sobre el área que esta evaluando.

En nuestro país la auditoria de sistemas informáticos no es tan ejercida como otros tipos de auditoría (auditoría financiera, administrativa, operacional, integral, de cumplimiento fiscal). Según la investigación realizada este suceso se debe en primer lugar a la falta de capacitación del personal para realizar ese tipo de auditoría y en segundo lugar a la falta de recursos tecnológicos.

La naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevarla a cabo, requieren de un amplio conocimiento y capacitación de los auditores, ya que el avance de la auditoría no se detiene y requiere una mayor especialización en la evaluación de las áreas y ramas del desarrollo tecnológico, esta es la razón por la que las auditorias son cada vez mas singulares, lo que hace necesario la creación de programas de trabajo que permitan simplificar y desarrollar de una forma lógica la auditoría en esta área.

# INTRODUCCION

Al convertirse los sistemas de información cada vez más dependientes del computador y con el aparecimiento del internet y el comercio electrónico surge la necesidad de implementar nuevas técnicas y procedimientos para verificar que los sistemas informáticos funcionen correctamente y que la información que en él se procesa sea verídica.

En el Capítulo I Antecedentes y Marco Conceptual se detallan los antecedentes de la auditoria y del comercio electrónico que son los temas principales en los cuales se basa la investigación, así mismo se presentan conceptos y definiciones entorno a la auditoría de sistemas, dando los elementos fundamentales que ayudaran a la comprensión de la temática investigada.

En el Capítulo II se muestra la metodología utilizada para la obtención y análisis de los datos e interpretación de los resultados sobre los cuales se baso la investigación. Los resultados fueron obtenidos por medio de encuestas dirigidas a empresas dedicadas al comercio electrónico en

El Salvador, así como a los despachos de auditoría constituidos como Sociedad en Comandita Simple que se encuentran en el área de San Salvador.

En el Capítulo III se presenta la propuesta consistente en Programas de Trabajo Para la Obtención de Evidencia Sobre Las Operaciones Virtuales, en donde se plasman los procedimientos a seguir para la evaluación de las principales áreas de las empresas que se dedican al comercio electrónico.

En el Capítulo IV se presentan las conclusiones y recomendaciones las cuales están basadas en los resultados obtenidos en la investigación y ponen de manifiesto aquellas circunstancias a las cuales se enfrenta el profesional de la contaduría pública y auditoria hoy en día.

# CAPITULO I ANTECEDENTES Y MARCO CONCEPTUAL

## 1.1 ANTECEDENTES

### 1.1.1 ANTECEDENTES DE LA AUDITORÍA

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

La revolución industrial llevada a cabo en la segunda mitad del siglo XVIII, imprimió nuevas direcciones a las técnicas contables, especialmente a la auditoría, pasando a atender las necesidades creadas por la aparición de las grandes empresas (donde la naturaleza es el servicio es prácticamente obligatorio).

En los Estados Unidos de Norteamérica, una importante asociación cuida las normas de auditoría, la cual publicó diversos reglamentos, de los cuales el primero que conocemos data de octubre de 1939, en tanto otros

consolidaron las diversas normas en diciembre de 1939, marzo de 1941, junio de 1942 y diciembre de 1943.

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

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

Acreditase, que el término auditor evidenciando el titulo del que practica esta técnica, apareció a finales del siglo XVIII, en Inglaterra durante el reinado de Eduardo I.
En nuestro país se prevé un incremento en la profesión contable en el sector auditoría, razón por la cual deben crearse, en nuestro círculo de enseñanza cátedra para el estudio de la materia, incentivando el aprendizaje y asimismo organizarse cursos similares a los que en otros países se realizan.

### 1.1.2 COMERCIO ELECTRONICO

#### 1.1.2.1 ANTECEDENTES A NIVEL MUNDIAL

El comercio, actividad ancestral del ser humano, ha evolucionado de muchas maneras. Pero su significado y su fin es siempre el mismo. Según el diccionario consultor de economía, el Comercio es "el proceso y los mecanismos utilizados, necesarios para colocar las mercancías, que son elaboradas en las unidades de producción, en los centros de consumo en donde se aprovisionan los consumidores, último eslabón de la cadena de comercialización. Es comunicación y trato".

En líneas generales, y con un sentido amplio, el comercio implica la investigación de mercado con el fin de interpretar los deseos del consumidor, la publicidad que anuncia la existencia del producto, la posibilidad de adquirirlo, y en que lugar, a la vez que se utilizan los métodos de persuasión, la venta al por menor y finalmente, la adquisición por parte del público.

Según lo expuesto, a través de los años han aparecido diferentes formas o tipos de comercio. A principio de los

años 1920 en Los Estados Unidos apareció la venta por catálogo, impulsado por las grandes tiendas de mayoreo. Este sistema de venta, revolucionario para la época, consiste en un catálogo con fotos ilustrativas de los productos a vender. Este permite tener mejor llegada a las personas, ya que no hay necesidad de tener que atraer a los clientes hasta los locales de venta. Esto posibilitó a las tiendas poder llegar a tener clientes en zonas rurales, que para la época que se desarrollo dicha modalidad existía una gran masa de personas afectadas al campo. Además, otro punto importante de esto es que los potenciales compradores pueden escoger los productos en la tranquilidad de sus hogares, sin la asistencia o presión, según sea el caso, de un vendedor. La venta por catálogo tomó mayor impulso con la aparición de las tarjetas de crédito; además de determinar un tipo de relación de mayor anonimato entre el cliente y el vendedor.

A mediados de 1980, con la ayuda de la televisión, surgió una nueva forma de venta por catálogo, también llamada venta directa. De esta manera, los productos son mostrados con mayor realismo, y con la dinámica de que pueden ser exhibidos resaltando sus características. La venta directa

es concretada mediante un teléfono y usualmente con pagos de tarjetas de crédito.

A principio de los años 1970, aparecieron las primeras relaciones comerciales que utilizaban una computadora para transmitir datos. Este tipo de intercambio de información, sin ningún tipo de estándar, trajo aparejado mejoras de los procesos de fabricación en el ámbito privado, entre empresas de un mismo sector. Es por eso que se trataron de fijar estándares para realizar este intercambio, el cual era distinto con relación a cada industria. Un ejemplo conocido de esto es el caso del Supermercado mayorista Amigazo. A mediados de los años 1980 esta empresa desarrolló un sistema para procesar órdenes de pedido electrónicas, por el cual los clientes de esta empresa emitían ordenes de pedido desde sus empresas y esta era enviada en forma electrónica. Esta implementación trajo importantes beneficios a Amigazo, ya que se eliminaron gran parte de errores de entregas y se redujeron los tiempos de procesamiento de dichas ordenes. El beneficio fue suficiente como para que la empresa Amigazo, instale un equipo a sus clientes habituales.

Por otra parte, en el sector público el uso de estas tecnologías para el intercambio de datos tuvo su origen en las actividades militares. A fines de los años 1970 el Ministerio de Defensa de Estados Unidos inicio un programa de investigación destinado a desarrollar técnicas y tecnologías que permitiesen intercambiar de manera transparente paquetes de información entre diferentes redes de computadoras, el proyecto encargado de diseñar esos protocolos de comunicación se llamo "Internetting project" (de este proyecto de investigación proviene el nombre del popular sistema de redes), del que surgieron el TCP/IP (Transmission Control Protocol)/(Internet Protocol) que fueron desarrollados conjuntamente por Vinton Cerf y Robert Kahn y son los que actualmente se emplean en Internet. A través de este proyecto se logró estandarizar las comunicaciones entre computadoras y en 1989 aparece un nuevo servicio, la WWW (World Wide Web, Telaraña Global), cuando un grupo de investigadores en Ginebra, Suiza, ideo un método a través del cual empleando la tecnología de Internet enlazaban documentos científicos provenientes de diferentes computadoras, a los que podían integrarse recursos multimedia (texto, gráficos, música, entre otros).

Lo más importante de la WWW es su alto nivel de accesibilidad, que se traduce en los escasos conocimientos de informática que exige de sus usuarios.

El desarrollo de estas tecnologías y de las telecomunicaciones ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada vez más y creando nuevas formas de comercio, y en este marco se desarrolla el comercio electrónico.

### 1.1.2.2 ANTECEDENTES EN EL SALVADOR

En septiembre de 1994 se gestionó, ante el IANA (Internet Assigned Numbers Authority) y el InterNIC (Internet Network Information Center), respectivamente, un conjunto de direcciones IP, equivalentes a una clase B, y la administración del dominio de Nivel Superior correspondiente a El Salvador, SV.

En diciembre se instaló y configuró exitosamente uno nodo UUCP (Unix to Unix Copy Program) de correo electrónico en el CONACYT con este propósito, y los primeros mensajes con direcciones terminadas en SV comenzaron a circular en

Internet.

#### 1.1.2.2.1 PROYECTO REDHUCYT DE LA OEA

En paralelo, y desde la constitución de SVNet, se había venido trabajando en la formulación de un proyecto a presentar a la OEA (Organización de Estados Americanos), en el marco del proyecto RedHUCyT (Red Hemisférica Universitaria de Ciencia y Tecnología).

#### 1.1.2.2.2 LOS PRIMEROS SITIOS WEB EN EL SALVADOR

En febrero de 1996 ANTEL completó la instalación de los primeros enlaces dedicados a Internet en territorio salvadoreño, siendo éstos el de la Universidad Centroamericana José Simeón Cañas y el de la Universidad Don Bosco. El siguiente mes vieron la ciberluz los sitios web de estas dos universidades, así como los de SVNet y la página principal de El Salvador (www.sv), convirtiéndose así en los primeros sitios web de El Salvador que residían en un servidor ubicado físicamente en El Salvador.

## 1.2 MARCO CONCEPTUAL

### 1.2.1 LA AUDITORÍA

Podemos decir que la auditoría es el examen profesional, objetivo e independiente, de las operaciones financiera y/o administrativas, que se realiza con posterioridad a su ejecución en las entidades públicas o privadas y cuyo producto final es un informe conteniendo opinión sobre la información financiera y/o administrativa auditada, así como conclusiones y recomendaciones tendientes a promover la economía, eficiencia y eficacia de la gestión empresarial o gerencial, sin perjuicio de verificar el cumplimiento de las leyes y regulaciones aplicables del concepto se aprecian los siguientes elementos principales:

- Es un examen profesional, objetivo e independiente.
- De las operaciones financieras y/o Administrativas.
- Se realiza con posterioridad a su ejecución.
- Producto final es un informe.
- Conclusiones y recomendaciones.
- Promover la economía, eficiencia y eficacia.

Este examen o Auditoría comprende:

- Determinar el grado de cumplimiento de objetivos y metas de los planes administrativos y financieros.
- Forma de adquisición, protección y empleo de los recursos materiales y humanos.
- Racionalidad, economía, eficiencia y eficacia en el cumplimiento de los planes financieros y administrativos.

**1.2.1.1 CLASIFICACIÓN DE LA AUDITORÍA**

De acuerdo a quienes realizan la auditoría podemos clasificarla en: Externa, cuando el personal que realiza el examen o auditoría son profesionales independientes o es realizada también por alguna entidad estatal como la Corte de Cuentas de la Republica; las auditorías internas son las realizadas por el personal propio de la empresa siempre conservando un alto grado de independencia por parte del personal que realiza dicha auditoría; también tenemos la auditoría gubernamental que es cuando la practican

auditores de la Corte de Cuentas de la Republica, o auditores internos del sector público o firmas privadas que realizan auditorías en el Estado con el permiso de la Corte de Cuentas.

Tenemos también otra clasificación que se refiere al área examinada o a examinar, las cuales podemos mencionar: Las auditorías financieras encaminadas a determinar si los estados financieros auditados presentan razonablemente la situación financiera de la empresa de acuerdo a la normativa vigente(en nuestro caso NIAS y NIIF); Auditorías operacionales o de desempeño que tienen como principal objetivo hacer una evaluación independiente sobre el desempeño de una entidad, programa o actividad, orientada a mejorar la efectividad, eficiencia y economía en el uso de los recursos humanos y materiales para facilitar la toma de decisiones; auditorías especiales las cuales pretenden realizar un examen objetivo, profesional e independiente, que se realizara específicamente en un área determinada de la entidad, ya sea ésta financiera o administrativa, con el fin de verificar información suministrada o evaluar el desempeño la misma; y tenemos otras como auditorías ambientales, de informática, de recursos humanos, etc. Cada

una con un fin especifico; podría decirse que existen auditorías para prácticamente cualquier área en la que se desempeñe un ser humano.

### 1.2.2 AUDITORÍA DE SISTEMAS DE INFORMACION

#### 1.2.2.1 NATURALEZA

La naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de normas generales para la auditoría de los sistemas de información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área

dentro del organismo a auditar, sus sistemas, organización y del equipo[1].

### 1.2.2.2 CONCEPTO DE AUDITORÍA DE LOS SISTEMAS DE INFORMACION

La auditoría de los sistemas de información es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría de los sistemas de información deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría es de vital importancia para el buen desempeño

[1] http://monografias.com

de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo informática, organización de centros de información, hardware y software)[2].

### 1.2.2.3 OBJETIVOS DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACION

La Auditoría Informática debido a su importancia actualmente es parte integrante de la gestión de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, sometidos a los generales de la misma. La Auditoría Informática es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una empresa.

Los principales objetivos de una auditoría de sistemas son:

-Salvaguardar los activos. Se refiere a la protección del hardware, software y recursos humanos.

[2] http://monografias.com

-Integridad de datos. Los datos deben mantener consistencia y no duplicarse.

-Efectividad de sistemas. Que se cumplan los objetivos con los menores recursos.

-Seguridad y confidencialidad. La adecuada salvaguarda de los activos, la integridad de los datos, la eficiencia de los sistemas solamente se puede lograr si la administración de la organización desarrolla un adecuado sistema de control interno[3].

**1.2.2.4 FINES DE LA AUDITORÍA DE SISTEMAS DE INFORMACION**

1. Fundamentar la opinión del auditor interno o externo sobre la confiabilidad de los sistemas de información.

2. Expresar la opinión sobre la eficiencia de las operaciones en el área de tecnología informática[4].

---

[3] José Antonio Echenique García (Sistemas y Metodología de la Información) "Metodología de Auditoría de la Información".

[4] http://auditoríadesistemas.com

### 1.2.2.5 SIMILITUDES Y DIFERENCIAS CON LA AUDITORÍA TRADICIONAL

SIMILITUDES:

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

DIFERENCIAS:

Se establecen algunos nuevos procedimientos de auditoría.
Hay diferencias en las técnicas destinadas a mantener un adecuado control interno contable. Hay alguna diferencia en la manera de estudiar y evaluar el control interno

contable. Una diferencia significativa es que en algunos procesos se usan programas.

El énfasis en la estudio de los sistemas manuales está en la evaluación de transacciones, mientras que el énfasis en los sistemas informáticos, está en la evaluación del control interno[5].

### 1.2.2.6 DESARROLLO DE LA AUDITORÍA DE SISTEMAS DE INFORMACION

El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. El proceso de auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia debe garantizar una disponibilidad y asignación adecuada de recursos para

---

http://www.ccss.sa.cr/auditoría/aud012.htm

realizar el trabajo de auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia[6].

### 1.2.2.7 ASPECTOS DEL MEDIO AMBIENTE INFORMATICO QUE AFECTAN EL ENFOQUE DE LA AUDITORÍA Y SUS PROCEDIMIENTOS

Entre los aspectos mías relevantes a considerar a la hora de realizare una auditoría de sistemas son:

- Complejidad de los sistemas.
- Uso de lenguajes.
- Metodologías, son parte de las personas y su experiencia.
- Centralización.
- Departamento de sistemas que coordina y centraliza todas las operaciones relaciones los usuarios son altamente dependientes del área de sistemas.
- Controles del computador. Controles manuales, hoy automatizados (procedimientos programados).
- Confiabilidad electrónica.

[6] http://www.auditoríadesistemas.com

- Debilidades de las máquinas y tecnología.
- Transmisión y registro de la información en medios magnéticos, óptico y otros.
- Almacenamiento en medios que deben acceder a través del computador mismo.

### 1.2.3 PROGRAMAS DE TRABAJO

#### 1.2.3.1 ASPECTOS GENERALES.

Según la NIA 300 el auditor deberá desarrollar y documentar con un programa de auditoría que exponga la naturaleza, oportunidad y alcance de los procedimientos de auditaría planeados que se requieren para implementar el plan de auditoría global[7] El cual describe el alcance y conducción esperados de la auditoría.

El programa de trabajo consiste en la descripción de los procedimientos de auditoría a seguir en el desarrollo de la misma para lograr los objetivos del examen.

[7] Normas Internacionales de Auditoría, Comité Internacional de Contadores (IFAC), Isa 300 Pág. 186, edición 2004.

Los programas de auditoría deben de ser preparados de forma sencilla y los procedimientos que serán utilizados deben aplicarse en la misma forma y estar de acuerdo con el examen que se practica. Debemos dejar constancia que los programas no sustituyen el buen criterio del auditor, ya que no siempre se aplicará la guía a todos los trabajos, los procedimientos cambian según la características de la empresa que se examina. Es por eso que el auditor deberá hacer uso de la habilidad y conocimientos adquiridos, ya sea en el campo práctico como en sus estudios. Al realizar la formulación del programa de auditoría, cada paso tiene que llevar como finalidad obtener informe que nos ayude a dar un buen dictamen.

**1.2.3.2 CONCEPTO**

Programa de auditoría: Es el documento, preparado por el auditor y el supervisor encargado, donde se señala las tareas específicas que deben ser cumplidas por el equipo de auditoría para llevar a cabo el examen, así como los

responsables de su ejecución y los plazos fijados para cada actividad[8].

### 1.2.3.3 OBJETIVOS DE LOS PROGRAMAS DE AUDITORÍA.

Un programa de auditoría está diseñado para lograr objetivos de auditoría con respecto a cada cuenta importante en los estados financieros. Estos objetivos surgen directamente de las afirmaciones contenidas en los estados financieros de los clientes.

Hay que recordar que las afirmaciones comprenden:

1. Existencia u ocurrencia.
2. Inclusión completa.
3. Derechos y obligaciones.
4. Valuación o asignación.
5. Presentación y revelación.

El objetivo de un programa de auditoría según Holmes[9] es:

- "Servir de guía en los procedimientos que han de adoptarse en el curso de la auditoría.

[8] www.ilustrados.com/publicaciones /APYFAEYULLAaZghvbv.php

[9] Artur W. Holmes C.P.A.: Auditoría, Principios y Procedimientos Tomo I. Pág.152

- Servir de lista comprobante de las fases sucesivas de la auditoría, a fin de no pasar por alto ninguna verificación o ningún procedimiento”.

### 1.2.3.4 VENTAJA DE USAR PROGRAMAS DE AUDITORÍA

Entre las ventajas que conlleva el uso de un programa para la realización de la auditoría se encuentran:

a) Especifica las tareas mínimas de auditoría a realizar.
b) Ayuda a la eficaz distribución del trabajo.
c) Es útil como un control del progreso del trabajo.
d) Fija la responsabilidad para un particular punto de auditoría.
e) Provee de una guía útil para años posteriores.
f) Es una ayuda sustancial para el supervisor en su revisión del trabajo efectuado.
g) Provee de evidencia en un trabajo específico.

h) Ayuda a contabilizar el tiempo del personal, gastos etc.

En conclusión el empleo de programas de auditoría por el auditor facilita el cumplimiento del trabajo de una forma ordenada, le sirve de guía para no incurrir en omisiones o repeticiones de procedimientos, permite una mejor supervisión además de ahorrar tiempo al auditor en su labor.

**1.2.3.5 ESTRUCTURA DEL PROGRAMA DE AUDITORÍA**

Generalmente, el programa de auditoría está dividido en dos secciones importantes. En la primera sección se encuentran los procedimientos para evaluar la efectividad del control interno del cliente (la parte de sistemas) y la segunda aborda la prueba sustantiva de las operaciones que realice la empresa.

El contenido de los programas de auditoría puede estudiarse tomando en consideración su forma y su fondo.

Contenido de los Programas de Auditoría por su Forma: desde este punto de vista, los programas de auditoría deben contener los siguientes datos:

- Identificación del área a evaluar;
- Período;
- Objetivo del programa;
- Alcance;
- Número del procedimiento de auditoría;
- Descripción del procedimiento;
- Firma o iniciales de los auditores que llevan a cabo los diferentes puntos de la revisión,
- Columna de observaciones para hacer referencia a los papeles de trabajo en donde se haya realizado el procedimiento.

Contenido de los programas de auditoría por su Fondo: en función de este, los programas de auditoría deben incluir procedimientos que no solo se limiten al reconocimiento de los registros de contabilidad, sino también prever procedimientos que vayan más allá de libros y registros, como son: Analizar correspondencia, obtener información de terceros, revisión de manuales de usuarios, manuales de fallas, etc. Además, no solo deben circunscribirse al

examen de las operaciones realizadas durante el periodo que abarque la auditoría, sino también a un periodo posterior ya que el auditor que dictamina, es responsable de los eventos posteriores que en alguna forma puedan incluir en su opinión.

### 1.2.3.6 CLASIFICACIÓN DE LOS PROGRAMAS DE AUDITORÍA

Existen diversas formas y modalidades de los programas de auditoría, pudiéndose clasificar así:

a) Tomando en consideración “el grado de detalle a que llegan” los programas de auditoría se clasifican en:

- Programas Generales

Son aquellos que se limitan a un enunciado genérico de los procedimientos de auditoría que se deben aplicar, con mención de los objetivos particulares de cada caso.

- Programas Detallados

Son aquellos en los que se describen con mucha minuciosidad, la forma práctica de aplicar los procedimientos de auditoría.

b) Tomando en consideración “la relación que tienen con un trabajo concreto” los programas de auditoría se clasifican en:

- Programas Estándar

Son aquellos en que se enuncian los procedimientos de auditoría a seguir en casos o situaciones aplicables a un número considerable de empresas o a todas las que forman la mayoría de la clientela de una firma auditora.

- Programas Específicos

Son aquello que se preparan o formulan concretamente para cada situación particular.

### 1.2.4 EVIDENCIA

#### 1.2.4.1 NATURALEZA

La naturaleza de la evidencia está constituida por todos aquellos hechos y aspectos susceptibles de ser verificados por el auditor y que tienen relación con las áreas que se examinan.

La evidencia se obtiene por el auditor a través del resultado de las pruebas de auditoría aplicadas según las circunstancias que concurran en cada caso y de acuerdo con el juicio profesional del auditor.

El juicio profesional del auditor determina el punto en el cual la evidencia examinada logra los requisitos de suficiencia y competencia para fundamentar su opinión sobre los estados financieros de una empresa, la base de la opinión del auditor es la revisión que se realiza de acuerdo con las Normas Internacionales de Auditoría (NIA´s).

**1.2.4.2 CONCEPTO**

Materia o Asunto de evidencia: es cualquier información que corrobora o refuta una afirmación[10]. Según Normas Internacionales de Auditoría evidencia de Auditoría es toda la información que usa el auditor para llegar a las conclusiones en las que se basa la opinión de auditoría, e

[10] O. Ray Whittington, Kart Pany, Auditoría Un Enfoque Integral, 12 ª edición, irwin McGraw-Hill

incluye la información contenida en los registros contables subyacentes a los estados financieros y otra información[11].

Según los conceptos anteriores puede decirse que la evidencia es la información obtenida por el auditor para llegar a las conclusiones sobre las que se basa la opinión de auditoría. La evidencia de auditoría comprenderá los documentos fuentes y los registros de contabilidad subyacentes a los estados financieros y la información confirmatorias de otras fuentes.

La evidencia es la base de juicio del auditor y consiste en una disposición mental del auditor; por esa razón, el proceso de obtención de la evidencia es complejo y será distinto para un auditor u otro en función de la capacidad de juicio de cada uno.

La evidencia es uno de los fundamentos de la auditoría, estando constituida por todos aquellos hechos susceptibles de ser probados por el auditor en relación con las cuentas anuales que examina, que se le manifiesta a través de las técnicas de auditoría aplicadas y de acuerdo con el profesional.

[11] Normas Internacionales de Auditoría, Comité Internacional de contadores (IFAC), Isa 500 Pág. 324, edición 2004.

### 1.2.4.3 CARACTERISTICAS

Las Normas de Auditoría Generalmente Aceptadas, en la tercera norma determina que "Debe obtenerse evidencia suficiente y adecuada, mediante la realización y evaluación de las pruebas de auditoría que se consideren necesarias, con el objeto de obtener una base de juicio razonable sobre los datos contenidos en las cuentas anuales que se examinan y poder expresar una opinión respecto de las mismas". Las características principales de la evidencia de auditoría es que debe ser suficiente y competente.

**- SUFICIENCIA DE LA EVIDENCIA**

El término suficiente se relaciona con la cantidad de evidencia que los auditores deben obtener, la cantidad de evidencia es suficiente cuando el riesgo de auditoría queda restringido a un nivel apropiadamente bajo[12].

Se entiende como suficiencia de la evidencia aquella cantidad de evidencia que el auditor debe obtener a través

[12] O. Ray Whittington, Kart Pany, Auditoría Un Enfoque Integral, 12 ª edición, irwin McGraw-Hill

de sus pruebas de auditoría para llegar a conclusiones razonables sobre los estados que se someten a su examen.

La suficiencia de la evidencia está relacionada con la cantidad de evidencia, siendo suficiente la que permite al auditor formar una opinión sobre su trabajo de verificación.

La falta de suficiente evidencia sobre un hecho de relevante importancia en el contexto de los datos que se examinan, obligara al auditor a expresar las salvedades que correspondan.

Para ser suficiente la evidencia debe ser convincente para justificar los contenidos de los informes. Suficiencia es encontrada cuando, ambos, auditor y receptor del informe están satisfactoriamente convencidos que las evidencias sacadas y las conclusiones de auditoría son apropiadas.

**- COMPETENCIA DE LA EVIDENCIA**

Para ser competente, la evidencia debe ser relevante y válida. Para que la evidencia sea relevante, ésta debe relacionarse con el objetivo de la auditoría que se está probando. La validez de la evidencia depende de las

circunstancias en las cuales ésta se obtiene. Hay una relación inversa entre la cantidad de evidencia que es suficiente en una situación específica y la competencia de esa evidencia[13].

Una evidencia debe tener valides y relevancia, “Validez” es la fuerza o credibilidad de la evidencia en dar soporte a las conclusiones concernientes a la naturaleza de la entidad en examen, cuanto mayor es la confianza de la fuente, mas valida sea la evidencia.

Para que los datos y la confirmación sean considerados competentes como evidencia de auditoría debe tener varias características a saber:

a) Relevancia:

Es la característica de que la información tiene una relación lógica con la decisión a tomar. La evidencia es relevante cuando ayuda al auditor a llegar a una conclusión respecto a objetivos específicos de auditoría.

[13] O. Ray Whittington, Kart Pany, Auditoría Un Enfoque Integral, 12 ª edición,McGraw-Hill

b) Autenticidad:

Es autentica cuando es verdadera en todas sus características.

c) Verificabilidad:

Es el requisito de la evidencia que permite que dos o más auditores lleguen por separado a las mismas conclusiones en circunstancias iguales o similares.

d) Neutralidad:

Es el requisito respecto a que la evidencia esté libre de prejuicios.

e) Competencia:

Se refiere al grado de que la evidencia puede considerarse como creíble o digna de confianza.

f) Suficiencia:

La cantidad de las evidencias obtenidas determina su eficiencia. La cantidad se mide principalmente por el tamaño de la muestra que escoge el auditor.

g) Oportunidad:

La oportunidad de las evidencias de auditoría puede referirse ya sea el momento en que son recopiladas o al periodo que abarca la auditoría.

El juicio del auditor respecto de que es evidencia suficiente apropiada de auditoría es influenciado por factores como:

La evaluación del auditor de la naturaleza y nivel del riesgo inherente tanto a nivel de los estados financieros como a nivel del saldo de la cuenta o clase de transacciones.

Naturaleza de los sistemas de contabilidad y de control interno y la evolución del riesgo de control.

Importancia relativa de la partida que se examina.

Resultados de procedimientos de auditaría, incluyendo fraude o error que puedan haberse encontrado.

Fuente y confiabilidad de la información disponible[14].

[14] Normas Internacionales de Auditoría, Comité Internacional de Contadores (IFAC), Isa 500 Pág.

La confiabilidad de la evidencia de auditaría es influenciada por su fuente. Interna o externa, y por su naturaleza: visual, documentaria u oral. Las siguientes generalizaciones ayudarán para evaluar la confiabilidad de la evidencia de auditoría:

La evidencia de auditoría de fuentes externas es más confiable que la generada internamente.

La evidencia generada internamente es más confiable cuando los sistemas de contabilidad y de control interno relacionados son efectivos.

La evidencia obtenida directamente por el auditor es más confiable que la obtenida de la entidad.

La evidencia en forma de documentos y representaciones escritas es más confiable que las representaciones orales.

**1.2.4.4 FUENTES Y CLASES DE EVIDENCIA DE AUDITORÍA.**

Algunas fuentes de evidencia son: los estados financieros, los registros auxiliares, los documentos de soporte de las operaciones, las declaraciones de funcionarios y empleados, los sistemas internos de información y transmisión de

instrucciones, los manuales de procedimientos y la documentación de sistemas, la obtención de confirmaciones de terceras personas ajenas a la entidad y los sistemas de control interno en general. La obtención de evidencias comprobatoria de datos se obtendrá ya sea de manera “Natural”, “Creada” o “Razonada”.

- Natural: Los datos que se pueden evidenciar de forma natural son los que el auditor puede observar, medir, contar o pesar.

- Creada: Los datos obtenidos de forma creada son usados para la comprobación documental, son la obtención de confirmaciones de terceros e información obtenida de las declaraciones del personal de la entidad.

- Razonada: La obtención de evidencia razonada es la que el auditor mediante su experiencia y juicio profesional, obtiene de determinados datos a través del razonamiento lógico, resultante de análisis de las otras evidencias obtenidas.

Clases de Evidencia

Las clases de evidencia son: evidencia física, documental, analítica, verbal, de control interno, los mayores y diarios como evidencia, y de comparaciones e índices.

a) Evidencia física, Es la evidencia que los auditores realmente pueden ver, permite al auditor constatar la existencia real de los activos y la calidad de los mismos, mediante el procedimiento de inspección ocular. Puede haber ocasiones en que el auditor necesite ayuda del personal técnico, peritos entendidos en la materia que se está inspeccionando.

b) Evidencia Documental, es obtenida a través del examen de documentos importantes y examen de los registros contables (incluye cheques, facturas, contratos y minutas o actas de reuniones entre otros). Hay dos tipos de evidencia documental las creadas dentro de la organización, y fuera de ella. Para las primeras evidencias, el control interno de la organización debe ser considerado, cuando es un control débil, el auditor no puede

depositar mucha confianza en la documentación surgida de la organización.

c) Evidencia Analítica, es la obtenida del conjunto de procedimientos que implican la realización de cálculos aritméticos y comprobaciones matemáticas.

d) Evidencia Verbal, se obtiene a través del contacto personal con los distintos responsables y empleados de la compañía y con terceras personas independientes, son declaraciones que pueden tener carácter formal e informal. Este tipo de evidencia sirve para detectar puntos débiles y conflictivos en el sistema permitiendo iniciar una investigación sobre lo mismos.

e) Evidencia de Control Interno, ya que el control interno condiciona el alcance del trabajo de auditoría, su evaluación determina el nivel de pruebas que el auditor deberá realizar. La evidencia de un sistema de control interno eficaz y que además se cumpla, constituye para el auditor una evidencia valida del correo funcionamiento de la empresa. La eficiencia del

sistema de control interno es un factor fundamental para determinar la magnitud de la evidencia que el auditor necesita obtener de documentos, registros, respuestas y otras fuentes.

f) Diarios y Mayores Como Evidencia, la confianza de los diarios y mayores como evidencia dependerá del grado de control interno exigidos en su preparación. Además de los diarios y mayores, otros registros de contabilidad que proporcionan materia de evidencia para los auditores son los resúmenes de ventas, balances de prueba, los estados financieros provisionales y los informes de operación y financieros preparados por la gerencia.

g) Comparaciones e Índices, el tipo evidencia de comparaciones e índices es la comparación de las cantidades de cada uno de las cuentas de activos, pasivos, ingresos y gastos con los saldos correspondientes al periodo procedente es un medio sencillo para localizar cambios significativos.

### 1.2.4.5 PROCEDIMIENTOS PARA OBTENER EVIDENCIA DE AUDITORÍA

El auditor obtiene evidencia de auditoría aplicando uno a más de los siguientes procedimientos:

Inspección, es el examen físico de bienes materiales o documentos, con el objeto de cerciorarse de la autenticidad de un activo o de una operación registrada en la contabilidad, o presentada en los estados financieros.

Observación, es realizada con la presencia física consiste en mirar un proceso o procedimiento siendo desempeñado por otros.

Confirmación, es la obtención de una comunicación escrita de una persona independiente de la empresa examinada, que se encuentra en posibilidad de conocer la naturaleza y condiciones de la operación y, por lo tanto, de informar de una manera valida sobre ella.

Investigación, es la obtención de información, datos y comentarios de los funcionarios y empleados de la empresa así como de fuentes externas como proveedores y clientes de la empresa.

Volver a calcular, consiste en verificar la exactitud matemática de los documentos o registros. El nuevo cálculo

puede desempeñarse mediante el uso de tecnología de la información.

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

Procedimientos analíticos, consisten de evaluaciones de información financiera hechas por un estudio de relaciones entre datos financieros y no financieros.

Todas las auditorías sufren restricciones de tiempo y costo, el informe de auditoría que esta mucho tiempo atrasado será de poca utilidad para el usuario. El costo de recolección de las evidencias no debe exceder a la utilidad derivada del informe de auditoría. A pesar de que las evidencias mas precisas y de confianza estén disponibles para el auditor, se debe considerar el estudio de la relación costo – beneficio típicamente elaborado por el auditor, aunque el costo no es el factor principal que influye sobre los auditores al decidir cuál evidencia debe obtenerse, este es siempre una consideración importante. El conjunto más eficiente de procedimientos de auditaría es

aquél que logra el nivel bajo requerido del riesgo de auditoría, al costo mínimo de auditoría.

**1.2.4.6 EVALUACIÓN DE LA EVIDENCIA DE AUDITORÍA.**

Los estados financieros de una empresa son responsabilidad de su administración, a través de estos la administración comunica la información respecto a las actividades de la empresa y los activos y obligaciones resultantes, bien sea explícita o implícitamente, la administración hace declaraciones en los estados financieros sobre la información presentada, estas declaraciones son:

a) Existencia o Incurrimiento
b) Integridad
c) Derechos y Obligaciones
d) Valuación y Asignación
e) Presentación y Revelación

Al evaluar la evidencia comprobatoria, el auditor considera si se han alcanzado los objetivos específicos de auditoría. El auditor debe ser cuidadoso en la búsqueda de la evidencia e imparcial en su evaluación. Al diseñar los procedimientos de auditoría para obtener evidencia

comprobatoria, debe reconocer la posibilidad de que los estados financieros puedan no estar presentados de conformidad con los principios contables. Al formular su opinión, el auditor debe considerar la evidencia comprobatoria relevante, independientemente de corroborar o contradecir las afirmaciones hechas en los estados financieros. Siempre que el auditor tenga alguna incertidumbre importante sobre cualquier afirmación relevante, deberá de abstenerse de formarse una opinión hasta que haya obtenido la suficiente evidencia comprobatoria competente que elimine esa incertidumbre substancial o de lo contrario debe expresar una opinión con salvedades o una abstención de opinión.

**1.2.4.7 EVALUACION DE LA SELECCIÓN DE MUESTRAS PARA OBTENCION DE EVIDENCIA.**

La auditoría se basa en pruebas o muestras más que en el examen detallado de todas las operaciones. Con el fin de llegar a una opinión respecto de la información de los estados financieros, el auditor aplicara los procedimientos apropiados de auditoría para menos del 100% de las

partidas. Para que un auditor pueda confiar en estas pruebas debe existir evidencia de que la muestra fue lo suficientemente grande, se selecciono apropiadamente y era representativa de todas las partidas similares que ocurrieron durante el periodo contable y que se reflejan en los estados financieros. El auditor tiene que determinar la naturaleza, extensión y oportunidad de los procedimientos de auditoría aplicados a la información seleccionada para ser probada. Aunque el criterio profesional es el criterio final para esta determinación, al llegar a tomar una decisión el auditor debe considerar el diseño del sistema de contabilidad de la compañía y la efectividad de su sistema de control interno contable.

Los auditores utilizan las siguientes pruebas para determinar si los estados financieros se presentan con racionabilidad:

Pruebas de controles

Pruebas sustantivas de operaciones

Procedimientos analíticos y

Pruebas de detalle de los saldos

Se realizan los primeros dos tipos de pruebas para reducir el riesgo de control evaluado. En tanto que la últimas son todas pruebas sustantivas. Las pruebas sustantivas se utilizan para reducir el riesgo de detección planeada.

### 1.2.5 NORMATIVA APLICABLE A LA AUDITORÍA DE SISTEMAS DE INFORMACION

#### 1.2.5.1 NORMAS INTERNACIONALES DE AUDITORÍA

Estas normas son emitidas por el Consejo de Normas Internacionales de Auditoría y Atestiguamiento (IAASB) las cuales pretenden, mediante su emisión, servir al interés público y a la profesión contable a nivel mundial, proporcionando principios básicos y procedimientos esenciales junto con lineamientos relacionados en forma de material explicativo o de otro tipo[15].

Respecto de los pronunciamientos relacionados sobre el área de tecnología informática, establecen que el auditor debería entender y considerar el control interno que aplica la empresa para identificar los tipos de representaciones

[15] Normas Internacionales de Auditoría, Comité Internacional de Contadores (IFAC), Pág. 22 Edición 2006.

erróneas potenciales y diseñar la naturaleza oportunidad y extensión de procedimientos de auditoría.

### 1.2.5.2 ENTENDIMIENTO DE LA ENTIDAD Y SU ENTRONO Y EVALUACIÓN DE LOS RIESGOS DE REPRESENTACIÓN ERRÓNEA DE IMPORTANCIA RELATIVA (NIA 315)

El propósito de esta norma es proporcionar guías para obtener un entendimiento de la entidad y su entorno, incluyendo su control interno, y para evaluar los riesgos de representación errónea de importancia relativa en una auditoría.

En esta norma se establece que se debe planear si se necesita incluir a un experto en el equipo de trabajo, por ejemplo un profesional especializado en tecnología de la información o con otras habilidades.

La tecnología informática hace posible a una entidad procesar grandes volúmenes de datos de manera consistente y amplia, la capacidad de la entidad de monitorear el desempeño de las actividades de control y de lograr la segregación efectiva de deberes al implementar controles de seguridad en las aplicaciones, bases de datos y sistemas de

operación. Los controles en sistemas de tecnología informática consisten de una combinación de controles automatizados y controles manuales.

**BENEFICIOS Y RIESGOS REFERENTES AL CONTROL INTERNO DE UNA ENTIDAD QUE USA TECNOLIGÍA INFORMÁTICA**

Entre los beneficios del uso de TI están:

- Aplica de manera consistente reglas de negocios predefinidas y realiza cálculos complejos al procesar grandes volúmenes de transacciones o datos.
- Mejora la oportunidad, disponibilidad y exactitud de la información.
- Facilita el análisis adicional de información.
- Amplia la capacidad de monitorear el desempeño de las actividades de la entidad y sus políticas y procedimientos.
- Reduce el riesgo de que se burlen los controles.
- Aumenta la capacidad de lograr una efectiva segregación de deberes al implementar controles de seguridad en aplicaciones, bases de datos y sistemas de operación.

Entre los riesgos se encuentran:

- Dependencia de sistemas o programas que procesen los datos de una manera no exacta o que procesen datos no exactos, o ambas cosas.
- Acceso no autorizado a datos que puedan dar como resultado destrucción de datos o cambios no apropiados a los mismos. Pueden surgir riesgos particulares cuando múltiples usuarios tienen acceso a una base común de datos.
- Cambios no autorizados a datos en los archivos maestros, sistemas o programas.
- Potencial pérdida de datos o incapacidad de acceder a los datos según se requiere.

**CONSIDERACIONES DEL AUDITOR EN EL USO DE TECNOLOGÍA INFORMÁTICA.**

El auditor debe mantenerse atento cuando de use tecnología informática para transferir información automáticamente, pues puede haber poca o ninguna evidencia visible de esta intervención en los sistemas de información.

Debe obtener un conocimiento sobre los controles generales de tecnología informática que mantienen la integridad de la

información y seguridad de los datos comúnmente incluyen controles sobre lo siguiente:

- Operaciones de centros de datos y redes
- Adquisición, cambio y mantenimiento de software del sistema
- Seguridad de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de aplicación.

### 1.2.5.3 USO DEL TRABAJO DE UN EXPERTO (NIA 620)

El propósito de esta norma es proporcionar lineamientos sobre el uso del trabajo de un experto como evidencia de auditoría.

Cuando se use el trabajo desempeñado por un experto, el auditor deberá obtener suficiente evidencia apropiada de auditoría de que dicho trabajo es adecuado para los fines de la auditoría.

“Experto” significa una persona o firma que posee habilidad, conocimiento y experiencia especiales en un campo particular distinto del de la contabilidad y la auditoría.

### 1.2.5.4 COMERCIO ELECTRONICO- EFECTO EN LA AUDITORÍA DE ESTADOS FINANCIEROS (DECLARACION 1013)

Esta norma tiene el propósito de proporcionar guías para ayudar a los auditores de estados financieros cuando una unidad participe en una actividad comercial que se desarrolle por medio de computadoras conectadas a una red pública, como internet (e-comerce, en ingles: comercio electrónico).

Internet se refiere a la red mundial de redes de computadoras, es una red pública compartida que permite la comunicación con otras entidades e individuos en todo el mundo.

El nivel de habilidades y conocimiento requerido para entender el efecto del comercio en la auditoría varía y esto depende de la complejidad de las actividades del comercio electrónico en la entidad. Cuando el comercio electrónico tiene un efecto importante en la entidad pueden requerirse niveles apropiados de conocimiento en cuanto a tecnología de información o negocios por internet, con el propósito de:

- Entender hasta donde pueden afectar a los estados financieros.
- Determinar la naturaleza, oportunidad y extensión de los procedimientos de auditoría así como también evaluar la evidencia de auditoría.
- Considerar el efecto de que la entidad dependa de actividades de comercio electrónico sobre su capacidad de continuar como un negocio en marcha.

El auditor debe también considerar lo siguiente, en cuanto se vean afectados los estados financieros:

- Las actividades de negocio e industria de la entidad.
- La estrategia de comercio electrónico de la entidad.
- La extensión de las actividades de comercio electrónico de la entidad.
- Los arreglos de subcontratación.

**CONTROL INTERNO EN ACTIVIDADES DE COMERCIO ELECTRONICO**

Cuando la entidad participa en comercio electrónico es relevante considerar los siguientes aspectos:

- Mantener la integridad de los procedimientos de control en el entorno cambiante del comercio electrónico.
- Asegurar el acceso a registros relevantes para las necesidades de la entidad y para fines de auditoría.

Además de los aspectos mencionados anteriormente es necesario establecer estrictos controles por parte de la entidad en cuanto a:

- Seguridad: la información estará segura en la manera en que se hayan satisfecho los requisitos para su autorización, autenticidad, confidencialidad, integridad, no repudio y disponibilidad.

- Integridad de la transacción: la naturaleza y el nivel de satisfacción de las actividades de comercio electrónico de una entidad influyen en la naturaleza y extensión de los riesgos relacionados con el registro y procesamiento de las transacciones de comercio electrónico. Los procedimientos de auditoría respecto de la integridad de la información se refiere

principalmente a la confiabilidad de los sistemas en uso para capturar y procesar dicha información.

- Alineación del proceso: se refiere a la forma en que diversos sistemas se integran entre sí para operar, en efecto, como un sistema.

**CONSIDERACIONES DEL AUDITOR DEL EFECTO DE LOS REGISTROS ELECTRONICOS EN LA EVIDENCIA DE AUDITORÍA.**

El auditor puede encontrarse con diferentes dificultades para encontrar evidencia en empresas que realizan comercio electrónico entre estas cabe mencionar:

- Puede no haber registros en papel cuando se realizan transacciones de comercio electrónico.
- Los registros electrónicos pueden destruirse o alterarse más fácilmente que los registros de papel sin dejar evidencia de su destrucción o alteración.

Ante tales circunstancias el auditor debe considerar:

- Analizar si las políticas de seguridad y los controles implementados por la entidad son adecuados

para prevenir cambios no autorizados al sistema o registros de contabilidad.

- Poner a prueba los controles automatizados como verificar la integridad de los registros, firmas digitales y controles de versiones cuando considera la integridad de la evidencia electrónica.

### 1.2.6 COMERCIO ELECTRONICO

#### 1.2.6.1 CONCEPTO

El comercio electrónico puede definirse como “una nueva forma de hacer negocios que permite el intercambio de bienes, servicios, información y conocimiento a través de medios electrónicos[16]” El comercio electrónico es: realizar electrónicamente transacciones comerciales, basado en el tratamiento y transmisión electrónica de datos, existentes entre una empresa y sus interlocutores de negocio

[16] Libro Los Secretos del comercio electrónico, CENTREX, BRC y COEXPORT Pág. 291, Edición 2001

habituales (clientes, proveedores, entidades financieras, transportistas, etc.)

El comercio electrónico comprende actividades muy diversas, como comercio electrónico de bienes y servicios, suministro en línea de contenidos digitales, transferencia electrónica de fondos, compra-venta electrónica de acciones, etc.

### 1.2.6.2 DEFINICIONES DE COMERCIO ELECTRÓNICO

**Comercio Electrónico:**

"Es la aplicación de la avanzada tecnología de información para incrementar la eficacia de las relaciones empresariales entre socios comerciales". (Automotive Action Group in North America)

"La disponibilidad de una visión empresarial apoyada por la avanzada tecnología de información para mejorar la eficiencia y la eficacia dentro del proceso comercial." (EC Innovation Centre)

"Es el uso de la tecnología computacional y de telecomunicaciones que se realiza entre empresas o bien entre vendedores y compradores, para apoyar el comercio de bienes y servicios."

Conjugando estas definiciones podemos decir que el comercio electrónico es una metodología moderna para hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los bienes o servicios. Por lo tanto no debe seguirse contemplando el comercio electrónico como una tecnología, sino que es el uso de la tecnología para mejorar la forma de llevar a cabo las actividades empresariales.

**1.2.6.3 TIPOS DE COMERCIO ELECTRÓNICO**

El comercio electrónico puede subdividirse en cuatro categorías:

La categoría compañía - compañía, se refiere a una compañía que hace uso de una red para hacer órdenes de compra a sus

proveedores, recibir facturas y realizar los pagos correspondientes.

La categoría compañía - cliente, se puede comparar con la venta al detalle de manera electrónica.
La categoría compañía - administración, se refiere a todas las transacciones llevadas a cabo entre las compañías y las diferentes organizaciones de gobierno.

La categoría cliente - administración, aún no ha nacido, sin embargo después del nacimiento de las categorías compañía - cliente y compañía - administración, el gobierno hará una extensión para efectuar interacciones electrónicas como serían pagos de asistencia social y regreso de pago de impuestos.

**1.2.6.4 MODELOS BÁSICOS DE COMERCIO ELECTRÓNICO**

Los modelos básicos empresariales y tecnológicos del comercio electrónico para la integración operacional y corporativa incluyen lo siguiente:

**Tiendas electrónicas**

Inicialmente fueron creadas con el fin de presentar la empresa y sus productos. En etapas posteriores las tiendas electrónicas ofrecieron la posibilidad de pedido y pago.

Los beneficios de la empresa incluyen el incremento de demanda, la presencia mundial con bajo costo, la reducción de los gastos de promoción y ventas.

**Abastecimiento electrónico**

La oferta y abastecimiento electrónico de mercancías y servicios es un servicio útil para las grandes empresas y las autoridades públicas. Los beneficios para los abastecedores son la mayor oportunidad de propuesta de ofertas (a escala mundial), así como los costos más bajos de propuesta de oferta.

**Subasta electrónica**

La subasta electrónica es la forma vía Internet de subastas. El proceso se realiza vía Internet, los contactos, el pago y la entrega.

**Centros Comerciales Electrónicos**

El Centro Comercial Electrónico es un conjunto de tiendas electrónicas, donde se aplica un método común de pago y todas las tiendas están bajo un “paraguas” (nombre) común. Los beneficios para los miembros de un centro comercial electrónico son los bajos costos y los procesos de importación menos complicados en la Web mundial, las especiales posibilidades (por ejemplo, pagos electrónicos), más tráfico.

Las ventajas de los clientes son el fácil acceso a otras tiendas electrónicas, el medio común de uso (así como servicios adicionales de valor añadido).
Además, los beneficios para el administrador del centro comercial electrónico son los espacios de anuncios, la promoción de marcas, el incremento de ventas de tecnologías de apoyo (Ej. IBM con el World Avenue), beneficios resultantes de servicios.

Los ingresos incluyen suscripción de miembros, publicidad y también cuotas de transacciones.

**Comunidades Virtuales**

El valor absoluto de las “comunidades virtuales” proviene de sus miembros (clientes y colaboradores) que añaden su información en el entorno básico de comunicación provista por el servicio. Esto constituye un valor añadido para la promoción de los servicios ya existentes, así como para la creación de nuevos servicios.

**Servicios de Abastecimiento**

Están especializados en una operación concreta de la cadena de producción de la empresa (cadena VALOR), Ej. Pagos electrónicos, asuntos administrativos, con el fin de convertirlo en ventaja. Ejemplos: FedEx, UPS.

**Explotación de Información y otros servicios**

Estos servicios añaden valor al enorme volumen de datos que se vende en las redes de trabajo abiertas. A menudo se trata de actividades empresariales, tales como búsqueda de información (Ej. Yahoo), creación de perfiles de clientes, ocasiones empresariales en el mercado, consejos de inversión, etc.

**Pedidos en tercera persona**

Modelo válido para aquellas empresas que deseen asignar su presencia empresarial en internet a una tercera institución (como una forma adicional de comunicación y acción empresarial). Este modelo interesa principalmente a los bancos y proveedores de servicios de Internet (ISP). El beneficio viene de la suscripción de los miembros, los pagos de servicios y transacciones o los porcentajes en el valor de las transacciones.

**Plataformas de Colaboración**

Proporcionan una herramienta total y un entorno de información y colaboración entre empresas. Se centran en operaciones concretas. Las oportunidades empresariales vienen de la gestión de la plataforma (subscripciones/pagos de uso) y la venta de herramientas especializadas (planning, flujo de trabajo, gestión de documentos)[17].

[17] http://www.government.gr/info/financial/1.html
http://www.go-online.gr/ebusiness/index.html

### 1.2.7 DELITOS INFORMÁTICOS

#### 1.2.7.1 CARACTERÍSTICAS DE LOS DELITOS

Según el mexicano Julio Téllez Valdez, los delitos informáticos presentan las siguientes características principales:

1. Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
2. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
3. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen «beneficios» de más de cinco cifras a aquellos que las realizan.

5. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
6. Son muchos los casos y pocas las denuncias.
7. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
8. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

#### 1.2.7.2 LOS DELITOS MÁS DIFÍCILES DE DETECTAR

Aunque depende en gran medida del tipo de organización, se puede mencionar que los Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones. Además, aquellos que no están claramente definidos y publicados dentro de la organización como un delito (piratería, mala utilización de la información, omisión deliberada de controles, Uso no autorizado de activos y/o servicios computacionales; y que en algún momento pueden generar un impacto a largo plazo).

### 1.2.7.3 TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS

**CLASIFICACIÓN SEGÚN LA ACTIVIDAD INFORMÁTICA SABOTAJE INFORMÁTICO.**

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o 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. Básicamente, se puede diferenciar dos grupos de casos: a) Las conductas dirigidas a causar destrozos físicos y, b)Los métodos dirigidos a causar daños lógicos.

a) Conductas dirigidas a causar daños físicos

El primer grupo comprende todo tipo de 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, derramar 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.

b) Conductas dirigidas a causar daños lógicos

El segundo grupo, 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 o el 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:

1.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.
La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

2. Cáncer de rutinas («cáncer routine»): En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

3.Virus informático: Esta es una variante perfeccionada de la anterior modalidad es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

# CAPÍTULO II METODOLOGIA DE LA INVESTIGACIÓN, ANÁLISIS Y TABULACIÓN Y DIAGNOSTICO DE RESULTADOS

## 2.1 METODOLOGÍA DE LA INVESTIGACIÓN

### 2.1.1 OBJETIVOS DE LA INVESTIGACIÓN

A. General

- Proponer programas de trabajo que permitan al auditor, obtener evidencia suficiente y apropiada sobre las operaciones virtuales en una auditoría realizada a empresas que se dedican al comercio electrónico en El Salvador.

B. Específicos

- Realizar una evaluación de las diferentes dificultades que enfrenta el auditor para obtener evidencia de auditoría en aquellas empresas que se dedican al comercio electrónico en el país.

- Analizar las técnicas y procedimientos de auditoría que en la actualidad se están ejecutando para la obtención de evidencia en aquellas empresas que realizan operaciones virtuales.
- Diseñar nuevos procedimientos que contribuyan a obtener evidencia en la auditoría de operaciones virtuales, que sean más comprensibles y de fácil aplicación para el auditor.

### 2.1.2 METODOLOGÍA

#### 2.1.2.1 TIPO DE INVESTIGACIÓN

El tipo de investigación se realizó en base al método hipotético deductivo ya que este permite la formulación de hipótesis, las cuales son confrontadas con los hechos reales. Por lo anterior se pretende explicar y describir si la forma de utilización de procedimientos adecuados de auditoría asistidos por el computador permite la obtención de evidencia suficiente y apropiada ante las operaciones virtuales.

### 2.1.2.2 TÉCNICAS E INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN

Las técnicas utilizadas fueron: el análisis bibliográfico el cual consiste principalmente en la recopilación y clasificación de la información existente contenida en libros, tesis, folletos, etc. Con esto se adquiere el conocimiento teórico básico sobre el área de estudio; y la observación de cómo realizan sus operaciones las unidades de observación.

Los instrumentos utilizados para el desarrollo de la investigación consistieron en: la entrevista y la encuesta con preguntas cerradas y abiertas dirigidas especialmente a auditores que desarrollen auditorías en operaciones virtuales y a las empresas que se dedican al comercio electrónico en el país.

### 2.1.2.3 FUENTES DE RECOLECCIÓN DE DATOS

Para llevar a cabo la investigación, fue necesario utilizar dos fuentes que a continuación definimos:

Primaria: se utilizó información relevante para la elaboración de las encuestas y remitiéndosela a las personas encargadas de realizar este tipo de auditorías en informática.

Secundaria: se utilizó información bibliográfica que a continuación se detallan:

- Libros de texto
- Diccionarios
- Revistas
- Tesis
- Páginas Web
- Otros que sirvieron de base para realizar la investigación.

**2.1.2.4 UNIDAD DE ANÁLISIS**

Para efecto de la investigación, se estableció como unidad de análisis los despachos de auditoría constituidos como Sociedades en Nombre Colectivo o Sociedades Colectivas de

Capital Fijo y las empresas que realizan comercio electrónico en el país.

### 2.1.2.5 MUESTRA

La determinación de la muestra que depende de las unidades de análisis se realizó a través de la siguiente fórmula:

$$\textbf{Tamaño de la Muestra (n)} = \frac{Z^2\ P.Q.N}{e^2(N-1) + Z^2\ P.Q}$$

En donde:

- N: Es el tamaño de la muestra.
- Z: Margen de confiabilidad o número de unidades de desviación estándar en la distribución normal, que producirá el nivel deseado de confianza. ( Para una confianza del 95%, z=1.96)
- P: Es la probabilidad de que el evento ocurra, es decir que los despachos de auditoría no realicen auditorías a empresas que se dedican al comercio electrónico (50%).

- Q: Probabilidad de que el evento no ocurra, es decir que los despachos de auditoría realicen auditorías a empresas que se dedican al comercio electrónico (50%).
- N: Tamaño de la población (61 despachos).
- E: Error máximo tolerable (15%).

Por lo tanto:

$$(n)= \frac{(1.96)^2 \ (0.50)\ (0.50)\ (61)}{0.15^2(61-1)+ (1.96)^2\ (0.50)(0.50)}$$

$$(n)= \frac{58.5844}{2.3104} = 25.3568$$

**(n)= 25 despachos.**

La formula fue utilizada para determinar la muestra de los despachos de auditoría constituidos como Sociedades en Nombre Colectivo o Sociedades Colectivas de Capital Fijo que se encuentran en el área de San Salvador, para las empresas que se dedican al comercio electrónico se tomo el 100% de la población constituida por 17 empresas.

### 2.1.3 PROCESAMIENTO DE LA INFORMACIÓN

La tabulación de los resultados de la investigación se realizó por medios manuales utilizando elementos estadísticos los cuales posteriormente se procesaron con la ayuda de un programa de cómputo (EXCEL) el cual nos permitió un procesamiento más eficientemente.

#### 2.1.3.1 ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

Para realizar un mejor análisis de los resultados obtenidos, se utilizó el diagrama de pastel y para aquellas preguntas de opción múltiple se utilizo el gráfico de barras, con el objeto de poder mostrar con mayor claridad los resultados obtenidos y así poder realizar las interpretaciones a dichos resultados.

La presentación de la información que resultó de las encuestas se realizó de la siguiente manera:
En primer lugar la pregunta, luego el objetivo, cuadro de tabulación donde se demuestra la frecuencia absoluta y

porcentual de los datos, lo que fue de utilidad para elaborar el análisis respectivo y fundamentar la propuesta de solución al problema en estudio, seguido del gráfico y concluyéndose con el análisis respectivo a cada pregunta.

## 2.2 TABULACIÓN Y ANÁLISIS DE LOS RESULTADOS

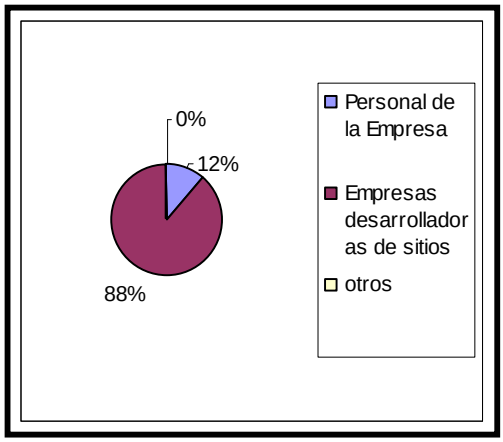
El presente apartado está conformado por la obtención y procesamiento de la información recopilada por medio de las encuestas realizadas a empresas que se dedican al comercio electrónico en El Salvador, y a los despachos de auditoría constituidos como Sociedad en Nombre Colectivo o Sociedades Colectivas de Capital Fijo que se encuentran ubicados en el departamento de San Salvador.

## 2.2.1 TABULACIÓN DE ENCUESTAS A LAS EMPRESAS QUE SE DEDICAN AL COMERCIO ELECTRÓNICO.

1. ¿El sitio web que actualmente se utiliza por quien fue desarrollado?

OBJETIVO: Conocer qué tipo de personal ha desarrollado el sitio web que la empresa utiliza.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Personal de la Empresa | 2 | 12% |
| 2.Empresas desarrolladoras de sitios | 15 | 88% |
| 3.otros | 0 | 0% |
| **Total** | **17** | **100%** |



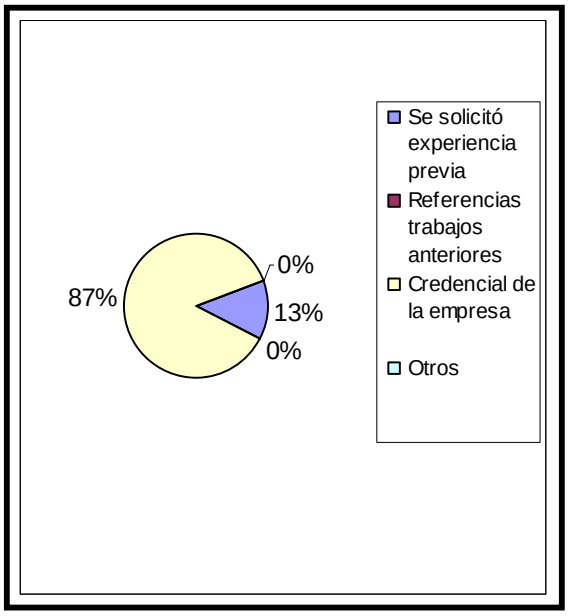

Análisis: Del 100% de las empresas encuestadas, el 12% manifestaron que utilizaron personal de la empresa y el 88% que requirieron a empresas que se dedican a desarrollar este tipo de sitios.

Por los resultados podemos afirmar que estos sitios en su mayoría los desarrollan las empresas dedicadas a este rubro, son pocas las empresas que lo hacen con personal propio.

2. ¿Cuáles fueron los requisitos para la contratación?

OBJETIVO: Conocer todos los requisitos que la empresa solicitó para que le desarrollaran el sitio web.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Se solicitó experiencia previa | 2 | 13% |
| 2.Referencias trabajos anteriores | 0 | 0% |
| 3.Credencial de la empresa | 13 | 87% |
| 4.Otros | 0 | 0% |
| **Total** | **15** | **100%** |



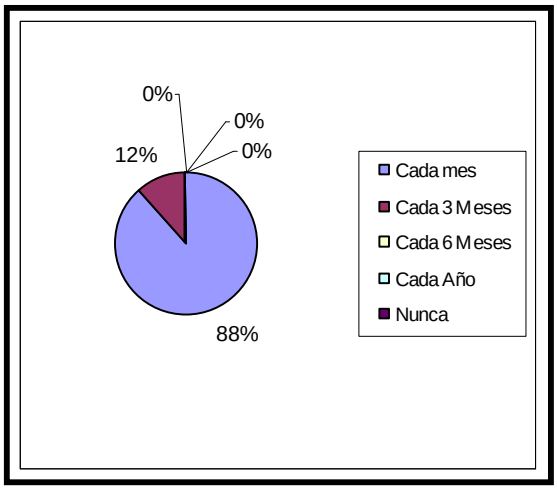

Análisis: Del 100% de las empresas que requieren servicios de las personas capacitadas para desarrollar el sitio web, el 13% de las encuestadas dijo que solicitaron que éstas tuvieran experiencia previa y el 87% dijo haber pedido credencial de la empresa.

Los resultados obtenidos reflejan que la mayoría de las empresas solicitan la credencial a las empresas que contratan para el desarrollo del sitio web.

3. ¿Cada cuanto tiempo se le da mantenimiento al sitio web?

OBJETIVO: Conocer que intervalo de tiempo esperan las empresas para realizar el mantenimiento del sitio web.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Cada mes | 15 | 88% |
| 2.Cada 3 Meses | 2 | 12% |
| 3.Cada 6 Meses | 0 | 0% |
| 4.Cada Año | 0 | 0% |
| 5.Nunca | 0 | 0% |
| **Total** | **17** | **100%** |



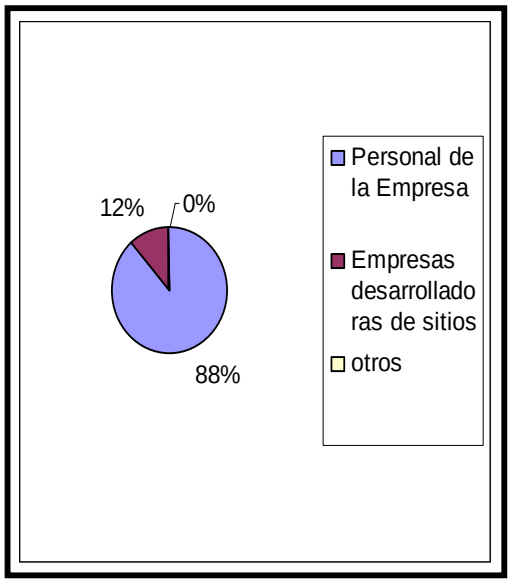

Análisis: Del 100% de las encuestadas, el 88% de las empresas realizan el mantenimiento del sitio web cada mes, mientras que 12% dijo que cada 3 meses.

Podemos observar que la mayoría de las empresas, se interesa por realizar el mantenimiento del sitio periódicamente.

4. ¿Quién realiza el mantenimiento al sitio web?

OBJETIVO: Que tipo de personal realiza el mantenimiento del sitio web.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Personal de la Empresa | 15 | 88% |
| 2.Empresas desarrolladoras de sitios | 2 | 12% |
| 3.Otros | 0 | 0% |
| **Total** | **17** | **100%** |



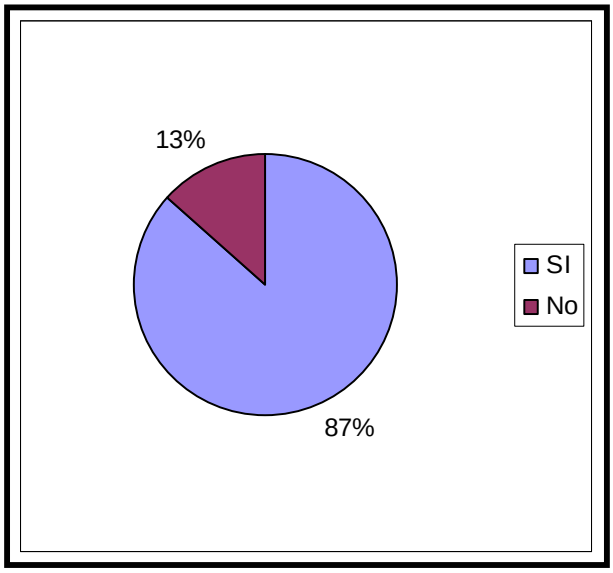

Análisis: Del 100% de las empresas, el 88% dijeron que utilizan el personal de la empresa y el 12% contrata los servicios de empresas desarrolladoras de sitios web.

Podemos analizar que en la mayoría empresas son los mismos empleados los encargados del mantenimiento del sitio y son muy pocas las que contratan a personas encargadas de dicha actividad y que por ser su ocupación principal pueden tener mayor experiencia.

5. Si lo realiza el personal propio ¿Poseen procedimientos escritos establecidos?

OBJETIVO: Conocer si existen procedimientos escritos establecidos, al cual se apegan los empleados al realizar el mantenimiento del sitio.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.SI | 13 | 87% |
| 2.No | 2 | 13% |
| **Total** | **15** | **100%** |



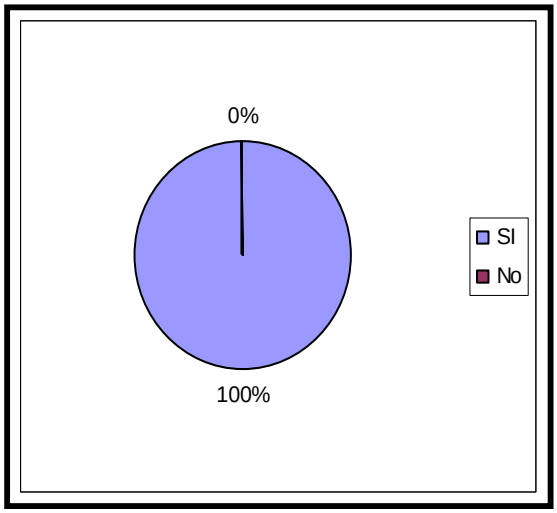

Análisis: El 87% de las empresas dijeron si tener procedimientos escritos para darle mantenimiento al sitio pero un 13% dijeron no contar con esta herramienta.

Se puede observa que para la gran parte de las empresas es de importancia el contar con procedimientos escritos que les ayude a los encargados de realizar el mantenimiento del sitio web ejecutar su trabajo eficientemente.

6. ¿Se realizaron pruebas para llevar a cabo la publicación del sitio web?

OBJETIVO: Determinar qué cantidad de empresas tienen el cuidado de realizar las pruebas necesarias antes de publicar su sitio.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.SI | 17 | 100% |
| 2.No | 0 | 0% |
| **Total** | **17** | **100%** |



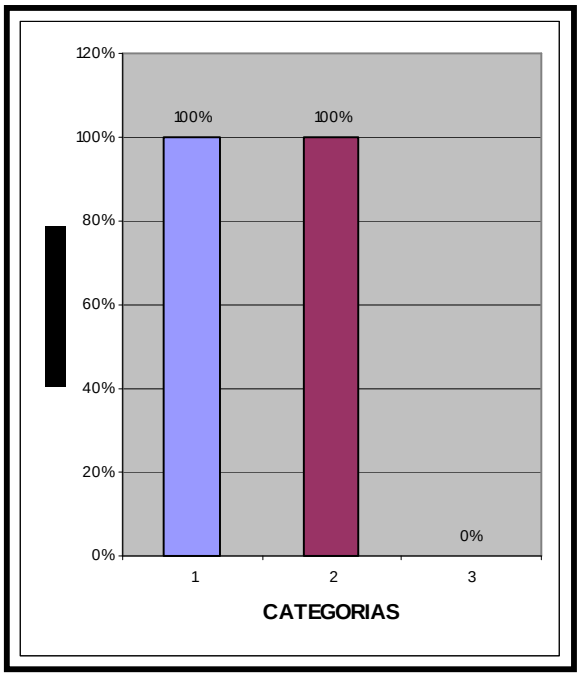

Análisis: El 100% de las empresas encuestadas respondieron que hicieron pruebas antes de la publicación del sitio.

Todas las empresas se mostraron interesadas para prevenir cualquier tipo de fallas y cerciorarse que la publicación del sitio funcione bien.

7. ¿Qué documentación acompañó al sitio web a su entrega?

OBJETIVO: Conocer qué tipo de documentación es la que acompaña al sitio web al momento que se concluye su instalación.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Manual de Usuario | 17 | 100% |
| 2.Diccionario de corrección de fallas | 17 | 100% |
| 3.Otros | 0 | 0% |
| **Total** | **17** | **100%** |



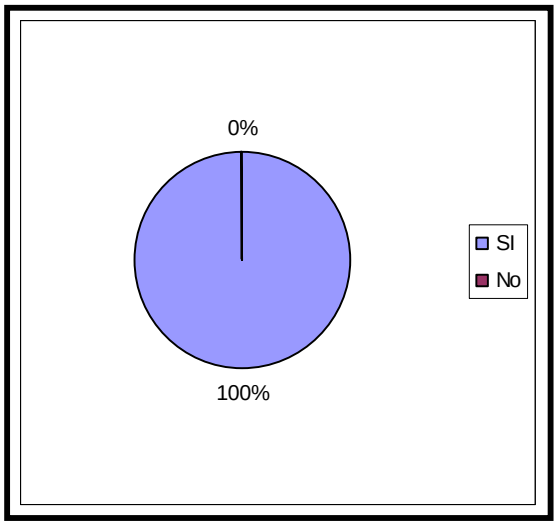

Análisis: El 100% de las empresas encuestadas, al momento de instalar y probar el sitio web, se les hace entrega del diccionario de corrección de fallas así como del manual de usuario.

A todas las empresas se les entrega esta documentación la cual deben de resguardar por cualquier inconveniente que resulte en el sitio web.

8. ¿Existe documentación sobre los errores ó fallas del sitio y la forma en que fueron corregidos?

OBJETIVO: Conocer si las empresas cuentan con antecedentes de errores o fallas del sitio web y de qué forma éstos fueron resueltos, si queda alguna documentación.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.SI | 17 | 100% |
| 2.No | 0 | 0% |
| **Total** | **17** | **100%** |



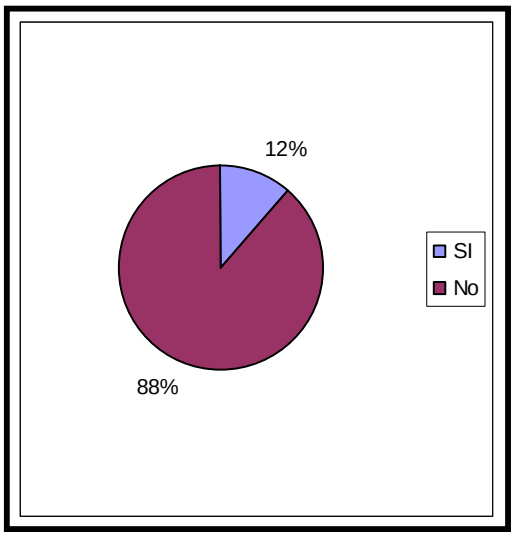

Análisis: El 100% dijeron contar con documentación sobre errores que se han cometido y como han sido corregidos los mismos.

Lo anterior refleja que resulta importante para las empresas archivar todo lo referente al sitio y más aún cómo resolver las fallas que hayan ocurrido en un momento determinado.

9. ¿En la fase de diseño fueron implementados procedimientos que proporcionen pistas de auditoría para recolectar evidencia de las transacciones realizadas en el sitio web?

OBJETIVO: Determinar si el sitio cuenta con algún tipo de dispositivo que registre todas las transacciones que se han realizado durante el día.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. SI | 2 | 12% |
| 2. No | 15 | 88% |
| **Total** | **17** | **100%** |



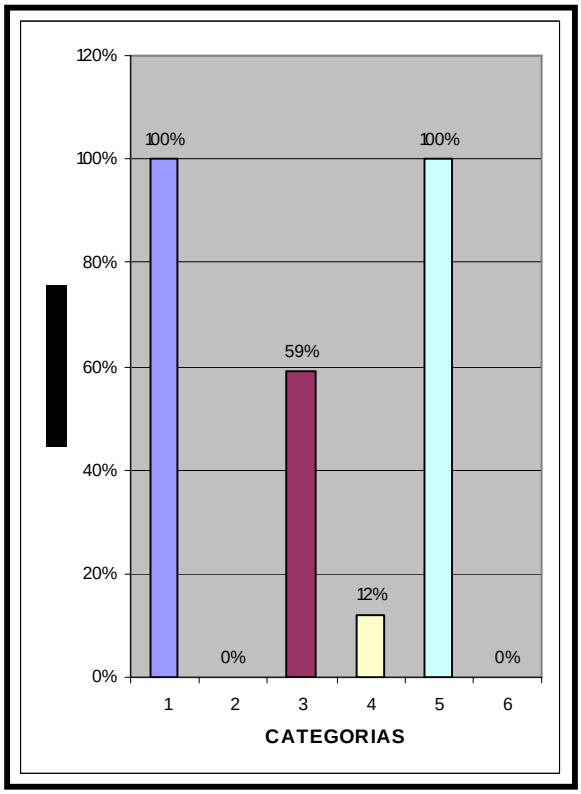

Análisis: Del total de encuestados el 88% dicen que su sitio web no cuenta con este tipo de procedimientos, mientras que el 12% si lo consideró importante.

Podemos observar que la minoría de empresas cuenta con este mecanismo que les ayudará a determinar qué tipo de transacciones se han realizado en el sitio web.

10. ¿Qué medidas de seguridad posee el centro de cómputo para combatir situaciones de desastre?

OBJETIVO: Conocer la percepción de las empresas en cuanto a las situaciones de desastre que puedan ocurrir.

| Categorías | Total | Porcentaje |
|---|---|---|
| 1.Extintores de Fuego | 17 | 100% |
| 2.Alarma Contra Incendio | 0 | 0% |
| 3.Alarma Contra Robo | 10 | 59% |
| 4.Censores de humo | 2 | 12% |
| 5.Vigilancia | 17 | 100% |
| 6.Otros | 0 | 0% |
| **Total** | **17** | **100%** |

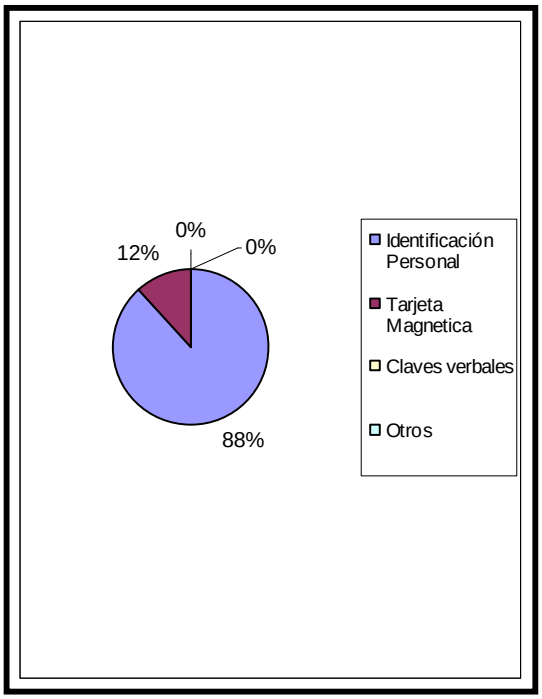



Análisis: Del total de las empresas el 100% de ellas respondieron que utilizaban extintores de fuego y vigilancia, el 59% de ellas utilizan también alarmas contra robo y el 12% de empresas tiene censores de humo instalados. Esto indica que las empresas implementan medidas de seguridad a fin de resguardar sus activos.

11. ¿Cómo se realiza el acceso al centro de cómputo?

OBJETIVO: Determinar qué tipo de medidas tienen las empresas para poder ingresar al centro de cómputo.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Identificación Personal | 15 | 88% |
| 2.Tarjeta Magnética | 2 | 12% |
| 3. Claves verbales | 0 | 0% |
| 4. Otros | 0 | 0% |
| **Total** | **17** | **100%** |



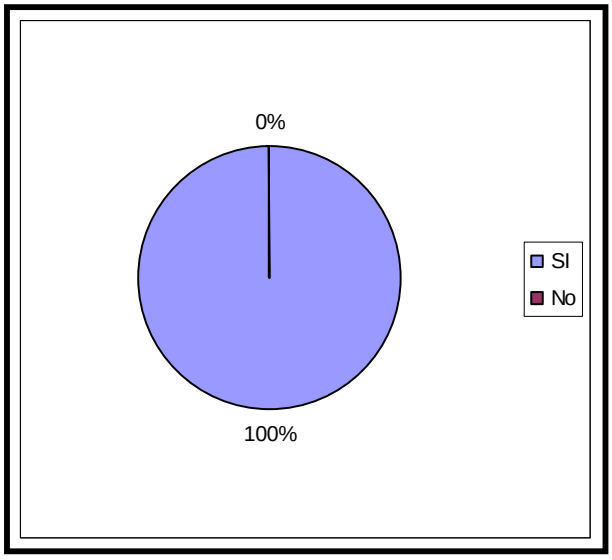

Análisis: Se observa que el 88% del personal de las empresas tienen que estar debidamente identificados para ingresar al departamento y el 12% de las empresas utiliza tarjetas magnéticas para poder ingresar al centro de cómputo.

Esto indica que de una u otra forma las empresas tratan de tener algún tipo de restricción en el área de cómputo.

12. ¿Además del personal de informática, existen otras personas que tienen acceso al centro de cómputo?

OBJETIVO: Conocer qué tipo de personal a parte del de informática tiene acceso a este departamento, para poder identificar qué tipo de responsabilidad tiene dentro de la empresa.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. SI | 17 | 100% |
| 2. No | 0 | 0% |
| **Total** | **17** | **100%** |

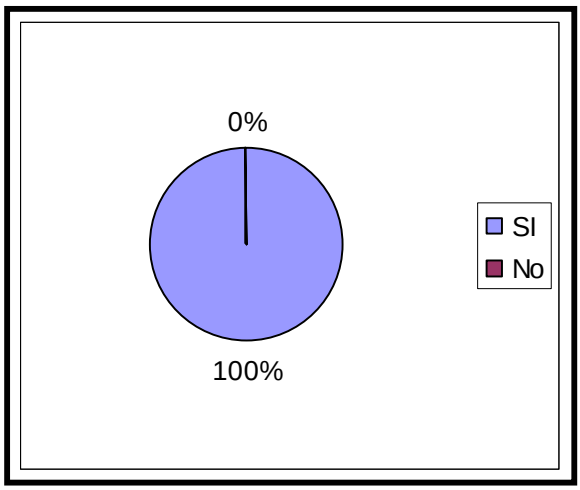



Análisis: De acuerdo a los resultados obtenidos el 100% de las empresas encuestadas mencionan que en el departamento de informática, ingresan también otro tipo de personal que de una u otra forma tiene acceso a esta unidad por el trabajo mismo.

13. ¿Poseen un lugar diferente al centro de cómputo para resguardar la información que se procesa en el sitio?

OBJETIVO: Saber si la empresa archiva en un lugar diferente al centro de cómputo la información procesada en el sitio web y si el lugar donde se resguarda dicha información reúne requisitos mínimos de seguridad.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.SI | 17 | 100% |
| 2.No | 0 | 0% |
| **Total** | **17** | **100%** |



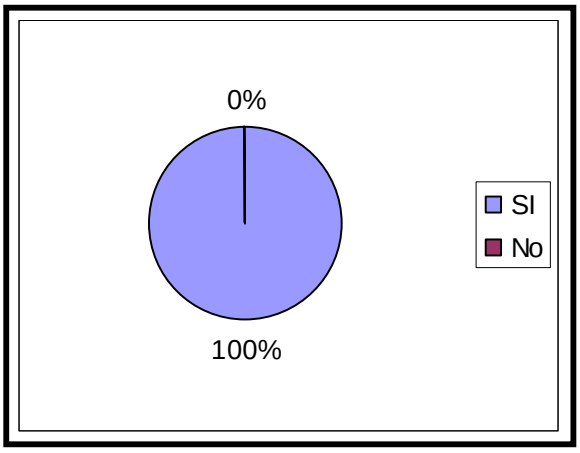

Análisis: El 100% de las empresas encuestadas respondió que si poseen en un lugar diferente al centro de cómputo la información procesada en el sitio web.

Según los datos obtenidos se puede determinar que es necesario resguardar la información importante que es procesada en el sitio web, en un lugar diferente al del procesamiento pues el riesgo de perder el 100% de la información se minimiza con este procedimiento.

14) ¿Existen políticas sobre confidencialidad en el manejo de la información de los clientes?

OBJETIVO: Investigar las políticas establecidas por la empresa para manipular la información de los clientes para saber si hay restricciones respecto a la obtención y manejo de información confidencial o si no existen políticas de control respecto a este tema.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.SI | 17 | 100% |
| 2. No | 0 | 0% |
| **Total** | **17** | **100%** |



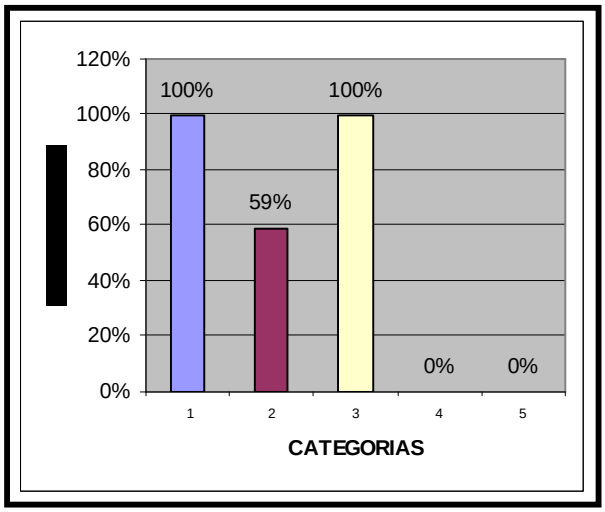

Análisis: De las empresas encuestadas el 100% respondió que poseen políticas de confidencialidad en el manejo de información de sus clientes.

Las empresas mantienen políticas de confidencialidad respecto a la información que los clientes transfieren a través de las transacciones que realizan por medio de la web, es una característica indispensable que mantiene la confianza que los clientes depositan en las empresas.

15) ¿Quiénes tienen acceso a obtener información de los equipos de cómputo clasificada como confidencial?

OBJETIVO: Identificar quien es el personal que tiene el acceso a sustraer la información confidencial para determinar si este tipo de información es manejada por el personal idóneo y no por cualquier persona.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Personal de Informática | 17 | 100% |
| 2.Gerentes | 10 | 59% |
| 3.Auditor Interno | 17 | 100% |
| 4.Personal de Mantenimiento (del Centro de Cómputo) | 0 | 0% |
| 5.Otros | 0 | 0% |
| **Total** | **17** | **100%** |

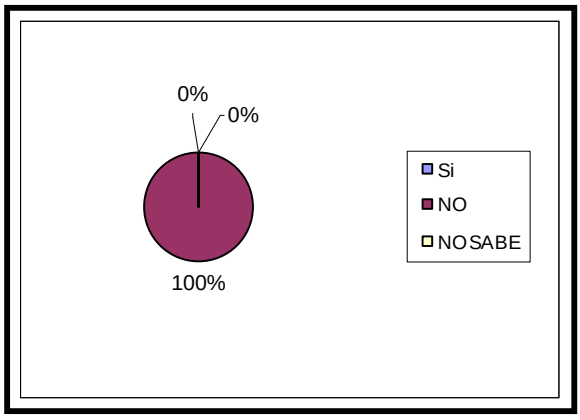



Análisis: El 100% de las empresas encuestadas respondieron que el personal que tiene acceso a información confidencial de los clientes es el de informática y de auditoría interna, el 59% de ellas respondieron que también los gerentes de la empresa. Según los datos obtenidos, el personal que tiene acceso a la información es el que está involucrado en el desarrollo de operaciones y el que interviene en la toma de decisiones.

16) ¿Si una persona realiza cambios a la información almacenada puede hacerlo sin dejar rastro alguno?

OBJETIVO: Investigar si existen procedimientos para detectar cuando se realizan cambios a la información de los clientes o si la información puede ser fácilmente modificada y no tener un control sobre dichas actuaciones.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 0 | 0% |
| 2. NO | 17 | 100% |
| 3. NO SABE | 0 | 0% |
| **Total** | **17** | **100%** |



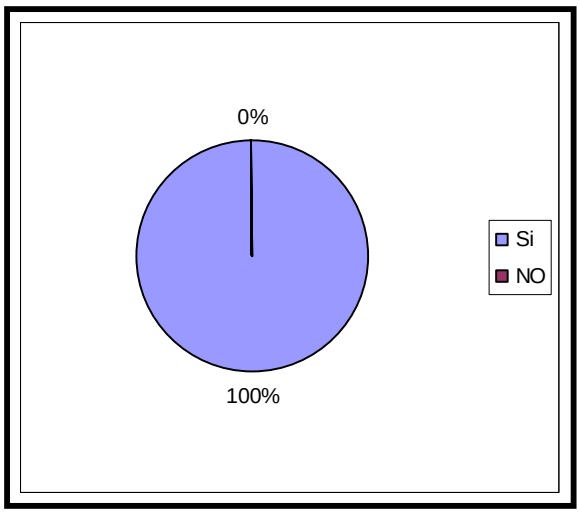

Análisis: El 100% de las empresas encuestadas respondieron que no pueden realizarse cambios a la información almacenada sin dejarse rastros de que se han realizado dichos cambios.

Según los comentarios realizados por las empresas en estudio, se menciono que la privacidad de los clientes y el resguardo de la información que ellos han confiado en la empresa son las características esenciales para mantener y aumentar su clientela, por lo que todos los recursos están enfocados en mantener segura dicha información.

17) ¿Existe algún programa que utilice la empresa que genere una bitácora de las operaciones que realizan los usuarios del sistema?

OBJETIVO: Saber si existe un programa que genere un reporte de las operaciones que realizan los usuarios del sistema.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Si | 17 | 100% |
| 2.NO | 0 | 0% |
| **Total** | **17** | **100%** |



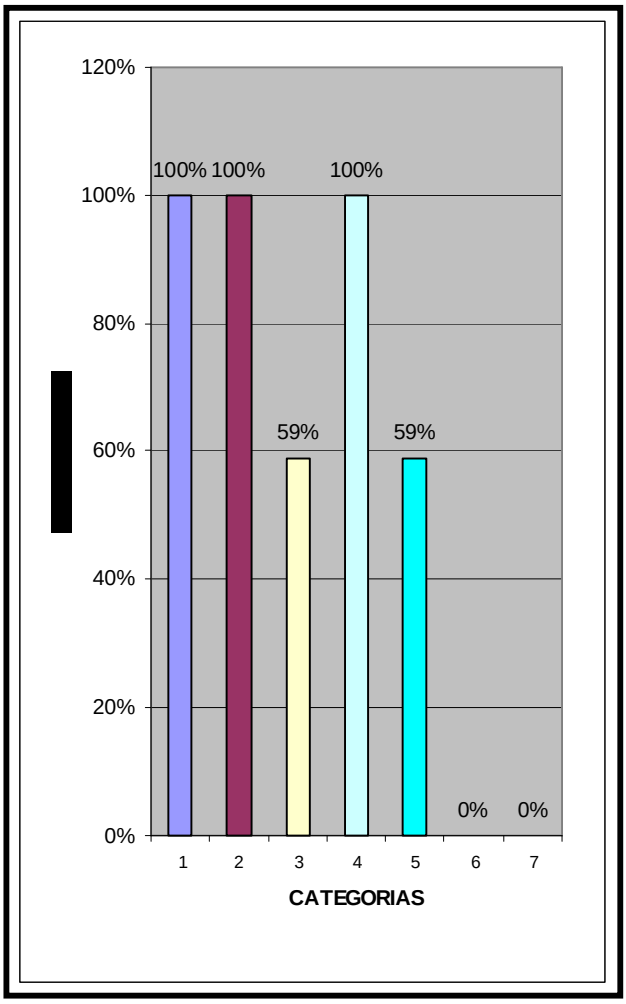

Análisis: El 100% de las encuestadas respondieron que si cuentan con programas que les permitan obtener información sobre las operaciones que son realizadas por los usuarios del sistema.

Se pone de manifiesto que las empresas buscan mantener la seguridad de la información que ellas manejan y sobre todo responsables de algún daño a la integridad de dicha información.

17-A) Si la respuesta fue afirmativa, ¿Qué tipo de información le detalla el programa anterior?

OBJETIVO: Obtener el detalle de la información que genera el programa para identificar si es factible obtener datos sobre alteraciones realizadas a la información confidencial de la empresa.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Nombre del usuario que acceso | 17 | 100% |
| 2. Hora de acceso y tiempo de permanencia | 17 | 100% |
| 3. Información que reviso | 10 | 59% |
| 4. Cambios realizados a la información | 17 | 100% |
| 5. Realizó copias de backup de la información | 10 | 59% |
| 6. Cambios al sistema | 0 | 0% |
| 7.Otros | 0 | 0% |
| **Total** | **17** | **100%** |



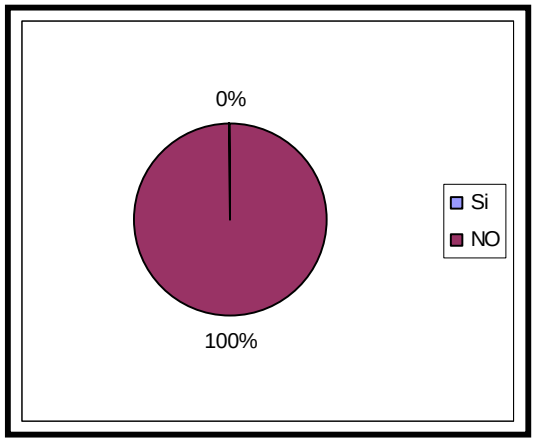
Análisis: El 100% de las empresas manifestaron que el programa que utilizan para obtener informes de las operaciones que realizan los usuarios del sistema les detalla información referente a: El nombre del usuario, hora de acceso y tiempo de permanencia y los cambios que dicho usuario realizo a la información, el 59% de las empresas también menciono que el sistema les detalla la información que reviso y si realizo copias de backup de la información.

Es de gran importancia y ayuda a las empresas el uso de un programa que les permita obtener datos importantes de los usuarios del sistema y los datos que dichos usuarios pudieron haber modificado o introducido, con el objeto de minimizar los riesgos de ataques a la información.

18) ¿Puede ser modificado el detalle de la información que genera el programa que menciona la pregunta anterior?

OBJETIVO: Conocer si la información que proporciona el programa que genera el reporte de las actuaciones de los usuarios puede ser fácilmente modificada por personal no autorizado y no dejar rastro alguno de las modificaciones realizadas ni del autor de dichas alteraciones.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Si | 0 | 0% |
| 2. NO | 17 | 100% |
| **Total** | **17** | **100%** |



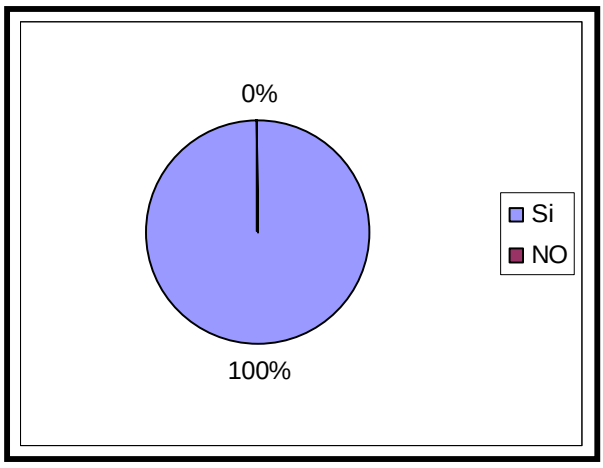

Análisis: El 100% de las empresas encuestadas respondió que no pueden ser modificados los datos que genera el programa que ellos utilizan para obtener información sobre las operaciones que son realizadas por los usuarios del sistema.

Las empresas se encargan de que las actuaciones de los usuarios del sistema estén estrictamente controladas para evitar la fuga de información de sus clientes.

19) ¿Posee políticas para garantizar la privacidad de los datos de los clientes obtenidos a través del sitio web en las transacciones de comercio electrónico?

OBJETIVO: Determinar el grado de importancia que la empresa otorga a la privacidad de la información que obtiene de sus clientes a través de la web por medio de la implementación de políticas que aseguren la integridad de dicha información.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 17 | 100% |
| 2.NO | 0 | 0% |
| **Total** | **17** | **100%** |



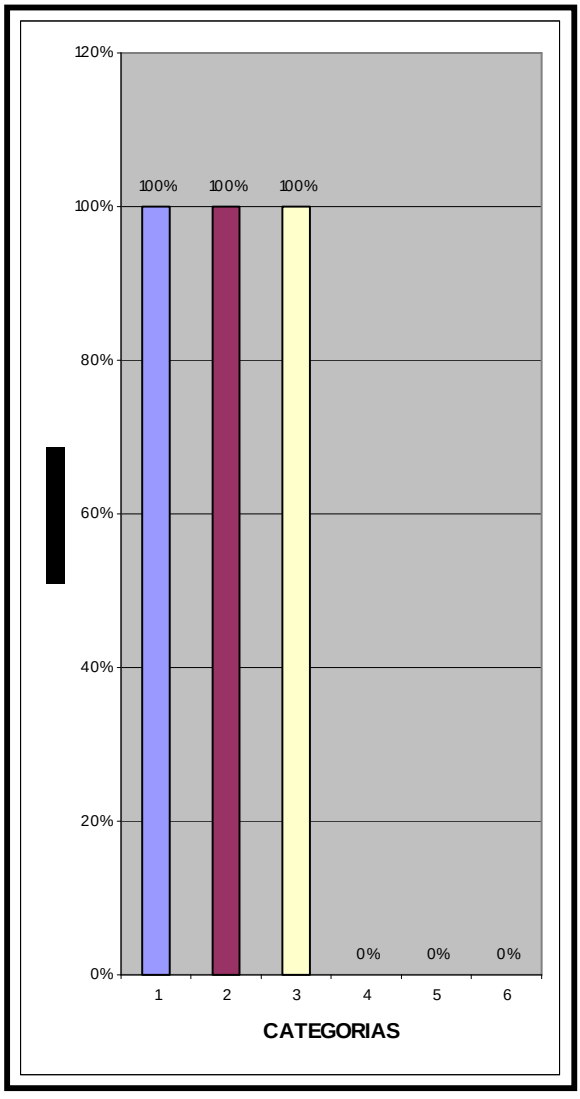

Análisis: El 100% de las empresas contestaron que si poseen políticas para garantizar la privacidad de los datos de los clientes obtenidos a través del sitio web.

Para las empresas que realizan comercio electrónico es importante la privacidad de la información que obtiene de sus clientes a través de la web por lo que cuentan con políticas que aseguren la integridad de dicha información.

20) ¿Cuáles son las políticas de seguridad empleadas en el sitio web para garantizar la privacidad de los datos de sus clientes?

OBJETIVO: Identificar las políticas de privacidad que son implementadas por la empresa para resguardar lo datos obtenidos de los datos de los clientes a través de la web.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Evitar compartir con otras personas los datos de un usuario sin la autorización explicita del mismo | 17 | 100% |
| 2.Siempre que se envíe un correo electrónico a los usuarios explicarles como se obtuvo su dirección y como puede hacer para darse de alta a la lista de distribución si así lo desea | 17 | 100% |
| 3. Restringir el acceso a las bitácoras | 17 | 100% |
| 4. Evitar el proporcionar información personal de los usuarios | 0 | 0% |
| 5. Establecer políticas de privacidad con los empleados | 0 | 0% |
| 6. Otros | 0 | 0% |
| **Total** | **17** | **100%** |



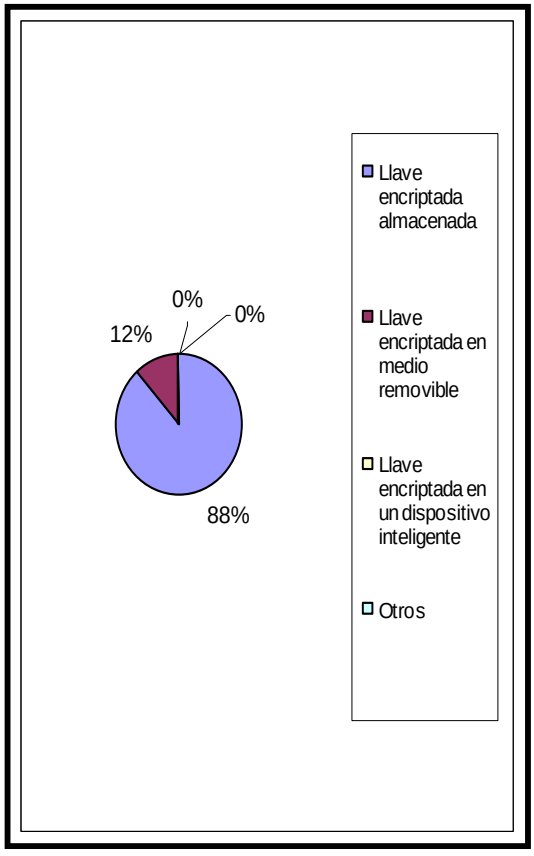
Análisis: El 100% de los resultados muestra que las empresas adoptan políticas como: evitar compartir con otras personas los datos de los usuarios sin la autorización del mismo, que siempre que se envía un correo electrónico a los usuarios se explica cómo se obtuvo su dirección y como puede hacer para darse de alta a la lista de distribución si así lo desea, y restringe el acceso a las bitácoras.

Para las empresas es importante establecer políticas de seguridad en el sitio web para garantizar la privacidad de los datos obtenidos de los clientes.

21) Si utiliza la técnica de identificación de firma digital ¿Cuáles de lo siguientes medios físicos usa para soportar la tecnología de la llave digital?

OBJETIVO: Investigar los medios físicos que utiliza la empresa para soportar la llave digital para verificar que la tecnología utilizada sea la mas segura disminuyendo el porcentaje de vulnerabilidad ante usuarios de la computadora o programas hostiles.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Llave encriptada almacenada en disco duro | 15 | 88.24% |
| 2. Llave encriptada en medio removible | 2 | 11.76% |
| 3. Llave encriptada en un dispositivo inteligente | 0 | 0% |
| 4. Otros | 0 | 0% |
| **Total** | **17** | **100%** |



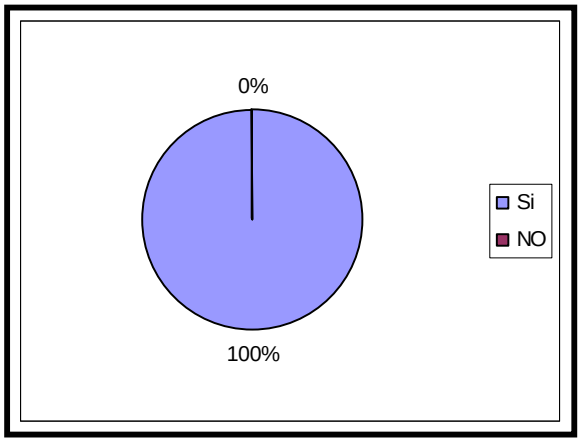
Análisis: Del 100% de las empresas, el 88% respondieron que el medio físico que utilizan para soportar la tecnología de la llave digital es el de llave encriptada almacenada en disco duro y el 12% contestaron que utilizan la llave encriptada en medio removible.

Según datos obtenidos en la investigación, el medio físico más seguro ante programas hostiles para soportar la llave digital es la llave almacenada en un dispositivo inteligente, la llave encriptada en medio removible y la almacenada en disco duro son más vulnerables a los usuarios de la computadora y a programas hostiles, pero según los resultados son los que más utilizan la empresas actualmente.

22) ¿Utiliza la criptografía como herramienta de seguridad de su sitio web al realizar transacciones electrónicas?

OBJETIVO: Conocer si la empresa utiliza técnicas como la criptografía para conservar la información que viaja a través del sitio web de forma segura disminuyendo el riesgo de alteraciones o sustracciones por personas no autorizadas.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 17 | 100% |
| 2. NO | 0 | 0% |
| **Total** | **17** | **100%** |



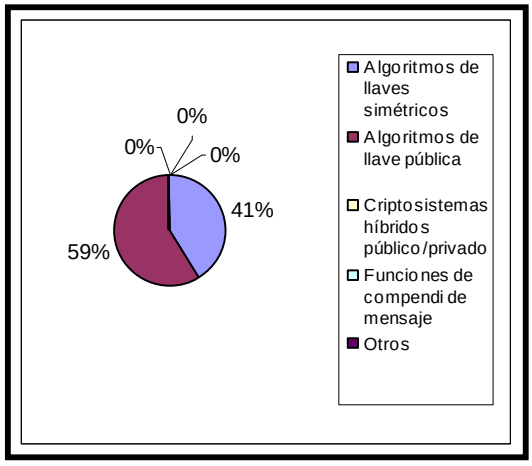

Análisis: El 100% de las empresas encuestadas respondió que utiliza la criptografía como herramienta de seguridad de su sitio web al realizar transacciones electrónicas.

La criptografía es un conjunto de técnicas empleadas para conservar la información de forma segura, pues se basa en la transmisión de datos de forma tal que sea incomprensible para los receptores no autorizados, por lo que en la actualidad las empresas lo utilizan en las transacciones realizadas con sus clientes.

23) ¿Cuál es el algoritmo de encriptación que utiliza para su sitio web en las transacciones de comercio electrónico?

OBJETIVO: Saber cuál es el algoritmo de encriptación (métodos de transposición y sustitución) que utiliza la empresa para enviar y recibir información de sus clientes a través de la web para determinar la capacidad del algoritmo de proteger a la información contra un ataque.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Algoritmos de llaves simétricos | 7 | 41.18% |
| 2. Algoritmos de llave pública | 10 | 58.82% |
| 3. Criptosistemas híbridos público/privado | 0 | 0% |
| 4.Funciones de compendio de mensaje | 0 | 0% |
| 5.Otros | 0 | 0% |
| **Total** | **17** | **100%** |

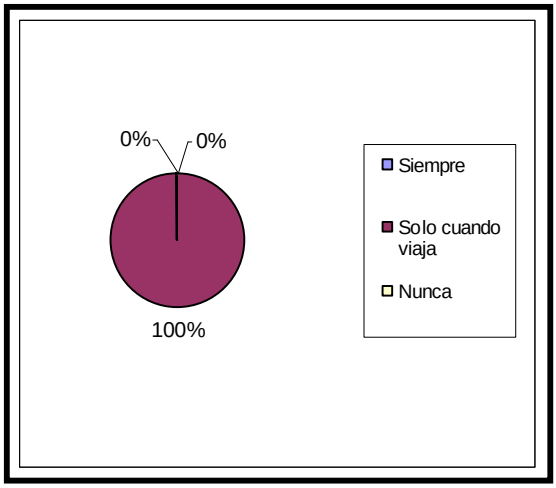



Análisis: Del 100% de los resultados obtenidos, el 41% respondió que utiliza algoritmos de llaves simétricas y el 59% respondió que utiliza algoritmos de llave pública. Actualmente los algoritmos de encriptación, utilizan los métodos de sustitución y transposición combinados, los más utilizados son los de llave simétrica y llave pública que son los que utilizan las empresas encuestadas en las transacciones de comercio electrónico.

24) ¿La información manejada por el sitio web permanece encriptada en todo momento o únicamente cuando viaja a través de la red?

OBJETIVO: Identificar el momento en que la información que se maneja en el sitio web esta encriptada para determinar el riesgo de sustracción de información confidencial.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Siempre | 0 | 0% |
| 2. Solo cuando viaja | 17 | 100% |
| 3. Nunca | 0 | 0% |
| **Total** | **17** | **100%** |



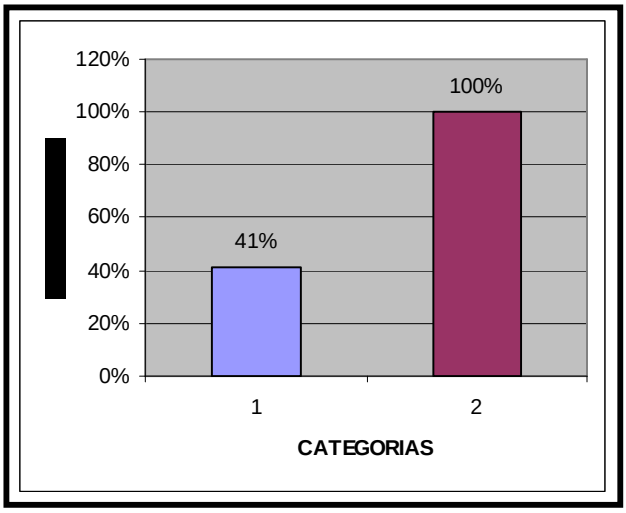

Análisis: El 100% de las encuestadas respondieron que la información permanece encriptada únicamente cuando viaja a través de la red.

Las empresas en estudio mencionaron que es importante mantener encriptada la información cuando viaja por la red y que no debe permanecer encriptada necesariamente en todo el proceso en que se esté realizando la operación de comercio electrónico.

25) ¿Cuál es la información de los clientes que es encriptada?

OBJETIVO: Saber si la información sensible y privada de los clientes es encriptada, para determinar el nivel de seguridad brindado por el sitio web.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Datos Generales | 7 | 41% |
| 2. Datos Privados | 17 | 100% |
| **Total** | **17** | **100%** |



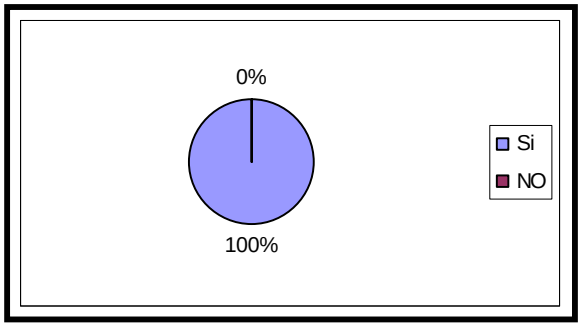

Análisis: El 100% de las empresas respondieron que los datos privados son los encriptados, aunque 41% de las empresas contestaron que ellas también encriptan los datos generales.

Para las empresas es importante mantener seguros los datos transmitidos a través de la web, especialmente los datos privados pues son los que tienen mayor riesgo de ser sustraídos por personas ajenas a la transacción que se ente realizando entre cliente y empresa.

26) ¿Poseen un plan de contingencias ante un incidente de seguridad del sitio web y cada cuanto tiempo es actualizado?

OBJETIVO: Determinar si la empresa posee un plan de contingencias que pueda poner en marcha si llegaran a presentarse problemas de seguridad en el sitio web y si el tiempo de actualización de dicho plan es conveniente para el nivel de transacciones realizadas.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 17 | 100% |
| 2. NO | 0 | 0% |
| **Total** | **17** | **100%** |



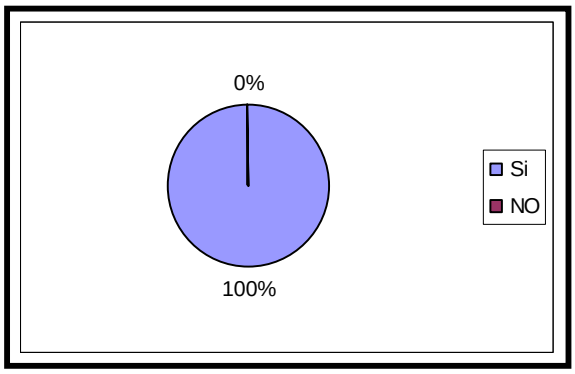

Análisis: El 100% de las empresas encuestadas respondieron que poseen un plan de contingencias ante probables incidentes de seguridad que puedan darse en el sitio web.

Las empresas mencionaron que mantienen un alto nivel de seguridad al tratar con datos importantes de sus clientes, pero que siempre debe mantenerse un plan de contingencias por si acaso se presentara algún incidente inesperado el cual debe actualizarse por lo menos cada 3 meses y de acuerdo al volumen de información.

27) ¿Considera necesario la implementación de programas de trabajo para la realización de auditorías a empresas que realizan comercio electrónico en el país?

OBJETIVO: Obtener información acerca de la necesidad de la elaboración de programas de trabajo para implementarlos en auditorías a empresas que realizan comercio electrónico en el país.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 17 | 100% |
| 2. NO | 0 | 0% |
| **Total** | **17** | **100%** |



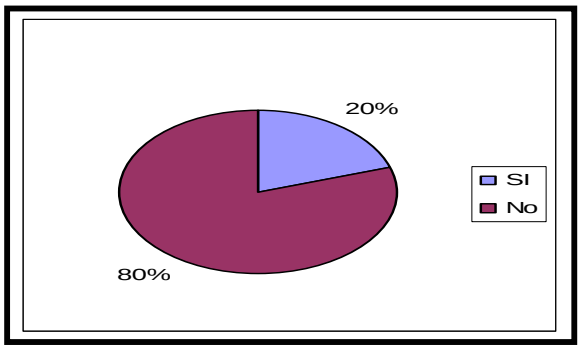

Análisis: El 100% de las encuestadas respondió que es necesaria la implantación de programas de trabajo en la realización de auditorías a empresas que realizan comercio electrónico. Las empresas manifestaron que son indispensables los programas de trabajo y que según su punto de vista auditar las operaciones que ellos realizan es complicado, por lo que la elaboración de programas de trabajo enfocados a este tipo de operaciones es de gran importancia.

**2.2.2 TABULACIÓN DE ENCUESTAS A DESPACHOS DE AUDITORÍA AUTORIZADOS POR EL CONSEJO DE VIGILANCIA DE LA PROFESIÓN DE LA CONTADURÍA PÚBLICA Y AUDITORÍA.**

1. ¿Realizan auditorías a empresas que se dedican al comercio electrónico?

OBJETIVO: Conocer el porcentaje de despacho pertenecientes a la muestra que se dedican a realizar auditorías a empresas que se dedican al comercio electrónico.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. SI | 5 | 20% |
| 2. No | 20 | 80% |
| **Total** | **25** | **100%** |



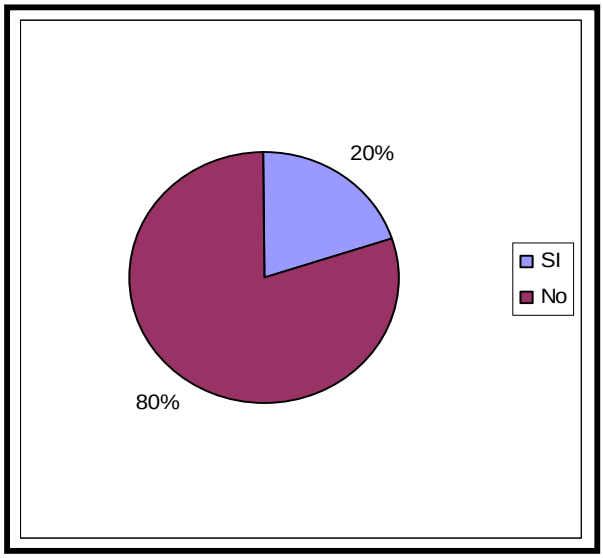

Análisis: El 80% de los despachos encuestados no ha realizado Auditorías a Empresas que se dedica al comercio electrónico y el 20% restante que son un total de 5 despachos si ha realizado algún tipo de auditoría a estas empresas.

Por los resultados podemos afirmar que este tipo de auditorías es poco solicitada.

2. ¿Ha realizado auditorías en las cuales ha evaluado el sitio web de la empresa?

OBJETIVO: Saber si los despachos han evaluado el sitio web de empresas que se dedican al comercio electrónico.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. SI | 5 | 20% |
| 2. No | 20 | 80% |
| **Total** | **25** | **100%** |

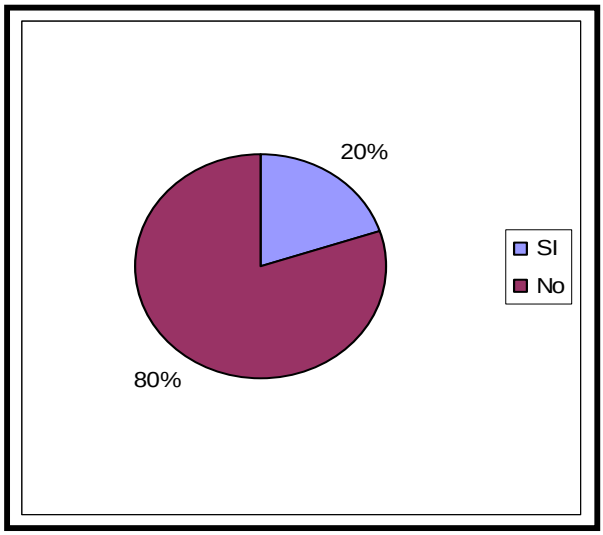



Análisis: El 80% de las empresas encuestadas no ha evaluado el sitio web de empresas que se dedica al comercio electrónico y el 20% restante que son un total de 5 despachos si lo han evaluado de alguna forma, los datos obtenidos nos dan una pauta de la poca periodicidad con que se desarrolla este tipo de auditoría.

3. ¿Ha evaluado el área de informática en esas empresas?

OBJETIVO: Conocer si se ha evaluado el área de informática de las empresas en mención.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. SI | 5 | 20% |
| 2. No | 20 | 80% |
| **Total** | **25** | **100%** |



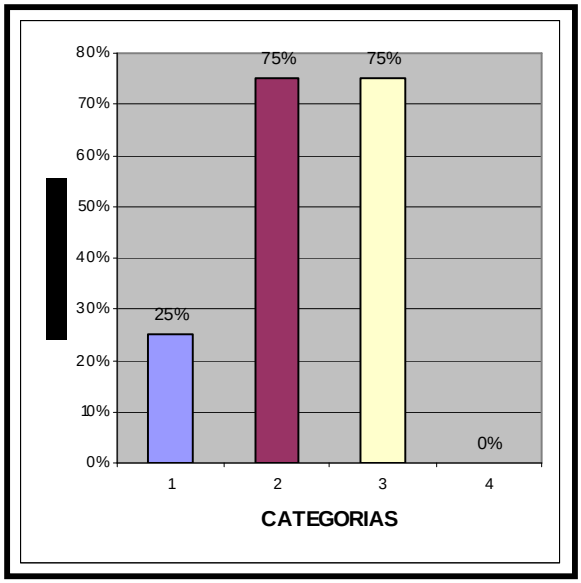

Análisis: Del 100% de los encuestados el 20% de los despachos que audita a empresas que se dedican al comercio electrónico evalúa el área de informática, el 80% restante no.

Los resultados nos muestran que los despachos que realizan auditorías a las empresas que se dedican al comercio electrónico evalúan el área de informática, lo cual indica que es un área de importancia en este tipo de auditorías.

4. Si su respuesta a la pregunta No.1 fue negativa, ¿Cuáles han sido los motivos por los cuales no ha realizado este tipo de auditorías?

OBJETIVO: Conocer cuáles han sido las principales causas por las que los despachos no ha realizado este tipo de auditorías.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. No ha sido requerido ese tipo de servicios | 5 | 25% |
| 2. Falta de personal capacitado | 15 | 75% |
| 3. Falta de herramientas tecnológicas | 15 | 75% |
| 4. Otros | 0 | 0% |
| **Total** | **20** | **100%** |

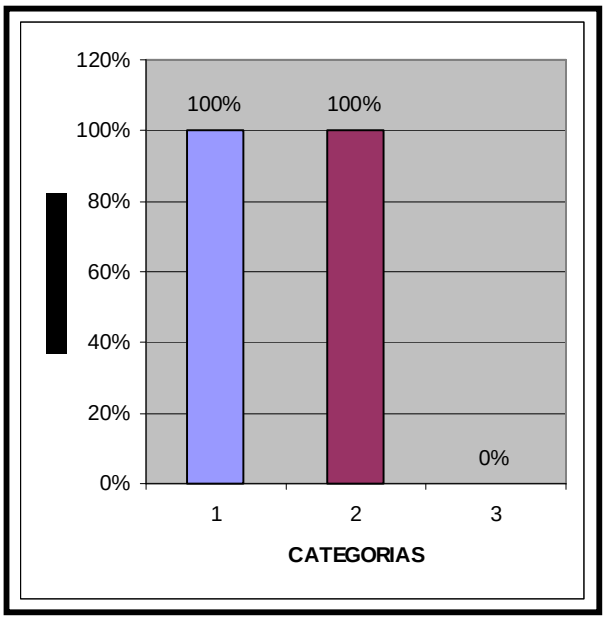



Análisis: Del 80% de las empresas que respondieron en la pregunta 1 que no han realizado ningún tipo de auditoría a las empresas que se dedican al comercio electrónico, entre las diferentes causas de porque no las realizan, el 75% contesto que no poseen el personal adecuado o capacitado ni los recursos tecnológicos necesarios para realizar estas auditorías, el 25% restantes contestó que no les ha sido requerido este tipo de auditorías.

5. Si su respuesta fue afirmativa a la pregunta No.2 ¿Qué áreas han sido evaluadas en ese tipo de auditorías?

OBJETIVO: Conocer cuáles han sido las áreas a evaluar por los despachos que ha realizado este tipo de auditorías.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1.Seguridad física | 5 | 100% |
| 2.Seguridad Lógica | 5 | 100% |
| 3. Otros | 0 | 0% |
| **Totales** | **5** | **100%** |

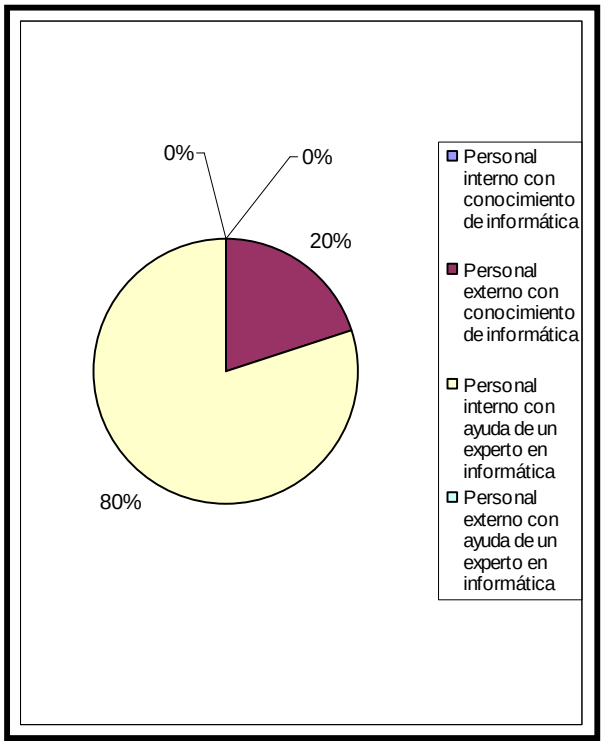



Análisis: Del 20% de las empresas que contestaron en la pregunta 1 que han realizado algún tipo de Auditoría a las empresas que se dedican al comercio electrónico, el 100% manifestaron que las áreas a evaluar fueron la seguridad física y la seguridad lógica.

6. ¿Por quienes han sido realizadas este tipo de auditorías?

OBJETIVO: Conocer el personal con que cuentan los despachos para realizar este tipo de auditorías.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Personal interno con conocimiento de informática | 0 | 0% |
| 2. Personal externo con conocimiento de informática | 1 | 20% |
| 3. Personal interno con ayuda de un experto en informática | 4 | 80% |
| 4. Personal externo con ayuda de un experto en informática | 0 | 0% |
| **Total** | **5** | **100%** |




Análisis: Sobre quienes realizaron este tipo de auditorías por parte de los despachos entrevistados, el 80% contestó que sí realizan este tipo de auditorías lo hacen con personal propio pero con ayuda de un experto con conocimientos en el área de informática y el 20% restante se auxilio solamente de la ayuda de un especialista ajeno al despacho.

7. ¿Qué áreas cree que sería conveniente evaluar en este tipo de auditorías?

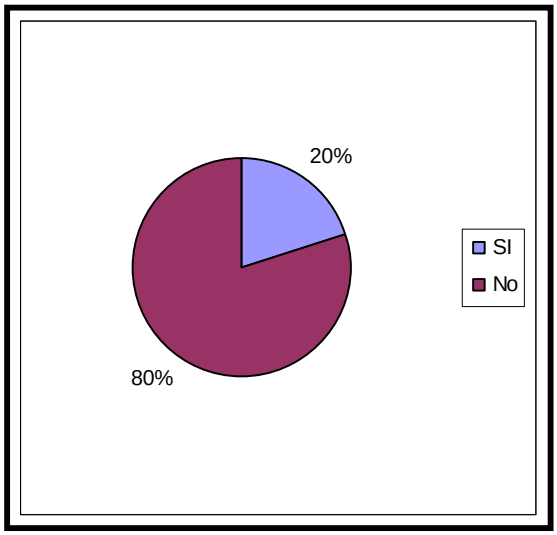
OBJETIVO: Conocer cuáles son las áreas que a criterio de los despachos se debería de evaluar a través de este tipo de auditorías.

Análisis: La mayoría de despachos coincidieron en que el área más importante a evaluar en este tipo de auditoría es el área física y lógica de la empresa, así como el control interno ya que es aquí donde se dan los principales problemas.

8. ¿Poseen procedimientos escritos específicos para realizar este tipo de auditorías?

OBJETIVO: Conocer si los despachos poseen procedimientos escritos para poder realizar las auditorías.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 4 | 80% |
| 2. No | 1 | 20% |
| **Total** | **5** | **100%** |

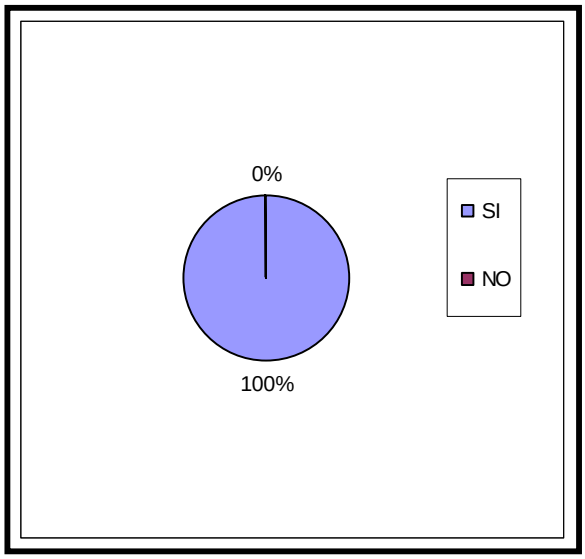



Análisis: Sobre si poseen procedimientos escritos para poder realizar este tipo de auditoría, el 80% de las empresas encuestadas respondieron que si poseen dichos procedimientos por escrito, mientras que el 20% restante manifestó que no. Lo que representa que existe un pequeño porcentaje de los despachos que no realizan las auditorías en base a procedimientos escritos.

9. ¿Cree usted que es necesario disponer de programas que permitan realizar este tipo de auditorías?

OBJETIVO: Conocer si los despachos consideran necesario el poseer programas que permitan realizar con mas facilidad la auditoría.

| Categorías | Total | Porcentajes |
|---|---|---|
| 1. Si | 25 | 100% |
| 2. No | 0 | 0% |
| **Total** | **25** | **100%** |




Análisis: El 100% de los encuestados manifestó que si consideraban necesario disponer de programas que permitan realizar este tipo de auditorías, lo cual indica que el aporte a realizar con la investigación que se está realizando será de mucha utilidad.

10. A su criterio ¿Cuál debería ser el contenido de los programas de auditoría?

OBJETIVO: Documentar que tipo de contenido debería (a criterio de los encuestados) formar parte de un programa de trabajo para auditorías de esta naturaleza.

Análisis: Ninguno de los encuestados respondió a la interrogante planteada, se supone que es debido a falta de documentación por parte de los encuestados que decidieron abstenerse de opinar en este punto

11. ¿Cuáles cree que son los principales problemas que se presentan al momento de obtener evidencia para sustentar los hallazgos?

OBJETIVO: Saber cuáles son las principales causas por la que los auditores tienen dificultad para poder sustentar de una manera adecuada los hallazgos en estas auditorías.

Análisis: Solo 2 despachos de los 5 que realizan estas auditorías contestaron la pregunta y manifestaron que la principal dificultad que ellos han tenido se muestra a la hora de llevar a un medio físico la evidencia para su documentación, ya que algunos archivos pueden ser alterados y el software que utilizan no puede guardar de forma inalterable la información, se menciono además que las capturas de pantalla no siempre logran sustentar de la manera que se quiere los hallazgos encontrados.

12. ¿Qué tipo de evidencia utiliza para documentar los hallazgos que sustentan en esas auditorías?

OBJETIVO: Conocer de que manera los despachos sustentan los hallazgos de estas auditorías en la actualidad.

Análisis: Los encuestados manifestaron que la mayoría de hallazgos se sustentaban con capturas de pantalla y que en algunos casos utilizaban algún software que les permitía correr pruebas en los sistemas y guardar los resultados en documentos PDF.

## 2.3 DIAGNOSTICO DE LA INVESTIGACION

### 2.3.1 DE LAS EMPRESAS QUE REALIZAN COMERCIO ELECTRONICO

DESARROLLO Y MANTENIMIENTO DEL SITIO WEB.

Durante el desarrollo de la investigación se pudo observar que el 88% de los encuestados prefirieron contratar los servicios de empresas desarrolladoras de sitios para poder publicar su sitio web, de estas empresas el 87% tomo como base de contratación la presentación de la credencial de la empresa encargada del desarrollo del sitio.

Una vez funcionando el sitio, el 88% de las empresas realizan el mantenimiento de este cada mes, el cual es realizado por personal de la empresa que cuenta con procedimientos escritos para llevarlo a cabo.

Las empresas realizaron pruebas antes de la publicación del sitio mostrando interés en prevenir cualquier tipo de falla; al momento de instalar y probar el sitio se les fue entregado el diccionario de corrección de fallas al igual que el manual de usuarios; Así mismo todas las empresas manifestaron poseer documentación sobre los errores o

fallas que se han presentado en el sitio y la forma en que estos han sido corregidos. El 88% de las empresas menciono que no fueron incluidos en la fase de diseño procedimientos que proporcionen pistas de auditoría para recolectar evidencia de las operaciones realizadas en el sitio web.

SEGURIDAD FISICA Y MANEJO DE LA INFORMACION

Las empresas encuestadas manifestaron que utilizan medidas de seguridad para combatir situaciones de desastre en el centro de cómputo y controlar el acceso al personal.

Según datos obtenidos, el 100% de las empresas consideran necesario resguardar la información en un lugar diferente al centro de cómputo esto minimiza el riesgo de pérdida de información.

Las empresas mantienen políticas de confidencialidad respecto a la información que los clientes transfieren a través de las transacciones que realizan por medio de la web, por ello el personal que tiene acceso a esta información es el de informática y auditoría interna y en un menor porcentaje los gerentes de la empresa.

El 100% de las empresas manifestó que posee programas que generan una bitácora de las operaciones que los usuarios del sistema realizan, razón por la cual, no pueden efectuarse cambios a la información almacenada sin dejar rastro alguno.

SEGURIDAD DEL SITIO WEB

En cuanto a la seguridad del sitio web, las empresas manifestaron que poseen políticas de seguridad para garantizar la privacidad de los datos de los clientes obtenidos a través del sitio entre las cuales se encuentran: evitar compartir con otras personas los datos de los usuarios sin la autorización del mismo, que siempre que se envía un correo electrónico a los usuarios se explica cómo se obtuvo su dirección y como puede hacer para darse de alta a la lista de distribución si así lo desea, y restringe el acceso a las bitácoras.

El 100% de las empresas encuestadas menciono que utiliza la criptografía como herramienta de seguridad de su sitio web al realizar transacciones electrónicas utilizando algoritmos de encriptación de llave simétrica y llave

pública en donde la información (datos privados) permanece encriptada solamente cuando viaja.

Las empresas expresaron que poseían un plan de contingencias que puede ser utilizando al presentarse un incidente de seguridad en el sitio.

El 100% de las encuestadas respondió que es necesaria la implantación de programas de trabajo en la realización de auditorías a empresas que realizan comercio electrónico.

### 2.3.2 DE LOS DESPACHOS AUTORIZADOS POR EL CONSEJO DE LA CONTADURÍA PÚBLICA Y AUDITORÍA.

De la investigación realizada a los despachos se observó que del 100% de la muestra tomada el 80% no realiza auditorías a empresas que realizan comercio electrónico, los principales motivos han sido: falta de personal capacitado, de herramientas tecnológicas y por no haber sido requeridos estos servicios; El 20% por ciento restante manifestaron que si realizan este tipo de auditorías con el apoyo de un experto y que han evaluado el área de informática y el sitio web en donde se han concentrado en la evaluación de seguridad física y lógica de las

transacciones realizadas. De los despachos que realizan este tipo de auditorías, solo el 80% manifestó que posee procedimientos escritos para realizarla.

Los despachos manifestaron que la mayoría de hallazgos se sustentaban con capturas de pantalla y que en algunos casos utilizaban algún software que les permitía correr pruebas en los sistemas y guardar los resultados en documentos PDF, pero que han tenido dificultad a la hora de llevar a un medio físico la evidencia para su documentación ya que algunos archivos pueden ser alterados y el software que utilizan no puede guardar de forma inalterable la información, se menciono además que las capturas de pantalla no siempre logran sustentar de la manera que se quiere los hallazgos encontrados.

El 100% de los despachos encuestados coincidieron en que consideraban necesario disponer de programas que permitan realizar este tipo de auditorías lo cual indica que el aporte a realizar con la investigación que se está realizando será de mucha utilidad.

# CAPITULO III PROPUESTA DE PROGRAMAS DE TRABAJO PARA LA OBTENCIÓN DE EVIDENCIA SOBRE LAS OPERACIONES VIRTUALES. CASO AUDÍTORIA REALIZADA A EMPRESAS SALVADOREÑAS QUE SE DEDICAN AL COMERCIO ELECTRÓNICO.

## 3.1 PROGRAMAS DE AUDÍTORIA

Como parte de la planificación de la auditoría, se elaboran los programas de trabajo para realizar el examen y obtener la evidencia necesaria, que respalde el informe. Como se establece en el capítulo 1, el programa de trabajo es el documento en el cual se detallan los procedimientos a seguir para la realización de la auditoría, logrando de esta forma los objetivos del examen que conllevan a emitir la opinión de audítoria basado en las pruebas obtenidas en el desarrollo de la misma.

A continuación se plantea una propuesta de programas de trabajo para la obtención de evidencia sobre las operaciones virtuales en audítoria realizada a empresas

salvadoreñas que se dedican al comercio electrónico, los programas se encuentran divididos en:

- programas sobre seguridad física: los cuales incluyen programas sobre la seguridad del centro de cómputo, sobre seguridad de los equipos de cómputo y sobre almacenamiento de la información.
- Programas sobre seguridad lógica: programas sobre mantenimiento del sitio Web, sobre los usuarios de la información (Claves de acceso), sobre la protección e integridad de los datos, sobre protección del sitio Web y sobre la obtención de evidencia de las operaciones virtuales.

Cabe mencionar que en algunas áreas puede ser necesaria la ayuda de un especialista, si en caso el personal de audítoria no posee los conocimientos suficientes del área a evaluar.

### 3.1.1 SOBRE SEGURIDAD FISICA

#### 3.1.1.1 PROGRAMA SOBRE SEGURIDAD DEL CENTRO DE CÓMPUTO

En la empresa deben observarse reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del

sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo, por lo tanto el auditor al evaluar esta área debe tener el cuidado de revisar los siguientes aspectos de importancia:

Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo, y si se cuenta con detectores de humo que indiquen la posible presencia de fuego.

El uso de reguladores de energía los cuales reducen el riesgo de tener un accidente por los cambios de corriente.

- En las instalaciones eléctricas de alto riesgo se cuente con equipo de fuente no interrumpible, tanto en la computadora como en la red.

- Con referencia a los cables del sistema eléctrico para reducir el riesgo de incendios a causa de la electricidad, observar que los cables estén colocados en paneles y canales resistentes al fuego los cuales deben estar aislados y fuera de los lugares de paso del personal, además que se cuente con protección contra roedores o fauna nociva pues este tipo de animales se comen el plástico de los cables.
- Si se cuenta con un dispositivo manual de emergencia para cortar el sistema eléctrico y el aire acondicionado lo cual es conveniente instalarlo en cada salida de emergencia del centro de cómputo.
- En cuanto a los extintores, se debe revisar el número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- Observar si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.

- Que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

Tomando en cuenta todos los aspectos mencionados anteriormente a continuación se presenta el programa de auditoría para evaluar esta área.

**PROGRAMA DE AUDITORÍA**

**SOBRE SEGURIDAD DEL CENTRO DE CÓMPUTO**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Verificar el adecuado mantenimiento del orden dentro del departamento de cómputo y el cumplimiento de las políticas de seguridad establecidas.

**ALCANCE:** Seleccionar las principales políticas establecidas para mantener la seguridad en el centro de cómputo y verificar su aplicación.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Realizar un recorrido por las instalaciones del centro de cómputo para verificar los dispositivos de control con los que se cuenta para el acceso del personal. | | |
| 2 | Revisar si se cuenta con equipo de emergencia como detectores de humo, alarmas contra incendio, alarma contra robo, extintores de fuego para enfrentar situaciones de desastres en el centro de cómputo. | | |
| 3 | Inspeccionar la existencia de información dentro del centro de cómputo, como carteles y cuadros informativos en los cuales se plasmen las políticas de seguridad implementadas en el lugar. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 4 | Verificar si en el centro de cómputo se cuenta con protección en los servidores para que estos no puedan ser desconectados y provocar daños al equipo o a las instalaciones. | | |
| 5 | Revisar la forma de control de acceso a las personas ajenas al centro de cómputo. | | |
| 6 | Investigar si existe vigilancia permanente en el centro de cómputo para evitar pérdidas tanto de los equipos como de la información que ahí es procesada. | | |
| 7 | Obtener información sobre la existencia de un plan de contingencias que permita el funcionamiento del centro de cómputo en caso de suceder un siniestro. | | |
| 8 | Evaluar la ubicación geográfica dentro de la empresa en la que se encuentra el centro de cómputo y los factores externos que pueden influir en él. | | |
| 9 | Elaborar cédula de conclusiones de visita realizada a las instalaciones. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.1.2 PROGRAMA SOBRE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO

En las empresas los programas y equipos que se manejan son altamente sofisticados y son pocas las personas que conocen el diseño de estos y la forma de operar; por lo tanto es necesario que esta área el auditor evalué las siguientes precauciones que las empresas deben tomar:

1) Si es restringido el acceso a programas y a los archivos.

2) Que los operadores no modifiquen los programas ni los archivos.

3) Si es restringida la entrada a la red a personas no autorizadas.

4) Si periódicamente realizan una verificación física del uso de terminales y de los reportes obtenidos.

5) Tener un estricto control sobre el acceso físico a los archivos.

6) En el caso de programas, si se asigna a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

En consideración a estos aspectos a evaluar a continuación se presenta el programa de auditoría del área.

**PROGRAMA DE AUDITORÍA**

**SOBRE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Verificar la existencia e implementación políticas que garanticen la seguridad de los equipos de cómputo.

**ALCANCE:** Revisión de la documentación y los procedimientos realizados por la empresa para garantizar la seguridad de los equipos de cómputo.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Revisar que los equipos de cómputo posean antivirus que cuenten con los requerimientos mínimos de seguridad y que estén actualizados (Un ejemplo de antivirus seguros son aquellos que poseen eurística avanzada). | | |
| 2 | Obtener una copia de la documentación (si la poseen) de todo el software que se encuentra instalado en los equipos de cómputo e indague el porqué de su uso. | | |
| 3 | Verificar el contenido de las bitácoras de los software más importantes del equipos para buscar posibles indicios de fallas o instrucciones (Ejemplos: Firewalls, Antivirus, Bitácoras producidas por el S.O.). | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 4 | Realizar por lo menos con 2 software diferentes a los que utiliza la empresa una serie de pruebas para localizar posibles debilidades del equipo (las pruebas incluyen localización de malware, sniffers, keyloggers, sondeo de puertos,virus,etc.) y documentar los hallazgos. | | |
| 5 | Verificar contra documentación el contenido del sitio web, por ejemplo código html, xlm, js, vbs, imágenes gif y si existe diferencias documentarlas. | | |
| 6 | Observar si en el centro de cómputo se cuenta con las medidas mínimas de seguridad para proteger los equipos (Ejemplos: ups, sistemas de vigilancia, etc.). | | |
| 7 | Verificar si existen políticas para la prevención, control y erradicación de la piratería del software y la contaminación de virus informáticos. | | |
| 8 | Evaluar la forma en que se administra y controla la configuración de servidores, terminales y PCs de la empresa, en cuanto a procesadores, tarjetas madres, cableado interno y externo, componentes del sistema computacional y demás peculiaridades de los sistemas de la empresa. | | |
| 9 | Verificar que toda la estructura de red se encuentre en uso y que aquellos puntos que no se encuentre en uso estén deshabilitados. | | |
| 10 | Elaborar cédula de conclusiones y hallazgos encontrados en la evaluación de la seguridad de los equipos de cómputo. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.1.3 PROGRAMA SOBRE ALMACENAMIENTO DE LA INFORMACIÓN

Otro de los puntos en los que la empresa debe mantener seguridad es en el manejo de información. Por lo que en esta área el auditor debe observar:

1) Que no se obtengan fotocopias de información confidencial sin la debida autorización.

2) Si Sólo el personal autorizado tiene acceso a la información confidencial.

3) Si se controla el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

4) Observar que todos los programas y archivos estén debidamente documentados, pues es el factor más importante de la eliminación de riesgos en la programación.

5) Otro factor en importancia es que se cuente con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- Equipo, programas y archivos

- Control de aplicaciones por terminal
- Definir una estrategia de seguridad de la red y de respaldos
- Requerimientos físicos.
- Estándar de archivos.
- Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

6) Los materiales más peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable los cuales en conveniente que sean almacenados en un lugar aparte de donde se encuentra el equipo de cómputo.

**PROGRAMA DE AUDITORÍA**

**SOBRE ALMACENAMIENTO DE LA INFORMACIÓN**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Evaluar la forma en que la información es almacenada e identificar las deficiencias que puedan existir en los procesos de almacenamiento.

**ALCANCE:** Revisión en base a una muestra del 50% de procedimientos aplicados al almacenamiento de la información.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Inspección al lugar donde es almacenada la información que maneja la empresa, para evaluar las condiciones en las que se encuentra dicho lugar y si esta ubicado en un lugar diferente a donde están ubicadas las instalaciones del centro de cómputo. | | |
| 2 | Verificar si existe acceso restringido al lugar donde se tienen almacenados los medios magnéticos que soportan la información. | | |
| 3 | Identificar a las personas que son responsables del almacenamiento de la información y obtener información en cuanto a la forma en que realizan su trabajo y si existe personal ajeno al lugar que pueda tener acceso a la información, saber su cargo. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 4 | Evaluar cuales son los medios magnéticos en donde se guarda la información y el nivel de seguridad que proporcionan. | | |
| 5 | Revisar si los medios magnéticos que soportan la información se encuentran en forma ordenada y si es posible la identificación de cada uno de ellos y la información que se ha almacenado. | | |
| 6 | Investigar la periodicidad con que se realizan los respaldos a la información que maneja la empresa y si dichos respaldos son llevados directamente al lugar donde es almacenada la información. | | |
| 7 | Obtener los documentos que posee la empresa en donde se detallen las políticas y procedimientos en cuanto al almacenamiento de la información. | | |
| 8 | Evaluar el nivel de protección con el que se cuente en el lugar para enfrentar cualquier situación de desastre que se presente. | | |
| 9 | Obtener información sobre si la empresa cuenta con un plan de contingencias para recuperar información almacenada en caso de presentarse un incidente. | | |
| 10 | Elaborar cédula de conclusiones de visita realizada a las instalaciones. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.2 SOBRE SEGURIDAD LOGICA

#### 3.1.2.1 PROGRAMA SOBRE MANTENIMIENTO DEL SITIO WEB

En esta área el auditor deberá realizar procedimientos de auditoría enfocados a conocer y documentar de qué manera es llevado a cabo el mantenimiento al sitio Web, si bien no es de las áreas más preocupantes a evaluar se hace necesario saber quiénes tienen acceso a poder modificar o adicionar código o rutinas al sitio, ya que con tan solo un par de instrucciones podría estarse fugando los números de las tarjetas de crédito de los clientes de la empresa evaluada a una cuenta de correo de un tercero. Se hace necesario también por parte del auditor tener suficiente conocimiento para poder entender cómo funciona determinada rutina en una página Web y cuáles son las causas de las modificaciones que se ha hecho desde que se publico el sitio.

Mostramos a continuación una serie de procedimientos sencillos que van más que todo enfocados a conocer y documentar la forma como la empresa evaluada ha realizado el mantenimiento al sitio Web (llámesele mejoras, adiciones, etc).

**PROGRAMA DE AUDITORÍA**

**SOBRE MANTENIMIENTO DEL SITIO WEB**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Conocer el funcionamiento y la forma en como se realiza y documenta el mantenimiento del sitio web.

**ALCANCE:** Revisión de la documentación y los procedimientos realizados por la empresa para realizar modificaciones al sitio web.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Verificar y obtener una copia del manual de usuario y de toda la documentación que posea la empresa del sitio web. | | |
| 2 | Ejecutar el sitio web en diferentes navegadores y documentar todos sus componentes y diferencias. | | |
| 3 | Solicitar una copia del sitio web en el servidor y de todos sus componentes y compararlo con lo que obtuvimos al ejecutarlo en el navegador. | | |
| 4 | Observar la forma y periodicidad con que se realiza el mantenimiento al sitio web, cotejar contra documentación existente referente al proceso. | | |
| 5 | Verificar contra documentación el contenido del sitio web por ejemplo codigo html, xlm, js, vbs, imágenes gif y si existen diferencias documentarlas. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 6 | Revisar la documentación que posee la empresa en donde se especifique el personal designado para realizar el mantenimiento del sitio y los procedimientos establecidos para ello. | | |
| 7 | Documentar y hacer una revisión de las diferentes bitácoras generadas por ejemplo de los Firewalls, IDS, Routers, etc. Documentar como y donde se almacenan, quienes las pueden modificar, cual es su contenido, etc. | | |
| 8 | Documentar la forma en que proporcionan la hora en la que se ejecutan los diferentes eventos tanto del sitio web como de los diferentes elementos que lo integran. | | |
| 9 | Solicitar una copia de la documentación que existe en la empresa sobre los cambios realizados al sitio web, documentar quien lo realizó, quien lo autorizó, quien lo solicitó, cual fue el cambio realizado y que lo originó, y compararlo con las diferencias obtenidas en los puntos anteriores (si las hubiere). | | |
| 10 | Elaborar cédula de conclusiones y hallazgos encontrados en la evaluación del mantenimiento del sitio web. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.2.2 PROGRAMA SOBRE USUARIOS DE LA INFORMACIÓN (PASSWORD)

El Auditor en este tipo de auditorías deberá usar no solo su juicio profesional sino también la experiencia acumulada a través de otras auditorías similares, deberá tener conocimiento mínimos sobre las políticas de seguridad que utilizan las empresas a la hora de asignar los usuarios y sus contraseñas.

Será necesario también que el auditor este suficientemente documentado sobre cuáles son las principales amenazas que existen en el medio, como por ejemplo sobre incidentes de seguridad en otras empresas similares a las que evalúa, bugs recientes del software que posee la empresa, incidentes de seguridad ocurridos con anterioridad de la entidad que este evaluado, etc.

Para todo lo anterior mostramos a continuación un programa sencillo con el cual el auditor podrá tener una pequeña idea de la efectividad de las políticas aplicadas por la empresa en la cuestión de los usuarios, restricciones y password.

**PROGRAMA DE AUDITORÍA**

**SOBRE USUARIOS DE LA INFORMACION (PASSWORD)**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Verificar la existencia y correcta aplicación de políticas mínimas de seguridad para el acceso de los usuarios.

**ALCANCE:** Seleccionar las principales políticas establecidas para mantener la seguridad en cuanto al acceso y restricciones que poseen los usuarios y verificar su aplicación.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Verificar si existen políticas de seguridad escritas en cuanto a los accesos (password) y restricciones de cada usuario del sistema y obtener una copia. | | |
| 2 | Averiguar quién o quiénes son los responsables de la asignación de password, privilegios y restricciones de los demás usuarios. | | |
| 3 | Asegurarse que todas las cuentas tengan password y que no sea débil. | | |
| 4 | Revisar en las políticas escritas con que periodicidad se obliga a los usuarios a cambiar los password. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 5 | Verificar si el sistema de validación de los password recuerda las contraseñas anteriores al cambio y si permite se repitan los password anteriores. | | |
| 6 | Verificar si la interfaz de validación de los usuarios hace uso de alguna herramienta de criptografía. | | |
| 7 | Cerciorarse de que los password usados por los administradores o desarrolladores del sitio hayan sido cambiados o eliminados una vez publicado el sitio web. | | |
| 8 | Obtener una copia de todos los usuarios, los recursos a los que tienen acceso y los cargos que estos ocupan dentro de la empresa. | | |
| 9 | Verificar que los usuarios de la base de datos coincidan con los usuarios registrados en el documento anterior y que los accesos sean los que les corresponden. | | |
| 10 | Elaborar cédula de conclusiones y hallazgos encontrados en la evaluación de los usuarios de la información. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.2.3 PROGRAMA SOBRE PROTECCION E INTEGRIDAD DE LOS DATOS

En esta parte de la evaluación, el auditor deberá hacer uso (en la media de lo posible y de sus conocimientos) de la ayuda de un especialista, para identificar y evaluar las áreas de la empresa que representan un atractivo para daños o alteraciones de la información.

Actualmente existen diferentes mecanismos para poder garantizar que la información que es digitada a través de un sitio Web ha viajado segura e íntegra a través de la red, aunque también es de considerar que las personas que buscan conocer, alterar o simplemente dañar esta información, poseen conocimientos avanzados en informática e incluso hasta mejores recursos de software y hardware para cometer sus delitos, es por ello necesario auxiliarse de un profesional que ayuden a cubrir los posibles huecos de seguridad que posea la empresa en general, para ello a continuación mostramos una serie de procedimientos que sirven para que el auditor se haga una idea de cómo son aplicadas las políticas de seguridad en cuanto a la conservación e integridad de la información.

**PROGRAMA DE AUDITORÍA**

**SOBRE PROTECCIÓN E INTEGRIDAD DE LOS DATOS**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Verificar la existencia e implementación de políticas que garanticen la protección e integridad de los datos que son almacenados a través del sitio web.

**ALCANCE:** Revisión de la documentación y los procedimientos establecidos por la empresa para salvaguardar los datos que son procesados en el sitio web.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Obtener una copia de la documentación disponible por la empresa que respalde la forma en que es encriptada la información que es ingresada al sitio web. | | |
| 2 | Documentar cuales son las políticas de seguridad que la empresa proporciona a los usuarios con respecto a los datos que son introducidos en el sitio web y al almacenamiento que estos reciben. | | |
| 3 | Verificar a través de un navegador si el sitio web explica que la información es encriptada. | | |
| 4 | Verificar la existencia y configuración del software y hardware disponible por la empresa para proteger el sitio web y los datos que son procesados por este. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 5 | Investigar y documentar, cual es la información que es encriptada y en que momento se realiza la encriptación. | | |
| 6 | Verificar con un software diferente al utilizado por la empresa, si la información que viaja del sitio web al servidor puede ser desencriptada con facilidad. | | |
| 7 | Investigar y documentar la nomina del personal que conoce el algoritmo de encriptación o tiene acceso a las claves de desencriptación. | | |
| 8 | Solicitar copia del diccionario de datos que posee la empresa y verificar:<br><br>-Si se detalla el total de los campos que contiene la base de datos y si describe el tipo, tamaño y descripción de dichos campos.<br><br>- Con base al documento anterior, verificar que sean los mismos campos que se detallan en la página web.<br><br>-Si las validaciones de los campos donde se introducen los datos en la página web corresponden al documento solicitado. | | |
| 9 | Consultar si existe documentación sobre algún incidente de seguridad en la empresa, en la que se vio comprometida la clave (o claves) de seguridad o la forma en cómo era encriptada la información. | | |
| 10 | Verificar si existen validaciones en los campos donde se introducen los datos en la página web y documentar los resultados. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 11 | Elaborar cédulas de conclusiones y hallazgos encontrados en la evaluación de la protección e integridad de los datos. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.2.4 PROGRAMA SOBRE PROTECCIÓN AL SITIO WEB

El auditor al evaluar esta área, debe tener conocimiento de las amenazas existentes a la seguridad del sitio web y de los métodos que hacen que la seguridad del servidor sea menos vulnerable, entre los principales métodos se encuentran:

- Definición de políticas de seguridad: las cuales tienen la función de guiar a los usuarios hacia el conocimiento de las acciones permitidas y a la elección en cuanto a la configuración y uso del sistema.
- Utilización de programas para mejorar la seguridad de un sitio.
- Utilización de dispositivos que aísle una red interna del resto de Internet, permitiendo pasar conexiones específicas y aislando otras (firewalls).
- Utilización de antivirus y la actualización de este periódicamente.

A continuación se presenta el programa para la evaluación de la protección del sitio web tomando en consideración los aspectos mencionados anteriormente.

**PROGRAMA DE AUDITORÍA**

**SOBRE PROTECCIÓN AL SITIO WEB**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Evaluar la forma en que la empresa realiza la protección al sitio web.

**ALCANCE:** Revisión de los principales procedimientos aplicados por la empresa para proteger al sitio web.

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 1 | Investigar si existe un plan de contingencias para que el servidor pueda continuar operando al presentarse una falla en el sitio web y si dicho plan es actualizado periódicamente. | | |
| 2 | Obtener información para saber si la empresa utiliza un certificado digital para verificar la autenticidad de sus clientes. | | |
| 3 | Verificar que las instalaciones del software y paqueterías sean las adecuadas para el servidor que utiliza la empresa. | | |
| 4 | Revisar la lista de sitios y usuarios externos que tienen acceso a la página web y a la información que en ella se presenta. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 5 | Verificar las herramientas de seguridad utilizadas en el sitio web para detectar cambios no autorizados por el personal de la empresa y por usuarios externos. | | |
| 6 | Revisar si la empresa utiliza firewalls para proteger la red interna de ataques externos. | | |
| 7 | Obtener información sobre el antivirus que utiliza la empresa y evaluar si esta actualizado y la periodicidad con que se actualiza. | | |
| 8 | Elaborar cédulas de conclusiones y hallazgos encontrados en la evaluación de la protección al sitio web. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

### 3.1.2.5 PROGRAMA SOBRE OBTENCION DE EVIDENCIA DE LAS OPERACIONES VIRTUALES

La evidencia digital es frágil y volátil. La información residente en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro, lo cual limita la labor del auditor para identificar y encontrar elementos claves para esclarecer los hechos relevantes de una auditoría.

La evidencia digital al ser un objeto relativamente fácil de manipular, generado por dispositivos electrónicos, de los cuales no sabemos nada sobre su funcionamiento, la susceptibilidad a las fallas, entre otras características, nos advierte que estamos entrando en un campo de investigación delicado y formal donde el conocimiento técnico es fundamental.

Es por eso que a continuación se presenta un programa que trata de establecer procedimientos de auditoría que permitan al auditor obtener elementos de admisibilidad de evidencia sobre las operaciones virtuales.

**PROGRAMA DE AUDITORÍA**

**SOBRE OBTENCION DE EVIDENCIA DE LAS OPERACIONES VIRTUALES**

NOMBRE DE LA EMPRESA _____

PERIODOS AUDITADOS _____

ACTIVIDAD ECONOMICA _____

**OBJETIVO:** Evaluar y documentar las operaciones que son realizadas en el sitio web.

**ALCANCE:** Revisar en base a muestra las transacciones virtuales realizadas por la empresa

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| | En un procedimiento conjunto con el jefe del área de informática solicitar acceso a la página web de la empresa para simular un proceso de compra en el cual se debe documentar: | | |
| 1 | - Obtenga copia de la documentación que posea la empresa sobre cuál es el proceso y respuesta del sitio durante la realización de una compra. | | |
| 2 | - Ingrese al sitio Web creando un usuario por medio del cual se simulará una compra; realice cédula narrativa donde se detalle los pasos a seguir, los datos requeridos y los datos ingresados, realice captura de pantalla y compare los pasos con la documentación obtenida en el procedimiento anterior. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 3 | - Cotejar los datos que el cliente envía a la empresa así como los datos que esta recibe, verificando así la totalidad, veracidad y confiabilidad de la información transferida. Capturar la pantalla de los datos enviados así como la de los datos que se reciben en el servidor. | | |
| 4 | -Verificar que exista un sistema de encriptación de datos que se ingresan al sitio (por medio del icono indicador que aparece en la parte inferior de la página simulando un candado o por la extensión https en la barra de direcciones del sitio). Realizar una narrativa de cómo y en que momento se realiza la encriptación de los datos y como son visualizados en el servidor una vez sean recibidos; Cotejar contra manuales o documentación que se posea del sitio. | | |
| 5 | - Observar el tiempo de respuesta desde el momento en que se introdujeron y enviaron los datos hasta el momento en que se recibieron en el servidor. Elaborar una narrativa. | | |
| 6 | -Tomar una muestra de las operaciones realizadas en el servidor y comparar los tiempos de respuestas con los obtenidos en las pruebas anteriormente realizadas. Indagar si la empresa posee una política referente al tiempo de respuesta de las transacciones. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 7 | - Al momento de pago de los productos, observar los procedimientos que realiza la empresa para verificar que el número de tarjeta de crédito que se introdujo en el sitio web posee fondos o no (confirmación en línea empresa-banco o un procedimiento manual por medio de llamadas telefónicas) documentar dicho procedimiento ya sea obteniendo copia de algún reporte de las confirmaciones de saldos(si el sistema lo realiza en el momento) o realice entrevistas con las personas que intervienen en la confirmación (si el proceso es manual). | | |
| 8 | - Una vez finalizado el proceso de compra, observar y documentar de que manera es confirmada la transacción, por ejemplo: si es a través del correo electrónico obtenga impresión del correo de confirmación, si es a través de un mensaje en la pantalla realice una captura de la pantalla. | | |
| 9 | - Obtenga una copia de los registros de compra en línea y verifique si el sistema confirmó cada una de las compras (puede auxiliarse de la ayuda de algún software como por ejemplo IDEA o ACL). | | |
| 10 | Verificar si el servidor tiene la capacidad de registrar la hora y fecha en que:<br>- El cliente envía la información.<br>- Se recibe y se crea el registro de la información.<br>- La información es modificada.<br>- Imprimir un reporte de la actualización. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 11 | Verificar la existencia de procedimientos de monitoreo de las actividades realizadas dentro del sitio web, observarlos y documentarlos (esto lo puede realizar verificando las bitácoras que guardan los software de auditorías algunos tienen la capacidad incluso de realizar demos de las operaciones sucedidas; o con ayuda de las mismas se pueden realizar diagramas de flujo para comprender cuales han sido los eventos que han sido registrados dentro del sistema y el sitio Web). | | |
| 12 | Consultar con el gerente de ventas cuales son las políticas y procedimientos a seguir para las siguientes transacciones:<br><br>-La entrega de los pedidos.<br>-Las devoluciones.<br>-Cuando los pedidos no han sido entregados.<br>Realizar una narrativa y obtener copia de los documentos que amparan las transacciones. | | |
| 13 | Consultar al jefe de informática si se modifican los registros que existen en el sistema cuando los pedidos no pueden ser entregados o se realizan devoluciones, obtener también la nómina del personal autorizado que puede realizar cambios a la información que se encuentra almacenada en el servidor. | | |
| 14 | Observar que haya una adecuada segregación de funciones para evitar la posibilidad de colusión de los miembros que intervienen en los procesos establecidos en el numeral 12 y 13. | | |

| No | PROCEDIMIENTO | HECHO POR | REF. PTS |
|---|---|---|---|
| 15 | En caso de existir el procedimiento que se detalla en el numeral 13 solicitar un reporte al gerente de ventas de los pedidos que han sido devueltos y los no entregados en el último año y realizar pruebas selectivas con una muestra de la base de datos. | | |
| 16 | Solicitar al jefe de informática una copia de los registros de las ventas que se han realizado en el sitio en los últimos seis un año y solicitar al jefe del departamento de ventas un reporte de las ventas realizadas en el mismo período, que contengan como mínimo: cantidad de productos, nombre del producto, código de inventario, precio de venta, nombre y dirección del comprador, fecha en que se realizó el pedido y fecha de entrega. Elaborar cédula comparativa de los datos obtenidos en ambos reportes. | | |
| 17 | Elaborar cédulas de conclusiones y hallazgos encontrados. | | |

**RECURSO HUMANO**

AUDITOR DESIGNADO _____

SUPERVISOR _____

ELABORADO POR _____

FECHA DE ELABORACION _____

FECHA DE EJECUCION _____

APROBADO POR _____

FECHA DE APROBACION _____

# CAPITULO IV CONCLUSIONES Y RECOMENCACIONES

## 4.1 CONCLUSIONES

- De acuerdo a la investigación realizada el 20% de los despachos de auditoría, autorizados por el Consejo de la Vigilancia de la Profesión de Contaduría Pública y Auditoría, han realizado auditorías a empresas que se dedican al comercio electrónico, auxiliándose para ello de un experto en informática, pues los despachos de auditoría no poseen ni los recursos ni el personal con amplios conocimientos en el área a evaluar.

- Es fundamental que el auditor obtenga un amplio conocimiento de las medidas de seguridad que la empresa implementa para proteger al sitio web, pues es aquí donde se llevan a cabo todas las transacciones virtuales.

- Una de las áreas más importantes a evaluar, por parte del auditor, es la protección e integridad de los datos, tanto generales (nombre, estado civil, sexo, etc.)como privados (No. de tarjetas de crédito, identificación personal, dirección, etc.), los cuales la empresa obtiene de sus clientes en las transacciones virtuales, ya que estos son uno de los recursos más valiosos de las organizaciones.

- Uno de los principales problemas que enfrenta los auditores al momento de realizar la auditoría es la forma de obtener evidencia de las operaciones virtuales, ya que durante el procesamiento de los mismos no hay documentación física que los respalde y los procedimientos realizados por el auditor no satisface completamente el tipo de trabajo a desarrollar.

## 4.2 RECOMENDACIONES

- Los despachos de auditoría beberían capacitar constantemente a su personal en los diferentes tipos de auditoría que están realizando, así como promover la investigación y desarrollo de nuevos procedimientos de auditoría haciendo uso de las herramientas tecnológicas actúales.

- Se recomienda que el auditor al evaluar la protección del sitio web, realice una amplia investigación sobre el tipo de amenazas más comunes que afectan el sitio, las medidas de seguridad (tales como: certificados digitales, firewalls y/o antivirus) y los planes de contingencia que las empresas generalmente adoptan al momento de presentarse una falla en el procesamiento de la información (Servidor auxiliar, planta eléctrica, ups.)

- Es aconsejable que el auditor al realizar la evaluación del área de protección e integridad de los datos, conozca tanto las políticas de seguridad que la empresa utiliza para garantizar la privacidad de los datos de los clientes obtenidos a través del sitio web en las transacciones de comercio electrónico, así como las herramientas de seguridad implementadas en el sitio para realizar las transacciones, al igual que, las políticas de seguridad y acceso de la información una vez se encuentren los datos en poder de la empresa.

- El auditor debería elaborar programas de trabajo enfocados a la evaluación de las transacciones electrónicas, auxiliándose para ello de los recursos informáticos necesarios (software, capturas de pantallas, demo, memorias, CD, etc.), es por ello que en el presente trabajo se proponen programas que ayuden al auditor a obtener evidencia en este tipo de operaciones.

**BIBLIOGRAFIA**

**Libros:**


- **Burgos Daniel, De-León Luz,**

  Comercio Electrónico, Publicidad y Marketing en Internet

  Año 2001.

- **Centro de Comercio Internacional**

  Secretos del Comercio Electrónico: Una guía para pequeños y medianos exportadores.

  El Salvador, 2001.

- **Comité Internacional de Prácticas de Auditoría**

  Normas Internacionales de Auditoría

  Edición 2004.

- **Echenique García, Jose Antonio**

  Auditoría en informática

  Editorial Mc Grall Hill, segunda edición, México, 2004.

- **Muñoz Razo, Carlos**

  Auditoría en Sistemas Computacionales

  Primera edición, México, 2002.

**Revistas:**

- Admisibilidad de la evidencia digital, agosto 2003.

- Buenas prácticas en la administración de la evidencia digital. Facultad de Derecho, Universidad de Los Andes.

- Criptografía para Principiantes, Jesús de Jesús Angel Angel.

- Manual de Supervivencia en Internet, No 16, agosto 2006.

- Pruebas electrónicas y computer forencics, e-newsletter, No 25, Marzo 2007.

- Prueba electrónica, No26, abril 2007.

**Páginas Web y similares:**

- http://www.segu-info.com.ar/tesis/
- http://www.delitosinformaticos.com/bibliografia/
- http://www.portablefreeware.com/
- http://mygnet.com/
- http://www.alfa-redi.org/
- http://www.textoscientificos.com/
- http://www.zonagratuita.com/
- http://www.itlp.edu.mx/publica/tutoriales/
- http://www.devjoker.com/
- http://www.kriptopolis.com/
- http://netacad.uv.es/

- http://www.criptored.upm.es/
- http://www.IN2.es/
- L:\Del Comercio Electrónico y otros Bichos Extraños.htm
- L:\INVESTIGACION\El Salvador en la era del comercio electrónico (e-business) - Monografias_com.htm
- L:\INVESTIGACION\El Salvador en la era del comercio electrónico (e-business) - Monografias_com_archivos

# ANEXOS

**ANEXO 1**

REVISTA DE PRUEBAS ELECTRONICAS.

e-newsletter

CYBEX | Editorial

Marzo | 2007 | nº25 | ÍNDICE | SALIR

JUAN DE LA TORRE
• Grupo Intelligence Bureau

SERGIO AGUD ANDREU
• Cybex

## PRUEBAS ELECTRÓNICAS : UNA NUEVA REALIDAD

La irrupción de las nuevas tecnologías y la evolución de los sistemas de información y de telecomunicaciones han aumentado exponencialmente la creación de documentos digitales en las organizaciones.

La creación, distribución y archivo de estos documentos electrónicos, lejos de remitir, se incrementa día a día. Cada año se envían en todo el mundo más de 2,8 trillones de correos electrónicos y, en la actualidad, más del 90% de los documentos que se crean en la organización son ya electrónicos, de los cuales menos del 30% llegan a imprimirse en papel.

Este nuevo entorno digital está cambiando radicalmente el lugar y las estrategias que abogados e investigadores deben seguir para recuperar y presentar estas pruebas tanto en procesos contenciosos como no contenciosos.

Las pruebas tradicionales están migrando desde el papel hacia un entorno virtual, donde los procesos de gestión y criterios de admisibilidad cambian por completo. Además, la Prueba Electrónica está adquiriendo una mayor importancia en los procesos judiciales, exigiendo a todos los actores del ámbito jurídico estas pruebas en sus estrategias legales.

Desde el momento en que se determina la necesidad de adquirir documentos electrónicos, los consultores de Cybex pueden asesorarle sobre la mejor línea a seguir para salvaguardar y adquirir las pruebas disponibles, así como el tiempo y los costes asociados.

**ANEXO 1**

e-newslette
CYBEX | Prueba electrónica
Marzo | 2007 | nº25 | ÍNDICE | SALI

MIGUEL LOMBARDÍA DEL POZO

- Magistrado de la Audiencia Provincial de Madrid y Profesor Asociado de Derecho Procesal, Facultad de Derecho, UNED.

## COMENTARIO SOBRE LA PRUEBA ELECTRÓNICA EN EL ÁMBITO CIVIL

El objeto del presente artículo es el de un análisis breve y reducido de algunas cuestiones en relación a la prueba electrónica dentro del ámbito civil, en el que, y sin un propósito exhaustivo, se examinen los aspectos más problemáticos en cuanto a la virtualidad de la prueba electrónica dentro de ese proceso, partiendo de su propia generación o nacimiento al derecho, para, sobre todo, destacar y analizar los aspectos relativos a su aportación al proceso, para terminar con la formulación de unas conclusiones que no pretenden ser nada más que eso, simples conclusiones que puedan operar incluso como mera aportación de materiales para una discusión y evaluación más en profundidad.

La principal preocupación del legislador en esta materia viene determinada por la regulación de la generación o del nacimiento al derecho del documento electrónico, y desde esta perspectiva, se promulgan las leyes 34/2002 de 11 de julio, Servicios de la Sociedad de la Información y de Comercio Electrónico; 59/2003 de 19 de diciembre de la Firma Electrónica; y recientemente y en el concreto ámbito del contrato de seguro, la ley 26/2006 de 17 de julio, de Mediación de Seguros y Reaseguros Privados.
Desde este punto de vista normativo se delimita el documento electrónico para su utilización en el tráfico jurídico y evidentemente para la producción de plenos efectos legales, pero no se contienen normas de tipo procesal que delimiten un campo propio y unos efectos específicos, así como, sobre todo, un mecanismo concreto de aportación al proceso y unas garantías de veracidad y en su caso de comprobación.

No contempla la Ley de Enjuiciamiento Civil una específica regulación de la prueba electrónica más allá de la genérica referencia en el art. 299.2 y 3, razón por la cual es opinión general en la doctrina la necesidad de algún modo de su asimilación a la prueba documental tradicional, (arts. 317 y ss.), y así incluso lo viene a prever la propia exposición de motivos de la Ley 1/2000, "no es de excluir, sino que la ley lo prevé, la utilización de nuevos instrumentos probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales", con inclusión para determinados procesos especiales de protección del crédito, (art. 812 LEC), como forma de tipo ordinario de documentación de la deuda

**ANEXO 1**



exigible, pero ello determina una serie de dificultades de interpretación, en primer lugar, cuando el legislador de la Ley de Enjuiciamiento de refiere a la prueba documental está teniendo en cuenta esencialmente el documento escrito y en soporte papel.
De ahí que regule expresamente la institución del cotejo para la adveración de copias y de documentos impugnados, institución de difícil aplicación a la prueba generada electrónicamente desde el momento en que el propio concepto de copia puede carecer de sentido, y en el supuesto concreto de la firma electrónica impide su constatación mediante la prueba pericial caligráfica.

Es evidente que a su vez, y tal y como ocurre con los documentos que podemos llamar ordinarios, el documento electrónico es susceptible de soportar tanto una prueba de naturaleza pericial como el simple reconocimiento judicial con las particularidades que puedan derivarse de su propia configuración.

En cuanto a lo que se refiere a la aportación inicial al proceso, la prueba electrónica deberá cumplir las mismas exigencias que las restantes pruebas, pudiendo ser objeto de su práctica anticipada o de su aseguramiento de concurrir los presupuestos procesales necesarios para ello, (arts. 293 y ss LEC), y siendo obligatoria su aportación inicial en cuanto está previsto en los arts. 264 y ss, en particular en el art. 265 LEC, debiéndose tener muy en cuenta que la posibilidad de simple designación de archivos queda limitada a las circunstancias del art. 265.2 LEC. Deberá aquí valorarse la posibilidad de conversión en documento escrito de la prueba electrónica, en cuyo caso la similitud con la prueba documental sería más clara con independencia de los hipotéticos problemas de ratificación, caso de ser precisa.

La práctica en el proceso

En cuanto a la práctica de la prueba electrónica en el proceso debe ponerse de relieve que el art. 384 LEC, menciona expresamente los supuestos de examen de aquellos medios de prueba que permitan archivar o reproducir palabras, datos o cifras, con los medios que las partes aporten o de los que el tribunal disponga.

Debe tenerse especialmente en cuenta que será precisa la oportuna documentación, ya sea mediante acta o por los sistemas de grabación oportunos del contenido y desarrollo de tales pruebas, para su debida unión a los autos y para su comprobación, caso de la formulación de los recursos procedentes.

Cuestión muy importante y que, sin duda, va a incidir en tales extremos va a ser la de la implantación de la nueva oficina judicial que opta claramente por la completa informatización del proceso. En este punto debe reseñarse la reciente publicación, (BOE de 13 de febrero de 2007), del REAL DECRETO 84/2007, de 26 de enero sobre la implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y

**ANEXO 1**



la realización de actos de comunicación procesal por medios telemáticos.

En cuanto a la valoración de la prueba electrónica, habrá de estarse a la fórmula genérica del art. 384.3 LEC, y a su asimilación a la prueba documental, (arts. 319,326 y 334 LEC).

Por último, el documento electrónico puede ser objeto tanto de reconocimiento judicial como de prueba pericial, ésta última de conformidad con la regla general de los arts. 335 y ss, como la específica del art. 382 LEC, siendo un problema de especial incidencia en todo caso el relativo a la denominada "cadena de custodia" del documento que permita descartar cualquier posibilidad de manipulación.

Conclusiones

1º No existe en nuestra legislación procesal un tratamiento diferenciado de la prueba electrónica más allá de las referencias genéricas puestas de relieve.
2º En función de ello, resulta procedente la asimilación de la prueba electrónica en lo que sea factible-documento electrónico-a la prueba documental que regula la Ley de Enjuiciamiento Civil.
3º En orden a la adveración y confirmación de la prueba electrónica, podrá tener especial importancia la prueba pericial informática.
4º Las exigencias para su incorporación al proceso serán las mismas que las que correspondan a los documentos ordinarios.
5º La valoración de la prueba electrónica se guiará por los mismos parámetros que la prueba documental análoga.
6º Sería deseable como reflexión de *lege ferenda*, una regulación más específica de la prueba electrónica en el ámbito del proceso teniendo en consideración sus especialidades. Tal extremo cobraría una importancia destacada teniendo en cuenta el diseño de la nueva oficina judicial.

BIBLIOGRAFÍA:

LOS CERTIFICADOS ELECTRÓNICOS EN LA LEY 59/2003, Ana I Berrocal Lanzarot, Revista de Derecho UNED, 1/2006.
EFICACIA FORMAL Y PROBATORIA DE LA FIRMA ELECTRÓNICA, Diego Cruz Rivero, ED Marcial Pons, Madrid 2006
LA PERITACIÓN COMO MEDIO DE PRUEBA EN EL PROCESO CIVIL ESPAÑOL, Pedro Mª Garciandía González. Editorial Aranzadi, Pamplona 1999.
LA PRUEBA POR SOPORTES INFORMÁTICOS (UNA PERSPECTIVA CIVIL Y PENAL), Carolina Sanchís Crespo, CGPJ, Madrid 2005
PERICIAL INFORMÁTICA, Antonio López-Silves Martínez, CGPJ, Madrid 2005.
LA PRUEBA ELECTRÓNICA, Juan Carlos Riofrío, Editorial Temis, (Bogotá-Colombia, 2004)

**ANEXO 2**

REVISTA DE MÉTODOS DE DOCUMENTACIÓN ESTRUCTURADA PARA LA GESTION DE INCIDENCIAS DE TECNOLOGÍA E INFORMACIÓN.

e-newsletter
CYBEX | Sobre el Terreno
Abril | 2007 | nº 26 | ÍNDICE | SALIR

SANDRA FRINGS
· Ingeniera informática y coordinadora de proyectos científicos del Instituto de Fraunhofer IAO, Stuttgart (Alemania)

## MÉTODO DE DOCUMENTACIÓN ESTRUCTURADA PARA LA GESTIÓN DE INCIDENCIAS DE TI (I)

La documentación es un tipo de control de calidad que nos ayuda a adquirir una idea general sobre una serie de acciones realizadas, sobre el seguimiento de problemas y errores reduciendo el tiempo que se invierte en un determinado problema recurrente, en el análisis de un fallo de seguridad o trabajando en métodos de prevención y recogida de pruebas relevantes para perseguir delitos. En general, esta documentación escrita cubre, como mínimo, las actividades de investigación llevadas a cabo, a qué hora se han realizado éstas, las personas que han participado en los trabajos, qué métodos se han aplicado, qué tipo de pruebas se han hallado y dónde. Teniendo en cuenta que esta operación está infravalorada porque implica mucho tiempo y carece de procedimientos concretos, dediqué mi tesis doctoral a la definición de un método para elaborar documentación bien estructurada sobre las incidencias de TI. Se trata de un enfoque holístico y orientado a procesos, que se centra en la gestión de la seguridad tecnológica en materia de dichas incidencias y pone el acento en el aspecto de la documentación.

### Introducción y extensión del problema

La buena noticia es que, según las estadísticas de la Oficina de la Policía Federal Criminal alemana (www.bka.de)[1], se percibe un descenso general de los incidentes tecnológicos registrados en Alemania durante 2005. Por ejemplo, en el campo de la piratería de software, la disminución ha sido del 43% y del 48% en cuanto al sabotaje informático. Si nos fijamos en otras categorías de delitos, las informaciones ya no son tan buenas: el número de incidentes relativos a fraudes informáticos creció alrededor de un 11%; el número de sustracciones de datos es un 35% superior a años anteriores y los delitos registrados en relación a la falsificación de pruebas electrónicas llegó a aumentar hasta un 75% en 2005.

Lo que no sabemos con seguridad es si muchas compañías decidieron comenzar a denunciar estos incidentes en 2005 -y no en 2004- pero lo cierto es que se nota la diferencia. Está claro que se dan demasiadas incidencias de TI en general y dos razones fundamentales explican esta situación: primeramente, utilizar soportes informáticos facilita la comisión de delitos; y segundo, dichos sistemas informáticos están actualmente en el punto de mira de la delincuencia al estar presentes en casi cualquier actividad que desempeñamos.

**ANEXO 2**



En realidad, las cifras asociadas a los incidentes no son tan importantes en sí. Los expertos creen que esto sólo es la punta del iceberg y que los números reales (y negros) son mucho más elevados. ¿Por qué? Por un lado, las compañías que ya han detectado un problema serio en sus sistemas de seguridad son reacias a sacar a la luz el tema. Por otro lado, las incidencias en el campo de la seguridad informática tampoco están consideradas como "actividades perjudiciales".

Aunque estos casos se suelen juzgar de manera correcta, por regla general, no existen procedimientos estandarizados que nos preparen para saber actuar ante estas situaciones. ¿Y por qué no hay procedimientos? Porque, por lo general, la llamada seguridad TI no se gestiona de manera "apropiada", es decir, de acuerdo con los requisitos de seguridad establecidos por la organización. Y conocer con exactitud cuáles son dichos requisitos exige realizar primeramente una auditoría de seguridad o un análisis de riesgos dentro de una compañía.

A pesar de todo lo expuesto antes, y aunque el ámbito de la gestión de la seguridad ha ganado protagonismo de forma bastante rápida en los últimos años, muchas organizaciones siguen sin querer invertir un presupuesto decente en asuntos de prevención, detección y gestión de incidencias de TI.

Pongamos el ejemplo del llamado *IT Baseline Protection Manual* (www.bsi.org)[2] publicado en Alemania, que contiene estándares de seguridad y recomendaciones a implementar. Existen muchos libros de este tipo en el mercado[3]. Pero la gestión de incidencias de TI pertenece al capítulo reactivo de la seguridad tecnológica. Esto significa que la incidencia ya se ha producido y ha de ser sometida a una investigación para averiguar si podría ser consecuencia de una mera acción fortuita de un usuario, o si es consecuencia de la acción de un delincuente en realidad. Mi opinión es que la gestión de las incidencias comienza con ciertas acciones de preparación frente a lo que pueda ocurrir y termina cuando la incidencia ya ha sido archivada.

Independientemente de cuál ha sido la causa de un incidente, examinarlo revelará de alguna manera la poca conciencia (o la falta de cualificación) de los usuarios, o bien evidenciará aquellos fallos del sistema que no han sido tratados, así como cualquier maldad intencionada. La complejidad de una indagación puede ir de echar un simple vistazo al archivo *log* y hacer las preguntas pertinentes a un usuario, a tener que llevar a cabo un análisis detallado del suceso, muy probablemente respaldado (e incluso emprendido) por las fuerzas legales.

Todo el mundo sabe - por las series de televisión - que en una investigación criminal el investigador escribe minuciosamente cada pieza o elemento en su cuaderno de notas para poder así reconstruir

**ANEXO 2**



el delito, conservar la cadena de pruebas y dar con el culpable al final. El mismo razonamiento es aplicable a aquellas investigaciones sobre incidencias informáticas. Si nos detenemos, por ejemplo, en el antes citado *IT Baseline Protection Manual*, vemos que la necesidad de una buena documentación se halla presente en todas y cada una de las secciones del libro. Este manual alemán se refiere a dos tipos diferentes de documentación: documentación relativa a todos los procesos de gestión de seguridad TI (decisiones a adoptar, infraestructuras, análisis de riesgos, etc.) y aquel tipo de documentación que se refiere a la investigación de una incidencia en sí. Ambos aspectos han de estar debidamente documentados.

La documentación es un tipo de control de calidad que nos ayuda a adquirir una idea general sobre una serie de acciones realizadas, sobre el seguimiento de problemas y errores reduciendo el tiempo que se invierte en un determinado problema recurrente, en el análisis de un fallo de seguridad o trabajando en métodos de prevención y recogida de pruebas relevantes para perseguir delitos, como comentaba al principio del artículo. La documentación en este soporte tiene diversos destinatarios, por ejemplo, los administradores de sistemas ven en la documentación una determinada finalidad, los gestores de TI en una organización ven otra finalidad, y los jueces ven otro fin distinto.

Para que la documentación escrita sea de valor para el usuario o lector-destinatario, tiene que cumplir diversos requisitos generales. Tiene que ser, por lo menos:

- Clara y comprensible (adecuada a la persona que la vaya a leer)
- Significativa y razonable (según la persona que la vaya a leer)
- Completa
- Estructurada (de acuerdo con la secuencia de los pasos descritos, por ejemplo)

Estos simples requisitos no parecen imposibles de alcanzar, a menos que en una organización nadie se moleste en solicitar esta documentación, o que realmente no exista conciencia sobre la importancia y ventajas que esto tiene.

Sin embargo, ¿qué pasaría en caso de que la investigación de un incidente resultase ser poco clara o incomprensible, insignificante o poco razonable, incompleta o mal estructurada? En estos casos, se llegaría a la situación en la que el destinatario final no utilizaría tal documentación porque no vería la utilidad de la misma. Y si el autor de la documentación tuviera que ponerse a elaborarla de nuevo otro día, seguramente no se lo tomaría tan en serio, excepto si él mismo se ha propuesto mejorar todo el procedimiento de documentación, si le han dado apoyo para hacerlo, o si directamente han delegado esta tarea en él.

**ANEXO 2**



Si echamos un vistazo a las pautas para documentar las incidencias de seguridad de los procesos TI, el libro *Baseline Protection Manual* (S2.201) menciona que la documentación debería constar de los siguientes puntos, como mínimo:

- Política de seguridad de la información
- Programas de activos de TI (incluyendo los planes de conectividad, etc.)
- Conceptos sobre seguridad TI
- Planes para la implementación de medidas de seguridad TI
- Procedimientos para el uso apropiado y seguro de instalaciones tecnológicas
- Documentación de revistas (listas de control, notas procedentes de entrevistas etc.)
- Actas de las reuniones y decisiones realizadas por el equipo responsable de la seguridad TI.
- Informes sobre la gestión de la seguridad TI
- Planes de seguridad TI
- Informes sobre incidencias de seguridad relevantes

En el este mismo manual alemán (S6.64), se incluye una pauta de documentación en caso de incidencia que viene a decir lo siguiente:

Toda acción realizada al abordar un problema relativo a la seguridad, debe estar documentada con todo lujo de detalles para:

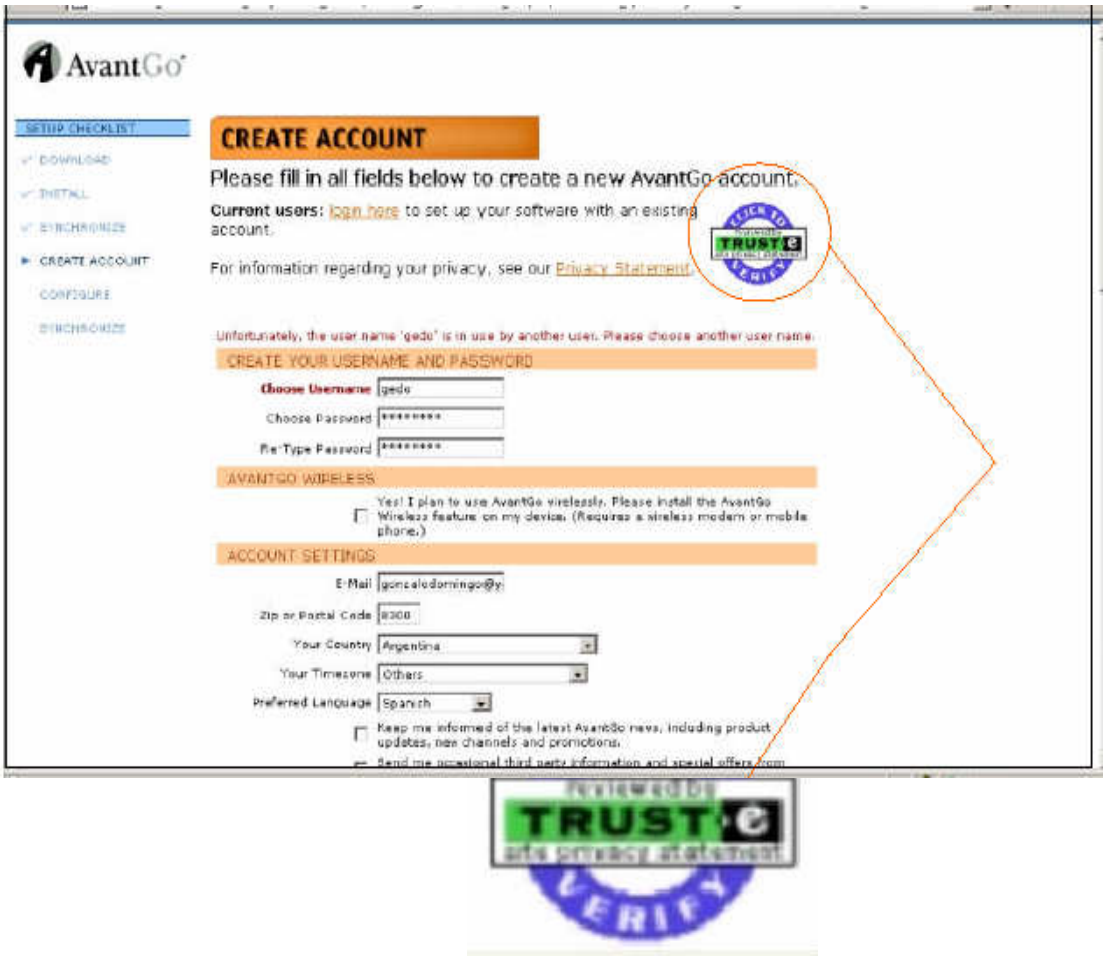
- Retener los detalles de lo sucedido
- Posibilitar que se pueda volver sobre el problema
- Poder rectificar cualquier incidente/fallo que resultara de una implementación de contramedidas precipitada
- Poder resolver problemas ya conocidos de forma más ágil y evitar que vuelvan a producirse
- Poder eliminar las debilidades relativas a la seguridad y diseñar medidas preventivas
- Recoger pruebas si se va a emprender un juicio

Toda esta documentación no sólo incluye una descripción de las acciones ejecutadas; también da buena cuenta de la hora en que fueron realizadas y de los *logs* de los sistemas informáticos afectados.

Pero estas pautas expuestas no son del todo suficientes para guiar las acciones de una organización. Por esta razón, cada organización que pretenda producir documentación de este tipo, se atendrá a los consejos ofrecidos en el manual alemán de acuerdo con el grado de conocimientos que tengan sus expertos. Esto supone mucho trabajo y no todas las compañías y organizaciones pueden permitirse este esfuerzo económico.

**ANEXO 3**

CERTIFICACION. ESTE SITIO ESTA CERTIFICADO POR E-TRUST Y LO PROMOCIONA.



**ANEXO 4**

DESCRIPCION EXTENSA DE UN CERTIFICADO DIGITAL

VeriSign™
The Sign of Trust on the Net®

**HBSRV.BOSTONACCESS.COM.AR es un Sitio Seguro CertiSur**

CertiSur

La **Seguridad** sigue siendo una de los principales preocupaciones para los consumidores on-line. El **Programa de Sitio Seguro de CertiSur** le permite a Ud. obtener más información sobre los sitios seguros que visita antes de enviarles información que considere confidencial. Por favor, verifique que la información que aparece en esta página coincide con la información del sitio que Ud. está visitando.

| | |
|---|---|
| Nombre | HBSRV.BOSTONACCESS.COM.AR |
| Estado | **Valido** |
| Periodo de Validez | 10-JAN-02 - 10-JAN-03 |
| Información de la Empresa | Country = AR<br>State = Buenos Aires<br>Locality = Capital Federal<br>Organization = BankBoston National Association<br>Organizational Unit = Sistemas<br>Organizational Unit = Terms of use at www.certisur.com/rpa (c) 00<br>Organizational Unit = Authenticated by CertiSur S.A.<br>Organizational Unit = Member, VeriSign Trust Network<br>Common Name = hbsrv.bostonaccess.com.ar |

Si la información es correcta, Ud puede enviar información sensible, (ej. número de tarjeta de crédito) con la seguridad que:

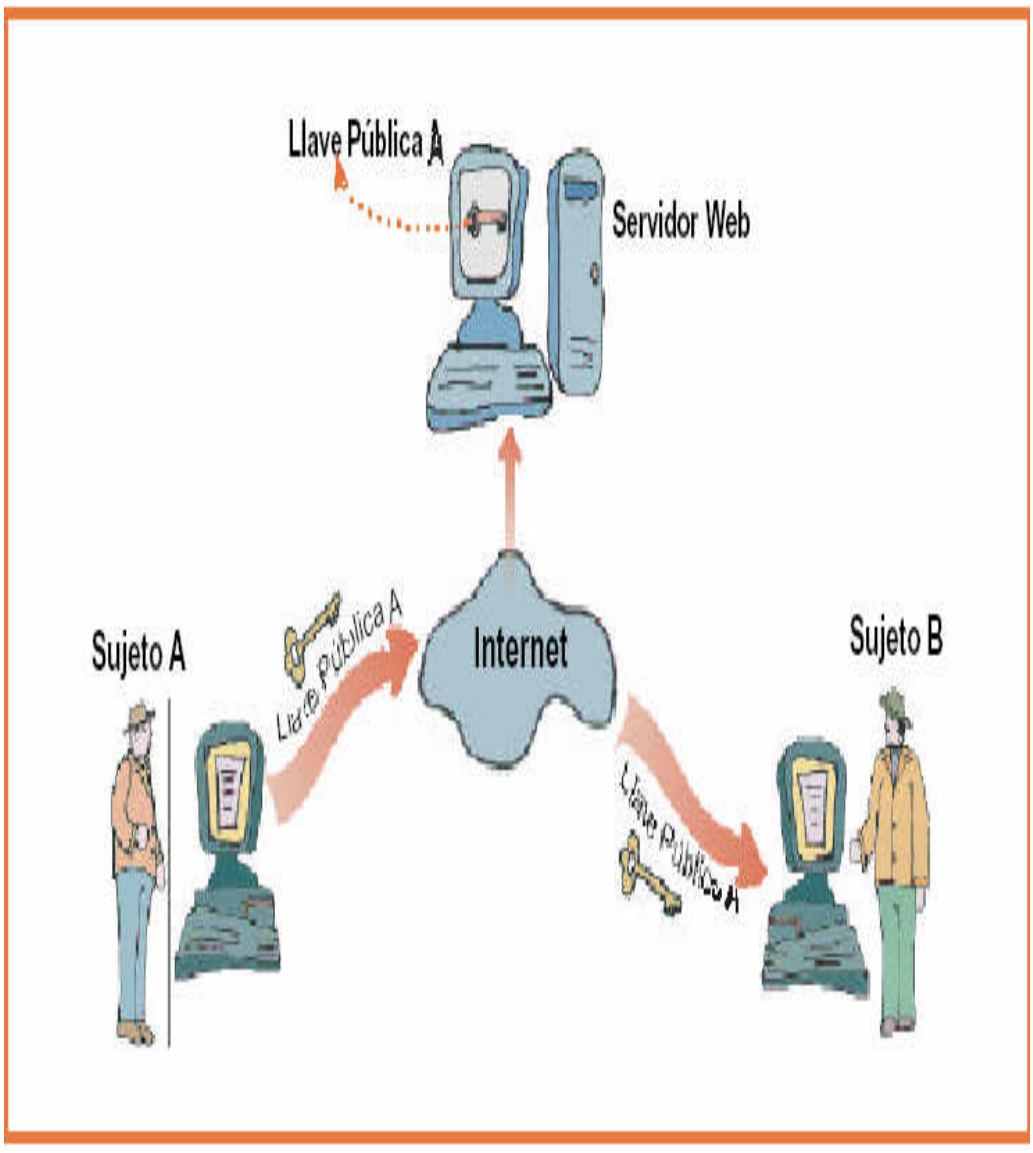
- Este sitio tiene un Server ID emitido por CertiSur S.A.
- CertiSur S.A. ha verificado el nombre de la Organización y que BANKBOSTON NATIONAL ASSOCIATION ha entregado documentación que demuestra el derecho a su uso.
- El sitio legítimamente opera bajo el auspicio de BANKBOSTON NATIONAL ASSOCIATION.
- Toda la información enviada a este sitio, si se encuentra bajo una conexión SSL, será encriptada, protegiendo su divulgación hacia terceras partes.

Para asegurar que este es un **Sitio Seguro CertiSur** legítimo, debe verificar:

1. El URL del sitio que Ud está visitando viene de HBSRV.BOSTONACCESS.COM.AR
2. El URL de esta página es https://digitalid.certisur.com/.
3. El Estado del Server ID es Válido.

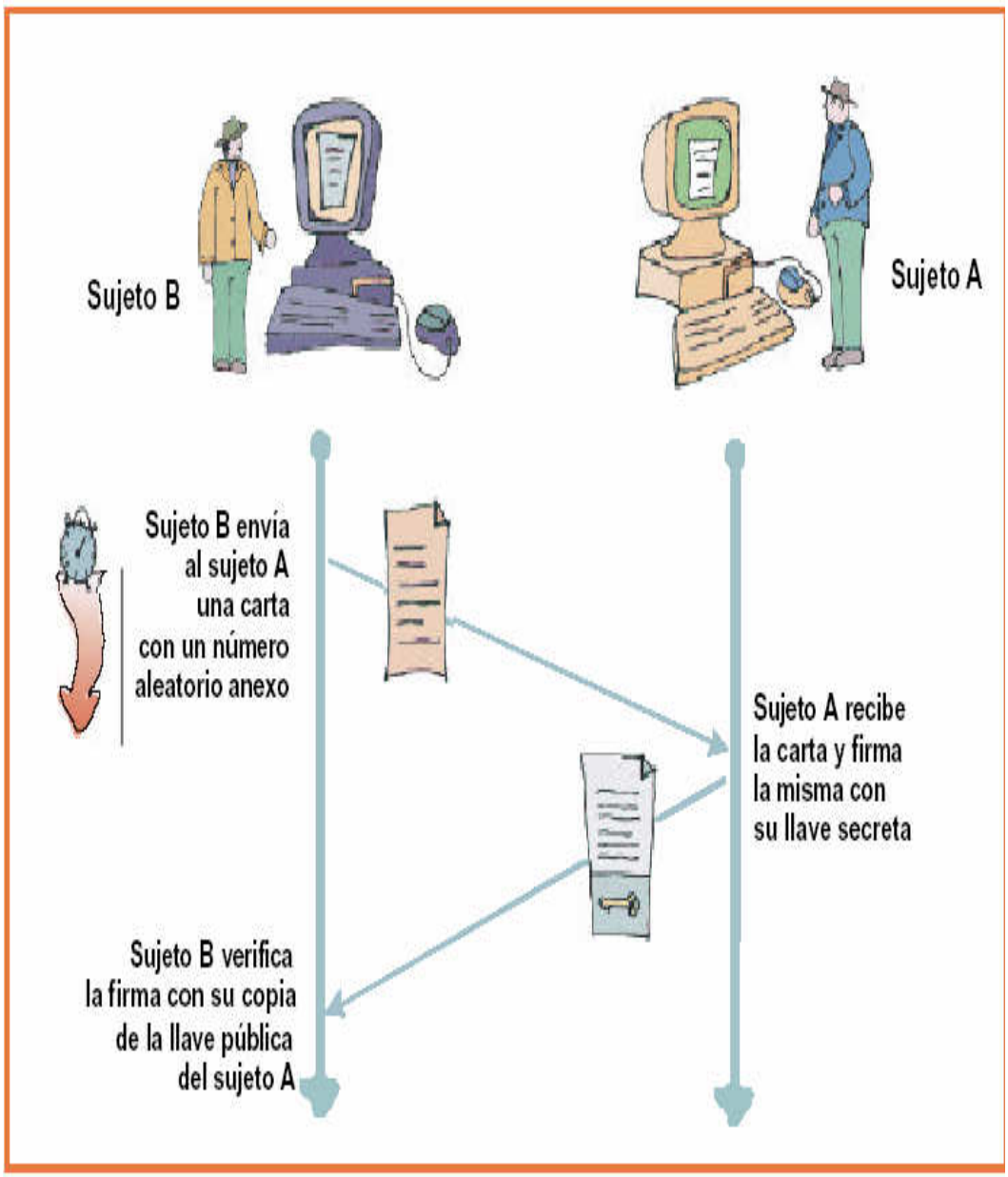
**ANEXO 5**

PROCESO DE DISTRIBUCIÓN DE UNA LLAVE PÚBLICA.



**ANEXO 6**

ESQUEMA DEL USO DE LA FIRMA DIGITAL PARA CONFIRMAR LA IDENTIDAD.

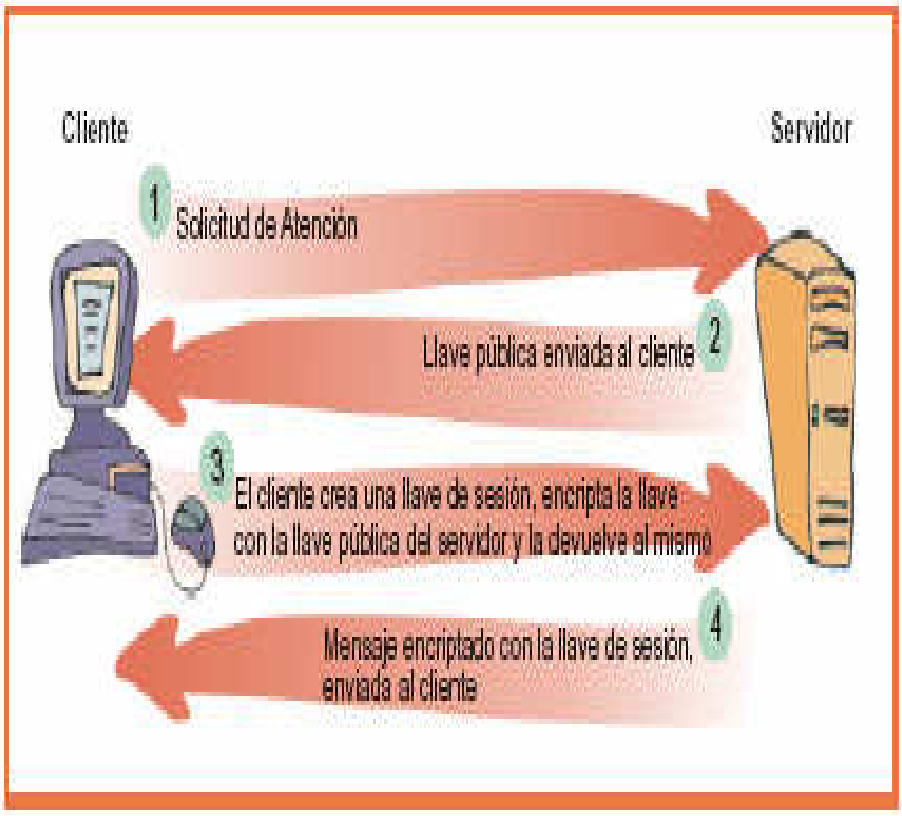


**ANEXO 7**

PANTALLA EN LA QUE SE MUESTRA EL ICONO INDICADOR DE QUE LA PÁGINA USA UN PROTOCOLO DE ENCRIPTACION PARA TRASFERENCIA DE DATOS.

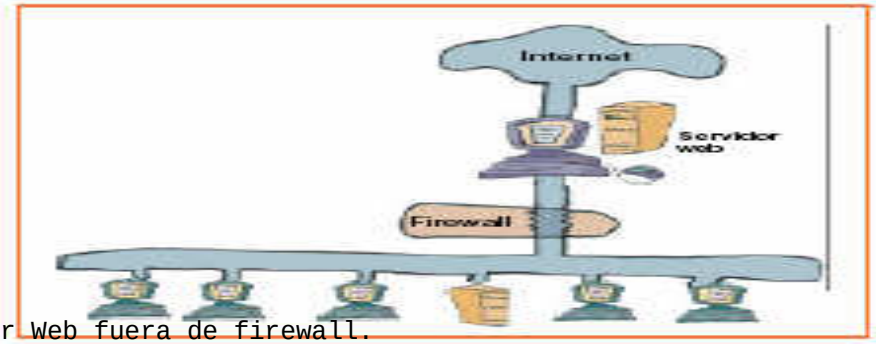
**ANEXO 8**

PROCESO DE INTERCAMBIO DE MENSAJES CLIENTE-SERVIDOR EN EL PROTOCOLO SSL.

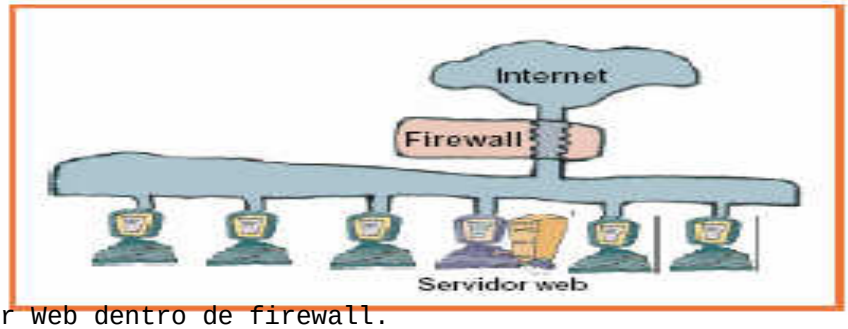


**ANEXO 9**

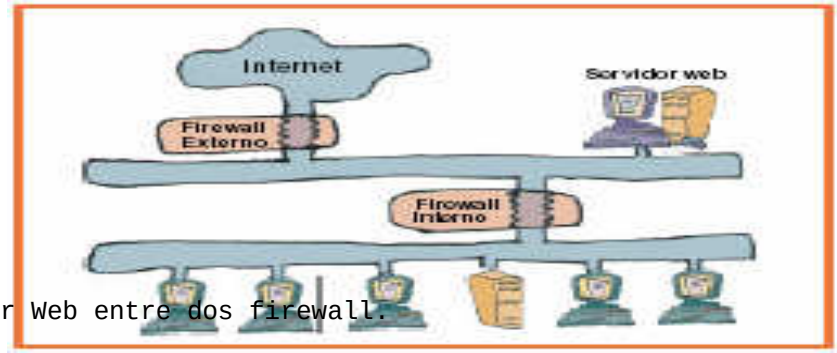
ESQUEMA DE UTILIZACION DE FIREWALL.




Servidor Web fuera de firewall.




Servidor Web dentro de firewall.




Servidor Web entre dos firewall.

## ANEXO 10

**LISTADO DE DESPACHOS CONTABLES Y DE AUDITORIA CONSTITUIDOS COMO SOCIEDADES COLECTIVAS DE CAPITAL FIJO QUE HAN ACTUALIZADO INFORMACION DEL REGISTRO, SEGÚN ARTICLO 7 DE LA LEY REGULADORA DEL EJERCICIO DE LA CONTADURÍA PÚBLICA.**

**(ACTUALIZADO HASTA FEBRERO 2007)**

1. AGUIRRE, LOPEZ Y ASOCIADOS
2. ALAS HERNANDEZ Y ASOCIADOS
3. AREVALO PINTO Y COMPAÑÍA
4. AREVALO, ALLEN Y ASOCIADOS
5. BENJAMIN WILFRIDO NAVARRETE Y CIA
6. BLANCO URQUIA Y ASOCIADOS
7. CALLES RICO Y ASOCIADOS
8. CARLOS ALVERTO MEJIA VALLE Y ASOCIADOS
9. CARRANZA Y CARRANZA Y ASOCIADOS
10. .CASTELLANOS GOMEZ Y ASOCIADOS
11. CASTILLO BARRIENTOS Y ASOCIADOS
12. CERRITOS CERRITOS Y COMPAÑIA
13. CHICAS ALFARO Y ASOCIADOS
14. CHICAS VILCHEZ Y COMPAÑÍA
15. CHILE MONROY ARTEAGA Y ASOCIADOS
16. CRUZ CHAVEZ & COMPAÑÍA
17. DAMAS COCAR Y COMPAÑÍA

18. DAVID LOPEZ GRANADINO Y ASOCIADOS
19. DIAZ MARTINEZ Y ASOCIADOS
20. ESQUIVEL Y ASOCIADOS
21. FERNANDEZ GUZMAN Y ASOCIADOS
22. FERNANDEZ Y FERNANDEZ ASOCIADOS
23. FIGUEROA JIMENEZ Y ASOCIADOS
24. FLORES ALAS ASOCIADOS
25. FREDY S. CHICAS Y COMPAÑÍA
26. GOMEZ SANCHES Y COMPAÑÍA
27. GUEVARA, CHICAS, PALACIOS Y ASOCIADOS
28. HERNANDEZ MARTINEZ Y ASOCIADOS
29. JEREZ GONZALEZ Y ASOCIADOS
30. J.H. VALIENTE Y ASOCIADOS
31. JULIO CESAR GARCIA LAZO Y CIA
32. LIRA PASASIN Y COMPAÑÍA
33. L.F. JOVEL Y COMPAÑÍA
34. LOPEZ GUERRERO Y ASOCIADOS
35. LOPEZ, SOLITO Y ASOCIADOS
36. LUIS ABEL CIUDAD REAL Y ASOCIADOS
37. LUIS ALONSO CORNEJO Y ASOCIADOS
38. MARTINEZ-GARCIA Y ASOCIADOS
39. MAURICIO J. ORELLANA MIXCO Y ASOCIADOS
40. MAYORGA ORTIZ Y COMPAÑIA

41. MEJIA HERNANDEZ Y COMPAÑÍA

42. MEJIA, AGUIRRE Y ASOCIADOS
43. MENA RODRIGUEZ Y ASOCIADOS
44. MORALES Y MORALES ASOCIADOS
45. ORELLANA MIXCO Y ASOCIADOS
46. ORELLANA UMANZOR Y ASOCIADOS
47. ORTEGA, CISNEROS, DOMINGUEZ Y CIA
48. OSCAR MORALES Y ASOCIADOS
49. PEREZ PORTILLO Y ASOCIADOS
50. QUIJANO MORAN Y COMPAÑÍA
51. QUIJANO TOCHEZ Y ASOCIADOS
52. R. GALLARDO Y COMPAÑÍA
53. RAMOS ALVARADO Y ASOCIADOS
54. RIVAS NUÑES Y ASOCIADOS
55. RIVERA PALMA ASOCIADOS
56. RIVERA, ZACAPA, GONZALEZ Y COMPAÑÍA
57. ROMERO MEZA Y COMPAÑÍA
58. SOL, ELIAS Y ASOCIADOS
59. SORIANO PERAZA Y COMPAÑÍA
60. VASQUEZ RETANA Y ASOCIADOS
61. ZELAYA RIVAS, ASOCIDOS Y COMPAÑIA

**ANEXO 11**

**LISTADO DE EMPRESAS QUE REALIZAN COMERCIO ELECTRÓNICO EN EL SALVADOR.**

| EMPRESA | PÁGINA WEB |
|---|---|
| ❖ ALMACENES SIMAN S.A. DE C.V. | www.siman.com |
| ❖ ARTE LATINO DE EL SALVADOR | www.artelatino.com.sv |
| ❖ CLUB COMPRA FÁCIL | www.clubcomprafacil.com |
| ❖ LA CURACAO | www.lacuracaonet.com |
| ❖ MERCADITOS | www.mercaditos.com |
| ❖ NEGOCIOS EL SALVADOR | www.negocioselsalvador.com |
| ❖ OFERTON | www.oferton.com.sv |
| ❖ PARA EL HOGAR | www.paraelhogar.com |

| EMPRESA | PAGINA WEB |
|---|---|

- PULGOTIENDA.COM www.pulgotienda.com
- RAF www.raf.com.sv
- TVOFFER www.grupotvoffer.com
- UPS S.A. DE C.V. www.regalosups.com
- FARMACIA SAN NICOLAS www.farmacialasamericas.com.sv
- FLORISTERIA BELLA FLOR www.floristeriabellaflor.com
- FLORISTERIA CELIFLOR www.floristeriaceliflor.com
- LIBRERIAS FEPADE www.fepade.com/libros
- VENDALO HOY www.vendalohoy.com

## ANEXO 12

**UNIVERSIDAD DE EL SALVADOR**

**FACULTAD DE CIENCIAS ECONOMICAS**

**ESCUELA DE CONTADURIA PÚBLICA**

Encuesta dirigida a firmas de auditoría autorizadas por el consejo de vigilancia de la profesión de contaduría pública y auditoría.

La información que se obtendrá en esta encuesta, es de carácter confidencial y de utilidad para la realización del trabajo de investigación titulado: "Programas de trabajo para la obtención de evidencia sobre las operaciones virtuales". Caso. Auditoría realizada a empresas salvadoreñas que se dedican al comercio electrónico. Para optar al grado de Licenciado en Contaduría Pública de la Facultad de Ciencias Económicas de la universidad de El Salvador.

**OBJETIVO:** Obtener información para el desarrollo de la investigación con el propósito de brindar una herramienta a aquellas personas que realizan auditorías a empresas dedicadas al comercio electrónico en el país.

**INDICACIONES:** marque con una X la(s) respuesta(s) que usted considere más conveniente o complementar según el caso.

1. ¿Realizan auditorías a empresas que se dedican al comercio electrónico?

   SI ____ NO____

2. ¿Ha realizado auditorías en las cuales ha evaluado el sitio web de la empresa?
SI ____ NO____

3. ¿Ha evaluado el área de informática en esas empresas?
SI_____ NO____

4. Si su respuesta a la pregunta número uno, fue negativa cuales han sido los motivos por los que no ha realizado este tipo de auditorías?

No ha sido requerido ese tipo de servicios _____
Falta de personal capacitado _____
Falta de herramientas tecnológica _____
Otros _____

Especifique_____
_____
_____

5. Si su respuesta fue afirmativa a la pregunta número dos ¿qué áreas han sido evaluadas en ese tipo de auditorías?

Seguridad física _____
Seguridad Lógica _____
Otros _____
Especifique
_____

6. ¿Por quienes han sido realizadas ese tipo de auditorías?

Personal Interno con conocimientos de informática _____

Personal Externo con conocimientos de Informática _____
Personal Interno con ayuda de un experto en
Informática _____
Personal Externo con ayuda de un experto
en informática _____
Otros _____

Explique_____

7. ¿Qué áreas cree que sería convenientes evaluar en este tipo de auditorías?
_____
_____
_____

8. ¿Poseen procedimientos escritos específicos para realizar ese tipo de auditorías?
SI_____ NO____

9. ¿Cree usted que es necesario disponer de programas que permitan realizar este tipo de auditorías?
SI_____ NO____

10. A su criterio ¿cuál debería ser el contenido de los programas de auditoría?
_____
_____
_____

11. ¿Cuáles cree que son los principales problemas que se presentan al momento de obtener evidencia para sustentar los hallazgos?
_____
_____
_____
_____

12. ¿Que tipo de evidencia utilizan para documentar los hallazgos que sustentan en estas auditorías?
_____
_____
_____

**GRACIAS POR SU VALIOSA COLABORACIÓN.**

# ANEXO 13

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

Encuesta dirigida al personal encargado del área de informática de las empresas que realizan comercio electrónico en El Salvador.

La información que se obtendrá en esta encuesta, es de carácter confidencial y de utilidad para la realización del trabajo de investigación titulado: "Programas de trabajo para la obtención de evidencia sobre las operaciones virtuales". Caso. Auditoria realizada a empresas salvadoreñas que se dedican al comercio electrónico. Para optar al grado de Licenciado en Contaduría Pública de la Facultad de Ciencias Económicas de la universidad de El Salvador.

**OBJETIVO:** Obtener información para el desarrollo de la investigación con el propósito de brindar una herramienta a aquellas personas que realizan auditorías a empresas dedicadas al comercio electrónico en el país.

**INDICACIONES:** marque con una X la(s) respuesta(s) que usted considere más conveniente o complementar según el caso.

**Agradecemos de antemano su valiosa colaboración.**

DESARROLLO Y MANTENIMIENTO DEL SITIO WEB

1)¿El sitio web que actualmente se utiliza por quien fue desarrollado?

a) Personal de la empresa _____
b) Empresas dedicadas al desarrollo de páginas web _____
c) Otros _____

Explique _____

2) Si su respuesta es b), ¿Cuales fueron los requisitos para la contratación de la empresa dedicada al desarrollo de páginas web?

a) Se solicitó experiencia previa. _____

b) Se solicitó referencias de trabajos realizados anteriormente. _____

c) Se solicitó la credencial de la empresa para realizar estos trabajos _____

d) otros _____

Explique _____

_____

3) ¿Cada cuanto tiempo se le da mantenimiento al sitio web?

a) cada mes _____

b) cada 3 meses _____

c) cada 6 meses _____

d) cada año _____

e) nunca _____

4) ¿Quién realiza el mantenimiento al sitio web?

a) Personal de la empresa _____

b) Empresas dedicadas al desarrollo de páginas web _____

c) Otros _____

Explique _____

5) Si el personal de la empresa realiza el mantenimiento al sitio web ¿Poseen procedimientos escritos establecidos para realizarlo?

SI _____

NO _____

Explique cuales son los principales procedimientos _____

6) ¿Se realizaron pruebas para llevar a cabo la implantación de el sitio web?

SI _____

NO _____

Explique cuales fueron las principales pruebas realizadas _____

_____

_____

7) ¿Qué documentación acompaña al sitio web una vez entregado a la empresa?

a) Manual de usuario _____
b) Diccionario de corrección de fallas _____
c) Otros _____

Explique_____

8) ¿Existe documentación sobre los errores o fallas que se han dado en el sitio web y la forma en que fueron corregidos?

SI _____
NO _____
Explique en que consiste la documentación _____
_____

9) ¿Fueron implementados en la fase de diseño del sitio procedimientos que proporcionen pistas de auditoria para recolectar evidencia de las transacciones realizadas en el sitio web?

SI _____
NO _____
Explique los principales procedimientos _____
_____

SEGURIDAD FISICA Y MANEJO DE LA INFORMACION POR EL PERSONAL DE LA EMPRESA

10) ¿Qué medidas de seguridad se poseen en el centro de cómputo para combatir situaciones de desastre?

a) Extintores de fuego _____
b) Alarmas contra incendios _____
c) Alarmas contra robo _____
d) Censores de humo _____
e) Vigilancia _____
f) Otros _____

Explique_____

11) ¿Cómo se realiza el acceso al centro de cómputo?

a) Por medio de una identificación personal _____
b) Por tarjeta magnética _____
c) Claves verbales _____
d) Otros _____

Explique _____

12) ¿Además del personal de informática, existen otras personas que tienen acceso al centro de cómputo?

SI _____
NO _____

Especifique el cargo_____

13) ¿Poseen un lugar diferente al centro de cómputo para resguardar la información que se procesa en el sitio web?

SI _____
NO _____

Describa el lugar _____

14) ¿Existen políticas sobre confidencialidad en el manejo de la información de los clientes?

SI _____
NO _____

Explique las principales políticas _____
_____

15) ¿Quiénes tienen acceso a obtener información de los equipos de cómputo clasificada como confidencial?

a) El personal de informática _____
b) Gerentes _____
c) Auditor interno _____
d) Personal de mantenimiento del equipo de cómputo _____
e) Otros _____

Explique _____

16) ¿Si una persona realiza cambios a la información almacenada puede hacerlo sin dejar rastro alguno?

SI _____

NO _____

SABE _____

17) ¿Existe algún programa que utilice a la empresa que genere una bitácora de las operaciones que realizan los usuarios del sistema?

SI _____

NO _____

Si la respuesta fue afirmativa, ¿Qué tipo de información le detalla el programa anterior?

a) Nombre del usuario que acceso _____
b) Hora de acceso y tiempo de permanencia _____
c) Información que revisó _____
d) Cambios realizados a la información _____
e) Realizo copias o backup de la información _____
f) Cambios al sistema _____
g) Otros _____

Explique _____

18) ¿Puede ser modificado el detalle de la información que genera el programa que menciona la pregunta anterior?

SI _____

NO _____

SEGURIDAD DEL SITIO WEB PARA REALIZAR COMERCIO ELECTRONICO

19) ¿Posee políticas para garantizar la privacidad de los datos de los clientes obtenidos a través del sitio web en las transacciones de comercio electrónico?

SI _____

NO _____

20) ¿Cuáles son las políticas de seguridad empleadas por el sitio web para garantizar la privacidad de los datos de sus clientes?

a) Evitar compartir con otras empresas los datos de un usuario sin la autorización explicita del mismo. _____
b) Siempre que se envié un mensaje de correo electrónico a los usuarios explicarles como se obtuvo su dirección y como puede hacer para darse de alta a la lista de distribución si así lo desea. _____
c) Restringir el acceso a las bitácoras. _____
d) Evitar el proporcionar información personal de los usuarios. _____
e) Establecer políticas de privacidad con los empleados _____
f) Otros. _____

Explique _____

21) Si utiliza la técnica de identificación de firma digital ¿Cuáles de lo siguientes medios físicos usa para soportar la tecnología de la llave digital?

a) Llave encriptada almacenada _____
b) Llave encriptada en medio removible. _____
c) Llave encriptada en un dispositivo inteligente _____
d) Otros _____

Explique_____

22) ¿Utiliza la Criptografía como herramienta de seguridad de su sitio web al realizar transacciones electrónicas?

SI _____
NO _____
Porque_____

23) ¿Cuál es el algoritmo de encriptación que utiliza para su sitio web en las transacciones de comercio electrónico?

a) Algoritmos de llaves simétricas. _____
b) Algoritmos de clave publica _____
c) Criptosistemas híbridos publico / privado. _____
d) Funciones de compendio de mensaje. _____
e) Otros _____

24) ¿La información manejada por el sitio web permanece encriptada en todo momento o únicamente cuando viaja a través de la red?

Siempre _____

Solo cuando viaja _____

Nunca _____

25) ¿Cuál es la información de los clientes que es encriptada?

a) Datos generales _____

(Nombre, estado civil, dirección electrónica, sexo, etc.)

b) Datos privados _____

(Numero de tarjeta de crédito, identificación personal, dirección, etc.)

26) ¿Poseen un plan de contingencias ante un incidente de seguridad del sitio web y cada cuanto tiempo es actualizado?

SI _____

NO _____

Explique en que consiste _____

_____

_____

27) ¿Considera necesario la implementación de programas de trabajo para la realización de auditorias a empresas que realizan comercio electrónico en el país?

SI _____

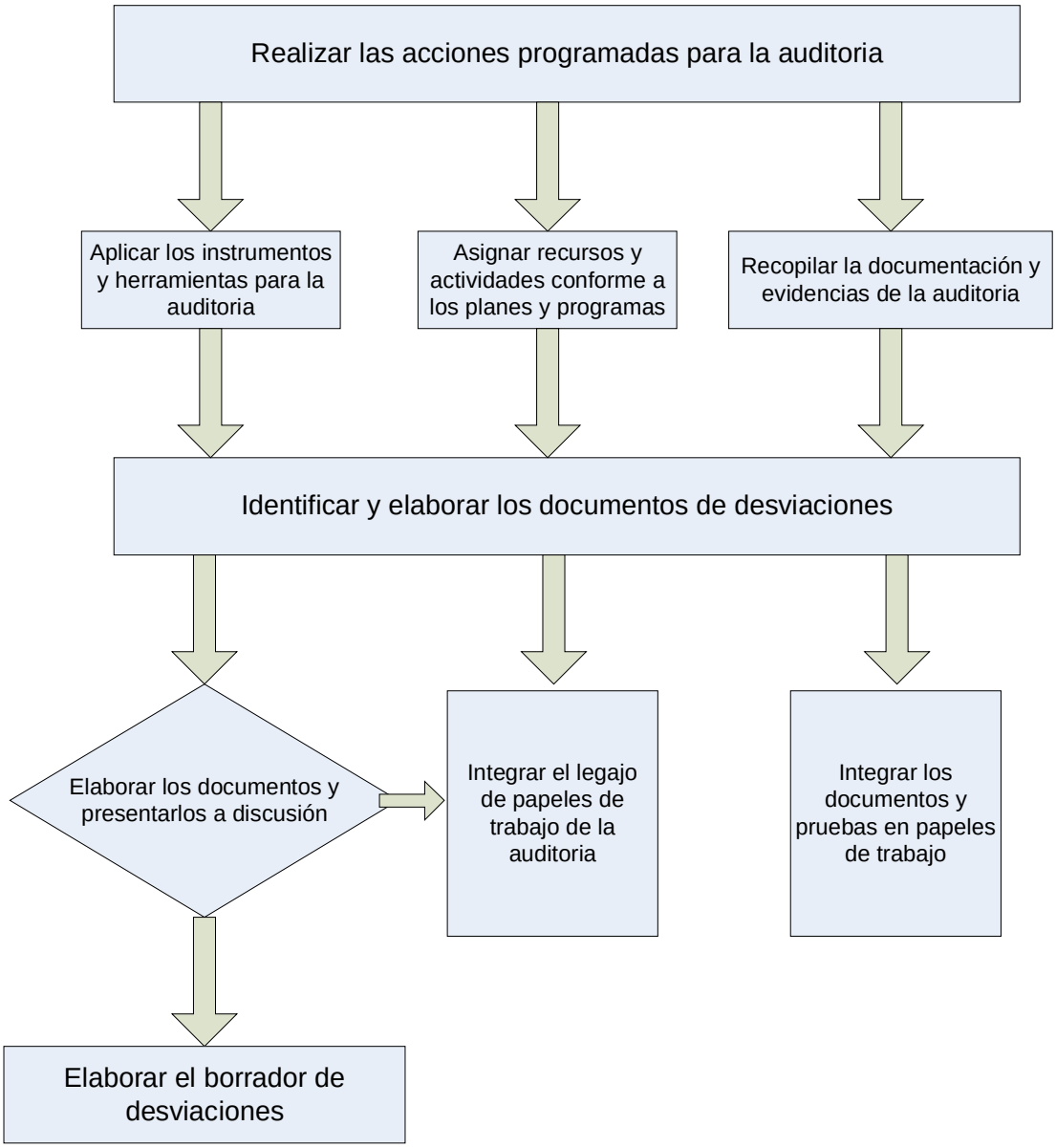
NO _____

Explique _____

**GRACIAS POR SU COLABORACION**

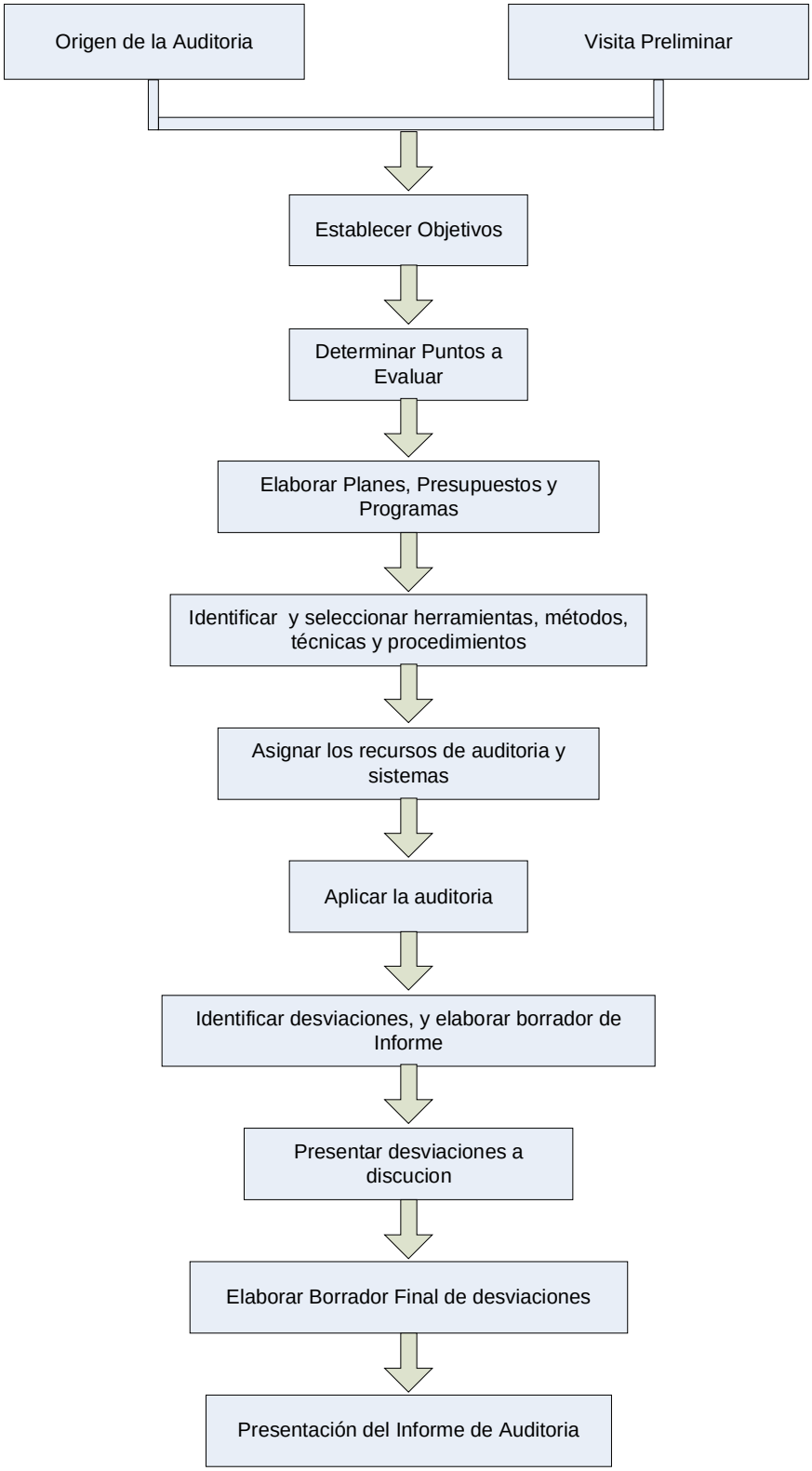
## ANEXO 14

PRINCIPALES PUNTOS EN LA AUDITORIA DE SISTEMAS



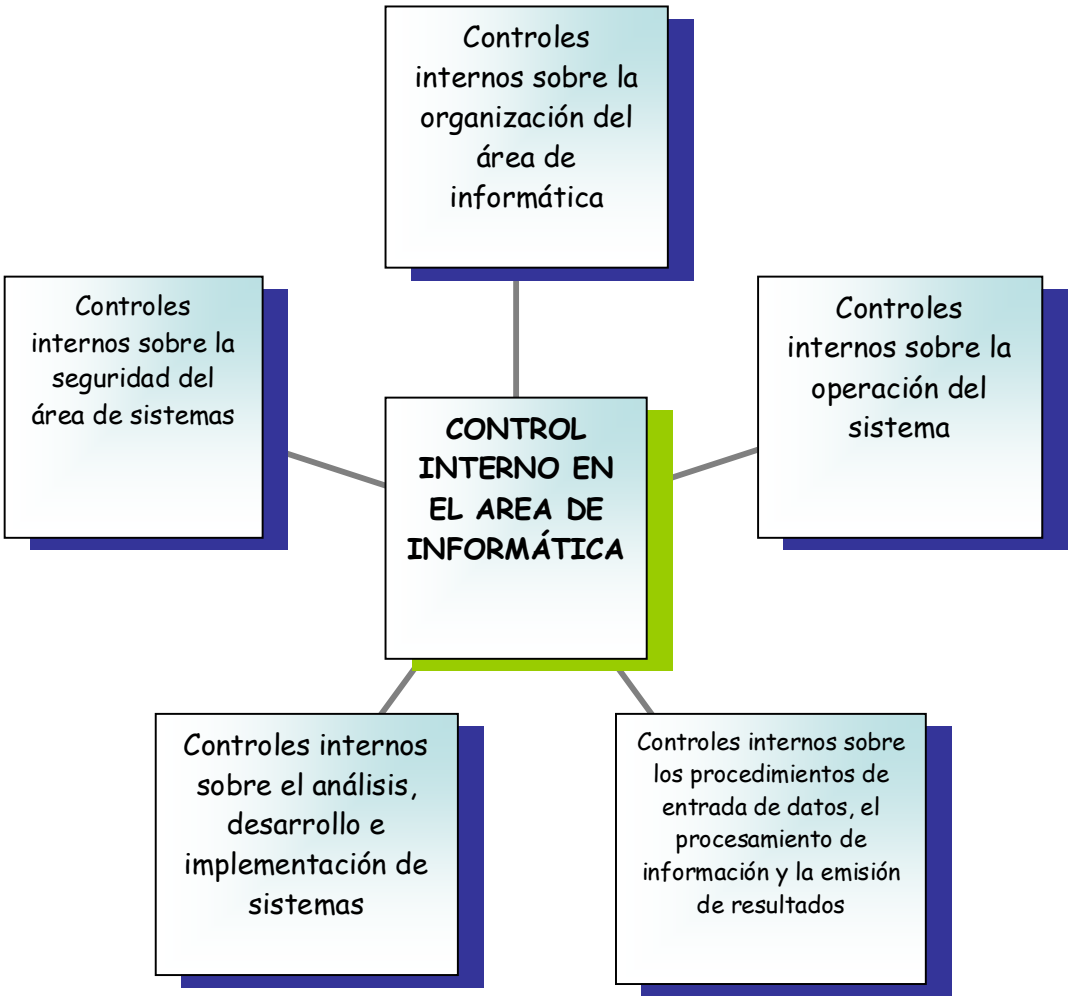
**ANEXO 15**

METODOLOGIA PARA DESARROLLAR UNA AUDITORIAS DE SISTEMAS COMPUTACIONALES



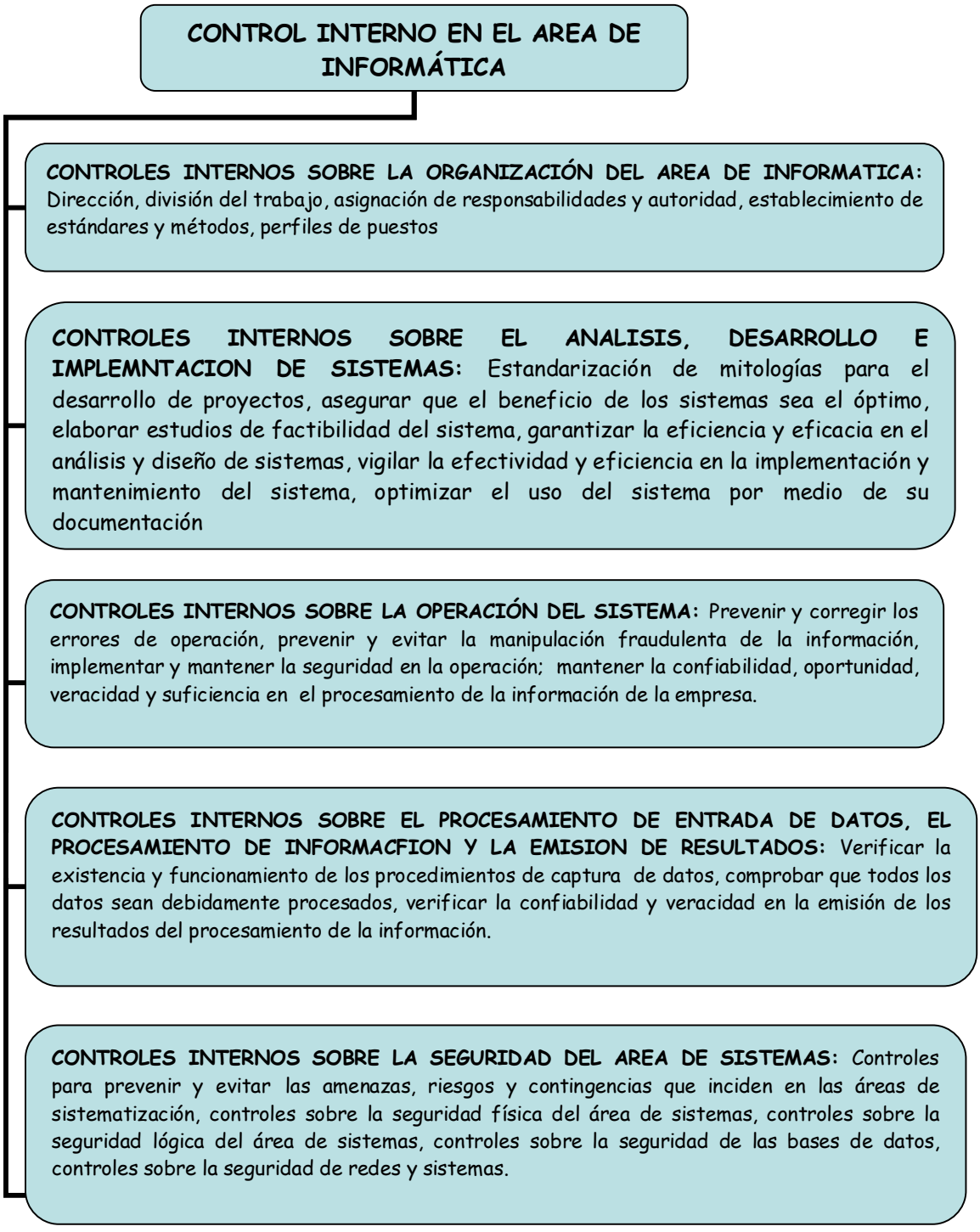
**ANEXO 16**

ESQUEMA DE CONTROL INTERNO EN EL AREA DE INFORMATICA



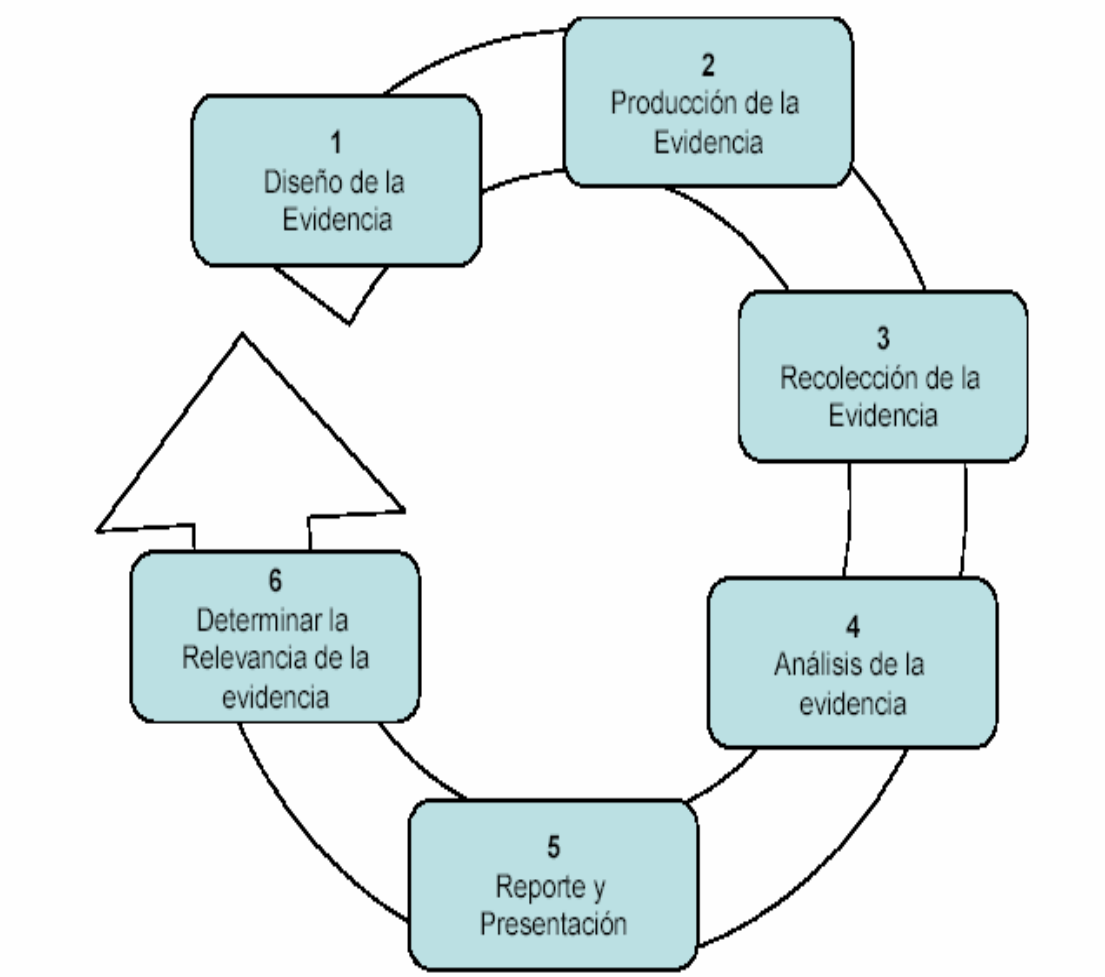
## ANEXO 16-A

CUADRO DE CONTROL INTERNO EN EL AREA DE INFORMÁTICA



**ANEXO 17**

CICLO DE VIDA DE LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL



## ANEXO 18

PROCEDIMIENTOS PARA ELABORAR EL INFORME DE AUDITORIA