UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"TÉCNICAS Y PROCEDIMIENTOS DE AUDITORÍA PARA OBTENER EVIDENCIAS VIRTUALES EN EMPRESAS QUE REALIZAN COMERCIO ELECTRÓNICO EN EL SALVADOR"

TRABAJO DE INVESTIGACION PRESENTADO POR:

CALDERÓN ORELLANA, MAYRA JEANNETTE

DELGADO RAMÍREZ, JUAN CARLOS

RIVAS HERNÁNDEZ, NELSON ORLANDO

PARA OPTAR AL GRADO DE
LICENCIADO(A) EN CONTADURÍA PUBLICA

ENERO DE 2005

SAN SALVADOR EL SALVADOR CENTROAMERICA

AGRADECIMIENTOS

Agradezco primeramente a Dios todo poderoso y a nuestra Madre la Siempre y Santísima Virgen Maria, a mis Padres: Israel Delgado Cruz, que desde el Cielo ha estado y estará intercediendo por mi; y Fidelina Ramírez, por su amor incondicional y su dedicación. Agradezco también a mi Familia y demás personas que de alguna u otra forma me ayudaron a dar este primer paso.

JUAN CARLOS DELGADO RAMÍREZ

Agradezco primeramente a Dios todo poderoso, a mis Padres: José Ramón Calderón y Yolanda Orellana, que son la fuente de mi inspiración, por su amor, su comprensión, su ayuda y su apoyo para con mi persona. Agradezco también a mi Familia y demás personas que de alguna u otra forma me ayudaron a culminar mis estudios.

MAYRA JEANNETTE CALDERÓN ORELLANA

Agradezco primeramente a Dios todo poderoso, a mis Padres: por su amor, su comprensión, su ayuda y su apoyo para con mi persona. Agradezco también a mi Familia y demás personas que de alguna u otra forma me ayudaron a culminar mis estudios.

NELSON ORLANDO RIVAS HERNÁNDEZ

AUTORIDADES UNIVERSITARIAS

Rector (a) : **Dr. Maria Isabel Rodríguez**

Secretario (a) General : Licda. Margarita Muñoz Vela

Facultad de Ciencias Económicas:

Decano : Lic. Emilio Recinos fuentes

Secretario (a) : Licda. Vilma Yolanda de Del Cid

Docente Director : Lic. Juan Vicente Alvarado

Coordinador de Seminario : Lic. Álvaro Calero

Docente Observador : Lic. Héctor Alfredo Rivas Núñez

Enero de 2005

San Salvador El Salvador Centro América

ÍNDICE

ANEXOS

CAPITULO III

3.1. DIAGRAMA DEL PROCESO DE VENTA: TIENDA VIRTUAL SENTIDO ESTRICTO

3.2. DIAGRAMA DEL PROCESO DE VENTA: TIENDA VIRTUAL EN SENTIDO AMPLIO

3.3. CORRIDA DE PROGRAMA DE FACTORES TÉCNICOS FUNDAMENTALES

3.4. INSTRUMENTOS DE EVALUACIÓN EN UNA AUDITORIA DE SEGURIDAD PARA EL COMERCIO ELECTRÓNICO

- 3.4.1. GUÍA DE EVALUACIÓN PARA EL CONOCIMIENTO DEL NEGOCIO
- 3.4.2. CUESTIONARIO DE CONTROL INTERNO
- 3.4.3. LISTA DE VERIFICACIÓN

RESUMEN EJECUTIVO

La informática, es aplicada a la mayoría de apartados de las ciencias (Medicina, ingeniería, climatología, etc.); las ciencias económicas no es la excepción, dentro de ésta, se encuentra el área sobre la cual se fundamenta el interés de la investigación, a saber: la forma de *obtención y documentación de evidencias virtuales* al realizar procedimientos de auditoría en empresas que se dedican al comercio electrónico.

Debido a esta nueva forma de comercializar, surge la inquietud en cuanto a cómo documentar y sustentar esta evidencia, por tanto el objetivo de este trabajo de investigación es proponer una guía objetiva que proporcione técnicas y procedimientos para realizar una auditoria de seguridad en empresas dedicadas al comercio electrónico con el fin de obtener evidencias virtuales, entendidas estas como evidencias que están vinculadas con operaciones de comercio electrónico y no por el hecho de su materialidad.

Para obtener la información que sustentó este trabajo se realizó una investigación Bibliografica y de campo, utilizando las técnicas de entrevistas, encuesta, observación, y para ellas se aplicaron guías de observación, cuestionarios y narrativas de las mismas.

Se definió que la estructura de las empresas dedicadas al comercio electrónico pueden ser de dos formas: Tienda virtuales y Canal virtual.

En base al estudio realizado se concluye que las áreas de seguridad a cubrir son: logística de operaciones, en red, en información de clientes y en lógica y física, estos aspectos son esenciales en una auditoria a un E-commerce, puesto que de ella depende en gran medida la confianza, que los clientes o potenciales consumidores, puedan depositar en la organización.

Es necesario tener en cuenta que el factor significativo tanto para el comercio como para el auditor es la confianza que el publico pueda depositar en la empresa y en la firma de auditoria, máxime en los países en vías de desarrollo como El Salvador, donde los consumidores aun no están familiarizados con este prototipo de negocios, a consecuencia, obviamente, de los atrasos tecnológicos y educacionales de la población. Por tanto los auditores y las firmas de auditoria, deben jugar un papel preponderante, en cuanto al avance y al auge que tiene y pueda tener el E-commerce en el país, siendo estos, los proveedores y garantes de este factor significativo al cual se le a denominado confianza, que asegura las expectativas de los consumidores ante este modelo de negocio del futuro, que comienza a forjarse en este presente al cual no somos ajenos.

Por lo tanto se recomienda que para enfrentarse a estos nuevos desafíos, se requiere que el auditor esté altamente calificado para realizar su trabajo de proveer confianza al publico, así se ha querido dar una herramienta útil, producto de una investigación cuidadosa, que contienen los puntos básico y esenciales de una auditoria de seguridad para este arquetipo de negocios, con lo cual no se pretende acabar el tema en cuestión. En consecuencia, se sugiere que se tomen en cuenta las herramientas proporcionadas en este trabajo al realizar una auditoria de esta naturaleza.

INTRODUCCIÓN

La Tecnología en El Salvador, es una herramienta que está incursionando cada día más en el mercado, surgiendo una nueva figura denominada Comercio Electrónico. Hoy en día los auditores se enfrentan a nuevos retos, de allí la necesidad de proveer al auditor de técnicas y procedimientos para la obtención de Evidencias en un Auditoría de este tipo, debiendo conocer aspectos desde lo general a lo específico; razón por la cual se presenta la siguiente estructura de Investigación:

En el Capítulo I, se exponen los aspectos esenciales que comprende una Auditoría en General, desde sus orígenes, conceptos adoptados, Las Fases que comprende, La Normativa Técnica aplicada en El Salvador, así como el papel importante que desempeñan las Medidas de Control Interno adoptadas por las empresas. Además se describen aspectos específicos de una Auditoría en Sistemas de Información, tales como Evidencias de Auditoría, Seguridad y Medios de Pago en El Comercio Electrónico, los cuales deben ser del conocimiento de los Auditores para poder ejecutar una Auditoría de este tipo.

El Capitulo II, comprende la metodología utilizada en la investigación, así como el diagnóstico resultante de la misma, el cual fue desarrollado destacando cinco áreas importantes,

tales como: Conocimiento del Negocio, Logística de Operaciones, Seguridad en Red, Seguridad y Confidencialidad con la Información almacenada de los Clientes y Seguridad Física y Lógica Interna.

En El Capitulo III se proponen Técnicas y Procedimientos de Auditoría para la Obtención de Evidencias Virtuales, las cuáles son idóneas de acuerdo a la Estructura de e- commerce que posea la empresa que se esté auditando, para ello se describe cada una de las áreas importantes, planteándose además un cuestionario para cada una de ellas, el cuál será necesario para que el auditor posea una primera aproximación al conocimiento del área, y finalmente se listan las técnicas y procedimientos que deberá ejecutar para determinar las áreas de Riesgo que posee la empresa.

En el Capítulo IV se exponen las conclusiones y recomendaciones producto del análisis e interpretación de datos de la Investigación realizada, de acuerdo a las estructuras de e-commerce que existen en El Salvador.

CAPITULO I: MARCO TEÓRICO

1.1 LA AUDITORÍA

1.1.1 ANTECEDENTES

Se posee evidencia, de que algún tipo de auditoría se practicó en tiempos remotos. El hecho de que los nobles, ricos y familias pudientes exigieran el mantenimiento y revisión de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrolló el comercio, surgió la necesidad de que existiera confiabilidad de los datos y registros financieros de las empresas, sobre todo en empresas comerciales y fue de esta manera como se contrataron revisores que verificaban las cuentas de los empresarios.

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 desde este año hasta 1905, la profesión de la auditoria creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900 debido a que ésta era necesaria, sobre todo para las empresas que cotizaban en bolsa de valores para ese entonces. En 1912; en los que podría llamarse, los días en los que se formó la auditoría, Montgomery dijo que los objetivos primordiales de la auditoría eran: La detección y prevención de fraude y la detección y prevención de errores; sin embargo, en los años siguientes hubo un cambio decisivo en la demanda y el servicio, y los propósitos actuales son: El cerciorarse de la condición

financiera actual y de las ganancias de una empresa. Paralelamente al crecimiento de la auditoría independiente en los Estados Unidos, se desarrollaba la auditoría interna y del Gobierno, lo que entró a formar parte del campo de la auditoría.

A medida que los auditores independientes se apercibieron de la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoría independiente, se mostraron partidarios del crecimiento de los departamentos de auditoría dentro de las organizaciones de los clientes, lo cual era una forma novedosa de la práctica de auditoría, que se encargaría del desarrollo y mantenimiento de buenos procedimientos del control interno, independientemente del departamento de contabilidad general. Actualmente, los departamentos de auditoría interna son revisiones de todas las fases de las corporaciones, de las que las operaciones financieras forman parte.

1.1.2. CONCEPTO

A lo largo de su historia, se concibió que auditoria es: “la actividad que se encarga de señalar faltas y errores en los registros contables y financieros de las empresas”. Pero con el pasar del tiempo y el desarrollo de la técnica, el concepto del vocablo *Auditoria* se ha venido modificando.

En la actualidad este concepto denota “la actividad de evaluar la eficiencia y eficacia con que se está operando, para que, por

medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien, mejorar la forma de actuación".

1.1.3. TIPOS

La auditoria, como se definió anteriormente, es un examen; pero este, para que sea efectivo, debe realizar análisis según las necesidades que las empresas presenten, de tal manera que es asi como surgen los diversos tipos de auditoria, estas varían según el enfoque de los autores, pero en general se pueden enunciar los siguientes enfoques:

1.1.3.1. Según el Lugar de Aplicación[1]

1.1.3.1.1 Auditoría Externa

Es la revisión independiente, que realiza un profesional de la auditoría, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de las actividades, operaciones y funciones que se realizan en la empresa que lo contrata, asi como de la razonabilidad en la emisión de sus resultados financieros.

1.1.3.1.2. Auditoría Interna

Es la revisión que realiza un profesional de la auditoría, cuya relación de trabajo es directa y subordinada a la institución donde se aplicará la misma, con el propósito de evaluar de forma

[1] Muñoz Razo, Carlos. Auditoria en sistemas computacionales. Editorial Prentice Hall. México, 2002.

interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, asi como evaluar la razonabilidad en la emisión de sus resultados financieros, cuyo objetivo es contar con un dictamen interno sobre las actividades de toda la empresa, que permita diagnosticar la actuación administrativa, operacional y funcional de empleados y funcionarios de las áreas que se auditan.

1.1.3.2. Según su Área de Aplicación

1.1.3.2.1. Auditoría Financiera

Es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la razonabilidad y veracidad de las cifras consignadas en los estados financieros obtenidos durante un período especifico, este proceso solo es posible llevarlo a cabo a través de un elemento llamado evidencia de auditoría, ya que el auditor hace su trabajo posterior a las operaciones de la empresa.

1.1.3.2.2. Auditoría Administrativa

Es el examen metódico y ordenado de los objetivos de una empresa, de su estructura orgánica y de la utilización del elemento humano, a fin de informar los hechos investigados. Su importancia radica en el hecho de que proporciona a los directivos de una organización un panorama sobre la forma como esta siendo administrada por los diferentes niveles jerárquicos y operativos, señalando aciertos y desviaciones de aquellas

áreas cuyos problemas administrativos detectados exigen una mayor o pronta atención.

1.1.3.2.3. Auditoría Operacional

Es el examen posterior, profesional, objetivo y sistemático de la totalidad o parte de las operaciones o actividades de una entidad, proyecto, programa, inversión o contrato en particular, sus unidades integrantes u operacionales específicas.

Su propósito es determinar los grados de efectividad, economía y eficiencia alcanzados por la organización y formular recomendaciones para mejorar las operaciones evaluadas.

1.1.3.2.4. Auditoría Integral:

Tiene por objeto el examen de la gestión de una empresa con el propósito de evaluar la eficacia de sus resultados con respecto a las metas previstas, los recursos humanos, financieros y técnicos utilizados, la organización y coordinación de dichos recursos y los controles establecidos sobre dicha gestión.

1.1.3.2.5. Auditoría de cumplimiento:

Es la comprobación o examen de operaciones financieras, administrativas, económicas y de otra índole de una entidad para establecer que se han realizado conforme a las normas legales, reglamentarias, estatuarias y de procedimientos que le son aplicables.

1.1.3.2.6 Auditoria Fiscal:

Es la revisión exhaustiva que se realiza a los registros y operaciones contables de una empresa, siguiendo la normativa

técnica y tributaria aplicable, con el propósito de dar una opinión sobre la razonabilidad de las cifras que componen los estados financieros, en relación al cumplimiento de las obligaciones tributarias, así como garantizar que las cifras de los estados financieros y declaraciones tributarias estén respaldadas según la norma tributaria aplicable.

1.1.3.2.7. Auditoría Ambiental:

Es la evaluación que se hace de la calidad del aire, la atmósfera, el ambiente, las aguas, ríos, lagos y océanos, asi como de la conservación de la flora y la fauna silvestre, con el fin de dictaminar sobre las medidas preventivas y, en su caso, correctivas que disminuyan y eviten la contaminación provocada por los individuos, las empresas, los automotores y las maquinarias, y asi preservar la naturaleza y mejorar la calidad de vida de la sociedad.

1.1.3.2.8. Auditoría de Sistemas de Información:

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, asi como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado

de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas informáticos de la empresa.

1.1.4. OBJETIVOS

Los objetivos generales de la auditoria, sin importar su tipo, son:

- Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.
- Hacer una revisión especializada, desde un punto de vista profesional y autónomo, del aspecto contable, financiero y operacional de las áreas de una empresa.
- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de los empleados y funcionarios de una institución, asi como evaluar las actividades que se desarrollan en sus áreas y unidades administrativas.
- Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, asi como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones.

1.1.5. NORMATIVA TÉCNICA

La profesión de auditoria se rige, al menos en el aspecto contable y financiero, por normas y criterios aceptados generalmente, los cuales son emitidos por asociaciones de profesionales quienes aportan experiencia, conocimientos y actualizaciones en esta materia, a fin de que los practicantes de esta profesión y similares conozcan estas normas y las cumplan en el desarrollo de algún tipo de auditoria, según la profesión que practiquen. En la actualidad existen muchas asociaciones de profesionales dedicados a la contabilidad financiera, debido a esto, en casi todos los países existe alguna asociación o colegio de contadores, los cuales tienen entre sus principales funciones regular la actuación profesional de sus agremiados, esto es, crear normativa técnica apropiada a las necesidades nacionales.

1.1.5.1. Normas de Auditoria Generalmente Aceptadas

Todo tipo de norma profesional se establece con el objetivo de evaluar la calidad y desempeño de los individuos y organizaciones, por lo tanto, el auditor no esta exento de tal situación y debe regirse por normas, la más genérica de ellas son las *Normas de Auditoría Generalmente Aceptadas* (NAGAS), en los cuales deben enmarcar su trabajo durante el proceso de la auditoría misma. El cumplimiento de estas normas garantiza la calidad del trabajo profesional del auditor. Estas normas por su carácter general se aplican a todo el proceso del examen y se

relacionan básicamente con la conducta funcional del auditor como persona humana y regula los requisitos y aptitudes que debe reunir para actuar como tal.

1.5.1.1. Definición

Normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y la información que rinde como resultado de este trabajo.

1.1.5.1.2. Clasificación de las NAGAs

a) Normas Personales.

- Entrenamiento y capacidad profesional.
- Independencia.
- Diligencia y Cuidado Profesional.

b) Normas de Ejecución del Trabajo.

- Planeación y supervisión.
- Estudio y evaluación del control interno.
- Evidencia suficiente y competente.

c) Normas de Información.

- Aplicación de los principios de contabilidad generalmente aceptados.
- Consistencia.
- Revelación suficiente.
- Opinión del auditor.

1.1.5.2. Normas Internacionales de Auditoria (NIAs)

Las Normas de Auditoria son determinadas por cada país, y dado el crecimiento de los mercados, ha surgido la necesidad de armonizar el ejercicio de la profesión para lo cual es necesario establecer normas de auditoría comunes.

La Federación Internacional de Contadores (IFAC) es una organización a nivel mundial, establecida para ayudar a fomentar una profesión de contaduría coordinada mundialmente con normas armonizadas, por otra parte, El Comité de Prácticas de Auditoría Internacionales como parte de IFAC, publica las Normas Internacionales de Auditoría, las cuales proporcionan una guía procesal y de presentación de informes para los auditores.

En Nuestro país estas son las Normas que el Auditor utiliza para ejercer su trabajo, las cuales han sido adoptadas como Normas de Auditoria Generalmente Aceptadas, para el desarrollo de una auditoria financiera.

1.1.6. CONTROL INTERNO

1.1.6.1. Definición

Es un instrumento de gestión que comprende el plan de la empresa, conjuntos y procedimientos adoptados para salvaguardar su patrimonio, verificar la exactitud y veracidad de su información financiera y administrativa, promover la eficiencia en las operaciones, estimular las políticas y comprender el cumplimiento de las metas y objetivos programados. Algunas de

sus herramientas son los organigramas, manuales de funciones, manuales o normas de procedimientos internos, matriz de autorizaciones, etc.

El control interno no tiene el mismo significado para todas las personas, lo cual causa bastante confusión entre las personas que deben generar los mecanismos que ayuden a que este sea más efectivo, en consecuencia se originan problemas de comunicación y varias alternativas para cumplir con las expectativas que se ha propuesto la empresa.

1.1.6.2. Objetivos

Los objetivos del control interno son los siguientes:

- Establecer la seguridad y protección de los activos de la empresa.
- Promover la confiabilidad, oportunidad y veracidad de los registros contables, asi como de la emisión de la información financiera de la empresa.
- Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.
- Establecer y hacer cumplir las normas, políticas y procedimiento que regulan las actividades de la empresa.
- Implantar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa.

1.1.6.3. Importancia

Independientemente del tipo de empresa que se trate, estas deben contar con instrumentos adecuados de control que les permitan llevar su administración con eficiencia y eficacia. Por esta razón es importante contar con un control interno en la empresa, para satisfacer sus expectativas en cuanto a la salvaguarda y custodia de sus bienes, confiabilidad, oportunidad y veracidad de sus registros contables y emisión de información financiera, a la implantación correcta de los métodos, técnicas y procedimientos que le permitan desarrollar adecuadamente sus actividades.

El establecimiento de un sistema de control interno facilita a las autoridades de la empresa la evaluación y supervisión y, en su caso, la corrección de los planes, presupuestos y programas que determinaran el rumbo a seguir en la empresa.

1.1.6.4. Componentes

1.1.6.4.1. Entorno de control

El entorno de control marca la pauta del funcionamiento de una empresa e influye en la concientización de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la empresa, la filosofía de dirección y el estilo de gestión, la manera en que la dirección asigna autoridad y responsabilidades, organiza y

desarrolla profesionalmente a sus empleados y la atención y orientación que proporciona en consejo de administración.

1.1.6.4.2. Evaluación de los riesgos

Cada empresa se enfrenta a diversos riesgos externos e internos que tienen que ser evaluados. Una condición previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

1.1.6.4.3. Actividades de control

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la empresa. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la empresa. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones. Incluyen una gama de actividades tan diversa como aprobaciones, autorizaciones,

verificaciones, conciliaciones, revisiones de rentabilidad operativa, salvaguarda de activos y segregación de funciones.

1.1.6.4.4. Información y comunicación

Hay que identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada. Dichos sistemas no sólo manejan datos generados internamente, sino también información sobre acontecimientos internos, actividades y condiciones relevantes para la toma de decisiones de gestión así como para la presentación de información a terceros. También debe haber una comunicación eficaz en un sentido más amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa. El mensaje por parte de la alta dirección a todo el personal ha de ser claro: las responsabilidades del control han de tomarse en serio. Los empleados tienen que comprender cual es el papel en el sistema de control interno y como las actividades individuales están relacionadas con el trabajo de los demás. Por otra parte, han de tener medios para comunicar la información significativa a los niveles superiores. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas.

1.1.6.4.5. Supervisión

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados.

Estos componentes, vinculados entre sí, generan una sinergia y forman un sistema integrado que responde de una manera dinámica a las circunstancias cambiantes del entorno. El sistema de control interno está entrelazado con las actividades operativas de la entidad y existe por razones empresariales fundamentales. El sistema de control interno es más efectivo cuando los controles se incorporan en la infraestructura de la sociedad y forman parte de la esencia de la empresa. Mediante los controles

incorporados, se fomenta la calidad y la iniciativa de la delegación de poderes, se evitan gastos innecesarios y se permite una respuesta rápida ante las circunstancias cambiantes.

1.1.7. FASES DE LA AUDITORIA

Con el propósito de interpretar adecuadamente la aplicación de las fases que comprenden una auditoría, las cuales pueden ser aplicables para cualquier tipo y en base a las Normas Internacionales. A continuación se presentan en forma genérica todas aquellas fases que se deben considerar para la realización de una auditoría, a saber:

1.1.7.1. Planeación

Según NIA[2] 300, la planeación ayuda a asegurar que se presta atención a áreas importantes, identificación de problemas potenciales y que el trabajo sea presentado en forma expedita.

El grado de planeación variará en base al tamaño de la entidad, complejidad de la auditoria y experiencia del auditor con la entidad y conocimiento del negocio.

1.1.7.1.1. Etapas de la Planeación

- *Conocimiento del negocio.*

Factores económicos generales, Características Importantes de la entidad y Nivel general de competencia de la administración.

- *Comprensión de los sistemas de contabilidad y control interno.*

[2] Normas Internacionales de Auditoria

Las políticas contables adoptadas y cambios en ellas, efecto de pronunciamientos nuevos de contabilidad y auditoria y conocimiento acumulable del auditor sobre los sistemas de contabilidad y control interno.

- *Riesgo e Importancia Relativa.*

Evaluación de riesgos y áreas, establecimiento de niveles de Importancia Relativa, posibles representaciones erróneas y fraudes, identificación de áreas contables complejas

- *Naturaleza, tiempos y alcances de procedimientos.*

Efecto de la Tecnología de Información sobre auditoría, Trabajo de auditoría interna y su esperado efecto sobre los procedimientos de auditoría externa.

- *Coordinación dirección, supervisión y revisión.*

El Involucramiento de otros auditores y expertos, número de locaciones y requerimientos de personal.

- *Otros asuntos.*

La posibilidad de que el supuesto de negocio en marcha pueda ser cuestionado, existencia de partes relacionadas, los términos de trabajo, naturaleza y oportunidad de los informes u otra comunicación de la entidad que se espera bajo términos del trabajo.

1.1.7.2. Ejecución

En esta fase, el Auditor realiza las acciones programadas para la auditoria, auxiliándose de las diferentes Técnicas y Procedimientos de Auditoria, con las cuales pretende obtener

evidencia Suficiente y competente con el propósito de tener una base razonable para expresar una opinión respecto de los Estados Financieros, integrando el legajo de papeles de trabajo de la auditoria.

1.1.7.3. Cierre

El cierre de la auditoria viene dado por la expresión de una opinión independiente y experta sobre la materia auditada. Esta opinión está expresada en el dictamen de auditoria y éste a su ves esta contenido en el informe de los auditores.

1.1.7.3.1. Conceptualización Básica

Un *Informe de auditoria* es el conjunto de estados financieros que se presentan a la entidad con un dictamen acerca de los mismos, más toda aquella información financiera y no financiera importante para sustentar la opinión del auditor.

Un Dictamen *de auditoria* comunica formalmente la opinión del auditor sobre la presentación de los Estados Financieros y explica la base para su opinión. Según NIA's el *Informe Anual* es un documento que incluye los estados financieros de una entidad auditada junto con el dictamen de auditoria correspondiente.[3]

La Norma Internacional de Auditoria 700 establece que el producto final de una auditoria de Estados financieros será el *dictamen* emitido por un auditor independiente; por lo cual, en el mismo, el auditor deberá plasmar el análisis y evaluación de

[3] Ver glosario de términos de Normas Internacionales de Auditoria 2001 Pág. 27

las condiciones de la empresa, por medio de la evidencia extraída en el proceso (Ver NIA 500).

Por eso el dictamen en la práctica profesional es fundamental, ya que usualmente es lo único que el público conoce de su trabajo. La opinión del auditor por ser independiente a la de la administración de la empresa y ser el resultado de normas que controlan la calidad que debe reunir el trabajo e información que emite el profesional, permite incorporar credibilidad al contenido de los estados financieros examinados.

1.1.7.3.2. Elementos del dictamen del auditor

Los elementos que componen la estructura de un dictamen, según NIA, son los siguientes:

a. Titulo, b. Destinatario, c. Párrafo Introductorio, d. Párrafo de Alcance, e. Párrafo de Opinión, f. Fecha de Dictamen, g. Dirección del Auditor, e. Firma del Auditor

1.1.7.3.3. Tipos de opinión del auditor

El dictamen del auditor puede tener diversas opiniones entre las cuales tenemos:

- Opinión Limpia.
- Énfasis en un Asunto.
- Opinión Modificada
    - Opinión con Salvedad
    - Abstención de Opinión
    - Opinión Adversa

1.2. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1.2.1. ANTECEDENTES

A partir del desarrollo de los sistemas de información, los negocios y empresas han echado mano de estos recursos e iniciaron un proceso de sistematización de su información de forma automatizada, esto obligó a los auditores a adquirir nuevos conocimientos para poder comprender el ambiente en que estas empresas operaban y de esta manera surge la necesidad de realizar una auditoría especializada en esos sistemas de información, en el cual distintos autores empiezan a desarrollarla con el propósito de establecer las bases para la práctica de una auditoría en sistemas con enfoque teórico-práctico.

1.2.2. DEFINICION

No existen definiciones oficiales sobre la misma, y algunas de las que aparecen en los libros son criterios personales de los autores, a continuación se mencionan las que se consideran más importantes:

- *Ramos González(1999)* propone la siguiente definición: "La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de

éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos".

- Para *Fernando Catacora Carpio(1997)*, "La Auditoría Informática es aquella que tiene como objetivo principal la evaluación de los controles internos en el área de PED (Procesamiento Electrónico de Datos).

1.2.3. OBJETIVOS GENERALES

- La *Auditoría de Sistemas* tiene como principal objetivo, evaluar el grado de efectividad de las Tecnologías de Información, dado que evalúa en toda su dimensión, en que medida se garantiza la información a la Organización, su grado de *Eficacia, Eficiencia, Confiabilidad e Integridad* para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.
- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados por el PAD.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados.
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.

- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de Tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los Sistemas de Información.

1.2.4 JUSTIFICATIVOS PARA EFECTUAR UNA AUDITORÍA DE SISTEMAS

- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos).
- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados con el computador.
- Falta de una planificación informática.

- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano.
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.

1.2.5 CONTROL INTERNO DE SISTEMAS DE INFORMACIÓN

1.2.5.1 Objetivos

- Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa.
- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.
- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

1.2.5.2 Elementos

1.2.5.2.1. Controles Internos sobre la Organización del área de Informática.

- Dirección: Incluye la coordinación de recursos, la supervisión de actividades, la delegación de autoridad y responsabilidad, la asignación de actividades y la distribución de recursos.
- División del Trabajo: Es necesario dividir las funciones Básicas del área de cómputo, que son: la dirección general del área, área de análisis y diseño, de programación, de sistema de redes, de operación, de telecomunicación y de administración.
- Asignación de Responsabilidad y Autoridad: este nos ayuda a garantizar la eficiencia y eficacia del control interno en las unidades de sistemas, ya que complementa la división del trabajo y delimita claramente la autoridad y responsabilidad que tendrá cada integrante del área.
- Establecimientos de estándares y Métodos: En lo concerniente al diseño e instalación del hardware, diseño, adquisición y uso de software, base de datos, sistema de redes, sistema de seguridad y protección al personal y usuarios.
- Perfiles de Puestos: se deben contemplar como mínimo los siguientes puntos: Nombre genérico, objetivo, líneas de autoridad, funciones, requisitos, experiencia. Características de personalidad, etc.

1.2.5.2.2. Controles Internos sobre el análisis, desarrollo e implementación de sistemas.

- Estandarización de metodologías para el desarrollo de proyectos: Este incluye estandarización de métodos para el diseño de sistemas, lineamientos en la realización de sistemas, uniformidad de funciones para desarrollar sistemas, políticas para el desarrollo de sistemas y normas para regular el desarrollo del proyecto.
- Asegurar que el beneficio de los sistemas sea el óptimo: Los beneficios pueden ser Tangibles o Intangibles
- Elaborar estudios de factibilidad del sistema: La viabilidad y Factibilidad debe ser operativa, económica, técnica y administrativa
- Garantizar la eficiencia y eficacia en el análisis y diseño de sistemas: Por medio de: Adopción y seguimiento de una metodología institucional, adoptar una adecuada Planeación y programación para el desarrollo del sistema, contar con la participación activa de los usuarios finales, contar con personal que tenga la disposición, experiencia, capacitación y conocimiento para el desarrollo del sistema, utilizar los requerimientos técnicos necesarios para el desarrollo del sistema, diseñar y aplicar las pruebas previas a la implementación del sistema y supervisar permanentemente el avance de actividades del proyecto.

- Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema: Esto ayudará a garantizar la implementación adecuada y el máximo funcionamiento de los nuevos sistemas de Información, con un plan de mantenimiento periódico, ya sea preventivo o correctivo.
- Optimizar el uso del sistema por medio de su documentación: Los principales documentos del sistema son los manuales e instructivos del usuario, manuales e instructivos de operación del sistema, manual técnico del sistema, manual para el seguimiento del desarrollo del proyecto, manual del mantenimiento del sistema.

1.2.5.2.3 Controles Internos sobre la operación del Sistema

- Prevenir y corregir los errores de operación:
- Prevenir y evitar la manipulación fraudulenta de la información.
- Implementar y mantener la seguridad en la operación.
- Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la Información de la Institución.

1.2.5.2.4 Controles Internos sobre los Procedimientos de entrada de datos, el procesamiento de Información y la emisión de resultados.

- Verificar la existencia y funcionamiento de los procedimientos de captura de datos.
- Comprobar que todos los datos sean debidamente procesados.

- Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.
- Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información.

1.2.5.2.5 Controles Internos sobre la seguridad del área de sistemas.

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

1.2.6. METODOLOGÍA DE UNA AUDITORÍA DE SISTEMAS

Existen algunas *metodologías de Auditorias de Sistemas* y todas dependen de lo que se pretenda revisar o analizar, pero como estándar se estudiaran las cuatro fases básicas de un proceso de revisión: a. Estudio preliminar, b. Revisión y evaluación de controles, c. Examen detallado de áreas criticas, d. Comunicación de resultados.

1.2.6.1. Estudio preliminar.

Incluye definir el grupo de trabajo, el programa de auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el control interno, solicitud de plan de actividades, Manuales de políticas, reglamentos, Entrevistas con los principales funcionarios del PAD.

1.2.6.2. Revisión y evaluación de controles y seguridades.

Consiste de la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas criticas, Revisión de procesos históricos (backups), Revisión de documentación y archivos, entre otras actividades.

1.2.6.3. Examen detallado de áreas criticas.

Con las fases anteriores el auditor descubre las áreas criticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance Recursos que usará, definirá la metodología de trabajo, la duración de la auditoría, Presentará el plan de trabajo y analizará detalladamente cada problema encontrado.

1.2.6.4. Comunicación de resultados.

Se elaborara el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el

cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría.

El informe debe contener lo siguiente: a. Motivos de la Auditoría, b. Objetivos, c. Alcance, d. Estructura Orgánico-Funcional del área Informática e. Configuración del Hardware y Software instalado, f. Control Interno, g. Resultados de la Auditoría.

1.3. EVIDENCIA DE AUDITORIA

1.3.1. DEFINICIÓN DE EVIDENCIA

Es toda la información obtenida por el auditor para llegar a las conclusiones sobre las que se basa su opinión.

La evidencia se obtiene, por el profesional, 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 Contador Publico.

El contador no pretende obtener evidencia absoluta, sino que determina los procedimientos y aplica las pruebas necesarias para la obtención de una evidencia suficiente y competente

1.3.2. EVIDENCIA SUFICIENTE Y COMPETENTE

1.3.2.1. Evidencia Suficiente

Es aquel nivel de evidencia que el contador público debe obtener a través de las pruebas de auditoria para llegar a conclusiones

razonables sobre las aseveraciones que se someten a su examen. Bajo este contexto no se pretende obtener toda la evidencia existente sino aquella que cumpla, con los objetivos de su examen.

Para decidir el nivel necesario de evidencia (cantidad) el contador deberá tomar en cuenta la importancia relativa que tienen las áreas a evaluar y el riesgo probable de error en el que incurre al decidir no revisar determinados hechos económicos, pero siempre deberá obtener la evidencia suficiente que le permita formar su juicio profesional sobre lo examinado.

1.3.2.2. Evidencia Competente

Se dice que es competente o adecuada cuando sea útil al contador publico para emitir un juicio profesional. Para ser competente la evidencia debe ser:

- Relevante : esta debe relacionarse con el objetivo de la auditoría que se está probando.
- Válida: esta depende de las circunstancias en las cuales esta se obtiene.

El concepto de competencia de la evidencia es la característica cualitativa, en tanto que, el concepto suficiencia es la característica cuantitativa; la confluencia de ambos elementos, debe proporcionar el conocimiento necesario para alcanzar una base objetiva de juicio sobre los hechos sometidos al examen.

Hay una relación inversa entre la cantidad de evidencia que es suficiente en una situación específica y la competencia de esa

evidencia. La materia de evidencia más competente conduce a una disminución en la cantidad de evidencia que se necesita para apoyar la opinión de los auditores. Además diversas partes de la evidencia relacionada pueden formar un paquete de evidencia que tiene una mayor competencia de la que tienen las partes al ser consideradas individualmente.

1.3.3. TIPOS DE EVIDENCIA

1.3.3.1. De acuerdo a su Fuente

- Interna: Es la información obtenida por personas de la empresa; son generalmente menos confiable que los externos, sin embargo, esto depende de los procedimientos de control interno existentes y aplicables en la empresa.
- Externa: Es la información obtenida por terceras personas, ajenas a la empresa; tienen un alto grado de confiabilidad, siempre y cuando sean enviadas directamente al auditor y recibido por él sin la intervención de personal del cliente.
- Creada por auditor: Ésta se obtiene mediante la realización de pruebas en la ejecución de la auditoria

1.3.3.2. De acuerdo a su Naturaleza

- Física: Es la evidencia que los auditores realmente pueden ver.
- Documental: Es el examen que hace el auditor de los documentos y archivos del cliente para apoyar la información que es o debe ser incluida en los estados financieros.

- Virtual: es cualquier hecho, circunstancia o información obtenida que sustente o refute una información obtenida durante el proceso de auditoria o evaluación del comercio electrónico en los componentes de seguridad.

  Una transacción de compra puede iniciarse automáticamente por el computador de un cliente enviando un mensaje electrónico directamente al sistema computarizado del proveedor; este mensaje electrónico remplaza la orden de compra tradicional. La otra documentación de la transacción de compra puede consistir en una factura y un conocimiento de embarque generado electrónicamente por el sistema del proveedor.

1.3.4. PROCEDIMIENTOS PARA OBTENER EVIDENCIA

Los auditores obtienen la evidencia realizando procedimientos de auditoria, ellos pueden aumentar la cantidad de la evidencia reunida alterando la naturaleza, oportunidad o la medida de los procedimientos realizados.

1.3.4.1. Concepto

Son el conjunto de técnicas de investigación y pruebas que el auditor utiliza para lograr la información y comprobación necesaria para poder presentar y fundamentar un informe de auditoria.

1.3.4.2. Naturaleza

Debido a que los sistemas de una organización son diferentes, hacen imposible establecer sistemas rígidos de pruebas para el

examen del auditor. Por esta razón el auditor deberá, aplicando su criterio profesional, decidir cual técnica o procedimiento de auditoria o conjunto de ellos, serán aplicables en cada caso para obtener la certeza moral que fundamente una opinión objetiva y profesional.

1.3.4.3. Oportunidad

La época en que los procedimientos de auditoria se van aplicar se conoce como oportunidad.

1.3.4.4. Tipos

- Inspección: Consiste en examinar registros, documentos o activos tangibles.
- Observación: Consiste en mirar un procedimiento siendo desempeñado por otro.
- Investigación y Confirmación: Buscar información de personas dentro y fuera de la entidad, la confirmación es la respuesta obtenida de una investigación para corroborar información contenida en libros contables.
- Procedimiento de Computo: Consiste en verificar la exactitud aritmética de documentos fuentes y registros contables o desarrollar cálculos independientes.
- Procedimiento Analítico: Consiste en el análisis de índices y tendencias significativas, incluyendo la investigación resultante de fluctuaciones y relaciones que son inconsistentes con otra información relevante o que se desvían de los montos pronosticados.

1.4. EL COMERCIO ELECTRÓNICO

1.4.1 INTRODUCCIÓN

El comercio electrónico ha tenido un gran auge en el ámbito mundial en los últimos años, de tal suerte, que desde la comodidad de casa se puede comprar cualquier artículo que es vendido en diferentes países del mundo; se puede realizar cualquier transacción bancaria (pago de recibos, contratación de créditos, transferencias de fondos, etc.), sin necesidad de asistir físicamente al banco (Banca online). El Salvador no se queda atrás en este estadio de desarrollo del comercio y se observa que muchas empresas ya poseen un sitio Web, por medio del cual hacen transacciones comerciales; los bancos son un ejemplo claro de esta idea con su famosa Banca *online,* así como también algunas empresas dedicadas a la venta de artículos electrodomésticos y del hogar.

1.4.2 SURGIMIENTO DE INTERNET COMO MEDIO PARA EL DESARROLLO DEL COMERCIO ELECTRÓNICO

El desarrollo del comercio electrónico ha sido impresionante en estas últimas décadas, ello se debe a la integración de un gran número de tecnologías de telecomunicaciones e informáticas, por consiguiente es menester hablar del desarrollo de estas tecnologías, para tener un marco de referencia más amplio del contexto estudiado.

1.4.2.1 Concepto de Internet

Se conoce como la “Red de Redes” o la “Autopista de la información”, ya que efectivamente es una Red puesto que gran cantidad de ordenadores locales están conectados entre si y estos a su vez están conectados con otros ordenadores a nivel mundial, esta conexión se da a través de satélites y cables.

Una de las ventajas de Internet es que posibilita la conexión con todo tipo de ordenadores, desde los personales, hasta los más grandes que ocupan habitaciones enteras. Incluso se puede ver conectados a la Red cámaras de vídeo, robots, y máquinas de refrescos, televisores, celulares, etc. Otra ventaja de esta Red es que: es barata, pública, fácil de usar y está de moda.

1.4.2.2 Historia de Internet

En el contexto de la guerra fría y la tensión y de miedo a una guerra nuclear, aunque difícil de creer, vio la luz la primera idea de lo que hoy es Internet. Los militares norteamericanos sintieron la necesidad de crear una red informática capaz de mantener en contacto los centros militares. Para lograr esto, la red debería ser descentralizada, es decir, debía establecer un método para que ante la destrucción de cualquiera de los trozos de la red (contemplando la posibilidad de un ataque nuclear), la información pudiera encontrar más de un camino alternativo para transportar los datos.

La primera experiencia tuvo lugar en septiembre de 1969 en manos de la DARPA (Defense Advanced Research Project Agency), nombre

que recibía el departamento del gobierno de Estados Unidos dedicado al desarrollo de proyectos para la defensa nacional. Con la colaboración de profesores y alumnos avanzados en las universidades más importantes del país, el organismo logró conectar cuatro centros de cómputos: el primero ubicado en la Universidad de California en Los Ángeles (UCLA), el segundo en la Universidad de California en Santa Bárbara, el tercero en el Centro de Investigaciones de Stanford y el cuarto en la Universidad de Nevada. Por primera vez en la historia, estas computadoras ubicadas en distintos puntos del país pudieron "hablar" entre sí. Pero las cosas no quedaron ahí.

Para que la red se pudiera extender era necesario establecer un lenguaje común que establezca las reglas de juego para que las computadoras técnicamente diferentes (con distinto hardware y software), se pudieran sumar al proyecto sin problemas de compatibilidad. La idea de un lenguaje capaz de ser entendido y hablado por diferentes computadoras se vio plasmada en un protocolo llamado NCP (Network Communications Protocol) (Protocolo de Comunicación de Redes).

Paralelamente al desarrollo de ARPANET se fueron creando otras redes como la BITNET, USENET y FIDONET. A diferencia de ARPANET, que tenía como finalidad sobrevivir a la Guerra Fría, estas redes eran experimentos cuyo objetivo era probar tecnología para la transmisión de mensajes. Pero cada una de estas redes tenía

su propio lenguaje o protocolo; por lo tanto, no podía establecer comunicación con las otras.

Con el tiempo, el protocolo NCP utilizado por ARPANET fue evolucionando hasta llegar al TCP/IP (Transmission Control Protocol / Internet Protocol) (Protocolo de Control de Transmisión) IP es el protocolo estándar utilizado hasta el momento y permite que una PC con Windows ubicada en El Salvador, se pueda comunicar con una ubicada en Bruselas.

El surgimiento de este protocolo llevó a las redes independientes a sumarse a ARPANET. El proyecto original de ARPANET pasó entonces a ser la columna vertebral de un conjunto de redes en distintos lugares y el concepto de Internet tal como se conoce hoy, había nacido. En 1973, ARPANET traspasó las fronteras cuando se realizó el primer enlace entre las redes de Estados Unidos y otras similares en Inglaterra y Noruega.

Así fue, como de poco se pasó de una red exclusivamente militar a otra más constructiva cuando se unieron a ARPANET centros de investigación y universidades de diversos lugares. Estas instituciones podían dar a conocer sus descubrimientos en forma rápida y sencilla. En 1990 ARPANET fue reemplazada por una red auspiciada por la Fundación Nacional de Ciencias de Estados Unidos (NSF), llamada NFSNET. La gente de la NSF estableció las bases técnicas para que esa red, hasta entonces privilegio de investigadores y militares, tuvieran los días contados.

Para darse una idea de cómo Internet se incorpora a la sociedad se debe recordar que la radio demoró 28 años en llegar a 40 millones de personas y la televisión solo tardó 10 años en llegar a la misma cantidad de gente, hoy dichos medios tienen una llegada masiva.

Internet apenas tardo 3 años en llegar al mismo número de personas y pronto será un elemento de comunicación más en la vida cotidiana

1.4.2.3 Servicios que ofrece Internet

Las posibilidades que ofrece Internet se denominan servicios. Cada servicio es una manera de sacarle provecho a la Red independiente de las demás. Una persona podría especializarse en el manejo de sólo uno de estos servicios sin necesidad de saber nada de los otros. Sin embargo, es conveniente conocer todo lo que puede ofrecer Internet, para poder trabajar con lo que más interese.

Hoy en día, los servicios más usados en Internet son: Correo Electrónico, World Wide Web, FTP, Grupos de Noticias, IRC y Servicios de Telefonía.

- El Correo Electrónico, permite enviar cartas escritas con el ordenador a otras personas que tengan acceso a la Red.
- La World Wide Web o WWW, como se suele abreviar, se inventó a finales de los 80 en el CERN, el Laboratorio de Física de Partículas más importante del Mundo. Se trata de un sistema de distribución de información tipo revista. En la Red quedan

almacenadas lo que se llaman Páginas Web, que no son más que páginas de texto con gráficos o fotos. Aquellos que se conecten a Internet pueden pedir acceder a dichas páginas y acto seguido a éstas, aparecen en la pantalla de su ordenador. Este sistema de visualización de la información revolucionó el desarrollo de Internet.

Hay dos propiedades de las páginas Web que la hacen únicas: que son interactivas y que pueden usar objetos multimedia.

A partir de la invención de la WWW, muchas personas empezaron a conectarse a la Red desde sus domicilios, como entretenimiento. Internet recibió un gran impulso, hasta el punto de que hoy en día casi siempre que se habla de Internet, se esta refiriendo a la WWW.

- El FTP (File Transfer Protocol)(Protocolo de Transferencia de Archivo) permite enviar ficheros de datos por Internet. Con este servicio, muchas empresas informáticas han podido enviar sus productos a personas de todo el mundo sin necesidad de gastar dinero en miles de disquetes ni envíos.
- Los Grupos de Noticias, son el servicio más apropiado para entablar debate sobre temas técnicos.
- El servicio IRC (Internet Relay Chat)(Platicar por Internet) permite entablar una conversación en tiempo real con una o varias personas por medio de texto.
- Los Servicios de Telefonía, son las últimas aplicaciones que han aparecido para Internet. Permiten establecer una conexión

con voz entre dos personas conectadas a Internet desde cualquier parte del mundo sin tener que pagar el costo de una llamada internacional. Algunos de estos servicios incorporan no sólo voz, sino también imagen, a esto se le llama Videoconferencia.

Se ha realizado un esbozo de los rasgos más importantes que han posibilitado el surgimiento y desarrollo del comercio electrónico, como lo es el Internet, pues, como ya se ha visto, sin la Red, no puede existir comercio electrónico, ya que éste se vale de casi todos los servicios proporcionados por Ella. En otras palabras esta Red de Redes a facilitado el surgimiento de la “Era Virtual del Siglo XXI”, en la cual, el Auditor tiene que ingeniar las maneras de cómo adaptarse a esta realidad sin perder de vista la finalidad de su trabajo que es poder seguir proporcionando Certeza Razonable de las operaciones que realizan las empresas, en este nuevo contexto. En este sentido es necesario conocer en que consiste el comercio electrónico, para profundizar en este estudio.

1.4.3 DEFINICIÓN

El Comercio Electrónico está contribuyendo a convertir al mundo en una aldea planetaria, y aunque su evolución principal está en países industrializados, las naciones en desarrollo también pueden beneficiarse con un mejor conocimiento de este elemento de gran potencial en un mundo cada vez más globalizado. El

Internet es una herramienta poderosa, que esta acercando cada día mas a las personas, a través del uso de un ordenador, este acercamiento hace posible la conyunción a una cultura mundializada, en donde las barreras geográficas desaparecen, ya que fácilmente se puede acceder a diferentes mercados internacionales sin necesidad de salir de casa, por supuesto que esta facilidad de acceso es posible debido a la homogenización de la tecnología entre los países industrializados y los subdesarrollados, puesto que sin ésta seria imposible llegar a ser la "Aldea Planetaria" de la cual se habla.

A continuación se presentan una serie de definiciones de comercio electrónico proporcionadas por diferentes organismos interesados en la materia:

- 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)[4]
- "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)[5]
- "Es el uso de las tecnologías computacional y de telecomunicaciones que se realiza entre empresas o bien entre

[4] BT Electronic Commerce Innovation Center, "An Introduction to Electronic Commerce", University of Cardiff, UK.
[5] Idem nota anterior.

vendedores y compradores, para apoyar el comercio de bienes y servicios."[6]

En cada una de estas definiciones esta la connotación "Uso de Tecnología de Información para hacer negocios (Comprar/Vender bienes y servicios)", como nota esencial de la definición de comercio electrónico.

1.4.4 ANTECEDENTES

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. 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

[6] Halchmi, Z., Hommel, K., y Avital., O., 1996. "Electronic Commerce",

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 electrónicos, 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.

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.

1.4.5 TIPOS

Dependiendo de las partes que hacen o interactúan en una transacción, existen diversas denominaciones para los negocios Electrónicos. Se mencionaran las más importantes:

- Empresas- Empresas (Business to Business)

  Abreviado B2B, se refiere a que las partes que hacen negocio o extienden sus procesos son dos empresas.

- Empresa- Consumidor (Business to Customer)

  Abreviado B2C, el más conocido, este tipo de tiendas virtuales han tenido mucha publicidad y precisamente está dirigida a los consumidores.

- Empresa- Gobierno (e – Government)

  A este tipo de negocio por Internet mencionado anteriormente se puede agregar bajo el mismo concepto la relación entre el gobierno y ciudadanos, que más que negocios propiamente dicho, se dedica a algún tipo de transacción o tramite por Internet. (Pago de impuestos, quejas o reclamos, denuncias)

- Consumidor- Empresa (Customer to Business)

  Las partes que hacen también son un consumidor y una empresa pero a diferencia del anterior aquí es el consumidor el que ofrece a las empresas a un precio, un producto o servicio.

- Consumidor – Consumidor (Customer to Customer)

  Conocido por las subastas por Internet, donde el consumidor ofrece a otro, sin mediar una empresa en la transacción, productos y servicios, pagando de ser requerida una comisión por la venta.

1.4.6 VENTAJAS Y DESVENTAJAS QUE OFRECE

El comercio electrónico como ya se mencionó esta teniendo un crecimiento acelerado y todos los actores involucrados tienden a

desarrollar medidas y hábitos para poder aprovechar al máximo sus ventajas y bondades, sin embargo, no todo es absolutamente bueno en la vida, el comercio electrónico tiene sus desventajas y altos riesgos como la seguridad por ejemplo, que pueden ser piedra de tropiezo para su pleno desarrollo, los cuales muchos organismos a nivel mundial están encaminando esfuerzos y proyectos tendientes a disminuir estos riesgos y balancear con un saldo positivo las ventajas de las desventajas.

Las ventajas que ofrece el comercio electrónico se pueden resumir de la siguiente manera:

- Permite hacer más eficientes las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
- Reduce las barreras de acceso a los mercados actuales, en especial para pequeñas empresas, y abre oportunidades de explotar mercados nuevos.
- Para el consumidor, amplía su capacidad de acceder a prácticamente cualquier producto y de comparar ofertas, permitiéndole además convertirse en proveedor de información.
- Reduce o incluso elimina por completo los intermediarios, por ejemplo en la venta de productos en soporte electrónico (textos, imágenes, vídeos, música, programas, etc.) que se pagan y entregan directamente a través de la red.

Más en general, el comercio electrónico obliga a redefinir el papel de los intermediarios entre productor y consumidor,

eliminándolos en algunos casos, pero también creando la necesidad de funciones de intermediación nuevas en otros. Pero el comercio electrónico plantea problemas nuevos o agudiza algunos ya existentes en el comercio tradicional, entre ellos:

- La validez legal de las transacciones y contratos “sin papel”.
- La necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio.
- El control de las transacciones internacionales, incluido el cobro de impuestos.
- La protección de los derechos de propiedad intelectual.
- La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales.
- La dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica.
- La seguridad de las transacciones y medios de pago electrónicos.
- La falta de estándares consolidados y la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.
- La congestión de Internet y la falta de accesos de usuario de suficiente capacidad.

Los problemas citados tienen, en mayor o menor medida, una componente legal o regulatorio y un componente tecnológico, por lo que su solución requiere actuaciones en ambos sentidos.

Los sistemas de comercio electrónico disponibles actualmente adolecen en general de alto costo y reducida interoperabilidad. En el comercio electrónico entre empresas predominan las soluciones diseñadas a medida para aplicaciones específicas o para sectores o grupos de empresas cerrados, con escasa reutilización de componentes estándar y, como consecuencia, con un elevado coste de desarrollo. Aún hay pocos estándares asentados en la industria y proliferan las propuestas de diversos consorcios, normalmente incompatibles entre sí. En esta situación es difícil establecer relaciones de comercio electrónico espontáneas entre empresas sin pasar por una fase previa de adaptación o integración de sus respectivos sistemas.

1.4.7 LA TIENDA VIRTUAL Y EL CANAL VIRTUAL

1.4.7.1 Definición de tienda virtual

De acuerdo a Manuel Vizuete Gómez en su articulo publicado en www.markenting.com menciona que “en primer lugar ser virtual, es decir, una tienda virtual no tiene escaparate… su escaparate es la pantalla de ordenador. No tiene vendedores… el vendedor es la pantalla de ordenador. No tiene almacén (en una situación de eficiencia ideal), trabaja bajo pedido, ya que ha logrado la eficiencia en sus tres bases fundamentales: cliente (pedidos),

proveedor y courier (transporte). Una tienda virtual es aquella que decide utilizar este canal para vender y distribuir sus productos. Independientemente si esa tienda existía ya como tienda física o no, la forma de gestionar la empresa cambia de forma radical a la hora de establecer un negocio en la Red.”

1.4.7.2 Definición de canal virtual

Un canal virtual es un medio de distribución de productos a través de la World Wibe Web por parte de una empresa, sin que esta sea precisamente una tienda virtual. En el medio son las que más rebosan, por lo tanto, la atención principal se cierne sobre el canal virtual de las empresas investigadas, puesto que es allí donde se dan las operaciones virtuales, y por ende, se deben establecer las técnicas y procedimientos de auditoria, para la obtención de las evidencias, con el fin de brindar seguridad y confianza al usuario y a la empresa misma.

1.5. SEGURIDAD

1.5.1. SEGURIDAD EN INTERNET

1.5.1.1. Introducción

La seguridad es un aspecto muy importante en cualquier transacción comercial, en el sentido que el cliente debe estar seguro que no será defraudado por su proveedor, y por el otro lado el proveedor debe estar seguro que el cliente cumplirá con su obligación de pago, para esto se establecen mecanismo en el comercio convencional, tales como la celebración de contratos,

firma de títulos valores entre otros, todo esto para afianzar a las partes involucradas en la transacción comercial y salvaguardar los intereses de cada una de ellas. A estos hay que sumarle los otros riesgos vinculados a cualquier transacción comercial (Calidad de Producto, seguridad en transito, etc.).

En el nuevo arquetipo de comercio, es decir, “El Comercio Electrónico”, además de los riegos antes mencionados, surgen otros nuevos de gran envergadura, como lo es “El Riesgo de Transferencia de Información”, cabe hacer mención, que las transacciones comerciales de este tipo de comercio se hacen a través de la Red, en donde transita muchísima información, y a la vez hay numerosísimas personas que están al asecho de esa información, los famosos Hacker y Cracker, los cuales son una amenaza muy grande para el E-Commerce. En este sentido el cliente tiene mucha desconfianza de introducir sus datos personales y su numero de tarjeta de crédito o débito por el temor a ser interceptado y que haya una “Usurpación de identidad. Rodolfo Lomáscolo en su articulo publicado en www.markenting.com, dice “En el caso de las grandes corporaciones y organizaciones empresariales la preocupación por la seguridad en Internet es fácil de entender: las organizaciones necesitan proteger la confidencialidad de la información reservada. Por otra parte, los usuarios de a pie también deberían vigilar de cerca todo lo referente a la

protección de sus datos y a la identidad de las fuentes y destinatarios de los mismos.”

Por supuesto que la seguridad afecta a todos: a las empresas por ser una tentación y por las consecuencias de una posible filtración, y a los usuarios individuales por su vulnerabilidad.

No obstante el concepto de seguridad no se limita solamente al campo técnico (algoritmos de cifrados, longitud de claves, seguridad entorno al hardware, etc.), lo cual es de suma importancia, si no mas bien se expande a un plano mucho más amplio y de sumo interés para las entidades oferentes y demandantes de bienes y servicios (privadas o publicas), que es la necesidad de generar confianza al usuario en el entorno del comercio electrónico. La seguridad como generadora de confianza no solamente consiste en la seguridad en red, esto es solamente uno de los componentes que intervienen en la seguridad del comercio electrónico en su conjunto. La desconfianza de los usuarios, por ejemplo enviar su número de tarjeta de crédito a través de Internet para efectuar un pago es una barrera inicial para el crecimiento del comercio electrónico. Esta barrera en países subdesarrollados donde se tiene una población poco familiarizada con esta tecnología puede ser todavía muy importante. En Estados Unidos donde casi toda la población posee un ordenador, tiene acceso a Internet y están más familiarizados con el comercio electrónico y en general con la venta a distancia, esta preocupación ha pasado a segundo plano. Mas que

la seguridad de pago los usuarios están interesados y comienzan a preocuparse en situaciones tales como:

¿Es el vendedor fiable?, ¿Se podrá devolver el producto comprado si no le gusta?, ¿Utilizaran datos personales para enviar publicidad que no desean?, ¿Cederán estos datos a otras empresas?, ¿Cuál es la validez de un pedido, factura, etc. Hechos electrónicamente?. Así, aunque las características de seguridad de las redes y sistemas de comercio electrónico son, obviamente muy importantes, el hecho de que los usuarios consideren el comercio electrónico como suficientemente seguro, probablemente depende menos de los detalles técnicos, y más de otras cuestiones como la confianza que inspiren las empresas vendedoras, financieras, etc.; la existencia y difusión de normas que, por ejemplo, limiten la responsabilidad del usuario en caso de uso indebido de una tarjeta de crédito y que garanticen su derecho a devolver un producto comprado electrónicamente; la creación de códigos éticos de comportamiento de las empresas y de procedimientos efectivos de solución de conflictos; etc.

En este sentido una auditoría de empresas que se dedican al comercio electrónico debe ir encaminada a evaluar todos estos aspectos de seguridad centrando un mayor énfasis en las políticas de seguridad que las empresas poseen para generar confianza en los usuarios, que por ejemplo, sus datos serán tratados con suma confidencialidad y no se utilizaran

abusivamente para otros fines diferentes a los que el usuario había previsto. Por supuesto que la seguridad en el pago por un bien o un servicio sigue siendo un componente importante en la evaluación del auditor así como todas aquellas políticas y procedimientos encaminados a salvaguardar el software y el hardware, ya que todos estos factores concluyen en la imagen y la credibilidad de las empresas en el mercado.

1.5.1.2. Definición

Rodolfo Lomáscolo, define que la seguridad en Internet consiste en “implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor. Las contraseñas y palabras clave ya no son un mecanismo suficientemente fiable y seguro, ya que éstas pueden ser interceptadas durante su transmisión, de lo que desgraciadamente nos damos cuenta muy tarde o cuando la prensa se hace eco de un caso de estafa electrónica”.

1.5.1.3. Tipos

La seguridad puede dividirse en interna y externa.

La primera es aquélla que intenta mantener privados y accesibles sólo para los usuarios autorizados, aquellos datos internos o sensibles de la organización en cuestión.

La seguridad externa puede parecer más compleja de controlar, aunque en realidad no lo es tanto, ya que los usuarios externos no utilizan el sistema interno de la empresa, en principio no

deberían disponer de ninguna clave de acceso, aunque sea a nivel de visitante, por lo que con dedicación y conocimiento se pueden crear sistemas altamente seguros.

Los firewall permiten aislar la red interna de la externa, con control del tipo de protocolo que circula y su origen y destino.

Hoy no se puede decir que la conexión a Internet o a cualquier otra red abierta no se pueda realizar de forma segura, existen las herramientas y la mayoría de ellas seguro que se encuentran incorporadas en el sistema operativo de sus servidores y estaciones de trabajo.

1.5.1.4. Herramientas

Las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:

- Confidencialidad: evita que un tercero pueda *acceder a* la información enviada.
- Integridad: evita que un tercero pueda *modificar* la información enviada sin que lo advierta el destinatario.
- Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.
- No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.

La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra).

A continuación se definirán las herramientas más importantes utilizadas para la seguridad de la información en la Red.

1.5.1.4.1. Encriptación.

Es el conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada.

1.5.1.4.1.1. Proceso de encriptación

Internet es prácticamente una puerta abierta, sobre la cual ninguna entidad ejerce un control en cuanto a qué publicar o no, pero si es posible monitorear desde qué lugar se conectan los usuarios a la red, con qué frecuencia lo hacen, incluso lograr apoderarse de alguna información. Naturalmente, como usuarios se teme por el peligro que al enviar datos personales, caigan en manos de un extraño o los llamados piratas cibernéticos (hackers), sin embargo, un servidor seguro garantiza que la información llegará protegida a su destino, mediante un proceso de encriptación:

La información se encripta desde el momento en que se pulsa el botón “enviar”, al llenar un formulario de compra, y es el ordenador el encargado de cifrar y “esconder” los datos.

Todo dato que se digitalice se codifica en binario, es decir en ceros y en unos.

Para encriptarlo, se aplica al mensaje un algoritmo u operación matemática que devuelve un mensaje indescifrable, también en binario.

Para descifrar el mensaje original, se aplica el mismo algoritmo al llegar al lugar de destino.

Solamente el emisor y el receptor podrán descifrar el algoritmo y el mensaje contenido con una información en clave que cada uno de ellos conoce. Estas claves pueden ser privada (que conocerá solo el emisor) y pública (que conocerán los destinatarios).

Cada usuario deberá disponer de este par de claves que van asociadas. De esta manera si alguien quiere enviar un mensaje cifrado a un usuario, tendría que conocer su clave pública y solo la clave privada podría descifrarlo. (Ver Anexo 1.7. a y 1.7.b.)

1.5.1.4.1.2. La criptología

La criptología se define como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Abarca por tanto a la criptografía (datos, texto, e imágenes), la criptofonía (voz) y el criptoanálisis, ciencia que estudia los

pasos y operaciones orientados a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave.

1.5.1.4.2. El Protocolo SET (Seguridad Electrónica de Transacciones)

Secure Electronic Transactions es un conjunto de especificaciones desarrolladas por VISA y MasterCard, con el apoyo y asistencia de GTE, IBM, Microsoft, Netscape, SAIC, Terisa y Verisign, que da paso a una forma segura de realizar transacciones electrónicas, en las que están involucrados: usuario final, comerciante, entidades financieras, administradoras de tarjetas y propietarios de marcas de tarjetas. SET constituye la respuesta a los muchos requerimientos de una estrategia de implantación del comercio electrónico en Internet, que satisface las necesidades de consumidores, comerciantes, instituciones financieras y administradoras de medios de pago.

Por lo tanto, SET dirige sus procesos a: a. Proporcionar la autentificación necesaria, b. Garantizar la confidencialidad de la información sensible, c. Preservar la integridad de la información, d. Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

SET utiliza para sus procesos de encriptación dos algoritmos:

De clave pública RSA (algoritmo simétrico), diseñado por Rivest, Shamir y Adleman, cuyas iniciales componen su nombre.

De clave privada DES (Data Encryption Standard), de fortaleza contrastada y excelente rendimiento, conocido también como algoritmo asimétrico ya que emplea dos claves diferentes: una para encriptación y otra para desencriptación.

La base matemática sobre la cual trabajan los algoritmos, permite que, mientras un mensaje es encriptado con la clave pública, es necesaria la clave privada para su desencriptación.

El mensaje original es encriptado con la clave pública del destinatario; este podrá obtener el mensaje original después de aplicar su clave privada al mensaje cifrado.

Para evitar que la clave pública de un usuario sea alterada o sustituida por otra no autorizada, se crea una entidad independiente llamada Autoridad Certificadora (Certifying Authority, CA), cuya labor consiste en garantizar y custodiar la autenticidad de las claves públicas de empresas y particulares, a través de la emisión de certificados electrónicos (Ver anexo 1.7.c.).

1.5.1.4.3. Algoritmos de Destilación

Además de estos algoritmos de encriptación asimétrica existen otros algoritmos de compresión necesarios para conseguir que la firma digital tenga los mismos efectos que la manuscrita. Se trata de los algoritmos de comprensión hash que se aplican sobre un determinado texto en cuestión (por ejemplo el contrato on-line). Son algoritmos que aplican funciones de no retorno. Estas funciones que realizan son peculiares en el sentido de que no es

necesario la tenencia de una clave, ya que aplican funciones matemáticas sencillas para cifrar, pero para poder descifrar los cálculos matemáticos a realizar serían prácticamente imposibles de encontrar. Luego nadie, ni si quiera la persona que cifra el texto, podría llegar al documento original. La comprensión crea un texto limitado y reducido de entre 128 y 160 bits, el cual representa de forma fehaciente la integridad del documento, ya que si se cambia un solo bit del documento original el resultado obtenido al volver a aplicar la función hash sería totalmente diferente. Además de estas peculiaridades las probabilidades para que dos textos distintos tuviesen el mismo hash serían prácticamente nulas. Estos algoritmos también son conocidos como algoritmos de destilación, algoritmos de huella digital o algoritmos de función resumen, los cuales son vitales y necesarios para la introducción de la firma digital en la sociedad de la información.

1.5.1.4.4. La Firma Digital

La firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación). De esta forma, el autor queda vinculado al documento de la firma.

Por último la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor. La firma se realizaría de la siguiente forma: el software del firmante aplica un algoritmo hash sobre el texto a firmar (algoritmo matemático unidireccional, es decir, lo encriptado no se puede desencriptar), obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor. Los algoritmos hash más utilizados para esta función son el MD5 ó SHA-1. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits (según el algoritmo utilizado), se somete a continuación ha cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA. De esta forma obtenemos un extracto final cifrado con la clave privada del autor el cual se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

Sin embargo, es necesario comprobar que la firma realizada es efectivamente válida. Para ello es necesaria la clave pública del autor. El software del receptor, previa introducción en el mismo de la clave pública del remitente (obtenida a través de una autoridad de certificación), descifraría el extracto cifrado del autor; a continuación calcularía el extracto hash que le

correspondería al texto del mensaje, y si el resultado coincide con el extracto anteriormente descifrado se consideraría válida, en caso contrario significaría que el documento ha sufrido una modificación posterior y por tanto no es válido(Ver anexo 1.7.d)

1.5.1.4.5. Las Autoridades de Certificación

Si todos estos medios de seguridad están utilizando el procedimiento de encriptación asimétrico, habrá que garantizar tanto al emisor como al receptor la autenticación de las partes, es decir, que éstas son quienes dicen ser, y sólo a través de una autoridad de certificación (CA certification authority) podrá corregirse dicho error, certificando e identificando a una persona con una determinada clave pública. Estas autoridades emiten certificados de claves públicas de los usuarios firmando con su clave secreta un documento, válido por un período determinado de tiempo, que asocia el nombre distintivo de un usuario con su clave pública.

Una autoridad de certificación es esa tercera parte fiable que acredita el vínculo entre una determinada clave y su propietario real. Actuaría como una especie de notario electrónico que extiende un certificado de claves, el cual está firmado con su propia clave, para garantizar la autenticidad de dicha información. Los certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública

pertenece a una determinada persona, evitando que alguien utilice una clave falsa para suplantar la personalidad de otro.

1.5.1.4.6. Medidas para la mala administración de la clave secreta

Es decir, es posible que exista una mala administración de la clave secreta por parte del usuario provocando la quiebra del sistema. En su caso ¿qué parte respondería? ¿El usuario, el banco o la empresa?, ¿Cómo se prueba una mala administración de la clave secreta? Ante esta posible quiebra se podría argumentar que el individuo cambia frecuentemente de clave, pero si lo hace la infraestructura de la clave pública podría verse viciada por la transmisión entre las distintas autoridades de distintos ficheros de claves que no están actualizados. Dicho problema está adquiriendo importancia en Estados Unidos, de ahí que se estén implementando soluciones como:

- Los repositorios: o listas de revocación de certificados por extravío o robo de claves privadas.
- Las autoridades de fechado digital: que permiten al verificador determinar fehacientemente si la firma digital fue ejecutada dentro del período de validez del certificado, previenen fechados fraudulentos antes o después de la fecha consignada, o impiden alterar el contenido del documento posteriormente al instante de la firma.
- Incorporar la clave en un chip adjunto por ejemplo a una tarjeta magnética. Esta solución sería factible siempre y

cuando nuestro ordenador tuviera un lector de bandas magnéticas o chips, de forma que en el momento de la transacción o la firma del contrato pueda leer perfectamente de que persona se trata y que clave pública o privada tienen asociadas.

Otras soluciones apuntan hacia la Biometría, ciencia que estudia la encriptación de los datos a través de partes del cuerpo humano que sean características únicas e individualizables de una persona, tales como el iris del ojo, las huellas dactilares, etc.

1.5.1.5 Amenazas

1.5.1.5.1 Los piratas informáticos (Hackers)

El principal objetivo de los Hackers no es convertirse en delincuentes sino “pelear contra un sistema injusto” utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente. Se dedican a la penetración de sistemas informáticos a través de la red. La cultura popular define a los hackers como aquellos que, con ayuda de sus conocimientos informáticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra.

1.5.1.5.2 Usurpadores de claves (Crackers).

1.5.1.5.2.1. Cracker pirata.

El Cracker pirata, es inofensivo excepto para los bolsillos de los productores de video-juegos, películas, música, etc. Es el que se dedica a copiar juegos entre otras cosas.

1.5.1.5.2.2. Cracker vándalo.

Este personaje es algo parecido a un “hacker dañino”. Se dedica a asaltar a los navegantes, meterse en sus computadoras y destruir, sólo por el placer de hacerlo. Son peligrosos por que estos controlan bastante de computadoras y pueden generar graves problemas. Si lo comparamos con la realidad, estos serían los maleantes del ciberespacio.

1.5.2. SEGURIDAD FÍSICA Y LÓGICA DE LOS SISTEMAS DE INFORMACIÓN EN RED

1.5.2.1. Introducción

Se ha hecho énfasis en los aspectos de seguridad y protección de los datos que transitan por Internet utilizando técnicas y algoritmos de encriptación. Esta sección trata acerca de la seguridad interna de hardware y el software y las principales medidas que poseen algunos sistemas operativos del mercado frecuentemente utilizado como sistemas operativos del servidor, donde se encuentra almacenada la información sensible para cualquier entidad. Estos aspectos de seguridad están enfocados siempre a las entidades que poseen una red interna (Intranet) y

que a su vez están conectadas a la red mundial (Internet), para lo cual se requieren medidas de protección que posibiliten el aseguramiento de la información.

El objetivo principal de todas las medidas de seguridad es salvaguardar la información que la entidad considera importante, por lo que se requiere que se integren una serie de factores y recursos tanto humanos, tecnológicos y físicos.

1.5.2.2. Políticas y medidas de seguridad

Es importante diferenciar entre seguridad y protección. La seguridad consiste en lograr que los recursos de un sistema, sean utilizados para lograr el fin previsto por la entidad, para ello es que se utilizan los mecanismos de protección. Los sistemas operativos proveen algunos mecanismos de protección para la implementación de políticas de seguridad, sin embargo estos mecanismos deben complementarse con otros que no tienen nada que ver con los sistemas operativos como por ejemplo: impedir el acceso físico de personas no autorizadas a los sistemas, segregación de funciones, diferentes niveles de acceso a los sistemas, etc.

Un aspecto importante de la seguridad es impedir que se pierda información, lo cual puede darse por diferentes causas, tales como: guerras, desastres naturales, errores de hardware, software o errores humanos. La solución para aminorar este riesgo es mantener la información respaldada, de preferencia en un lugar lejano al origen.

Otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos: lectura de datos, modificación de datos, destrucción de datos, uso de recursos ciclos de CPU, impresora, almacenamiento.

Aquí el sistema operativo juega un rol fundamental, ofreciendo mecanismos de autorización y autentificación.

Toda organización debe estar a la vanguardia de los procesos de cambio, donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental; donde la información se reconoce como:

- Crítica: indispensable para garantizar la continuidad operativa de la organización.
- Valiosa: es un activo corporativo que tiene valor en sí mismo.
- Sensitiva: debe ser conocida por las personas que necesitan los datos.

En este sentido la seguridad informática debe garantizar: la disponibilidad de los sistemas de información, la recuperación rápida y completa de los sistemas de información, la integridad de la información, la confidencialidad de la información, implementación de políticas de seguridad informática y la identificación de problemas. Para esto es necesario tener en cuenta algunos principios básicos de seguridad, tales como: suponer que el diseño del sistema es público; el defecto debe ser sin acceso; chequear permanentemente; los mecanismos de protección deben ser simples, uniformes y construidos en las

capas más básicas del sistema y los mecanismos deben ser aceptados psicológicamente por los usuarios.

A continuación se dictan algunas políticas y medidas de seguridad lógicas y físicas para salvaguardar la información contenida en los servidores y que viaja por una red interna.

1.5.2.2.1 Políticas de seguridad de redes de comunicación

Para lograr el objetivo de salvaguarda de la información se deben establecer los siguientes preceptos:

a. Revisión de costos y la asignación formal de proveedores, b. Crear y aplicar estándares de comunicación, c. Tener una gerencia de comunicaciones con plena autoridad de voto y acción, d. Llevar un registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones, e. Mantener una vigilancia constante sobre cualquier acción en la red, f. Registrar un costo de comunicaciones y reparto a encargados, g. Mejorar el rendimiento y la resolución de problemas presentados en la red.

Para lo cual se debe comprobar:

a. El nivel de acceso a diferentes funciones dentro de la red, b. Coordinación de la organización de comunicación de datos y voz, c. Que existan normas de comunicación, d. El Uso de conexión digital con el exterior como Internet, d. La responsabilidad en los contratos de proveedores, e. La creación de estrategias de comunicación a largo plazo, f. Planificación de cableado, g. Planificación de la recuperación de las

comunicaciones en caso de desastre, h. Tener documentación sobre el diagramado de la red, i. Pruebas sobre los nuevos equipos, j. Establecer las tasas de rendimiento en tiempo de respuesta de las terminales y la tasa de errores.

1.5.2.2.2. Políticas de seguridad de la red física

Se debe garantizar que exista:

a. Áreas de equipo de comunicación con control de acceso, b. Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos, c. Prioridad de recuperación del sistema, d. Control de las líneas telefónicas.

Comprobando que:

a. El equipo de comunicaciones ha de estar en un lugar cerrado y con acceso limitado, b. La seguridad física del equipo de comunicaciones sea adecuada, c. Se tomen medidas para separar las actividades de los electricistas y de cableado de líneas telefónicas, d. Las líneas de comunicación estén fuera de la vista, e. Se dé un código a cada línea, en vez de una descripción física de la misma, f. Hayan procedimientos de protección de los cables y las bocas de conexión para evitar pinchazos a la red, g. Existan revisiones periódicas de la red buscando pinchazos a la misma, h. El equipo de prueba de comunicaciones ha de tener unos propósitos y funciones específicas, i. Existan alternativas de respaldo de las comunicaciones.

1.5.2.2.3. Políticas de seguridad de la red lógica

En ésta, debe evitarse un daño interno, como por ejemplo, inhabilitar un equipo que empieza a enviar mensajes hasta que satura por completo la red.

Para éste tipo de situaciones:

a. Se deben dar contraseñas de acceso, b. Controlar los errores, c. Garantizar que en una transmisión, ésta solo sea recibida por el destinatario (Para esto, regularmente se cambia la ruta de acceso de la información a la red), d. Registrar las actividades de los usuarios en la red, e. Encriptar la información pertinente, f. Evitar la importación y exportación de datos.

En cada sesión de usuario, se debe:

a. Revisar que no acceda a ningún sistema sin autorización, b. Inhabilitar al usuario que tras un número establecido de veces yerra en dar correctamente su propia contraseña, c. Obligar a los usuarios a cambiar su contraseña regularmente, d. No mostrar las contraseñas en pantalla tras digitarlas, e. Dar información a cada usuario sobre su última conexión a fin de evitar suplantaciones, f. Inhabilitar el software o hardware con acceso libre, g. Tener procedimientos correctivos y de control ante mensajes duplicados, fuera de orden, perdidos o retrasados, del software de comunicación, h. Hacer un análisis del riesgo de aplicaciones en los procesos, i. Hacer un análisis de la conveniencia de cifrar los canales de transmisión entre

diferentes organizaciones, j. Asegurar que los datos que viajan por Internet vayan cifrados.

1.6. MEDIOS DE PAGOS EN EL COMERCIO ELECTRÓNICO

1.6.1. INTRODUCCIÓN

Los elementos fundamentales en el comercio en general y en el comercio electrónico en particular, es la realización del pago correspondiente por los bienes o servicios adquiridos.

En este ámbito el comercio electrónico presenta una problemática semejante a la que se plantea en otros sistemas de compra no presencial, es decir, en aquella en la que las partes no se reúnen físicamente para realizar la transacción, como por ejemplo en la compra por catálogo o telefónica:

El comprador debe tener garantía sobre calidad, cantidad y características de los bienes que adquiere, el vendedor debe tener garantía del pago y la transacción debe tener un aceptable nivel de confidencialidad. En ocasiones, se entiende que para garantizar estos hechos, comprador y vendedor deben acreditar su identidad, pero realmente sólo necesitan demostrar su capacidad y compromiso respecto a la transacción. De esta manera cada vez, más sistemas de pago intentan garantizar la compra "anónima". En el comercio electrónico se añade otro requerimiento que generalmente no se considera en otros sistemas de venta no presencial, aún cuando existe:

- El comprador debe tener garantía de que nadie pueda, como consecuencia de la transacción que efectúa, suplantar en un futuro su personalidad efectuando otras compras en su nombre y a su cargo.
- El costo por utilizar un determinado medio de pago debe ser aceptable para el comprador y el vendedor.

Al igual que cuando se utiliza una tarjeta de crédito para pagar en una tienda, el comerciante acepta el pago de un porcentaje sobre el importe de la compra a cambio del mayor número de ventas que espera realizar aceptando este medio de pago; los medios de pago asociados al comercio electrónico suelen conllevar un costo que los puede hacer inapropiados o incluso inaceptables para importes pequeños, los denominados micro pagos. Para realizar estos micros pagos los sistemas suelen ser de uno de estos dos tipos:

- El comprador adquiere dinero anticipadamente (prepago) para poder gastarlo en pequeños pagos.
- El comprador mantiene una cuenta que se liquida periódicamente y no transacción a transacción. Este sistema se utiliza frecuentemente para el acceso a pequeñas piezas de información de pago.

En el comercio electrónico pueden distinguirse varios tipos de medios de pago.

1.6.2 GENERALES

1.6.2.1 Contra reembolso

Es el único medio de pago utilizado en el comercio electrónico que implica la utilización de dinero en efectivo. Desde el punto de vista del vendedor este medio de pago conlleva dos inconvenientes fundamentales: el retraso del pago y la necesidad de recolectar físicamente el dinero por parte de quien realiza la entrega.

1.6.2.2 Cargos en cuenta (domiciliación)

Suele emplearse para cargos periódicos o suscripciones.

1.6.3. ESPECÍFICOS

Para el nuevo entorno del comercio electrónico, especialmente Internet. Por ejemplo: Existen tarjetas de crédito o débito, sólo utilizable para el comercio electrónico e Intermediarios electrónicos para sistemas basados en tarjetas de crédito tradicionales: Cyber Cash y First Virtual (Moneda electrónica). En cualquiera de los casos, los medios de pago utilizados pueden ser de pago anticipado (prepago o "pay before"), inmediato ("pay now") o posterior ("pay after").

1.6.3.1 Tarjetas de crédito y débito

Ampliamente usadas hoy en día como medio de pago en el comercio electrónico, las tarjetas de crédito y débito tradicionales han permitido la realización de transacciones comerciales en el

nuevo medio a través de la utilización de los procedimientos de liquidación y pago preestablecidos.

Si se realiza una compra en Internet utilizando una tarjeta de crédito como medio de pago, la transacción comercial se ordena en la red, pero la validación y la realización efectiva del pago se efectúa a través de los circuitos tradicionales de procesamiento de operaciones con tarjeta de crédito. En el esquema más general, intervienen en este proceso los siguientes actores: a. El comprador, b. El vendedor ("merchant"), c. El banco emisor ("issuer") de la tarjeta de crédito o débito que presenta el cliente, d. El banco que en nombre del vendedor recibe la transacción ("acquirer") y en el cual reside la cuenta en la que a éste se le va a liquidar el pago, e. La red de medios de pago ("scheme") como VISA o MasterCard.

El proceso de pago es como sigue:

1. Una vez realizado el pedido, el comprador proporciona su número de tarjeta al vendedor a través de la red.
2. El centro servidor donde reside el vendedor envía la transacción al banco "acquirer" o directamente a la red de medios de pago. Este envío suele producirse fuera de la red pública y se realiza de forma análoga a como se efectuará desde una Terminal punto de venta (TPV) físico que existiese en una tienda real.
3. El banco receptor pide autorización al banco emisor a través de la red de medios de pago.

4. Si la transacción se autoriza, la liquidación del pago (transferencia de dinero desde la cuenta del comprador en el banco emisor hasta la cuenta del vendedor en el banco receptor) se realiza a través de la red tradicional de medios de pago.

Como puede observarse el punto crítico de este proceso se produce cuando el comprador envía su número de tarjeta al vendedor a través de una red pública potencialmente insegura como Internet. El estándar que se utiliza en Internet para asegurar esta transferencia de datos es el SSL (del Inglés, Secure Sockets Layer). Para la realización de una transacción utilizando SSL se requiere de dos elementos:

1. Que el vendedor se haya certificado con una organización reconocida por las partes, lo que supone un procedimiento administrativo y el pago de unas tarifas de alta, así como la renovación de tal certificación.
2. Que el comprador utilice un visor o navegador ("browser") compatible como SSL.

Con el uso del SSL:

1. El comprador tiene garantía de que el vendedor es quien dice ser y que por tanto, no está entregando su número de tarjeta a un posible impostor.
2. La información que envía el comprador se cifra, impidiendo el acceso a la misma por alguien distinto al vendedor.

3. Se garantiza la no-manipulación de los datos entre el comprador y el vendedor.

La versión 3 de SSL permite la autenticación del comprador, que debe recibir sus claves previamente de una autoridad de certificación.

Lo que SSL no garantiza es el aspecto económico de la transacción, de tal manera que sólo con proporcionar un número de tarjeta válido con saldo suficiente cualquier persona podría intentar comprar electrónicamente de forma fraudulenta, sobre todo si no existe una entrega física de los bienes en sí con una autoridad de certificación.

1.6.3.2. Tarjetas chip

En pleno desarrollo, las tarjetas chip o tarjetas inteligentes son aquellas que poseen una capacidad de almacenar información en un chip que incorporan.

Fundamentalmente esta información suele ser:

- Una identificación que incluye determinadas claves cifradas.
- Una cantidad de dinero disponible.

Antes de comprar es preciso cargarlas con dinero a través de un cajero automático. Tras realizar esta operación funcionan como si contuvieran dinero en efectivo ("cash"). Este tipo de tarjetas son ideales para realizar micro pagos, tanto en el comercio del mundo físico como en el virtual. No obstante, su utilización en el comercio electrónico requiere de un dispositivo conectado a la computadora personal, un módem o

línea de teléfono que permita su lectura y actualización al realizar transacciones por la red.

1.6.3.3. Cyber cash

Procedente de la compañía Verifone, especializada en terminales punto de venta, Cybercash es un sistema de realización de transacciones en Internet mediante el uso de tarjetas de crédito.[7] Una vez realizada la compra, el comprador envía sus datos cifrados al vendedor. Este añade sus propios datos que lo identifican y solicita autorización a CyberCash. A partir de aquí, CyberCash se comunica con la red tradicional de medios de pago, y una vez obtenida la autorización de la transacción, se la pasa a la empresa vendedora.

1.6.3.4. First Virtual

First Virtual (FV) es un sistema de pagos operado por First USA y EDS, basado en el mantenimiento de cuentas virtuales de clientes que se liquidan periódicamente contra tarjetas de crédito. Cada posible comprador debe darse previamente de alta, recibiendo un número de identificación personal (NIP) sólo utilizable en transacciones por Internet. Al hacer cada transacción, el comprador envía su NIP por correo electrónico al vendedor, el cual lo comprueba contra FV. Una vez realizada la operación de compra, FV solicita a través de correo electrónico la aceptación del comprador, por lo que no se precisa ningún elemento de cifrado para proteger los mensajes, y procede a

[7] Cybercash, 1999. (Disponible en http://www.cybercash.com)

realizar el cargo en la cuenta. FV se convierte así en un centro de compensación independiente de los bancos tradicionales y al liquidar las operaciones periódicamente, posibilita el uso de este medio para micro pagos.

CAPITULO II: METODOLOGÍA DE LA INVESTIGACIÓN

2.1. METODOLOGÍA DE LA INVESTIGACIÓN

2.1.1. TIPOS DE ESTUDIO

2.1.1.1. Descriptivo / Analítico

El propósito fundamental del estudio descriptivo analítico, es describir situaciones y eventos, en el cual se busca especificar las propiedades importantes de personas, grupos, comunidades o fenómenos sometidos a análisis, considerando además hechos relativos a su aparición, frecuencia y desarrollo, siendo estos medidos independientemente para describir lo que se investiga. Por lo tanto, se considera que este tipo de estudio, constituye la base para explicar y predecir el comportamiento de un fenómeno dado.

2.1.1.2.Exploratorio

Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si se desea

indagar sobre temas y áreas desde nuevas perspectivas o ampliar las existentes.

2.1.2. UNIDADES DE ANÁLISIS Y OBSERVACIÓN

Para realizar este estudio acerca de los procedimientos y técnicas para la obtención de evidencia en operaciones virtuales en empresas dedicadas al comercio electrónico fue necesario visitar las fuentes primarias de investigación, las cuales son: Empresas que realizan Comercio Electrónico de Bienes Muebles en El Salvador, estas pueden realizar dicho comercio por dos vías:

- A través de Un Canal virtual
- A través de una tienda virtual

2.1.3. TIPO DE INVESTIGACIÓN.

2.1.3.1. Bibliográfica

Se utilizaron fuentes primarias y secundarias, tales como: revistas, libros, periódicos, películas, boletines, tesis, etc., en el cual se desarrolló, investigó y se dio respuesta al tema, problema e hipótesis respectivamente, a través de un enfoque meramente teórico, fundado en una investigación bibliográfica exhaustiva.

2.1.3.2. Estudio de campo

En esta investigación se desarrolló el tema, problema, objetivos y planteamiento de la hipótesis, con el fin de arribar a las conclusiones y recomendaciones para generalizarse a toda la

población de donde se determinó la muestra, si esta es muy representativa. Sin embargo, la investigación se limitó a una, de campo descriptivo debido a que la problemática se desarrolló sin arribar a la prueba de hipótesis.

2.1.4.. DEFINIR UNIVERSO Y DETERMINACIÓN DE MUESTRA

2.1.4.1. Universo

El *Universo* para esta investigación fueron todas las empresas que realizan comercio electrónico de bienes muebles en El Salvador. (Ver Anexo 1)

Esta base de datos o listado del universo la obtuvimos por dos vías, a saber:

La primera de ellas fue a través de un concurso de paginas Web, en la cual existe la categoría de e-comerce que son las empresas que nos interesan para el estudio, este concurso denominado la "Arroba de Oro", se realiza anualmente a nivel Centroamericano, y la lista fue tomada de la sección de e-comerce de El Salvador período 2004.

La segunda vía fue a través de los medios de comunicación masiva como periódicos, televisión, radio., Internet y páginas amarillas,

2.1.4.2. Determinación de la Muestra

Para determinar la muestra se utilizó el método de Muestreo Aleatorio Simple el cual consiste en tomar una muestra al azar del universo.

Para determinar el tamaño de la muestra, se debe tener en cuenta que la población es finita, además las variables son cualitativas, y con un margen de error del 10%.

La formula para determinar la muestra es la siguiente:

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

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** Probabilidad de que el evento ocurra, es decir que las empresas dedicadas al comercio electrónico no realicen "auditorias de seguridad "(50%)
- **Q** Probabilidad de que el evento no ocurra, es decir que las empresas dedicadas al comercio electrónico realicen auditorias de seguridad. (50%)
- **N** Tamaño de la población (27 empresas)
- **E** Error máximo tolerable (15%)

$$n = \frac{1.96^2 (0.50)(0.50)(27)}{0.15^2 (27-1) \ + \ 1.96^2 (0.50)(0.50)}$$

$$n = \frac{25.9308}{1.5454}$$

$$n = 17 \text{ empresas}$$

La Muestra fue de 17 empresas que realizan comercio electrónico de bienes muebles.

2.1.5. INSTRUMENTOS PARA RECOLECTAR LA INFORMACIÓN

Para la recolección de la información se utilizaron varias técnicas e instrumentos a saber:

- Encuestas: Estas se realizaron y administraron a personal idóneo de las empresas y para ello se elaboraron Cuestionarios de preguntas abiertas / cerradas.
- Análisis de Documentos: Esta técnica se utilizó para analizar el material impreso, para la elaboración del marco teórico.
- Entrevista: Técnica orientada con el fin de establecer contacto directo con las personas que se consideran Fuentes de Información.
- Observación Directa: Esta técnica se utilizó para proporcionar una mayor seguridad en la obtención de información directa y confiable, el instrumento será la redacción de Narrativas.

2.2. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN RECOLECTADA

2.2.1. PROCESAMIENTO DE LA INFORMACIÓN.

La información recolectada mediante la investigación de campo, se procesó a través de las siguientes herramientas estadísticas:

- Distribución de frecuencias y representaciones gráficas
- Medidas de tendencia central
- Medidas de dispersión

Estas herramientas se ejecutaron en Microsoft Excel, a través del uso de tablas dinámicas.

2.2.2. ANÁLISIS DE LA INFORMACIÓN

El análisis de la información se hizo de forma ilustrativa y narrativa.

2.3. DIAGNOSTICO DE LA INVESTIGACIÓN

Se ha hecho un análisis de los aspectos más relevantes que influyen en la obtención de evidencias de auditoría en operaciones virtuales. Sin embargo es importante aclarar que de lo que se está hablado es de un tipo especial de Auditoría denominado “Auditoría de Seguridad”, y no hay que confundirla con otra, ya que el objeto de evaluación es diferente. Alrededor de esta consideración es que se ha dirigido la investigación esbozada en las páginas precedentes; por tanto la frase “evidencias virtuales” no atiende a su significancia

etimológica, sino más bien, busca denotar una cualidad de la evidencia obtenida, es decir, se está refiriendo al tipo de evidencia que surge de operaciones de las empresas que se dedican a comercializar en línea, siendo una gran parte ellas "operaciones virtuales", es decir, carentes de corporalidad y tangibilidad; pero no todas las transacciones realizadas a través del flujo del negocio son intangibles, los productos, los estados de cuenta, entre otros, se pueden ver y tocar. Por tanto, para este estudio se entenderá como evidencias virtuales "*cualquier hecho o circunstancia que sustente o refute una información obtenida durante el proceso de auditoria o evaluación del comercio electrónico en los componentes de seguridad*" ésta será la acepción o significado con la que se designara este término. En este estudio se ha determinado el ciclo de operaciones que realizan las empresas, al mismo tiempo se ha evaluado la seguridad del comercio electrónico en su conjunto, para poder estipular los riesgos asociados al mismo, con el objeto de establecer las técnicas y procedimientos para la evaluación y la obtención de evidencias, de tal manera que se pueda proponer las técnicas y procedimientos más apropiados y oportunos para las Auditorías de Seguridad, en este prototipo de negocio; para lo cual se ha dividido en cinco áreas o componentes esenciales en toda "auditoria de seguridad", en empresas que se dedican al comercio electrónico, las cuáles deben tomar en cuenta.

2.3.1.CONOCIMIENTO DEL NEGOCIO

Al igual que cualquier tipo de auditoría, el conocimiento del negocio es esencial, esto incluye, el volumen de operaciones, los niveles de ingresos de un período, la cantidad de recurso humano con el que cuenta, segmentos de mercado, arquitectura del comercio, etc. Todo esto confluye para que el auditor se forme una idea de la magnitud de la compañía y de sus operaciones, con el ánimo de diseñar una estrategia efectiva que le permita una evaluación eficaz, eficiente y oportuna para poder dar una opinión razonable en la materia auditada. En este estudio en concreto, se tomó en cuenta este componente para poder hacer una abstracción de lo que se debería evaluar en base a la magnitud del comercio y de sus operaciones, resultando que la mayoría de compañías encuestadas se clasifican como mediana o pequeña empresa (alrededor de un 88.24%), en base a sus ingresos, empleados y volumen de operaciones.

2.3.2.LOGÍSTICA DE OPERACIONES

La logística de las operaciones es otro componente básico en este prototipo de auditoria, ya que es necesario evaluar la capacidad instalada que poseen los comercios para hacerles frente a las exigencias inherentes al negocio. Esta evaluación incluye factores fundamentales que no se deben dejar de lado como lo son: el tiempo de respuesta para cada pedido del

cliente, los pedidos rechazados durante un lapso de tiempo, el momento de facturación y los medios de pago aceptados.

En esta parte, tal como se mencionó en el análisis de la información presentada, una buena porción de las empresas encuestadas, poseen indicadores aceptables sobre su desempeño, para citar algunos, se tiene que, un 47.06% posee una capacidad de respuesta a los pedidos de 6 horas o menos, los productos que se transan a través de la red cumplen con las expectativas de los clientes ya que el 52.94% de las empresas no tienen rechazo en los productos enviados y el 88.24% de las empresas encuestadas tiene alguna infraestructura que les permite aceptar cuando menos alguna tarjeta de crédito.

2.3.3.SEGURIDAD EN LA RED (INTERNET)

Otro aspecto clave, objeto de evaluación es la seguridad que puedan proporcionar los comercios para la transmisión de información confidencial a través de Internet, tomando en cuenta que ésta, es una red pública y una autopista de información. Para ello, técnicamente, el problema está solucionado, con la utilización de técnicas criptográficas que codifican la información que transita a través de esta Red, utilizando ciertos protocolos que proporcionen dicha garantía, como lo son: SSL o SET, sin embargo, para esto, los servidores de las compañías donde está montado el comercio electrónico deben estar

certificados por una entidad autorizada para tal efecto; es allí donde precisamente se configura la evaluación de esta área.

Según estas consideraciones la mayor parte de empresas en este estudio, que se dedican a hacer transacciones y validaciones en línea, ya sea por cuenta propia o por cuenta de terceros, poseen un certificado de seguridad, lo cual proporciona la certeza razonable que poseen un sitio web seguro y por lo tanto brindan un canal seguro para la transferencia de información en cualquier vía.

2.3.4.SEGURIDAD Y CONFIDENCIALIDAD CON LA INFORMACIÓN ALMACENADA DE LOS CLIENTES.

Este componente fundamental de evaluación y quizá en países desarrollados el más importante, por las implicaciones que la información personal pueda tener en cualquier ámbito. En este punto, los clientes se muestran reticentes a enviar datos que contengan información personal, si el comercio que lo solicita no es fiable, si este hace un uso abusivo de dicha información. Por lo tanto esto se vuelve un aspecto que necesita una supervisión continua y políticas de seguridad robustas, entre estas debe ser la misma arquitectura del comercio electrónico. En el estudio que se ha llevado acabo se puede verificar que las empresas almacenan información muy importante de la vida del consumidor, como lo es: su nombre y su número de tarjeta de crédito, estos datos son muy importantes para el cliente, por

las implicaciones económicas y jurídicas que esto trae. Otro factor importante es el uso que se le da a los datos de los clientes, un 87.92% de las empresas los utilizan para hacerse un perfil del cliente, ya que de esta manera pueden enviar ofertas y/o publicidad, ajustado a las necesidades perfiladas, lo cual si se hace un uso irrestricto y abusivo de este medio de publicidad puede causar molestias al consumidor. Un aspecto bastante preocupante es la arquitectura de comercio electrónico montada por algunas empresas (47.06%) ya que personas externas y fuera del ámbito de control de ellas, puede tener acceso a la información del consumidor, siendo esto una amenaza no sólo para el consumidor, sino también para la imagen del comercio.

2.3.5.SEGURIDAD FÍSICA Y LÓGICA INTERNA

Por último hay otro aspecto que no deja de ser relevante, las medidas y políticas de seguridad que las empresas tengan para con el hardware y software que soportan el comercio electrónico, tanto en elementos físicos como lógicos. Ello puede determinar las garantías que internamente se pueden implementar para salvaguardar el equipo (físico) y para salvaguardar el sistema (lógico). En este estudio algunas empresas no cuentan con estas garantías de seguridad por no poseer un servidor propio (52.94%) lo que implica que no administran de primera mano el comercio electrónico, además aunque en un porcentaje muy pequeño (11.76%), algunas de ellas han sido victimas de algún fraude.

CAPITULO III:

PROPUESTA DE TÉCNICAS Y PROCEDIMIENTOS DE AUDITORÍA PARA LA OBTENCIÓN DE EVIDENCIAS VIRTUALES EN EMPRESAS QUE SE DEDICAN AL COMERCIO ELECTRÓNICO EN EL SALVADOR.

3.1. ASPECTOS INTRODUCTORIOS

Se ha hecho una investigación en empresas que realizan comercio electrónico para conocer su arquitectura o estructura de operaciones, con el propósito de generalizar y de esa forma categorizar y definir por áreas de importancia relativa las transacciones virtuales que dichas empresas realizan. Para lo cual, tal como se puede apreciar en el resultado de la encuesta (Ver anexo 2.2), se han determinado dos modelos diferentes de operación del comercio electrónico, en cuanto a su arquitectura; los cuales serán explicados en esta sección, esto con el fin de diseñar las técnicas y procedimientos de auditoría idóneos y oportunos de aplicación general para ambas estructuras de E-commerce (comercio electrónico) que actualmente opera en El Salvador. Es importante aclarar que esta investigación **no está enfocada a la planeación de auditoría**, no obstante se retomaran ciertos aspectos de dicho proceso, ya que son indispensables para llevar acabo lo que se pretende realizar. Por tanto, a continuación se ha elaborado una guía de procedimientos con sus respectivas técnicas, consecuente y metódica, que el auditor

debe seguir para obtener evidencias virtuales en una auditoría de comercio electrónico.

3.2. CONOCIMIENTO DEL NEGOCIO

El conocimiento del negocio o del cliente es uno de los aspectos preponderantes en toda auditoría de cualquier naturaleza (Financiera, Gubernamental, Integral, Tributaria, entre otras.), puesto que es una primera aproximación a la estructura organizativa y al entorno del negocio, con todo lo que esto implica, en tanto es necesario que, "Al desempeñar una auditoría [...], el auditor debería tener u obtener un conocimiento del negocio suficiente para que sea posible al auditor identificar y comprender los eventos, transacciones y practicas que, a juicio del auditor, puedan tener un efecto importante [...] o en el examen o en el dictamen de auditoría"[8]. Este conocimiento esta íntimamente relacionado con la identificación de áreas criticas en donde los riesgos inherentes y de control pueden ser altos, y por supuesto, para determinar el alcance y la naturaleza de los procedimientos de auditoría que se han de correr.

En el caso que nos ocupa, el conocimiento del negocio, servirá de marco de referencia dentro del cual el auditor ejerce su juicio profesional, tal como lo estipula la Norma Internacional

[8] Norma Internacional de Auditoria 310, Párr. 2

de Auditoria 300 Párr. 9, asi dicho conocimiento y comprensión del negocio se utiliza para:

a) Evaluar riesgos e identificar problemas y
b) Evaluar evidencia de auditoría.

A continuación se hace una descripción de la estructura y funcionamiento de los dos prototipos de arquitectura de comercio electrónicos utilizados en El Salvador.

3.2.1. COMERCIO ELECTRÓNICO EN TIENDA VIRTUAL

Este es aquel en el cual se realizan operaciones de negocios a través de un canal virtual, siendo este el único medio de distribución, el cual no posee un escaparate físico, sino que la pantalla de la computadora sirve para mostrar y vender la mercadería. Este posee las siguientes características:

- Posee una estructura organizacional relativamente pequeña,
- No posee una plaza física y
- Tiene poca inversión en activo fijo.

Sobre la base del estudio realizado y diagnostico determinado en el capitulo dos, se ha establecido, que en el país este tipo de comercio electrónico adopta dos arquitecturas o estructuras de operación básicas, las cuales se detallan a continuación:

3.2.1.1. Tienda Virtual en Sentido Estricto: como Vendedor

3.2.1.1.1. Definición

Estas son aquellas empresas que adquieren productos para venderlos de forma directa a sus clientes y por consiguiente

asumen los riesgos de envió de la mercadería, al igual que un vendedor tradicional, con la diferencia que no se tienen inventarios físicos sino que se posee, generalmente, un sistema de inventarios "*justo a tiempo*"[9] .

3.2.1.1.2. Características Particulares:

- Asume riesgo de Envió: Esto significa que al recibir un pedido, es la misma empresa quien se encarga de realizar el envió, ya sea con su propio personal o través de subcontrataciones.
- Posee un Sistema de Inventario "Justo a Tiempo": esto significa que en la medida que se reciben ordenes de productos específicos, se realizan los pedidos a los proveedores, con la finalidad de no incurrir en costos de mantenimiento de inventario, ofrecer y mantener una diversidad de artículos, ofrecer artículos sin riesgos de obsolescencia, deterioro o daños, y sobre todo evitar una gran carga financiera con el capital inmóvil que representa el inventario. De aquí se deduce que ésta posee un inventario, pero bajo un sistema especial.
- Los clientes no conocen al proveedor del artículo comprado al vendedor: Esto en virtud a que la empresa es la que asume los riesgos de envió y los riesgos de imagen; por lo tanto se constituye en la responsable de cualquier problema e inconveniente que se suscite con respecto al producto o envió

[9] Eficiencia en sus tres bases fundamentales: cliente, proveedor y courier.

y por lo tanto el proveedor del articulo queda libre de responsabilidad en cuanto a logística del envió o reclamo por parte del cliente (por daño durante el envió, por especificaciones erróneas del articulo, etc.).

3.2.1.1.3. Procedimiento de Comercialización de un producto:

Después de haber conceptualizado este tipo de comercio electrónico y descrito sus características esenciales, se detalla el procedimiento generalizado que sigue una orden de compra (pedido por parte del cliente) en este tipo de negocios.

Procedimiento:

1. El cliente accesa por medio de una terminal conectada a Internet al sitio web de la tienda virtual.
2. Selecciona el producto que desea adquirir, previo lectura de precio, políticas de envió, devolución y otras especificaciones vinculadas con el producto.(Este paso puede repetirse dependiendo del número de productos que quiera adquirir)
3. Confirmación de selección del producto.
4. Inicia el procedimiento de pago, el cual tiene las siguientes fases:
    a. Solicitud de información personal del cliente por parte del comercio, la cual puede ser variada de acuerdo a la tienda virtual (nombre, teléfono, dirección, numero de tarjeta de crédito o débito o medio de pago electrónico, entre otras)

b. Confirmación de pedido y pago de producto, tiene dos formas

   i. Si es en línea, la confirmación es inmediata (cuestión de segundos)

   ii. Si es a través de un proceso análogo, la confirmación puede tardar un poco mas (cuestión de horas).

5. Cuando el pago se ha efectuado, la orden de compra llega a la empresa virtual, en donde se captura y se envía el pedido al proveedor para que este lo entregue en el tiempo especificado según contrato al comercio.
6. El proveedor recibe la orden de compra y realiza su gestión hasta entregar el producto a la tienda virtual.
7. Cuando la tienda ha recibido el artículo, revisa las especificaciones y condiciones del producto.
8. Luego pasa a despacho para ser enviado al cliente, de manera directa o a través de un subcontratante.
9. Realiza el proceso Post venta, consultando al cliente acerca de la satisfacción del pedido recibido
10. Si existiera causales para una devolución el proceso se realizará en base a políticas especificadas según empresas.

(Ver anexo 3.1.)

3.2.1.2. Tienda Virtual en Sentido Amplio: Como Intermediario

3.2.1.2.1. Definición:

Este tipo de empresas son las que operan típicamente como un intermediario entre el comercio y el cliente, como encargadas de efectuar la validación, los cobros en línea y el mantenimiento del sitio web, absteniéndose de soportar los riesgos de envió y de imagen.

3.2.1.2.2. Características Particulares:

- No Asume riesgo de Envió: Esto debido a que por su propia naturaleza actúa como un intermediario entre el cliente y el comercio, siendo este ultimo quien asume la responsabilidad de envió; ya que cuando la tienda virtual recibe un pedido, de manera directa lo pasa a su proveedor, el cual puede o no ser conocido por el cliente, para que este conozca las especificaciones de dicho pedido y comience con la gestión del mismo, culminando con la entrega del producto al cliente y de aquí surge su denominación "*En sentido Amplio*".
- No posee inventario: Esto es lógico, debido a que únicamente sirve como intermediario y por lo tanto no tiene la necesidad de poseer un inventario, sino que solamente se encarga de informar de los pedidos u ordenes de clientes al proveedor para que éste realice la gestión correspondiente (logística de entrega).
- Los clientes generalmente conocen al proveedor: esto como una estrategia de mercadeo, ya que las empresas utilizan la imagen

y posicionamiento del mercado que tienen los proveedores, a tal grado que en su pagina web principal vinculan a los clientes, según artículos, con las paginas web de los proveedores creadas especialmente por la tienda virtual, por lo tanto de una manera aparente los clientes contratan con los proveedores a los cuales les realizan los pedidos, aunque en esencia es la tienda virtual quien tiene dominio de la transacción. Dentro de esta, existe una excepción y es que algunas veces los proveedores no son conocidos por los clientes y por lo tanto la tienda virtual no explota el nombre comercial de dicho proveedor, esto sin menoscabo de la función que este último tiene de asumir el riesgo de envió.

Aclaración Importante: Muchas veces, los proveedores conocidos por los clientes, es decir, aquellos de los cuales la tienda virtual esta explotando su imagen y prestigio, tienen la idea que son empresas que poseen un canal virtual para la comercialización de sus productos y precisamente así lo promocionan en anuncios publicitarios, no obstante, no cumplen las características básicas de una empresa de E-commerce con canal virtual (ver sección siguiente), por lo que solamente se ven limitadas a ser proveedores de una tienda virtual en sentido amplio. Por lo general este tipo de empresas poseen las siguientes características:

Solamente se encarga de la logística de las operaciones, Por lo general no cuentan con servidor propio, No necesitan montar una

estructura tecnológica de Internet, No procesan pagos en línea, No manejan el riesgo de seguridad en línea, No incurren en el riesgo de seguridad física y logística del comercio electrónico, No almacenan información de los clientes, No poseen personal encargado específicamente del comercio electrónico, Poseen muy bajos costos en el mantenimiento del canal virtual.

3.2.1.2.3. Procedimiento de Comercialización de un producto

Una vez descritas las características esenciales y básicas de las tiendas virtuales en sentido amplio se narra de manera general el proceso de las operaciones de dicha arquitectura de negocio.

Procedimiento:

1. El cliente accesa por medio de una terminal al sitio web de la tienda virtual o directamente al sitio web del proveedor que para tal efecto ha diseñado la tienda virtual.
2. Selecciona el producto que desea adquirir, previo lectura del precio, políticas de envió, devolución y otras especificaciones vinculadas con el producto (Este paso puede repetirse dependiendo del número de productos que quiera adquirir).
3. Confirmación de selección del producto.
4. Inicia el proceso de pago, el cual tiene los siguientes procedimientos:
    a. Solicitud de información personal del cliente por parte del comercio, la cual puede ser variada de acuerdo a la

tienda virtual (nombre, teléfono, dirección, número de tarjeta de crédito o debito o medio de pago electrónico, entre otras).

b. Confirmación del pedido y pago del producto, tiene dos formas:

   i. Si es en línea, la confirmación es inmediata (cuestión de segundos).

   ii. Si es a través de un proceso análogo, la confirmación puede tardar un poco más (cuestión de horas).

5. Cuando el pago se ha efectuado, la orden de compra llega a la empresa virtual, en donde se captura y se envía el pedido al proveedor para que este asuma la responsabilidad y riesgos de envío.
6. El proveedor recibe la orden de compra y realiza su gestión hasta entregar el producto al cliente.
7. Se realiza el proceso Post venta, consultando al cliente acerca de la satisfacción del pedido recibido.
8. Si existiera causales para una devolución el proceso se realizara en base a políticas especificadas según empresas.

(Ver Anexo 3.2.)

3.2.2. COMERCIO ELECTRÓNICO EN CANAL VIRTUAL

Estas son empresas que poseen diversos canales de distribución de sus productos en los cuales está incluido el canal virtual, por lo general éstas ya tienen un posicionamiento del mercado

con una imagen establecida, y sus operaciones comerciales ya están plenamente establecidas. Su forma de operar con respecto al canal virtual es de manera análoga a las Tiendas Virtuales en Sentido Estricto, (Ver apartado 3.2.1.1) Con la diferencia que éstas mantienen inventario y por consiguiente no utilizan el sistema de inventario Justo a tiempo.

Las Características Básicas de este tipo de empresas son las siguientes: Posee una estructura organizacional relativamente grande, Posee una plaza física y una plaza virtual (canal virtual), Posee un Inventario Físico, Tiene gran inversión en activo fijo, Asume los riesgos de envió, Sus proveedores no son conocidos por el cliente, entre otras.

Los proceso y procedimientos que sigue un pedido en las empresas con un canal virtual, son los mismos que para las tiendas virtuales en sentido estricto, con la diferencia que en el punto seis no se hace referencia al proveedor sino mas bien la bodega de la misma empresa. Hay que recordar que este tipo de comercio posee un stock de inventario, y por lo tanto una bodega con su personal correspondiente, asi como también, tiene sus políticas de manejo y mantenimiento de inventario.

3.2.3. DETERMINACIÓN DE ÁREAS DE RIESGO.

Según la investigación realizada, se han establecido, en todas las arquitecturas o estructuras de comercio electrónico, cuatro

áreas de riesgo las cuales engloban todo el accionar de los E-commerce. Estas áreas son las siguientes:

3.2.3.1.Logística de operaciones.

En donde se tienen riesgos asociados sobre:

- Eficiencia y eficacia de la empresa frente a las exigencias de los clientes.
- Satisfacción de expectativas de los consumidores.
- Calidad de los productos ofrecidos a través del sitio web
- Procesamiento de las órdenes de compra.
- Capacidad de respuesta y tiempos de envío de pedidos.
- Posibilidades de devoluciones.
- Medios de pago aceptados y Procedimiento de pagos.
- Validaciones de tarjetas de crédito y débito.
- Facturación de pedidos.

3.2.3.2.Seguridad en la Red (Internet).

Esta área comprende los siguientes riesgos asociados:

- Transacciones en línea.
- Posesión de un servidor seguro (SSL).
- Vigencia del certificado de seguridad.
- Empresa certificador y Calidad del certificado.

3.2.3.3.Seguridad y confidencialidad con la información almacenada de los clientes.

Esta área comprende los riesgos siguientes:

- Tipo de información almacenada de los clientes.

- Medidas y políticas de control y seguridad con la información de los clientes.
- Acceso del personal interno a la información en cuestión.
- Acceso de personas extrañas (externos) a la información de los clientes.
- Uso y manejo de la información.

3.2.3.4.Seguridad Física y Lógica.

Comprende los siguientes riesgos asociados:

- Software

i. Robustez del sistema operativo y Cortafuegos (Firewall).

ii. Claves escalonadas o diferencias para el acceso a la información.

iii. Respaldos de información y Antivirus

iv. Aplicaciones conexas de desarrollo y aplicación de sitios web.

v. Velocidad de la conexión a Internet

vi. Actualizaciones. Y Licencias.

- Hardware

vii. Capacidad del servidor tanto en procesamiento como en almacenamiento.

viii. Seguridad física del hardware y de la red.

ix. Seguridad de los dispositivos de almacenamiento.

- Conexiones a Internet

x. Velocidad de la conexión.

xi. Eficiencia, eficacia y responsabilidad del proveedor del servicio.

Una vez conceptualizada y descrita la estructura básica, para cada una de las arquitecturas de comercio electrónico y las áreas de riesgo que son interés para la evaluación, se sugiere una guía de técnicas y procedimientos para tener un conocimiento suficiente del negocio, que ayude a realizar de manera eficiente y eficaz una auditoría de seguridad para los E-commerce; tomando en cuenta que el auditor, puede tomar de base los modelos de arquitectura de comercio electrónicos explicados en esta investigación, de tal manera que no será necesario –al menos por un tiempo que el auditor dedique esfuerzos redundantes para determinar la estructura general del negocio examinado, por lo cual con esta guía se pretende que el auditor determine la diferencia, en cada caso concreto, el prototipo de arquitectura de comercio electrónico (según como se han establecido en esta sección), para que pueda enmarcar su auditoria de acuerdo a las características y particularidades de cada estructura de E-commerce.

3.2.4. TÉCNICAS Y PROCEDIMIENTOS DE AUDITORIA PARA OBTENER EL CONOCIMIENTO DEL NEGOCIO

A continuación se presenta un instrumento, el cual contiene los procedimientos con sus respectivas técnicas de auditoria, para obtener evidencia respecto al conocimiento del negocio.

GUÍA PARA EL CONOCIMIENTO DEL NEGOCIO

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: Conocer apropiadamente el negocio, el tipo de arquitectura de comercio electrónico, determinación de riesgos asociados en las distintas áreas de seguridad.

Objetivo de la evaluación: Conocer de manera general el volumen de operaciones de comercio electrónico que realizan las empresas, a través de un canal virtual o de tienda virtual (arquitectura del e-commerce). Con el fin de determinar la materialidad y la importancia relativa de las operaciones y áreas de seguridad de las empresas

REF	Actividad que será Evaluada	Procedimiento de Auditoria	Herramientas que serán utilizadas	Observación
	Determinar condiciones económicas que afectan al negocio	Determinar las empresas de comercio electrónico que son la principal competencia del cliente. Determinar los productos que ofrece el cliente.	❑ Revisión: de los Sitios Web que ofrecen productos similares ❑ Revisión: del Sitio Web de la Empresa, realizando una lista de los productos ofertados. ❑ Inspección: de los Artículos ofrecidos	
	Evaluar la administración y propiedad de la entidad	Determinar el tipo de empresa en base a lo mercantil. Conocer quienes son los dueños y cómo esta compuesto el patrimonio de la empresa. Conocer la estructura organizacional de la empresa.	❑ Revisión Documental de: Escritura de Constitución y Organigrama. ❑ Entrevista con Funcionarios de la empresa, corroborando niveles Jerárquicos	

	Evaluar la Actividad de administración y gestión de la tienda virtual o canal virtual.	Solicitar la visión, misión, objetivos, metas de la administración. Evaluar la existencia, congruencia y apego a la estructura organizacional. Evaluar la existencia y aplicación del perfil de puestos para la selección y promoción del personal del área. Evaluar la división adecuada del trabajo y departamentalización de las funciones y actividades del personal. Evaluar las relaciones personales y de trabajo entre los directivos y empleados. Evaluar la suficiencia o carencia de personal o recursos informáticos para cumplir con las actividades del área	❑ Entrevista: con el Gerente General de la Empresa ❑ Revisión de Organigrama y Manual de Puestos de la Empresa. ❑ Observación Participativa ❑ Revisión de Manual de Procedimientos. ❑ Entrevista con empleados del área de ventas (e- commerce)	
	Determine el número de empleados de la empresa	Solicitar al gerente el número de empleados que laboran en la empresa y luego Contrastar la respuesta solicitando la planilla de pago	❑ Entrevista: con el Gerente ❑ Revisión Documental de la planilla de pago ❑ Observación Participativa	

	Determinar el promedio de ingresos mensuales del comercio electrónico	Solicitar al encargado de ventas el monto de las ventas del comercio electrónico del mes anterior. Verificar dicho dato, con el encargado de contabilidad	❑ Revisión Documental: de las Ventas e-commerce.	
	Determinar la naturaleza del E-commerce: estructura o arquitectura	Determine si posee inventarios la empresa Determine si corre los riesgos de envió e imagen. Determine si los clientes conocen a los proveedores de la empresa	❑ Inspección de los Inventarios ❑ Revisión Documental de: Políticas de Venta y Envío la Empresa. ❑ Entrevista a Clientes	
	Evaluar la existencia de inventarios de la empresa	Conocer si poseen inventarios físicos Determinar el sistema de inventarios que utilizan Evaluar la eficiencia y eficacia del manejo de sus inventarios	❑ Revisión de la Arquitectura del e- commerce ❑ Inspección de los Inventarios Físicos que la empresa posee. ❑ Entrevista: para conocer las Políticas. ❑ Revisión de tarjetas de Inventarios	
	Determinar los proveedores importantes de la empresa	Solicitar la lista de los proveedores usuales de la empresa. Realizar la confirmación de algunos de ellos. Determinar las competencias del proveedor con respecto al pedido.	❑ Revisión Documental de Lista de proveedores, entregada por área: e-commerce. ❑ Confirmación por escrito a Proveedores. ❑ Revisar los	

			Contratos existentes con Proveedores.	
	Determinar el número de pedidos que recibe cada día	Realizar una evaluación durante un día, verificando todos los pedidos que se efectúan, realizar este proceso por lo menos dos veces más en un período corto. Solicitar al Gerente de Ventas la cantidad promedio de ventas recibido por día, según temporada	❑ Observación Participativa, en el proceso de pedidos por día. ❑ Revisión documental de Ventas por Cliente	

3.3. ÁREA DE SEGURIDAD EN LOGÍSTICA DE OPERACIONES

3.3.1. DEFINICIÓN

Esta área es un punto muy importante a evaluar y asegurar, ya que representa la imagen de la empresa dentro de un mercado competitivo y difícil de posicionarse, por lo tanto, es menester que los gerentes y auditores le presten suma atención, ya que trasciende a la parte técnica de redes y componentes informáticos(hardware y software), y pasa a ser un componente vital, donde confluyen los elementos de una buena gestión de negocios con el conocimiento informático de e-commerce; que fusionados de una manera correcta lograrán que la entidad funcione de manera eficiente y eficaz en el desempeño de sus actividades.

3.3.2. CONDICIONES PARA POSEER SEGURIDAD

Para que una empresa dedicada al comercio electrónico, posea una logística de operaciones segura, **debe cumplir con los siguientes criterios**:

- Seguir una política de marketing que tenga como principal estrategia el servicio de atención al cliente.
- Satisfacer las expectativas del cliente en cuanto a las especificaciones del producto adquirido.
- Poseer eficacia en los procesos de pago y envío de productos.
- Debe poseer políticas de devoluciones claras y precisas.
- Debe existir una facilidad de compra, de medios de pago aceptados, de facturación y procesamiento de órdenes de compra, de navegabilidad, diseño e idiomas.
- Ser eficiente en la relación cliente-vendedor-courier.

3.3.3. RIESGOS ASOCIADOS

De lo anterior se deducen los **Riesgos existentes en esta área o Riesgos Asociados (Inherentes)**:

- Satisfacción de expectativas del cliente
- Eficacia en cuanto a que el producto entregado al cliente cumpla con las especificaciones.
- Eficacia en el proceso de venta: facilidad de compra, aceptación de medios de pago, facturación de producto, elaboración de orden de compra, envío del producto.
- Eficiencia en cuanto al tiempo de entrega del producto.

- Existe la posibilidad de devoluciones

3.3.4. MEDIDAS DE CONTROL PARA LA DISMINUCIÓN AL MÍNIMO DE LOS RIESGOS ASOCIADOS

Para disminuir estos riesgos al mínimo, las empresas deben:

- Establecer políticas en las cuales los productos que se muestran en la Vitrina Virtual (escaparate) cuenten con especificaciones establecidas.
- Poseer claridad en cuanto al la arquitectura del comercio electrónico que se realiza para poder comprender y manejar el proceso de operación de ventas que se sigue o adopta.
- Establecer políticas en las cuales se determine de manera inequívoca, la forma de realizar el envío, la entidad responsable de realizarlo, los tiempos máximos y mínimos de entrega considerando el área o región en donde el producto será entregado.
- Asegurarse que los productos que adquieran los clientes sean entregados en base:
    - Si es una tienda virtual en sentido estricto, se deben subcontratar los servicios de envío del producto, con el objetivo de disminuir los riesgos asociados tales como: extravió, avería, etc.
    - Si es una tienda virtual en sentido amplio, se debe especificar en los contratos efectuados con los proveedores, cláusulas claras respecto a que la calidad

de productos que se esta ofreciendo sea la misma que envían los proveedores a los clientes.

- Establecer políticas de devoluciones de productos, especificando los supuestos de hecho, para que estas procedan.

Cabe aclarar que la logística de operaciones, y por lo tanto la forma de validar su seguridad, variará en base a la arquitectura o estructura del comercio electrónico que se posea (Ver *sección 3.2.1. y 3.2.2. conocimiento del negocio*) pero que para efectos de la propuesta, los modelos son aplicables, con algunas diferencias que se detallaran en su oportunidad, a todo tipo de comercio electrónico.

3.2.5. TÉCNICAS Y PROCEDIMIENTOS DE AUDITORIA PARA LA EVALUACIÓN

A continuación se presentan los instrumentos de evaluación referentes a esta área: el cuestionario de control interno, como una primera aproximación para una comprensión suficiente de la logística de operaciones y un programa de auditoria en el cual se describen taxativamente los procedimientos con sus respectivas técnicas de auditoria, necesarias para la evaluación de la seguridad en esta área, por consiguiente, para corroborar la existencia de las medidas de control, con el fin de atenuar al mínimo los riesgos asociados, con miras a determinar, si existe o no, una gestión segura de la logística de operaciones del comercio electrónico según su arquitectura, se sugiere lo siguiente:

1. Pasar un cuestionario, a los encargados de informática de cada E-commerce como una primera aproximación al conocimiento especifico de esta área

CUESTIONARIO PARA LA EVALUACIÓN
DE LA SEGURIDAD EN LA LOGISTICA DE OPERACIONES

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: Satisfacción de las expectativas del cliente en cuanto a la eficiencia del tiempo de entrega del producto y eficacia de las especificaciones del producto, así como del proceso logístico de venta.

Objetivo de la evaluación: Conocer la capacidad instalada que poseen las empresas para hacer frente a las exigencias de este modelo de negocios, así como para asegurar que la logística de operación de venta al recibir un pedido u orden de compra es eficiente y eficaz. Todo esto incluye el tiempo de respuesta para cada orden, los pedidos rechazados durante un lapso de tiempo, el momento de facturación, los medios de pago aceptados, el proceso de envió del producto y políticas de devolución.

N°	Preguntas	Si	No	N/A	Comentarios
1	¿En el sitio Web los productos tienen especificaciones claras de los mismos?				
2	¿Estos detalles o especificaciones se pueden conocer antes de haber adquirido o cancelado el producto?				
3	¿Se puede seguir agregando productos al “carrito de compras” hasta que se esté listo para pagar?				
4	Cuando un cliente tiene duda acerca de un producto o acerca de cómo llenar un formulario de datos personales, ¿Puede dirigirse a la empresa y ésta le responde eficientemente?				
5	¿A cuánto asciende el promedio de pedidos recibidos durante el día (24 horas)? ❑ 0-10 ❑ 11-20 ❑ 21-40 ❑ 41-60				

	❑ 61 o más				
6	¿El tiempo promedio de respuesta a los pedidos se hace de manera inmediata?				
7	¿Se confirma el pedido realizado a través de un correo electrónico o llamada telefónica al cliente?				
8	¿Qué medios de pago acepta la empresa? ❑ Tarjeta de Crédito ❑ Tarjeta de Debito ❑ Contra reembolso ❑ Transferencia bancaria ❑ Financiación				
9	Si el pago es a través de tarjetas de crédito, ¿Cuándo se recibe el número de la misma? el proceso de pago es: ❑ Convencional con el Sistema POS, y la notificación se hace de manera mediata ❑ El servidor esta conectado con la red de pagos y automáticamente se hace la notificación.				
10	¿Cuándo se confirma el pago es cuando se envía la orden de venta a bodega o a los proveedores?				
11	¿Qué tipo de arquitectura de comercio electrónico posee la empresa? ❑ Tienda Virtual en sentido estricto o Canal Virtual ❑ Tienda Virtual en sentido Amplio				
12	Dependiendo del tipo de arquitectura del comercio electrónico: ❑ <u>Tienda Virtual en sentido Estricto o Canal Virtual</u>: Cuándo se confirma el pago, ¿Es cuando se envía la orden de venta a los proveedores o a bodega para que envíen en producto a despacho? ❑ <u>Tienda Virtual en sentido Amplio</u>: Cuándo se confirma el pago, ¿Es cuando se envía la orden a los proveedores para que envíen el producto a los clientes?				
13	Dependiendo del tipo de arquitectura del comercio electrónico:				

	❑ Tienda Virtual en sentido Estricto o Canal Virtual: ¿La empresa utiliza su propio personal para la entrega del producto? ¿La empresa posee una subcontratación para entregar el producto y disminuir riesgos de envío? ❑ Tienda Virtual en sentido Amplio: ¿Existe un contrato con el proveedor donde establezca la cláusula en la cual éste último se compromete a entregar un producto de manera eficiente (tiempo de entrega) y eficaz (calidad del producto).				
14	¿Cuál es el tiempo de entrega de los productos? ❑1 día ❑2 días ❑3 días ❑4 días ❑5 días o más				
15	¿ Todos los productos se ofrecen con envío sin restricciones de lugar o país? (debe existir una cláusula o información acerca de esto en la página Web)				
16	¿En qué momento se factura el pedido del cliente? ❑Cuando se recibe el pedido ❑Cuando se recibe el pago ❑Cuando se envía el producto ❑Cuando se entrega el producto ❑				
17	En caso de consultas sobre envíos específicos ¿Puede el cliente dirigirse, esperando una solución o respuesta, a la tienda o canal virtual?				
18	¿Posee la empresa una política de posventa?				
19	Si posee dicha política ¿a través de qué medio hace la confirmación del producto? ❑ Correo electrónico ❑ Confirmación escrita ❑ Llamada telefónica				
20	¿El cliente tiene la posibilidad de devolver el producto si no le gusta o le sale defectuoso?				
21	¿La devolución del producto consiste en remplazar el producto?				

22	¿Existe la posibilidad de rembolsar el dinero obtenido del cliente, del producto devuelto?				
23	¿El número de pedidos rechazados o devueltos en el mes por los clientes es aceptable o bajo?				
24	¿Cuál es el promedio de pedidos (en porcentaje) rechazados por el cliente en el mes? ❑ 0-10 ❑ 11-25 ❑ 25-50 ❑ 50 o más				
25	¿Es la tienda o canal virtual la responsable de cualquier reclamo o devolución por parte del cliente?				

2. Una vez obtenidas las respuestas, es necesario corroborarlas a través de pruebas de control, para lo cual se sugieren las siguientes técnicas y procedimientos de auditoria, materializadas en el programa que a continuación se presenta:

PROGRAMA DE AUDITORIA
PARA EVALUAR LA SEGURIDAD EN LA LOGISTICA DE OPERACIONES

Cliente: _____
Periodo de auditoría: _____

Factor de riesgo: Satisfacción de las expectativas del cliente en cuanto a la eficiencia del tiempo de entrega del producto y eficacia de las especificaciones del producto, así como del proceso logístico de venta.

Objetivo de la evaluación: Conocer la capacidad instalada que poseen la empresa para hacer frente a las exigencias de este modelo de negocios, así como para asegurar que la logística de operación de venta al recibir un pedido u orden de compra es eficiente y eficaz. Todo esto incluye el tiempo de respuesta para cada orden, los pedidos rechazados durante un lapso de tiempo, el momento de facturación, los medios de pago aceptados, el proceso de envió del producto y políticas de devolución.

N°	PROCEDIMIENTO	Ejec.	Hecho	Fecha	Refer.
1	Solicitar el catálogo de productos que ofrece la tienda y Revisar si cada producto posee especificaciones claras y precisas.				
2	Si no existe un catálogo de productos ofertados en el sitio Web: a) Entrevistarse con el gerente de ventas o e-commerce y hacer una narrativa en donde se pueda identificar las razones por las cuales no se ha elaborado. b) Comparar lo expuesto por el gerente ventas con lo que expresa el encargado de despacho o bodega				
3	Ingresar al sitio Web de la empresa y simular una compra y antes de pagar: ❑ Verificar si los productos ofrecidos tienen detalles o especificaciones claras. Leer detalles y capturar una pantalla. ❑ Verificar si se puede seguir comprando o seleccionando productos. capturar pantalla ❑ Verificar si existen indicaciones acerca de aclaraciones o dudas de productos o algún procedimiento. Capturar pantalla				
4	Realizar Punto Fijo: Observación participativa, durante un día completo (dicho día debe ser considerado normal, en una temporada normal) en el servidor de la entidad con el fin de: ❑ Verificar cuántos pedidos se reciben durante un día y documentarlo a través de una narrativa. ❑ Verificar el tiempo promedio que se tarda la empresa en confirmar el pedido a sus clientes. ❑ Verificar el medio utilizado por la empresa para confirmar el pedido a sus clientes.				
5	Ingresar al sitio Web de la empresa y simular una compra: ❑ Al momento de pagar, observe el medio o medios de pago que acepta la empresa. Capture la Pantalla ❑ Si se puede pagar con tarjeta de crédito, determine si dicho pago se notifica de manera inmediata, ❑ Observe si la confirmación de la compra se hace antes, durante o después del pago. Utilice una Narrativa				

6	Inspeccione en la empresa si se posee un Sistema POS para validar la operación de pago				
7	Dependiendo de la Arquitectura de comercio electrónico que posee la empresa, Observe: ❑ Tienda Virtual en sentido Estricto o Canal Virtual: Verifique si cuando se confirma el pago, es cuando se envía la orden de venta a los proveedores o a bodega para que envíen el producto a despacho. Documente a través de una narrativa ❑ Tienda Virtual en sentido Amplio: Verifique si cuándo se confirma el pago, es cuando se envía la orden a los proveedores para que envíen el producto a los clientes. Documente a través de una narrativa.				
8	Dependiendo de la Arquitectura de comercio electrónico que posee la empresa, Observe: ❑ Tienda Virtual en sentido Estricto o Canal Virtual: 1. Solicite a la empresa sus políticas de envió, y determine cual es la forma para realizarlo. 2. Si fuere realizado dicho envió, a través del personal de la empresa, solicitar los manuales de descripción de puestos, para determinar las funciones y responsabilidades de los empleados con el fin de disminuir los riesgos adheridos a dicha función de envío. 3. Si fuere bajo subcontrataciones, solicite una copia del contrato para determinar las competencias y responsabilidades de dichas entidades que prestan el servicio de courier ó ❑ Tienda Virtual en sentido Amplio: Solicite el contrato para verificar las cláusulas en donde se compromete el proveedor a entregar el producto en el tiempo mínimo previsto y en condiciones según especificaciones determinadas				
9	Sin importar la estructura del comercio electrónico, verifique, cuál es el tiempo promedio de entrega de los artículos, para esto: ❑ Ingrese a la página Web de la empresa y busque la sección de políticas de envío, en la cual debe especificar el tiempo de entrega según productos y localidad.				

	Capture la pantalla ❑ Entreviste al gerente de la empresa para solicitar información, basada en la experiencia, de cuanto es el tiempo de entrega de productos al cliente, ya sea que lo realice la misma empresa, subcontratantes o sus proveedores. ❑ Envié una confirmación a varios clientes seleccionados al azar, para corroborar el período de entrega de productos.				
10	Desarrolle el mismo procedimiento anterior para determinar si existen restricciones de envíos de productos en base a su localidad o país.				
11	Realizar una entrevista con el encargado de ventas o e-commerce para consultar el momento específico en que se factura el pedido. Las razones del porque ese momento. Redacte una Narrativa para sustentar. Verifique la respuesta del encargado de ventas, por medio de observar el proceso que sigue al recibir un pedido escogido al azar. Redacte una Narrativa para sustentar.				
12	Solicitar el manual de políticas y procedimientos de la empresa y verificar la existencia de políticas de postventa, en la cual se establece, entre otras: ❑ El mecanismo para confirmar la satisfacción del cliente con el producto vendido ❑ Evaluar la eficiencia de la empresa en el envió del producto				
13	Solicitar el manual de políticas y procedimientos de la empresa y verificar la existencia de políticas de devolución, en la cual se establece, entre otras: ❑ Si existe la posibilidad de devolver productos ❑ Cuáles son las causas que proceden para una devolución de productos ❑ Qué efectos tiene la devolución del producto, el reemplazo del artículo o el reembolso del dinero ❑ Si la empresa es la responsable de dicho reclamo o si traslada la responsabilidad al proveedor. Redacte una narrativa de dicho procedimiento				

14	Realice un procedimiento similar al anterior, solamente que a través de una Entrevista al encargado de e-commerce. Redacte una narrativa de dicho procedimiento				
15	Ingresar al sitio Web de la empresa y:: ❑ Verificar si existen las políticas de devolución escritas en la página Web. Capturar pantalla ❑ Si dichas políticas coinciden con la descrita en el manual de políticas de la empresa u opinión del encargado de e-commerce				

3. Dependiendo de los resultados de la evaluación obtenidos con la aplicación del programa propuesto, así será el riesgo de auditoria del área en cuestión, por tanto éste dependerá de la ponderación de los siguientes factores materiales:

a. Establecer políticas de e-commerce, en las cuales los productos que se oferten cuenten con especificaciones establecidas.

b. Poseer claridad en cuanto a la arquitectura del comercio electrónico, para conocer y aplicar correctamente la logística del mismo.

c. Establecer políticas de Envió especificas.

d. Seguridad de la eficiencia y eficacia de la entrega de productos.

e. Establecer políticas de devoluciones de productos, especificando los supuestos de hecho, para que estas procedan.

Para hacer la valoración del riesgo, se sugiere que se utilice el siguiente procedimiento: Si el resultado de la evaluación para cada uno de estos factores es favorable (sí se tienen políticas de e-commerce, sí posee claridad en cuanto a la arquitectura del comercio, sí se establecen políticas de envió clara, etc.) se le asigna una ponderación de 6 puntos; si la referida evaluación no es muy favorable, se le asignan 4 puntos; y si la evaluación es desfavorable es decir que no concurra ninguno de los factores señalados, la ponderación para cada uno será de 2 puntos. La calificación máxima que se puede obtener es de 30 puntos, esto dará un 100% de seguridad. El parámetro para validar la seguridad en esta área será del 90%, por debajo del cual se enciende la luz roja de alarma para el auditor, indicándole que existe una grave desviación y deficiencia en la seguridad correspondiente a esta región. A continuación se presenta una matriz ejemplificando el procedimiento antes descrito.

Área evaluada		**Factores de riesgo**					
		Establecimiento de políticas de e-commerce	Poseer claridad en cuanto a la arquitectura del comercio electrónico	Establecer políticas de Envió especificas	Seguridad de la eficiencia y eficacia de la entrega de productos	Establecer políticas de devoluciones de productos	Total
Seguridad en logística de operaciones	Ponderación	6	6	6	5	6	30
	Puntaje	20%	20%	20%	16.67%	20%	96.67%

3.4. ÁREA DE SEGURIDAD EN RED

3.4.1. DEFINICIÓN

Esta área representa un punto critico que amerita una evaluación taxativa por parte del auditor, ya que presenta los riesgos asociados de transmitir información confidencial a través de Internet, considerando que ésta es una red publica y que en ella transitan miles de datos, los cuales pueden ser interceptados por terceras personas (Hacker y/o Cracker Vándalo) pudiendo hacer un mal uso de la información robada.

3.4.2. CONDICIONES PARA POSEER SEGURIDAD

En tal sentido las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:

- Confidencialidad: evita que un tercero pueda *acceder a* la información enviada.
- Integridad: evita que un tercero pueda *modificar* la información enviada sin que lo advierta el destinatario.
- Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.
- No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación.

3.4.3. RIESGOS ASOCIADOS (INHERENTE)

Por tanto se pueden considerar los siguientes riesgos asociados (inherente) a esta área:

Utilización de una red pública para la transmisión de datos:

- Robo de información
- Alteración de información
- Autenticación del propietario del sitio Web
- Repudio

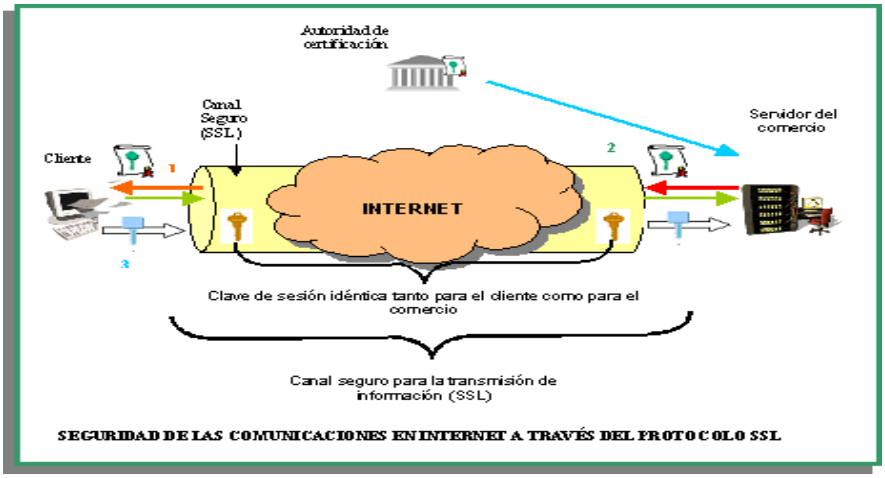
3.4.4. MEDIDAS DE CONTROL PARA LA DISMINUCIÓN AL MÍNIMO DE LOS RIESGOS ASOCIADOS

Para disminuir estos riesgos al mínimo, las empresas deben contar, con:

- Un servidor seguro, por lo menos con un protocolo de seguridad SSL (Secure Socket Layer) de 40 bits, el cual utiliza técnicas de encriptación asimétricas con un par de llaves: publicas y privadas (ver sección 1.5), además;
- La autoridad certificadora que proporciona el servicio de servidor seguro debe ser fiable (conocimiento en el mercado)
- La fecha actual de operancia del servicio, debe estar dentro del intervalo de vigencia del certificado de seguridad.

A continuación se muestra un esquema sobre el proceso que se sigue para establecer un canal seguro en la comunicación de datos sensibles a través de Internet utilizando el protocolo SSL.

Figura 1: Seguridad de Comunicaciones (SSL)



PROCESO DE UNA COMUNICACIÓN SEGURA A TRAVÉS DE INTERNET UTILIZANDO EL PROTOCOLO SSL

1. La fase **Hola**, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.

2. La fase de **autenticación**, en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).

3. La fase de **creación de clave de sesión**, en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.

4. Por último, la fase **Fin**, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

3.4.5. TÉCNICAS Y PROCEDIMIENTOS DE AUDITORIA PARA LA EVALUACIÓN

A continuación se presentan los instrumentos de evaluación referentes a esta área: el cuestionario de control interno, como una primera aproximación para una comprensión suficiente de la seguridad en red y un programa de auditoria en el cual se describen taxativamente los procedimientos con sus respectivas técnicas de auditoria, necesarias para la evaluación de la

seguridad en la transmisión de información a través de Internet, por consiguiente, para corroborar la existencia de las medidas de control, encaminadas a disminuir al mínimo los riesgos asociados, con miras a determinar, si existe o no, un canal seguro para la transmisión de información a través de Internet, entre el cliente y el comercio, se sugiere lo siguiente:

1. Pasar un cuestionario, a los encargados de informática de cada E-commerce como una primera aproximación al conocimiento especifico de esta área, para lo cual proporcionamos el modelo siguiente.

CUESTIONARIO PARA LA EVALUACIÓN DE LA SEGURIDAD EN LA TRANSFERENCIA DE INFORMACIÓN A TRAVÉS DE INTERNET Y LA AUTENTICIDAD DEL SITIO WEB

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: Transmisión de información confidencial a través de una red pública y autenticidad del Sitio Web

Objetivo de la evaluación: Determinar si el E-commerce posee una canal seguro para el tránsito de información entre el comercio y el cliente, y comprobar la autenticidad de Sitio Web (Si el Comercio es quien dice Ser)

N°	Preguntas	Si	No	N/A	Comentarios
1	¿Existe una persona encargada de velar por la seguridad de la red (vigilante) tanto interna como externa (Internet)?				
2	¿Se tienen políticas de seguridad para la transferencia segura de datos a través de Internet?				
3	¿Se puede garantizar a los clientes la autenticidad del sitio Web donde se tiene instalado el canal virtual?				
4	¿Se posee un certificado de seguridad emitido por una compañía autorizada?				

5	¿Cuál es el nombre de la compañía que ha emitido el certificado de seguridad?				
6	¿El certificado de seguridad esta vigente a la fecha?				
7	¿Se tiene un certificado de seguridad robusto?				
8	¿Cuántos bits tiene la longitud de clave en el proceso de encriptación (según el servicio contratado con la autoridad certificadora)?				
9	¿La autoridad certificadora es reconocida en el mercado?				
10	¿De qué nivel es la compañía certificadora?				
11	¿Se posee firma digital?				
12	¿Se puede proveer un canal seguro de transmisión de información a los clientes?				
13	¿Qué protocolo de seguridad se posee para una transmisión segura de datos?				
	En el caso de los comercios en sentido amplio preguntar adicionalmente lo siguiente:				
14	¿Se prestan servicios de Hosting para la independización de los comercios, de tal manera que ellos tengan la administración completa de su Sitio Web desde el diseño, la información en él contenida hasta que la validación del pago se haga por las mismas empresas independientes o terceras contratadas por estas, diferente al comercio?				
15	¿Para cada nombre de domino de los hosting en el servidor del comercio, se tiene un certificado de seguridad (para cada uno).				
16	¿Es el comercio (prestador del servicio) o la empresa alojada (prestataria) quien tiene la obligación de contratar un certificado de seguridad?				

2.Una vez obtenidas las respuestas es necesario corroborarlas a través de pruebas de control, para lo cual se sugieren las siguientes técnicas y procedimientos de auditoria:

PROGRAMA DE AUDITORIA
PARA EVALUAR LA SEGURIDAD ENTRANSFERENCIA DE INFORMACIÓN A TRAVÉS DE INTERNET Y LA AUTENTICIDAD DEL SITIO WEB

Cliente: _____

Periodo de auditoria: _____

Factor de riesgo: Transmisión de información confidencial a través de una red publica y
autenticidad del Sitio Web

Objetivo de la evaluación: Determinar si el E-commerce posee una canal seguro para el tránsito de información entre el comercio y el cliente, y comprobar si se tiene un mecanismo para la autenticidad de Sitio Web donde se encuentra el Comercio Electrónico (Si el Comercio es quien dice ser.)

N°	PROCEDIMIENTO	Eje.	Hecho por	Fecha	Ref.
1	Preguntar si existe una persona encargada de vigilar la seguridad de la red tanto interna como externa, y: a) Establecer contacto con dicha persona b) Entrevistarlo, y hacer una narrativa de sus funciones. c) Preguntar las políticas y medidas de control que se tienen e implementan para lograr una seguridad en red satisfactoria d) Establecer un perfil de idoneidad para el cargo que ostenta.				
2	Solicitar el manual de políticas y procedimientos de la empresa y verificar la existencia de políticas y medidas especificas para la seguridad en las transacciones efectuadas a través de Internet (transferencia de información).				
3	Si no existen políticas y procedimientos de control escrito: c) Entrevistarse con el gerente general y hacer				

	una narrativa en donde se pueda identificar las líneas generales establecidas por éste en cuanto a la seguridad en red. d) Comparar lo expuesto por el gerente general con lo que expresa el encargado de la seguridad (si lo hay).				
4	Desde cualquier ordenador, con los siguientes requerimientos mínimos a la fecha de este trabajo, sin embargo con el avance continuo y acelerado de la tecnología en un futuro cercano pueden ser mayores: a) Hardware • Pentium III 1 GHZ, Celeron 1 GHZ, AMD Duron 1500, Athlon 2600 u otras equivalentes. • Memoria de 256 MB • Disco duro de 10 GB b) Software • Windows 98 o equivalente (Linux, UNIX) • Navegador Microsoft Internet Explorer 4.0 o Netscape Navigator 4.0 c) Conexión a Internet • Con MODEM 56 kbps, preferiblemente conexión a través de cable de 128 kbps o más. Realizar las siguientes pruebas:				
5	Ingresar al sitio Web del comercio evaluado				
6	Verificar la existencia de un logotipo de alguna autoridad certificadora				
7	Dar clic a dicho logotipo y verificar: a) Que los datos de identificación del certificado tales como, denominación o razón social de la empresa y nombre de dominio, coincidan con los datos reales del comercio. b) Que la fecha actual este dentro del periodo de validez del certificado.				
8	Ingresar al sitio Web de la autoridad certificadora y verificar: a) El servicio contratado por la empresa (SSL de 40 o 128 bits) b) Evaluar si dicha entidad certificadora es fiable, si es de raíz o intermedia, puede tomar como parámetro para dicha evaluación, las compañías proporcionadas por Microsoft Internet Explorer más reciente, en el menú de Herramientas, submenú opciones de Internet ficha de contenido, opción certificados. Esto no obsta que haya muchas más compañías fiables				

	en Internet que las proporcionadas en dicha lista.				
9	Simular un proceso de compras, y documentado paso a paso por medio de captura de pantallas y comprobar los siguientes acontecimientos en momentos cruciales: a) En el momento de enviar los datos personales tales como: nombre, dirección, teléfono, número de tarjeta de crédito, en el proceso de pago en línea, verificar que el explorador (si se esta trabajando con Microsoft Explorer), despliegue una ventana donde diga que la información que se intercambie con este sitio no puede ser vista o cambiada por otros, en dicha ventana, se estipula si se tiene o no confianza en el certificado, si el certificado es válido, si el certificado coincide con la pagina que se desea ver. b) Corroborar que en la parte inferior derecha del Navegador, aparezca un candado cerrado, el cual indica que la comunicación entablada con el sitio Web es segura, esto debe ser en el momento del proceso de pago. Es importante aclarar que muchas veces el Navegador no despliega la ventana señalada en el literal a), sino solamente el candado cerrado en la parte inferior derecha. c) Dar clic sobre el candado cerrado, y verificar el certificado de seguridad, en el cual aparecen datos tales como: El propósito del certificado, nombre del comercio al cual ha sido emitido, nombre de la autoridad certificadora, período de validez, el algoritmo hash utilizado para la firma digital, la clave publica y su extensión, la huella digital, entre otros datos de importancia. d) Extraer dicho certificado, copiándolo a un medio de almacenamiento flexible, tal como un disco magnético, una memoria flash o un disco óptico.				
10	En el caso de los comercios en sentido amplio adicionalmente a lo anterior corroborar lo siguiente: a) Si la empresa presta servicios de hosting independientes a otras empresas diferentes de los proveedores definidos, para lo cual se debe preguntar al gerente general y al encargado de informática. b) Si los proveedores definidos, son realmente proveedores o un comercio independiente, para				

	lo cual se debe ingresar a un 10% de las paginas de los proveedores albergados en el servidor del comercio y simular un proceso de compras en cada uno de ellos en donde se debe verificar, que en el momento de pago, quien valide la transacción, sea el comercio y no otra empresa. c) Si los proveedores son una empresa independiente, que solamente ha contratado un servicio de hosting (albergue) en el servidor del comercio, verificar que posea su propio certificado de seguridad.				

(ver Anexo 3.3. ejemplo de corrida del programa)

3. Dependiendo de los resultados de la evaluación obtenidos con la aplicación del programa propuesto, así será el riesgo de auditoria del área en cuestión, por tanto, éste dependerá de la ponderación de los siguientes factores materiales:

a. La existencia de políticas de seguridad en redes

b. La existencia de un servidor seguro con un protocolo Secure Socket Layer (SSL).

c. La posesión de un certificado de seguridad

d. La fiabilidad de la autoridad certificadora

e. La vigencia del certificado de seguridad

Para hacer la valoración del riesgo se sugiere se utilice el siguiente procedimiento: si el resultado de la evaluación para cada uno de estos factores es favorable (sí se tienen políticas de seguridad, sí existe un servidor seguro, sí se posee un certificado de seguridad, etc.) se le asigna una ponderación de 3 puntos para la existencia de políticas de seguridad en redes y 6 punto a los restantes; si la referida evaluación no es muy favorable, se le asignan 2 puntos para la existencia de

políticas de seguridad en redes y 3 punto a los restantes; y si la evaluación es desfavorable es decir que no concurra ninguno de los factores señalados, la ponderación para cada uno será de 1 punto. La calificación máxima que se puede obtener es de 27 puntos, esto dará un 100% de seguridad. El parámetro para validar la seguridad en esta área será del 92.59%, por debajo del cual se enciende la luz roja de alarma para el auditor, indicándole que existe una grave desviación y deficiencia en la seguridad correspondiente a esta región. A continuación se presenta una matriz ejemplificando el procedimiento antes descrito.

Área evaluada		**Factores de riesgo**					
		Existencia de políticas de seguridad en redes	Existencia de un servidor seguro (SSL)	Posesión de un certificado de seguridad	Fiabilidad de la autoridad certificadora	Vigencia del certificado de seguridad	Total
Seguridad en Red	Ponderación	1	6	6	6	6	25
	Puntaje	3.70%	22.22%	22.22%	22.22%	22.22%	92.59%

Tal como se puede apreciar en la matriz, la inexistencia de políticas de seguridad en redes (ponderación 1, puntaje 3.70%), no influye de manera significativa en la calificación total, por tanto el nivel de riesgo del área sigue siendo el mínimo permitido, ya que el parámetro es precisamente 92.59%, por debajo del cual el riesgo es intolerable. Obsérvese que una ponderación inferior a la máxima, para los restantes factores,

produciría un riesgo irresistible, y es lógico, ya que éstos, tienen un mayor grado de ponderación, por la importancia que ostenta cada uno de ellos, en la seguridad en redes sujeta de valoración.

3.5. ÁREA DE SEGURIDAD CONFIDENCIALIDAD CON LA INFORMACIÓN DE LOS CLIENTES

3.5.1 DEFINICIÓN

La seguridad con la información de los clientes es un aspecto preponderante a considerar al realizar una auditoría de seguridad en un E-commerce, ya que constituye un punto neurálgico para el desarrollo de confianza en la subjetividad del cliente, se podría decir que de ésta depende, en gran medida, el auge y desarrollo del comercio electrónico, por tanto, es obligación del auditor hacer una evaluación exclusiva y precisa en cuanto al *manejo y uso* que hacen los comercios de estos datos.

Definición :"La seguridad y confidencialidad con la información de los clientes consiste en montar todo un aparataje normativo, tecnológico y humano, encaminado a garantizar un buen uso y manejo de los datos recavados del consumidor, para lo cual es necesario tener en cuenta que: la información no debe ser objeto de comercialización ni de alianzas estratégicas entre empresas; el compendio de estos datos no debe ni tiene por que salir del comercio; el acceso a éstos debe estar limitado a un número muy

reducido de personal interno; el uso que se le da debe ser restringido, de tal manera que, se debe evitar la utilización abusiva de los mismos, para la publicidad a través del correo electrónico (Spam) o de Cookies”

3.5.2. RIESGOS ASOCIADOS

En consecuencia, los factores de riesgo asociados a dicha área son los siguientes:

- Uso apropiado
  - Existencia de alianzas estratégicas de intercambio de información entre los comercios, para la extensión o incursión de mercados.
  - Abuso en el envió excesivo de propaganda no deseada (Spam y Cookies)
- Manejo apropiado
  - Acceso externo por cualquier medio a la información confidencial
    - Hurto de información, tal como el robo de datos personales incluyendo el número de tarjeta de crédito, para perpetuar fraudes, usurpación de identidad o cualquier otro ilícito.
  - Acceso irrestricto por la mayor parte del personal de la empresa (acceso interno)
    - Hurto de información para usos fraudulentos, sin poder asignar responsabilidades directas.

- Extravío o pérdida de datos por negligencia de parte de unas de las muchas personas (empleados) que puedan tener acceso a ellos.
- Riesgos elevados de pérdida y hurto de información con el despido o retiro de un empleado.

3.5.3. MEDIDAS DE CONTROL PARA LA DISMINUCIÓN AL MÍNIMO DE LOS RIESGOS ASOCIADOS

Las medidas de control que las empresas deben tener para mitigar o disminuir al mínimo los referidos riesgos son las siguientes:

- Establecimiento de políticas encaminadas a normar el uso y manejo de la información, de tal manera que pueda proporcionar una confianza razonable al cliente sobre la confidencialidad y seguridad de sus datos, así como la declaración de voluntad sobre la utilización y conducción de los mismos.
- Definición de medidas organizativas encaminadas a garantizar la confidencialidad, seguridad e integridad de la información proporcionada por el consumidor.
- Aplicación de medidas tecnológicas que garanticen al máximo la seguridad, confidencialidad e integridad de las comunicaciones con los clientes (seguridad en red), así como, el resguardo interno de la misma.

3.5.4. TÉCNICAS Y PROCEDIMIENTOS DE AUDITORIA PARA LA EVALUACIÓN

A continuación se presentan los instrumentos de evaluación referentes a esta área: el cuestionario de control interno, como una primera aproximación para una comprensión suficiente de la seguridad y confidencialidad con la información de los clientes y un programa de auditoria en el cual se describen taxativamente los procedimientos con sus respectivas técnicas de auditoria, necesarias para la evaluación de la seguridad en el uso y manejo de la información de los clientes, por consiguiente, para corroborar la existencia de todas o algunas medidas de control, con el fin de evaluar la importancia o materialidad de los riesgos asociados a ésta área, y determinar la existencia de seguridad, confidencialidad e integridad de los datos proporcionados por el consumidor, se sugiere lo siguiente:

1. Pasar un cuestionario a al gerente general del E-commerce así como a todos los encargados de los diferentes departamentos o secciones en las que esta dividido el comercio, como un instrumento que servirá para una primera aproximación al área evaluada, para lo cual se proporciona el modelo siguiente.

(En el presente cuestionario se presentan algunas preguntas abiertas las cuales no coinciden con la estructura cerrada del instrumento presentado, sin embargo se ha hecho de esta forma para no limitar algunos aspectos que requieren mayor amplitud,

en cuanto a las respuestas de los encuestados, para lo cual se debe acomodar dicho instrumento a tal circunstancia.)

CUESTIONARIO PARA LA EVALUACIÓN DE LA SEGURIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN PROPORCIONADA POR LOS CLIENTES

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: Seguridad, confidencialidad e integridad de la información proporcionada por el consumidor

Objetivo de la evaluación: Determinar si el E-commerce posee medidas y políticas para un uso y manejo seguro, confiable, confidencial e íntegro de la información proporcionada por los clientes

N°	*Preguntas*	Si	No	N/A	Comentarios
1	¿Qué tipo de información se recolecta de los clientes?				
2	¿Se tienen políticas de privacidad para el uso y manejo de los datos proporcionados por el cliente?				
3	¿Si se tienen políticas de privacidad, estas son comunicadas a los clientes a través de un link en el sitio Web del comercio?				
4	¿Para que se utiliza la información proporcionada por el consumidor?				
5	¿Personas externas al comercio pueden acceder a dicha información?				
6	¿Quién recolecta la información? ¿La empresa o un tercero?				
8	¿Se tienen alianzas con otros comercios en cuanto al intercambio de información?				
9	¿El cliente puede tener acceso a su propia información y eliminarla por completo de la base de datos del comercio?				
10	¿Se envía publicidad constantemente a los clientes, con relación al perfil formado por medio de sus datos almacenados?				

11	¿Se utilizan Cookies en el ordenador del cliente para publicitar los productos proporcionados por el E-commerce?				
12	¿Qué personal dentro de la empresa puede tener acceso a la información?				
13	¿Existe un responsable directo de la custodia, gestión y distribución de datos?				
14	¿Se tiene algún reglamento o documento donde se implemente la normativa de seguridad de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información que los gestionan?				
15	¿Se tienen implementados procedimientos de identificación y autenticación que establecen de forma inequívoca y personalizada la identificación de todo aquel usuario que intente acceder al sistema de información y la verificación de que está previamente autorizado?				
16	¿Sólo el personal autorizado podría tener acceso a los locales donde se encuentren ubicados los sistemas de información que gestione los datos de carácter personal?				
17	¿Se lleva un inventario y registro de la gestión de los soportes informáticos que puedan contener datos de carácter personal de los Usuarios?				
18	¿Se tiene algún procedimiento de notificación y gestión de incidencias (anomalías que afecten o pudieran afectar a la seguridad de los datos) y un procedimiento de recuperación de los datos y de gestión de copias de respaldo?				
19	¿Se posee un software robusto y suficiente para manejar, asegurar y gestionar la información de los clientes?				
20	¿Los ficheros o base de datos contenedores de los datos personales de clientes, son accesibles en línea por el personal autorizado desde un punto remoto?				
21	¿Se posee servidor propio donde se encuentre alojado el E-commerce?				

22	¿Se contrata servicio de hosting para mantener el E-commerce (en caso de no tener servidor propio)				
23	¿El Sitio Web está publicitado en otro portal ajeno al E-commerce, en donde, por medio de él se realicen transacciones de venta, de tal manera que, éste pueda contener bases de datos propias donde almacena información de los clientes del comercio?				
24	¿Se utiliza cifrado en aquellos casos en que: (a) la información a transferir sea sensible y (b) la transmisión se realice en canales abierto de comunicaciones?				
25	¿Se llevan a cabo operaciones de interfuncionamiento entre sistemas de información altamente seguros y otros menos seguros (como por ejemplo un servidor seguro con encriptación de 128 bits con un ordenador con navegador que soporta una encriptación menor de 40 bits)				

2. Una vez obtenidas las respuestas es necesario corroborarlas a través de pruebas de control, para lo cual se sugieren las siguientes técnicas y procedimientos de auditoria:

PROGRAMA DE AUDITORIA
PARA LA EVALUACIÓN DE LA SEGURIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN PROPORCIONADA POR LOS CLIENTES

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: Seguridad, confidencialidad e integridad de la información proporcionada por el consumidor

Objetivo de la evaluación: Determinar si el E-commerce posee medidas y políticas para un uso y manejo seguro, confiable, confidencial e integro de la información proporcionada por los clientes

N°	PROCEDIMIENTO	Eje.	Hecho por	Fecha	Ref.
1	Desde un ordenador con las especificaciones proporcionadas en el área de seguridad en red Ingresar al Sitio Web del comercio y realizar los siguiente procedimientos: a) Efectuar el proceso de compras desde el inicio hasta el fin, documentándolo a través de la captura de pantallas. b) Algunos comercios solicitan registro del socio, para que éste pueda acceder a utilizar el E-commerce como tienda virtual, documentar dicha situación capturando las pantallas correspondientes. c) Cerciorarse que quien pida la información sea el E-commerce y no un tercero. d) Corroborar que en el momento de ingresar y enviar cualquier tipo de información personal, ya sea en el momento de registro o de pago, se esté en un canal de comunicación seguro (tal como se ha establecido en el área de seguridad en red) e) Si fuese posible ingresar al sitio Web con un navegador Internet Explorer o Netscape versión 1.0 o menor, y comprobar si se puede establecer una conexión segura (Debido que estos navegadores no soportan el protocolo de seguridad SSL) f) Verificar y documentar el tipo de información solicitada por el comercio.				
2	Durante el transcurso de diez días después de haber efectuado el procedimiento anterior verificar las siguientes situaciones: a) Ingresar al correo electrónico proporcionado en el momento de enviar los datos solicitados por el comercio, y determinar:				

	❑ Si se ha recibido Spam publicitarios ❑ La frecuencia con que se recibe dicha publicidad por día. ❑ Documentar las situaciones anteriores por medio de: captura de pantallas y narrativas taxativas de las observaciones realizadas. b) Ingresar periódicamente al sitio Web del comercio y observar: ❑ Si en el momento de cargar la pagina Web del E-commerce, automáticamente aparecen ventanas, del comercio o de terceros con contenido publicitario. ❑ Si estas páginas publicitarias son propiedad del comercio. ❑ ¿Cuál es el contenido de las referidas páginas?, ya que muchas veces, pueden ser link a sitios pornográficos. ❑ Documentar las situaciones anteriores por medio de: captura de pantallas y narrativas taxativas de las observaciones realizadas c) Si confluyen los aspectos señalados en el literal anterior es por que el comercio está haciendo uso de Cookies, para verificar los Cookies implantados en el ordenador del cliente, realizar los siguientes procedimientos: ❑ Ingresar al menú de herramientas del navegador, y escoger opciones de Internet, dentro de esta acceder a la opción de configuración, y seleccionar “ver archivo”, allí se le mostrará una lista de Cookies almacenados en su ordenador, buscar los relativos a las ventanas observadas en el momento de cargar las páginas Web de E-commerce (si se utiliza Internet Explorer). ❑ Documentar las situaciones anteriores por medio de: captura de pantallas y narrativas taxativas de las observaciones realizadas d) Determinar y evaluar si existe o no exceso en el uso de estas técnicas publicitarias (Spam y Cookies), con relación a las observaciones hechas al respecto, lo cual quedará a criterio del auditor, sin embargo, dicho aspecto se debe documentar en una narrativa razonada del criterio adoptado.				

3	Entrevistarse con el Gerente General, y preguntar si existen políticas de privacidad, si existieren, solicitar el documento escrito, y revisar lo siguiente: a) Las cláusulas relativas, a la privacidad, confidencialidad, seguridad e integridad de los datos b) Los usos, fines y manejo de la información c) Preguntar al gerente si se está ligado a algún código de ética en cuanto a la protección, manejo y uso de datos, tal como el de garantía de protección de datos de la AECE en Europa. d) Evaluar y hacer una narrativa, sobre los aspectos antes mencionados, soportándolo con la copia de las políticas de privacidad si están escritas, de lo contrario inferirlas acorde a la entrevista suscitada con el gerente y corroborarla con otro personal de la empresa.				
4	Dentro del sitio Web del comercio verificar que: a) En cualquier proceso, ya sea de pago o de registro, exista un link perfectamente visible para desplegar la página que contiene las políticas de privacidad. b) En los procesos mencionados en el literal anterior, se pida consentimiento al cliente, sobre el uso y manejo de la información recavada. c) Exista algún logotipo como sello de garantía, de la adhesión del E-commerce a algún código de ética que regule lo relativo a la protección, uso y manejo de los datos del usuario. d) El cliente o usuario pueda tener acceso a su información personal para eliminar su registro.				
5	Solicitar al gerente un reglamento donde se encuentren plasmadas normas prohibitivas e imperativas que vinculen directamente a los empleados responsables del tratamiento de los datos, así como a cualquier otro, aunque no esté directamente ligado a dicha responsabilidad. Dicho documento debe contar con sanciones por contravenciones a las normas previstas. a) Hacer una narrativa sobre el contenido de dicho documento, evaluándolo y comparándolo con los parámetros antes mencionados y con el juicio razonable del auditor. b) De no existir dicho documento expresarlo y documentarlo a través de la narrativa				

	correspondiente.				
6	Observar el proceso del flujo de la información, desde que se recaba y almacena hasta que utiliza para cualquier fin previsto, como por ejemplo, para: procesar y enviar el pedido, notificar el envió, hacer estudios internos (estadísticos, demográficos, gustos y preferencias, etc.), el envió de publicidad, etc. y determinar: a) El personal que interviene en el proceso en cuanto: ❑ La existencia de un responsable general, en cuanto a la guardia, distribución y manejo de la información. ❑ Los departamentos o áreas del negocio usuarios de la información ❑ La cantidad de personas en cada departamento que acceden a los datos para los fines antes mencionados. ❑ Los niveles de acceso a dicha información dependiendo el departamento o área y la persona. ❑ Hacer una narrativa y un flujograma de lo observado. b) Para ejecutar los cometidos antes mencionados, se debe realizar lo siguiente: ❑ Observar por un tiempo prudencial las labores ejecutadas por cada persona relacionada con el procesamiento de los datos de los clientes. ❑ Pedir una muestra de las labores ejecutadas por cada persona vinculada al procesamiento de la información de los clientes. ❑ Capturar las pantallas donde se muestren, los accesos y el tipo información procesada por el empleado respectivo. c) En el caso de las tiendas virtuales ya sea en sentido estricto o amplio, se vuelve mucho más sencillo la ejecución de los procedimientos antes señalados, debido que la organización es menos compleja, no así con los comercios que poseen un canal virtual, sin embargo esto no obsta para obviar su ejecución. Lo que se tiene que tener mas en cuenta en este prototipo de negocios, son los niveles de acceso que cada empleado, departamento o área tiene a la información en cuestión.				

7	Solicitar al encargado principal de la guardia, y manejo de la información, que le proporcione el ordenador de trabajo de él, y realice las siguientes pruebas: a) Tratar de ingresar a la base de datos que contiene la información de los clientes. b) Pedir al encargado que ingrese a dicho fichero y observar, su nombre de usuario. c) Documentar lo realizado anteriormente mediante la captura de pantallas. Realizar el mismo procedimiento anterior, con una muestra significativa de personas con acceso a la información de los clientes.				
8	Solicitar al administrador del servidor que le proporcione una lista, de los accesos a la base de datos o fichero que contiene la información del consumidor, durante el período en el cual se corrió el procedimiento anterior y verificar: a) Que se haya registrado los accesos denegados así como todos los accesos no denegados. b) Corroborar que coincidan con los nombres de usuarios muestreados. c) Documentar estos procedimientos a través de narrativas y captura de pantallas.				
9	Elaborar un inventario del software que se encarga de gestionar, manejar y asegurar los datos de los clientes.				
10	Pedir al encargado de informática que muestre la copia de respaldo de los datos almacenados en el servidor.				
11	En el caso que cualquier información almacenada en el servidor del E-commerce, fuere accesible por personal autorizado desde un punto remoto, verificar: a) La seguridad en cuanto a la transferencia de información a través de Internet (Seguridad en Red) b) La seguridad en cuanto a las claves y niveles de acceso.				
12	Corroborar, que se tenga servidor propio y que en éste se encuentre alojado el E-commerce, esto se hace mediante una inspección física, y la consecuencia de los procedimientos anteriores lo indica. De no contar con servidor propio es obvio que personas ajenas a la empresa pueden acceder a				

	cualquier tipo de información relacionada con el comercio electrónico, en este caso el prestador de servicio de Hosting.				
13	Los procedimientos adicionales a cerca de la seguridad física (Hardware) y lógica (software) se detallaran en el área que para tal efecto se tiene segregada.				

3. Dependiendo de los resultados de la evaluación obtenidos con la aplicación del programa propuesto, así será el riesgo de auditoria del área en cuestión, por tanto éste dependerá de la ponderación de los siguientes factores materiales:

a) Existencia de políticas de privacidad
b) Existencia de alianzas estratégicas de intercambio de información entre los comercios, para la extensión o incursión de mercados.
c) Abuso en el envió excesivo de propaganda no deseada (Spam y Cookies).
d) Acceso externo por cualquier medio a la información confidencial
e) Acceso irrestricto por la mayor parte del personal de la empresa (acceso interno).

Para hacer la valoración del riesgo se sugiere se utilice el siguiente procedimiento: si el resultado de la evaluación para cada uno de estos factores es favorable (sí se tienen políticas de privacidad, sí no existen alianzas estratégicas con otras empresas para el intercambio de información personal de los clientes, etc.) se le asigna una ponderación de 3 puntos para

abuso en el envió excesivo de propaganda no deseada y 6 punto a los restantes; si la referida evaluación no es muy favorable, se le asignan 2 puntos para el abuso en el envió excesivo de propaganda no deseada y 3 punto a los restantes; y si la evaluación es desfavorable es decir que no concurra ninguno de los factores señalados, la ponderación para cada uno será de 1 punto. La calificación máxima que se puede obtener es de 27 puntos, esto dará un 100% de seguridad. El parámetro para validar la seguridad en esta área será del 92.59%, por debajo del cual se enciende la luz roja de alarma para el auditor, indicándole que existe una grave desviación y deficiencia en la seguridad correspondiente a esta región. La matriz elaborada de tal ponderación, será similar a la propuesta en el área de seguridad en red.

3.6. ÁREA DE SEGURIDAD LÓGICA Y FÍSICA

En este apartado, se facilitarán las técnicas y procedimientos básicos para evaluar los componentes físicos (Hardware e infraestructura) y lógicos (Software y procesos), que sirven de soporte infraestructural al comercio electrónico. Es importante aclarar que en ésta área tiene mucha relevancia la auditoría de sistemas de información, por lo que, precisamente de ésta se tomaran la mayoría de herramientas, no obstante con un enfoque distinto, el cual es el de auditoría de seguridad en sentido amplio para los E-commerce.

3.6.1. DEFINICIÓN

El hardware y el software es la materia prima para echar andar cualquier sistema de información; por tanto, es importante proporcionar la debida protección del mismo lo cual pende de la responsabilidad y visión de la administración.

La seguridad lógica consiste en la protección del software, los datos, procesos; así como el ordenado y autorizado acceso de los usuarios a la información.

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

3.6.2. RIESGOS ASOCIADOS

Los riesgos esenciales asociados a esta área son los siguientes:

- **Lógicos**
  - Destrucción de información: Virus, Sistemas operativos frágiles, Inexistencias de copias de respaldo de la información
  - Funcionamiento deficiente del software
  - Sistema operativo, programas y aplicaciones sin un control oportuno y eficaz en cuanto al registro de usuarios y sus niveles de acceso a los datos.

- Inexistencia de Firewall que aíslen y protejan el software y las bases de datos de importancia para la organización
- Vulnerabilidad del sistema en cuanto al ataque de piratas informáticos

- **Físicos**
  - Infraestructura física inapropiada (Edificios y lugar donde se encuentra el equipo informático): Alto riesgo de destrucción total del equipo informático en caso de cualquier contingencia tales como: incendio, terremoto, inundaciones, etc.
  - Condiciones ambientales inadecuadas: Falta de aire acondicionado y Problemas de humedad y filtración de agua.
  - Seguridad de las instalaciones que albergan el equipo informático deficiente: Acceso irrestricto al personal y Faltas de mecanismos de seguridad en cuanto a cerraduras especiales y cámaras de vigilancia.

3.6.3. MEDIDAS DE CONTROL PARA LA DISMINUCIÓN AL MÍNIMO DE LOS RIESGOS ASOCIADOS

Las medidas para mitigar o disminuir al mínimo los riesgos asociados son las siguientes:

Seguridad lógica:

- Implementación de políticas, normas y estándares y velar por su fiel cumplimiento
- Existencia de un sistema operativo seguro y robusto
- Existencia de una plataforma de software eficientes y eficaces que garanticen la seguridad y el funcionamiento del E-commerce de manera apropiada
- Implementación de protocolos que garanticen una comunicación segura y crear protocolos con detección de errores
- Administración eficiente y segura de las bases de datos
- Proveedores de Internet responsables que aseguren una conexión eficaz
- Establecimiento de Firewall (cortafuegos) eficaces, que protejan de manera reforzada las áreas más sensibles del sistema, como lo son, las bases de datos o ficheros de información.
- Existencia de antivirus potentes con actualización constante
- Establecer procedimientos para recuperar los datos en casos de caída del sistema o de corrupción de los archivos.
- Evitar la importación y exportación de datos.
- Implementación de Procedimientos para prohibir el acceso no autorizado a los datos.
- Implementación de Procedimientos para restringir el acceso a los datos para lo cual se debe identificar los distintos perfiles de usuario que accederán a los archivos de la

aplicación y los subconjuntos de información que podrán modificar o consultar.

- Establecimiento de Procedimientos para mantener la consistencia y corrección de la información en todo momento.

Seguridad física:

- Establecimiento de políticas de uso de los equipos
- Existencia de Contratos vigentes de compra, renta y servicio de mantenimiento y de contratos de seguros para el equipo
- Implementación de equipo con configuraciones y capacidades necesarias para realizar operaciones electrónicas
- Ubicación correcta del equipo en las Instalaciones
- Control de acceso a las áreas donde se encuentra el equipo principal de almacenamiento, gestión y procesamiento de información.
- Aseguramiento de las instalaciones donde se encuentra el equipo informático, respecto a la protección en caso de siniestros o desastres naturales.

3.6.4. TÉCNICAS Y PROCEDIMIENTOS DE AUDITORIA PARA LA EVALUACIÓN

A continuación se presentan los instrumentos de evaluación referentes a esta área: el cuestionario de control interno, como una primera aproximación para una comprensión suficiente de la seguridad lógica y física y un programa de auditoria en el cual se describen taxativamente los procedimientos con sus respectivas técnicas de auditoria, necesarias para la evaluación

de la seguridad tanto del software como del hardware, por consiguiente, para corroborar la existencia de las medidas mínimas que conlleven a la protección de la infraestructura informática (software y hardware) que soporta el E-commerce, se sugiere lo siguiente:

1. Pasar un cuestionario, a los encargados de informática de cada E-commerce como una primera aproximación al conocimiento especifico de esta área, para lo cual se proporciona el modelo siguiente.

(En el presente cuestionario se presentan algunas preguntas abiertas las cuales no coinciden con la estructura cerrada del instrumento presentado, sin embargo se ha hecho de esta forma para no limitar algunos aspectos que requieren mayor amplitud, en cuanto a las respuestas de los encuestados, para lo cual se debe acomodar dicho instrumento a tal circunstancia.)

CUESTIONARIO DE EVALUACION
PARA LA SEGURIDAD FÍSICA Y LÓGICA INTERNA

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: La existencia de Garantías de Seguridad, en cuanto a las medidas y políticas que se tengan para salvaguardar el Hardware y Software.

Objetivo de la evaluación: Conocer si las empresas poseen una infraestructura física, lógica y segura de comercio electrónico; como base para realizar transacciones en línea, que provean confianza al consumidor.

N°	Preguntas	Si	No	N/A	Comentarios
1	¿Existe un único responsable de implementar la política de autorizaciones de entrada al lugar donde se encuentra el equipo informático vital				

	para el funcionamiento del E-commerce.				
2	¿Quiénes saben cuales son las personas autorizadas?				
3	¿Se tienen alguna medida de seguridad tal como uso de tarjetas magnéticas o contraseña, para ingresar al lugar donde se tiene el equipo informático importante (el servidor)?				
4	¿Existe control de acceso al Centro de Cómputo?				
5	¿Existe una persona encargada de evaluar y velar por la seguridad de la red interna y externa (Internet)?				
6	¿Existe en la empresa un gerente de tecnología diferente al del área de informática?				
7	¿Existe en la empresa alguien capaz de solucionar problemas críticos de la red y del comercio electrónico, tales como?: • Ataques de piratas informáticos (Hacker) • Ataques de virus • Daño físico de la red o del servidor, entre otros				
8	¿Se le explica al usuario todo lo que está permitido en cuanto al uso de la maquina, y todo lo que expresamente no esté permitido está prohibido?				
9	¿Se posee servidor propio en donde se encuentra la información y se muestra el sitio Web de la empresa?				
10	¿Cuántas personas tienen acceso de administrador al servidor?				
11	¿Cuáles son los niveles de acceso que posee el servidor y cuál es el número de personas en cada nivel de acceso?				
12	¿Existen niveles escalonados de acceso al sistema?				
13	¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?				
14	¿Se ha instruido los usuarios sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?				

15	¿Se tienen políticas de contraseña, en cuanto a?: • La longitud mínima y máxima • El periodo de vigencia de la misma				
16	¿Se posee una red interna de información administrada por un servidor?				
17	¿El servidor que administra la red interna esta conectado a Internet?				
18	¿Qué tipo de conexión se posee?				
19	¿Cuál es la velocidad de la conexión?				
20	¿Cuántas veces se cae el servicio de Internet en el mes (Estimado)?				
21	¿Cuál es el promedio de tiempo sin servicio de Internet en cada caída del servicio (Estimado)?				
22	¿Cuál es la velocidad de respuesta del proveedor del servicio de Internet en caso de falla?				
23	¿Se poseen planes de contingencia en caso de daño en el equipo que posee el comercio electrónico que lo imposibiliten a estar conectado a la red o por cualquier falla en el proveedor del servicio, tales como?: • Cierre del servidor • Clausura del servidor donde se tiene alojado el sitio Web del comercio electrónico, entre otros				
24	¿Se poseen políticas en cuanto al uso del software y del hardware?				
25	¿Qué sistema operativo tiene instalado el servidor?				
26	¿El sistema operativo con el que cuenta su servidor, le permite llevar un registro o bitácora de todos los sucesos surgidos en la red que administra?				
27	¿Se tiene la política de realizar auditoria al sistema operativo por lo menos una vez cada semana?				
28	¿Qué tipo de auditoria se realiza? 1) Auditoría de cuentas de usuario:				

	• Inicio y cierre de sesión. • Acceso a ficheros, directorios o impresoras. • Ejercicio de los derechos de un usuario. • Seguimiento de procesos. • Inicio, reinicio y apagado del sistema. 2) Auditoría del sistema de archivos: • Rastrea sucesos del sistema de archivos • Los sucesos que se pueden auditar • *Cambio de permisos* y *Toma de posesión*. 3) Auditoría de impresoras: • Registro de sucesos de aplicaciones. • Registro de sucesos de seguridad. • Registro de sucesos del sistema				
29	¿Existe una sola persona con el cargo de administrador del servidor?				
30	¿Alguna vez su servidor ha sido atacado por un pirata informático (hacker)?				
31	¿Alguna vez su servidor a sido atacado por algún virus lanzado desde Internet?				
32	¿Alguna vez han sido víctimas de Fraude?				
33	¿Se tienen instalados Firewall (Cortafuego) en su equipo, que le provean certeza en cuanto a la infiltración de datos o personas no autorizadas a la red?				
34	¿Se tienen programas antivirus con actualización continua capaz de detectar a priori cualquier tipo de virus que se introduzca a la red?				
35	¿Se tienen registrados a nombre de la empresa todo el software de desarrollo, de plataforma y de utilidades del comercio electrónico?				
36	¿Se lleva un inventario del software utilizado por la empresa?				
37	¿Las aplicaciones o software de soporte y utilitarios para el E-commerce son: • Desarrollados por la empresa • Adquirido en el mercado • Mandados hacer a la medida				

38	¿Existe una persona responsable de la Seguridad del hardware?				
39	¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?				
40	¿El Hardware y Software poseen la capacidad necesaria para realizar operaciones e-commerce?				
41	¿Se han adoptado medidas de seguridad en el departamento de sistemas de información, tales como: reguladores de voltaje que adecuen la energía eléctrica para dicho departamento, UPS, extinguidores, entre otros?				
42	¿Son adecuadas las instalaciones para el buen funcionamiento del equipo informático?				
43	¿Se tienen rutinas de mantenimiento preventivo?				
44	¿Se tiene inventariado cada uno de los dispositivos componentes del Hardware, tales como, ordenadores con sus características individuales (Disco duro, Motherboard, Micro procesador, memoria RAM, CD-Rom u otros dispositivos), periféricos, enrutadores, entre otros.				
45	¿Se cuenta con un plan de actualización de hardware a medida que van surgiendo los avances tecnológicos, de tal manera que se adecua a las nuevas exigencias de los clientes en cuanto a eficiencia?				

2. Una vez obtenidas las respuestas es necesario corroborarlas a través de pruebas de control, para lo cual se sugieren las siguientes técnicas y procedimientos de auditoria:

PROGRAMA DE AUDITORIA
PARA EVALUAR LA SEGURIDAD FÍSICA Y LOGICA INTERNA

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: La existencia de Garantías de Seguridad, en cuanto a las medidas y políticas que se tengan para salvaguardar el Hardware y Software.

Objetivo de la evaluación: Conocer si las empresas poseen una infraestructura física, lógica y segura; de comercio electrónico; como base para realizar transacciones en línea, que provean confianza al consumidor.

N°	PROCEDIMIENTO	Ejec	Hecho	Fecha	Referencia
1	Entrevistarse con el gerente general del E-commerce y preguntarle los siguientes aspectos: ❑ Quién es responsable especifico del área de informática. ❑ Quién es el responsable de autorizar a los usuarios en cuanto al acceso al equipo informático y al software especifico. ❑ Cuales son las políticas y medidas de seguridad generales adoptadas por la empresa en cuanto a la seguridad del equipo informático en todos sus aspectos. ❑ Si existe un manual de políticas y procedimientos por escrito donde se detalle taxativamente las políticas y procesos que debe cumplir y seguir cada empleado. ❑ Si existe un manual de inducción para cada empleado en cuanto a las labores que ejecuta. ❑ Hacer una narrativa de lo expuesto por el gerente general.				
2	Entrevistarse con cualquier empleado del departamento de informática del E-commerce y preguntar lo siguiente: ❑ Quién es su jefe superior inmediato. ❑ Quién le ha autorizado su acceso al equipo y al software. ❑ Si se le ha explicado todo lo que está permitido y prohibido en lo referente a la utilización del software y hardware. ❑ Si se le ha hecho una descripción				

	taxativa de sus funciones. ❑ Si conoce las políticas y procedimientos. ❑ Y en general si ha recibido un adiestramiento en lo referente a su trabajo.				
3	Solicitar el manual de políticas y procedimientos y el manual de descripción de funciones y de puesto en lo referente al área de informática.				
4	Solicitar al encargado de informática que le muestre el o los servidores que administran y gestionan la información y verificar lo siguiente: ❑ Capacidad de procesamiento. ❑ Capacidad de almacenamiento. ❑ Capacidad de memoria. ❑ Velocidad de conexión a la red. ❑ Documentar dicha información.				
5	Solicitar al administrador del servidor que le permita ingresar al sistema operativo y verificar lo siguiente: ❑ Los grupos y usuarios que tienen acceso al sistema operativo. ❑ Cantidad de usuarios que tienen acceso de administradores. ❑ Si los usuarios ordinarios tienen acceso restringido. ❑ En base a lo anterior, indagar cuál es el nivel de acceso de los programadores y analistas.				
6	Comprobar que los sistemas utilizados para manejar la información vital del E-commerce tales como aplicaciones, tendientes a gestionar y manipular bases de datos posean seguridad de acceso a través del uso de nombres de usuario y contraseñas.				
7	Cerciorarse que las bases de datos que contienen información valiosa para el E-commerce principalmente datos de clientes, proveedores e información financiera, estén debidamente protegidas contra el acceso no autorizado, a través de claves o que sus datos se encuentren cifrados o inteligibles. Para lo cual se debe extraer una base de datos y tratar de ingresar a ella, si es necesario, solicitar la colaboración de un experto para realizar este procedimiento.				

8	Preguntar al encargado de autorizar los accesos a los sistemas la política de contraseñas en lo referente a: ❑ Longitud mínima y máxima. ❑ Periodo de vigencia.				
9	Solicitar el listado de todos los usuarios con su respectiva longitud de contraseñas y sus períodos de vigencia.				
10	Cerciorarse que exista una verdadera y eficaz rotación de contraseñas y que los períodos de validez de la misma no sean muy largos o prolongados como máximo 90 días.				
11	Solicitar la diagramación de la red interna y corroborar si el servidor principal que la administra, esta conectado a Internet.				
12	Confirmar el tipo de conexión que posee el E-commerce, en lo referente a: a) Medios de comunicación de la red interna con Internet. ❑ Satelital. ❑ Cable. ❑ Modem con conexión a línea telefónica. b) Velocidad de conexión. c) Hacer una evaluación en cuanto a la idoneidad de la conexión y su velocidad en cuanto al volumen de transacción de E-commerce (Vistas por días al sitio Web).				
13	En el transcurso del período de auditoría ingresar al sitio Web del comercio por lo menos unas tres veces al día, distribuido de forma aleatoria con intervalos prudenciales, durante cuatro días a la semana y observar: ❑ Que el sitio Web se cargue correctamente, es decir que no presente errores de página. ❑ Que el servidor se encuentre funcionando durante las 24 horas del día. ❑ Que la velocidad en la exploración y la realización de las operaciones sea razonable. ❑ Que se encuentre en pleno trabajo todas las funciones y servicios proporcionados en la página Web.				
14	Revisar los contratos de servicio de Internet y verificar las garantía que ofrece el				

	proveedor del servicio en caso de fallas o clausura de éste.				
15	Solicitar los planes de contingencia que poseen en caso de cualquier contingencia que imposibilite parcial o totalmente el funcionamiento del E-commerce, y evaluar la razonabilidad y factibilidad material de los mismos.				
16	Solicitar un inventario de todo el software que posee el comercio (aplicaciones y utilitarios) y realizar los siguientes procedimientos: ❑ Verificar que cada uno de ellos este registrado a nombre de la empresa (los que no son gratuitos). ❑ Realizar un muestreo del 5% y corroborar su existencia así como su pleno funcionamiento. ❑ Corroborar que se encuentre almacenados en el ordenador indicado según el inventario.				
17	Ingresar al servidor principal y corroborar el sistema operativo que posee (Windows 2000, Windows 2000 Server, Windows NT, UNÍX, LINUX, entre otros)				
18	Dependiendo el sistema operativo así serán los sistemas y rutinas de seguridad que posean, sin embargo éstos deben contar con componentes básicos de seguridad, por tanto, revisar que el sistema posea: ❑ Bitácora de todos los sucesos surgidos en la red que administra. ❑ Auditorias del sistema en cuanto a rastreo de sucesos y procesos.				
19	Cerciorarse que se estén realizando auditorias a la red o al sistema, en lo referente, a cuentas de usuario, sistemas de archivo e impresoras.				
20	Corroborar la existencia de cortafuegos. Hacer una lista de los mismos describiendo su función principal y verificar su última actualización.				
21	Enlistar los antivirus que se poseen tanto en el servidor como en cada estación de trabajo. Verificar su última actualización.				
22	Verificar que se estén haciendo copias de				

	respaldo de la información importante periódicamente, ya sea a través de medios de almacenamiento óptico, magnéticos, o backup de servidor en otras regiones.				
23	Solicitar el inventario de las copias de seguridad, y cerciorarse que se encuentren en un lugar distinto al establecimiento del comercio.				
24	Solicitar la colaboración de un experto para evaluar si el hardware y software de la compañía tiene la capacidad necesaria para soportar E-commerce con un volumen de transacciones cuantioso.				
25	Solicitar el inventario de Hardware y verificar a través de una muestra razonable: ❑ La existencia. ❑ La obsolescencia. ❑ El buen funcionamiento. ❑ Que se encuentren ubicados, según inventario.				
26	Observar y evaluar si las instalaciones físicas son idóneas para resguardar el equipo informático, para lo cual se debe verificar que: ❑ Exista una temperatura apropiada para el mantenimiento del sistema (Aire acondicionado). ❑ Las instalaciones sean herméticas en cuanto a la humedad. ❑ Existan sistemas de alarma contra incendios y suficientes extinguidores. ❑ Se tenga una adecuada tensión eléctrica. ❑ Se posean polarizaciones en los tomacorrientes donde se conecta el equipo. ❑ Se tengan reguladores de voltaje y UPS. ❑ En el lugar donde se encuentra el equipo principal tal como el servidor sea de acceso restringido, solo para personal autorizado y que cuente con las medidas de seguridad tendientes a cumplir con estas condiciones, tal como la utilización de cerraduras eléctricas, donde el personal autorizado posea claves de acceso o tarjetas magnéticas.				

3. Dependiendo de los resultados de la evaluación obtenidos con la aplicación del programa propuesto, así será el riesgo de auditoria del área en cuestión, por tanto éste dependerá de la ponderación de los siguientes factores materiales:

   a) Seguridad de cumplimiento de normas y estándares.
   b) Seguridad de Sistema Operativo.
   c) Seguridad de Software.
   d) Seguridad de Comunicaciones.
   e) Seguridad de Base de Datos.
   f) Seguridad de Proceso.
   g) Seguridad de Aplicaciones.
   h) Seguridad Física.

Para hacer la valoración del riesgo se sugiere se utilice el siguiente procedimiento: si el resultado de la evaluación para cada uno de estos factores es favorable (sí hay seguridad de cumplimiento de normas y estándares, si existe seguridad de Sistema Operativo, etc.) se le asigna una ponderación de 3 puntos para la seguridad de cumplimiento de normas y estándares y 6 punto a los restantes; si la referida evaluación no es muy favorable, se le asignan 2 puntos para la seguridad de cumplimiento de normas y estándares y 3 punto a los restantes; y si la evaluación es desfavorable es decir que no concurra ninguno de los factores señalados, la ponderación para cada uno será de 1 punto. La calificación máxima que se puede obtener es

de 45 puntos, esto dará un 100% de seguridad. El parámetro para validar la seguridad en esta área será del 70%, por debajo del cual se enciende la luz roja de alarma para el auditor, indicándole que existe una grave desviación y deficiencia en la seguridad correspondiente a esta región. La matriz elaborada de tal ponderación, será similar a la propuesta en el área de seguridad en red.

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

4.1.1. Las empresas dedicadas al comercio electrónico en El Salvador poseen dos estructuras básicas de comercio: una como tienda virtual, es decir, aquella que hace uso de Internet como único canal de distribución de sus productos, y la otra como canal virtual, en la cual el Internet es un canal mas de distribución.

4.1.2. Cualquier estructura básica de comercio electrónico (tienda virtual o canal virtual), posee cuatro áreas básicas de evaluación, en cuanto a los aspectos de seguridad en su contenido integral: Seguridad en Logística de Operaciones, Seguridad en Red, Seguridad en el Uso y Manejo de la Información de los Clientes y Seguridad Lógica y Física.

4.1.3. La tecnología esta haciendo su parte para asegurar las transacciones en línea, de tal forma que, como se ha mencionado en el cuerpo de este trabajo, se han desarrollado protocolos de seguridad que proveen confianza razonable en las comunicaciones de datos sensibles a través de Internet, además, existen compañías que certifican la autenticidad del comercio en la gran telaraña mundial.

4.1.4. Amarrada a la seguridad en la logística de operaciones y en la red, se encuentra la “Seguridad y Confidencialidad con la Información recabada de los Clientes”, y es que, en este mundo informatizado, el factor preponderante es la información, en consecuencia los datos recabados del publico son la materia prima para los E-commerce, es su fuente de sustento para realizar sus operaciones. Sin embargo esto choca con la reticencia de los consumidores a enviar sus datos personales como su nombre, dirección, teléfono, numero de tarjeta de crédito, entre otros; ya no por la seguridad de éstos en su transito a través de Internet, sino mas bien por el uso o trato del que serán objeto por los comercios.

4.1.5. En el Salvador, la mayoría de empresas que se dedican al comercio electrónico, no poseen un servidor propio para alojar el comercio electrónico, lo cual es favorable para que terceras personas puedan tener acceso a información confidencial.

4.2. RECOMENDACIONES

4.2.1. Con la finalidad de determinar y evaluar riesgos en el área de logística de operaciones es necesario que el auditor conozca con claridad frente a que estructura de comercio electrónico esta trabajando (tienda virtual en sentido amplio o estricto, o canal virtual), por tanto se recomienda utilizar el instrumento proporcionado en este trabajo donde se plasman los

procedimientos para conocer la estructura del comercio electrónico .

4.2.2. En lo que respecta a la seguridad en red, el auditor solamente se tiene que limitar, hacer una evaluación taxativa de los aspectos esenciales a los cuales se ha hecho alusión en este compendio, de tal forma, que no es necesario ahondar en asuntos técnicos, sin embargo esto no obsta para que conozca de manera general sobre estos aspectos; si fuese necesario el conocimiento a fondo de ellos lo mas prudente es acudir a la ayuda de un experto.

4.2.3. El auditor al evaluar un Comercio Electrónico, debe examinar a fondo las políticas de privacidad y uso de la información recabada de los clientes para poder detectar cualquier tipo de deficiencias normativas en cuanto a la seguridad de los datos, así mismo debe hacer un examen de la base tecnológica soporte de la información, como lo es la robustez tanto del software como del hardware.

4.2.4. Ante la carencia de un servidor propio, donde se albergue el sitio web, el auditor debe ser acucioso y tener el debido cuidado, en la revisión concerniente al manejo de la información “confidencial de los clientes”, ya que como se ha hecho mención en este estudio, existe un alto riesgo en cuanto al manejo y uso de aquella, cuando existen empresas intermediarias que prestan

el servicio de alojamiento, debido que quien procesa la información de primera mano es el prestador del servicio y no el comercio electrónico.

4.2.5. En este trabajo se han elaborado los instrumentos que contienen las técnicas y procedimientos de auditoria para que el auditor pueda obtener evidencia virtual suficiente y competente correspondiente a cada área de evaluación en un comercio electrónico (Seguridad en Logística de Operaciones, Seguridad en Red, Seguridad en el Uso y Manejo de la Información de los Clientes y Seguridad Lógica y Física) incluyendo el conocimiento del negocio, por tanto se recomienda la utilización de estos instrumentos en la ejecución de una auditoria de seguridad en los E-commerce, adaptándolos a las particularidades de cada uno de ellos.

BIBLIOGRAFÍA

- **LIBROS**

  - Bernal, Cesar Augusto. Metodología de la investigación. Editorial Prentice Hall. Colombia, 2000.
  - Catacora Carpio, Fernando. Sistemas y procedimientos contables. Editorial Mc Gregor Hill. Colombia, 2000.
  - Echenique García, José A. Auditoria en informática. Editorial Mc Gregor Hill. Mexico, 2º edición, 1999.
  - Hernández Sampieri, Roberto. Metodología de la investigación. Editorial Mc Gregor Hill. México, 2º edición, 2001.
  - IFAC, Normas Internacionales de Auditoria. IFAC, edición 2001.
  - Muñoz Razo, Carlos. Auditoria en sistemas computacionales. Editorial Prentice Hall. México, 2002.
  - O´Brien, James A. Sistemas de información gerencial. Editorial Mc Gregor Hill. USA, 4º edición, 2001.
  - O. Ray Whittingtong y Kurt Pany. Auditoria un enfoque integral. Editorial Mc Gregor Hill. Colombia 12 º edición, 2001.

- **FOLLETOS**
  - Naranjo S. Alice. Auditoria de sistemas. Profesor de la universidad de Guayaquil Facultad de Filosofía - Especialidad informática.
  - Huertas, Ivonne L. E-Bussines: ¿Oportunidad o riesgos peligrosos de las nuevas formas de hacer negocios para el contador del nuevo milenio?. Conferencia Interamericana de Contadores. Puerto Rico. Noviembre, 2001.
  - Villarmarzo, Ricardo. Comercio electrónico y auditoria: un razonamiento posible y necesario. Conferencia Interamericana de Contadores. Noviembre, 2001.

- **PÁGINAS WEB VISITADAS**
  - www.monografias.com
  - www.arrobadeoro.com
  - www.cybercash.com
  - www.sociedaddeinternautas.org.es
  - www.ifac.org
  - www.yahoo.es

ANEXOS

ANEXO 1.1. CUADRO Nº 1: LA AUDITORIA

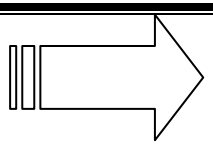
<table>
<tr><td rowspan="9">LA AUDITORIA

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la Ley
Fue hasta 1912, que Montgomery establece que los objetivos de la Auditoría eran
La detección y prevención de fraude y la detección y prevención de errores; sin embargo, en los años siguientes hubo un cambio decisivo en la demanda y el servicio, y los propósitos actuales son: El cerciorarse de la condición financiera actual y de las ganancias de una empresa</td><td>CONCEPTO</td><td colspan="3">“Es la revisión independiente de alguna o algunas actividades, funciones especificas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoria, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.” Muñoz Razo</td></tr>
<tr><td rowspan="8">TIPOS DE AUDITORIA</td><td rowspan="2">SEGÚN EL LUGAR DE APLICACION</td><td>INTERNA
NIA 610 Párr. 3</td><td>Es la revisión que realiza un profesional de la auditoría, cuya relación de trabajo es directa y subordinada a la institución donde se aplicará la misma,</td></tr>
<tr><td>❖EXTERNA</td><td>Es la revisión independiente, que realiza un profesional de la auditoría, con total libertad de criterio y sin ninguna influencia</td></tr>
<tr><td rowspan="6">SEGÚN EL AREA DE APLICACIÓN</td><td>❖FINANCIERA</td><td>Es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la razonabilidad y veracidad de las cifras consignadas en los estados financieros obtenidos durante un período especifico</td></tr>
<tr><td>❖ADMINISTRATIVA</td><td>Es el revisar y evaluar si los métodos, sistemas y procedimientos que se siguen en todas las fases del proceso administrativo, aseguran el cumplimiento de políticas, planes, programas, leyes y reglamentaciones</td></tr>
<tr><td>❖OPERACIONAL</td><td>Es el examen posterior, profesional, objetivo y sistemático de la totalidad o parte de las operaciones o actividades de una entidad, proyecto, programa, inversión o contrato en particular, sus unidades integrantes u operacionales específicas</td></tr>
<tr><td>❖INTEGRAL</td><td>Tiene por objeto el examen de la gestión de una empresa con el propósito de evaluar la eficacia de sus resultados con respecto a las metas previstas, los recursos humanos, financieros y técnicos utilizados, la organización y coordinación de dichos recursos y los controles establecidos sobre dicha gestión</td></tr>
<tr><td>❖DE CUMPLIMIENTO</td><td>Es la comprobación o examen de operaciones financieras, administrativas, económicas y de otra índole de una entidad para establecer que se han realizado conforme a las normas legales, reglamentarias, estatuarias y de procedimientos que le son aplicables.</td></tr>
<tr><td>❖FISCAL</td><td>El propósito de esta auditoria es la correcta elaboración de los resultados financieros de un Ejercicio Fiscal</td></tr>
</table>

Fuente: Elaborado por Equipo de Trabajo Nº 59

			❖AMBIENTAL	Es la evaluación que se hace de la calidad del aire, la atmósfera, el ambiente, las aguas, ríos, lagos y océanos, asi como de la conservación de la flora y la fauna silvestre, con el fin de dictaminar sobre las medidas preventivas y, en su caso, correctivas que disminuyan y eviten la contaminación provocada por los individuos, las empresas, los automotores y las maquinarias, y asi preservar la naturaleza y mejorar la calidad de vida de la sociedad.
			❖ DE SISTEMAS DE INFORMACION	Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes
	OBJETIVOS NIA 200 Par. 2		❖ Revisión independiente de las actividades, áreas o funciones especiales de una institución ❖ Revisión especializada del aspecto contable, financiero y operacional de las áreas de una empresa ❖Evaluar el cumplimiento de planes, programas, políticas y normas ❖Dictaminar Resultados	
	NORMATIVA TECNICA	**NAGAS**		
		NIAS	NIA 200 Párr. 5	
	CONTROL INTERNO NIA 400	**DEFINICION NIA 400 Párr. 8**	Es un instrumento de gestión que comprende el plan de la empresa, conjuntos y procedimientos adoptados para salvaguardar su patrimonio, verificar la exactitud y veracidad de su información financiera y administrativa, promover la eficiencia en las operaciones, estimular las políticas y comprender el cumplimiento de las metas y objetivos programados.	
		OBJETIVOS	❖ Establecer la seguridad y protección de los activos de la empresa. ❖ Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa. ❖ Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.	
		IMPORTANCIA	Permiten llevar la administración de la empresa con eficiencia y eficacia	
		COMPONENTES DE CONTROL INTERNO	❖ Entorno de Control ❖ Evaluación de Riesgos (NIA 400 Párr. 11-12, 21-24 y 41-42) ❖ Actividades de Control (NIA 400 Párr. 20) ❖ Información y Comunicación (NIA 400 Párr. 49) ❖ Supervisión	
	FASES	**PLANEACION**	NIA 300	
		EJECUCION		
		CIERRE	NIA 700	

ANEXO 1.2. CUADRO Nº 2: AUDITORÍA EN SISTEMAS DE INFORMACIÓN

<table>
<tr><td rowspan="8"> 

AUDITORIA EN SISTEMAS DE INFORMACION

Es el examen o revisión de carácter objetivo (independiente), crítico(evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a:
❖Eficiencia en el uso de los recursos informáticos
❖Validez de la información</td><td>OBJETIVOS GENERALES</td><td colspan="2">✓ Evaluar el grado de efectividad de las Tecnologías de Información, su grado de Eficacia, Eficiencia, Confiabilidad e Integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.</td></tr>
<tr><td>JUSTIIFICATIVOS PARA EFECTUAR UNA AUDITORIA DE SISTEMAS</td><td colspan="2">❖Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos)
❖Desconocimiento en el nivel directivo de la situación informática de la empresa
❖Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información, descubrimiento de fraudes efectuados con el computador, falta de una planificación informática
❖Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano
❖Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados</td></tr>
<tr><td rowspan="2">CONTROL INTERNO

DIPA 1002 Párr. 20-22</td><td>OBJETIVOS</td><td>❖Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa.
❖Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento y la emisión de informes en la empresa.
❖Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa</td></tr>
<tr><td>ELEMENTOS</td><td>❖Controles Internos sobre la Organización del área de Informática
❖Controles Internos sobre el análisis, desarrollo e implementación de sistemas
❖Controles Internos sobre la operación del Sistema
❖Controles Internos sobre los Procedimientos de entrada de datos, el procesamiento de Información y la emisión de resultados</td></tr>
<tr><td rowspan="4">METODOLOGIA DE UNA AUDITORIA DE SISTEMAS</td><td>ESTUDIO PRELIMINAR</td><td>Consiste en definir el grupo de trabajo, el programa de auditoría, plan de actividades, manuales de políticas reglamentos, entrevistas con los principales funcionarios del PAD, con el fin de evaluar preliminarmente el control interno.</td></tr>
<tr><td>REVISION Y EVALUACION DE CONTROLES Y SEGURIDADES</td><td>Consiste en la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas criticas, Revisión de procesos históricos (backups), Revisión de documentación y archivos, entre otras actividades.</td></tr>
<tr><td>EXAMEN DETALLADO DE ÁREAS CRÍTICAS</td><td>En esta fase el Auditor, establecerá los motivos, objetivos, alcance Recursos que usará, definirá la metodología de trabajo, la duración de la auditoría, Presentará el plan de trabajo y analizará detalladamente cada problema encontrado</td></tr>
<tr><td>COMUNICACIÓN DE RESULTADOS</td><td>Se realiza por medio de la presentación del Informe, en el cual se da a conocer los puntos críticos encontrados, los efectos y las recomendaciones de la Auditoría.</td></tr>
</table>

Fuente: Elaborado por Equipo de Trabajo Nº 59

ANEXO 1.3. CUADRO Nº 3: LA EVIDENCIA DE AUDITORIA

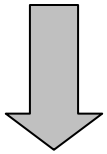
<table>
<tr><td rowspan="11">EVIDENCIA:
“Es toda la información obtenida por el auditor para llegar a las conclusiones sobre las que se basa su opinión”.

NIA 500 Párr. 4</td><td rowspan="2">CARACTERISTICAS
NIA 500 Párr. 7</td><td>SUFICIENTE</td><td colspan="2">Es aquel nivel de evidencia que el contador público debe obtener a través de las pruebas de auditoría para llegar a conclusiones razonables sobre las cuentas que se someten a su examen.</td></tr>
<tr><td>COMPETENTE</td><td colspan="2">Es competente o adecuada cuando sea útil al contador publico para emitir un juicio profesional.
Para ser competente la evidencia debe ser:
❖Relevante : esta debe relacionarse con el objetivo de la auditoría que se esta probando
❖Válida: esta depende de las circunstancias en las cuales esta se obtiene</td></tr>
<tr><td rowspan="5">TIPOS DE EVIDENCIA
NIA 500 Párr. 15-16</td><td rowspan="2">DE ACUERDO A SU FUENTE</td><td>INTERNA</td><td>Es la información obtenida por personas de la empresa; son generalmente menos confiables que los externos, sin embargo, esto depende de los procedimientos de controles internos existentes y aplicables en la empresa.</td></tr>
<tr><td>EXTERNA</td><td>Es la información obtenida por terceras personas, ajenas a la empresa; tienen un alto grado de confiabilidad, siempre y cuando sean enviadas directamente al auditor y recibido por él sin la intervención de personal del cliente.</td></tr>
<tr><td rowspan="3">DE ACUERDO A SU NATURALEZA</td><td>FÍSICA</td><td>Es la evidencia que los auditores realmente pueden ver</td></tr>
<tr><td>DOCUMENTAL</td><td>Es el examen que hace el auditor de los documentos y archivos del cliente para apoyar la información que es o debe ser incluida en los estados financieros</td></tr>
<tr><td>VIRTUAL</td><td>Es la información obtenida por el auditor con existencia aparente (visual) y no real, es decir no es presencial, lo que se hace o existe en el ciberespacio con el propósito de llegar a conclusiones para basar su auditoria, sin embargo no solo este tipo de factores constituyen evidencia virtual, sino que también toda aquella información, hecho o circunstancia derivada de transacciones realizadas por los E-commerce, en su mayoría virtuales, que sirvan para sustentar o refutar la información obtenida durante el proceso de auditoria o evaluación del comercio electrónico en los componentes de seguridad, en su contenido integral.</td></tr>
<tr><td rowspan="3">PROCEDIMIENTOS :DE AUDITORIA
NIA 500 Párr. 19</td><td>CONCEPTO</td><td colspan="2">Son el conjunto de técnicas de investigación y pruebas que el auditor utiliza para lograr la información y comprobación necesaria para poder presentar y fundamentar un informe de auditoria.</td></tr>
<tr><td>OPORTUNIDAD</td><td colspan="2">Son el conjunto de técnicas de investigación y pruebas que el auditor utiliza para lograr la información y comprobación necesaria para poder presentar y fundamentar un informe de auditoria.</td></tr>
<tr><td>TIPOS
NIA 500 Párr. 19-25</td><td colspan="2">❖Inspección (NIA 500 Párr. 20)
❖Observación (NIA 500 Párr. 21)
❖Investigación y Confirmación(NIA 500 Párr. 22-23)
❖Procedimiento de Cómputo (NIA 500 Párr. 24)
❖Procedimiento Analítico (NIA 500 Párr. 25)</td></tr>
</table>

ANEXO 1.4. CUADRO N° 4: EL COMERCIO ELECTRONICO

<table>
<tr><td rowspan="10">COMERCIO ELECTRONCIO

Es el uso de las tecnologías computacional y de telecomunicaciones que se realiza entre empresas o bien entre vendedores y compradores, para apoyar el comercio de bienes y servicios.”

TIENDA VIRTUAL
no tiene almacén, posee una estructura organizacional relativamente pequeña, no posee una plaza física y tiene poca inversión en activo fijo.

CANAL VIRTUAL
es un medio de distribución de productos a través de la World Wibe Web por parte de una empresa, sin que esta sea precisamente una tienda virtual.</td><td rowspan="2">INTERNET</td><td>DEFINICION</td><td>❖Se conoce como la “Red de Redes” o la “Autopista de la información”, ya que efectivamente es una Red puesto que gran cantidad de ordenadores locales están conectados entre si y estos a su vez están conectados con otros ordenadores a nivel mundial, esta conexión se da a través de satélites y cables. Prácticamente todos los países del mundo tienen acceso a Internet</td></tr>
<tr><td>SERVICIOS</td><td>❖Correo Electrónico,
❖World Wide Web, FTP,
❖Grupos de Noticias, IRC y
❖Servicios de Telefonía.</td></tr>
<tr><td rowspan="5">TIPOS DE COMERCIO ELECTRONICO</td><td>EMPRESA-EMPRESA</td><td>Las partes que hacen negocio o extienden sus procesos son dos empresas</td></tr>
<tr><td>EMPRESA-CONSUMIDOR</td><td>Se refieren a una empresa que vende sus productos o servicios a través de Internet, dirigida directamente al consumidor.</td></tr>
<tr><td>EMPRESA- GOBIERNO</td><td>La relación entre el gobierno y ciudadanos, que más que negocios propiamente dicho, se dedica a algún tipo de transacción o tramite por Internet. (Pago de impuestos, quejas o reclamos, denuncias)</td></tr>
<tr><td>CONSUMIDOR-EMPRESA</td><td>En este tipo de Comercio, el consumidor ofrece a las empresas a un precio, un producto o servicio</td></tr>
<tr><td>CONSUMIDOR-CONSUMIDOR</td><td>Consiste en que el consumidor ofrece a otro, sin mediar una empresa en la transacción, productos y servicios, pagando de ser requerida una comisión por la venta</td></tr>
<tr><td>VENTAJAS</td><td colspan="2">❖Permite hacer más eficientes las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
❖••Reduce las barreras de acceso a los mercados actuales, y abre oportunidades de explotar mercados nuevos.
❖••Para el consumidor, amplía su capacidad de acceder a prácticamente cualquier producto y de comparar ofertas, permitiéndole además convertirse en proveedor de información.
❖••Reduce o incluso elimina por completo los intermediarios</td></tr>
<tr><td>DESVENTAJAS</td><td colspan="2">❖La validez legal de las transacciones y contratos “sin papel”.
❖La necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio.
❖El control de las transacciones internacionales, incluido el cobro de impuestos.
❖La protección de los derechos de propiedad intelectual.
❖La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales.
❖La dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica.
❖La seguridad de las transacciones y medios de pago electrónicos.
❖La falta de estándares consolidados y la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.</td></tr>
</table>

Fuente: Elaborado por Equipo Nº 59

ANEXO 1.5. CUADRO Nº 5: LA SEGURIDAD

<table>
<tr><td rowspan="11">SEGURIDAD
Consiste en implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor.</td><td rowspan="2">TIPOS DE SEGURIDAD</td><td>INTERNA</td><td>Aquélla que intenta mantener privados y accesibles sólo para los usuarios autorizados, aquellos datos internos o sensibles de la organización en cuestión, se basa en la utilización de políticas de contraseñas, encriptado de material sensible y control de acceso a los contenedores de información</td></tr>
<tr><td>EXTERNA</td><td>Son todos aquellos mecanismos diseñados y empleados para bloquear el acceso a los usuarios externos a áreas de la red que están restringidas para uso interno.</td></tr>
<tr><td rowspan="9">HERRAMIENTAS DE SEGURIDAD

Características:

❖Confidencialidad
❖Integridad
❖Autenticación
❖Irrefutabilidad

AMENAZAS A LA SEGURIDAD EN INFORMATICA

POLITICAS Y MEDIDAS DE SEGURIDAD DIPA 1008 Párr. 8-11</td><td>ENCRIPTACION</td><td>Es el conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada.</td></tr>
<tr><td>FIRMA DIGITAL</td><td>Es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad)</td></tr>
<tr><td>PROTOCOLO SET</td><td>Seguridad Electrónica de Transacciones, utiliza para sus procesos de encriptación dos algoritmos: a) De Clave Pública RSA (Algoritmo Simétrico) y b) De Clave Privada DES (Algoritmo Asimétrico)</td></tr>
<tr><td>ALGORITMOS DE DESTILACION</td><td>Son Algoritmos de comprensión necesarios para conseguir que la firma digital tenga los mismos efectos que la manuscrita; los cuales se aplican sobre un determinado texto en cuestión, donde no es necesaria la tenencia de una clave, ya que aplican funciones matemáticas para cifrar.</td></tr>
<tr><td>HACKER (Piratas Informáticos)</td><td>Aquellos que, con ayuda de sus conocimientos informáticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra.</td></tr>
<tr><td rowspan="2">CRACKER (Usurpadores de Claves)</td><td>CRACKER PIRATA: Aquellos que se dedican a copiar Juegos.</td></tr>
<tr><td>CRACKER VÁNDALO; Se dedica a asaltar a los navegantes, meterse en sus computadoras y destruir, sólo por el placer de hacerlo</td></tr>
<tr><td colspan="2">Políticas de seguridad de redes de comunicación</td></tr>
<tr><td colspan="2">Políticas de seguridad de la red física</td></tr>
<tr><td colspan="2">Políticas de seguridad de la red lógica</td></tr>
</table>

Fuente: Elaborado por Equipo Nº 59

ANEXO 1.6. CUADRO Nº 6: MEDIOS DE PAGO EN EL COMERCIO ELECTRONICO

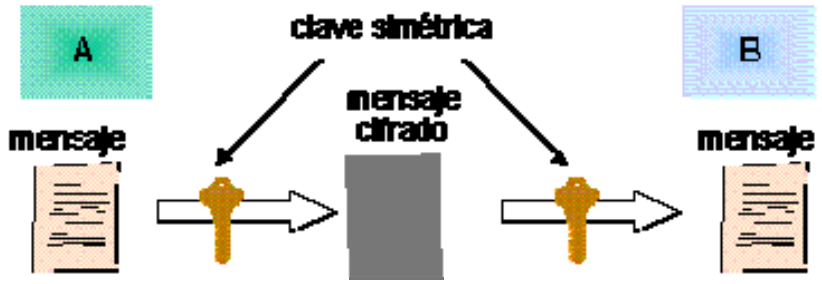
MEDIOS DE PAGO	**MEDIOS DE PAGO GENERALES**	**CONTRA REEMBOLSO**	Medio de pago, el cual implica la utilización del dinero en efectivo
		CARGOS EN CUENTA	Suele emplearse para cargos periódicos o suscripciones
	MEDIOS DE PAGO ESPECIFICOS	**TARJETAS DE DEBITO Y CREDITO**	Estas han permitido la realización de transacciones comerciales en el nuevo medio a través de la utilización de los procedimientos de liquidación y pago preestablecidos, en donde la transacción es ordenada en la red y la validación y realización efectiva del pago es realizada a a través de los circuitos tradicionales de procesamiento de operaciones con tarjeta de crédito.
		TARJETAS CHIP	Aquellas que poseen una capacidad de almacenamiento ya sea de una identificación que incluye determinadas claves cifradas o una cantidad de dinero disponible
		CIBERCASH	Es un sistema de realización de transacciones en Internet mediante el uso de tarjetas de crédito.
		FIRST VIRTUAL	Es un sistema de pagos operado por First USA y EDS, basado en el mantenimiento de cuentas virtuales de clientes que se liquidan periódicamente contra tarjetas de crédito

Fuente: Elaborado por Equipo Nº 59

ANEXOS 1.7.

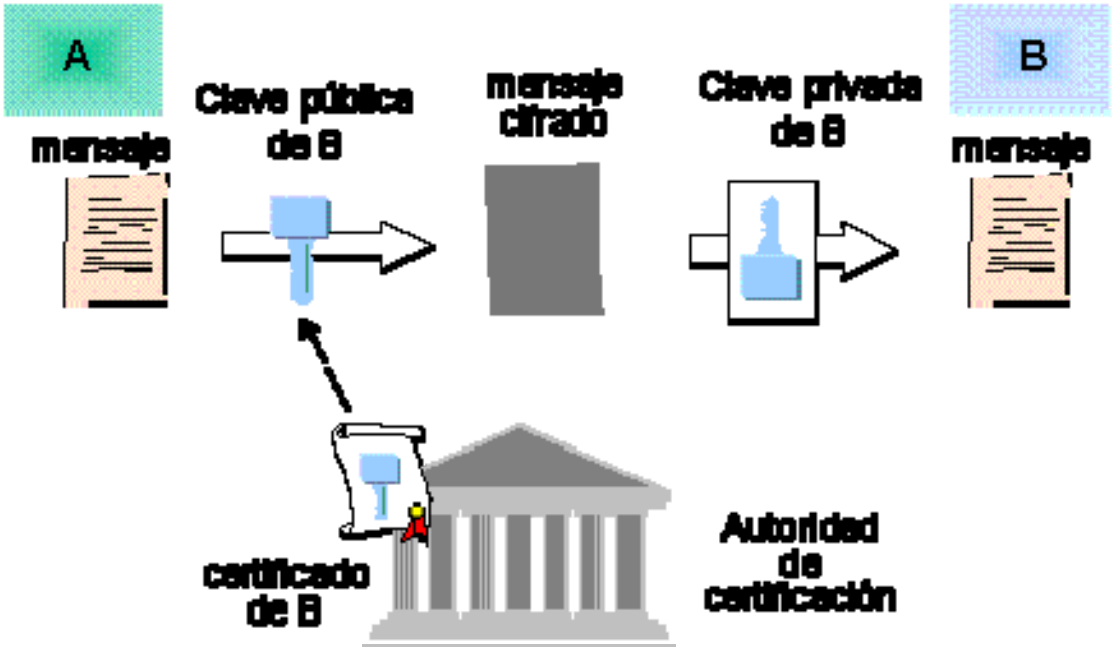
Anexo 1.7a

Proceso de encriptación simétrico, cifrado y descifrado simétrico



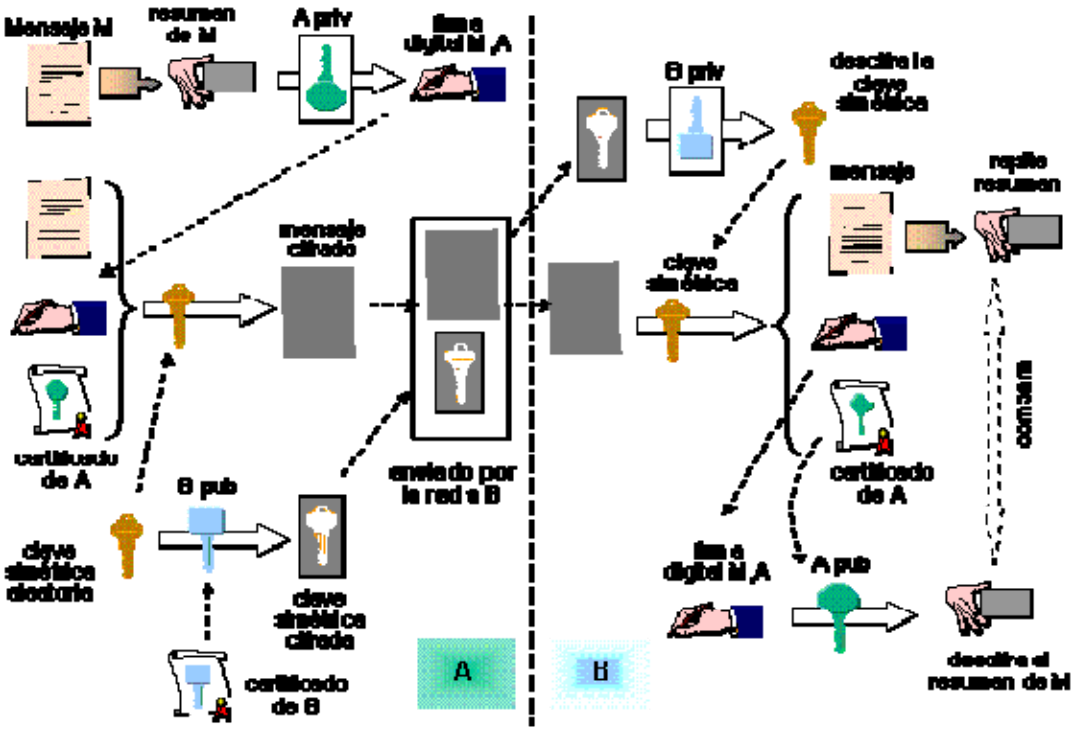
Anexo 1.7.b.

Cifrado asimétrico con consulta de clave pública a autoridad de certificación y descifrado con clave privada del destinatario



Anexo 1.7.c.

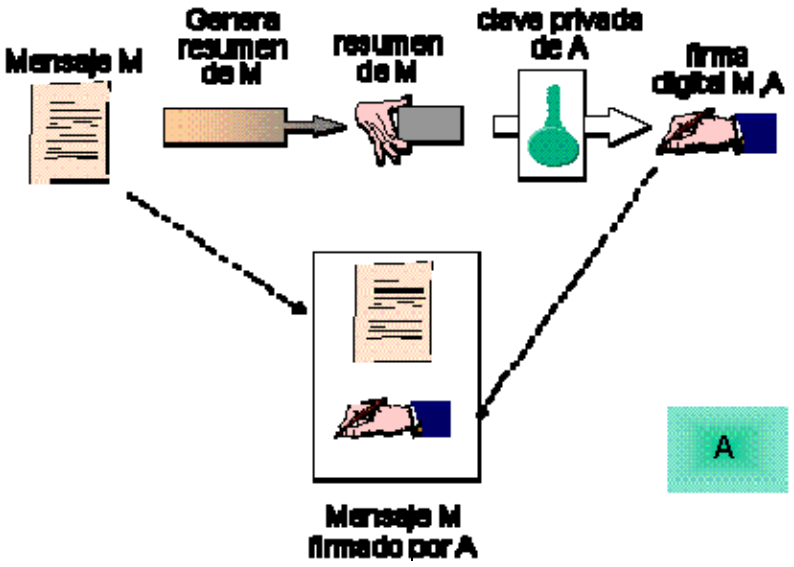
Esquema de cifrado en SET



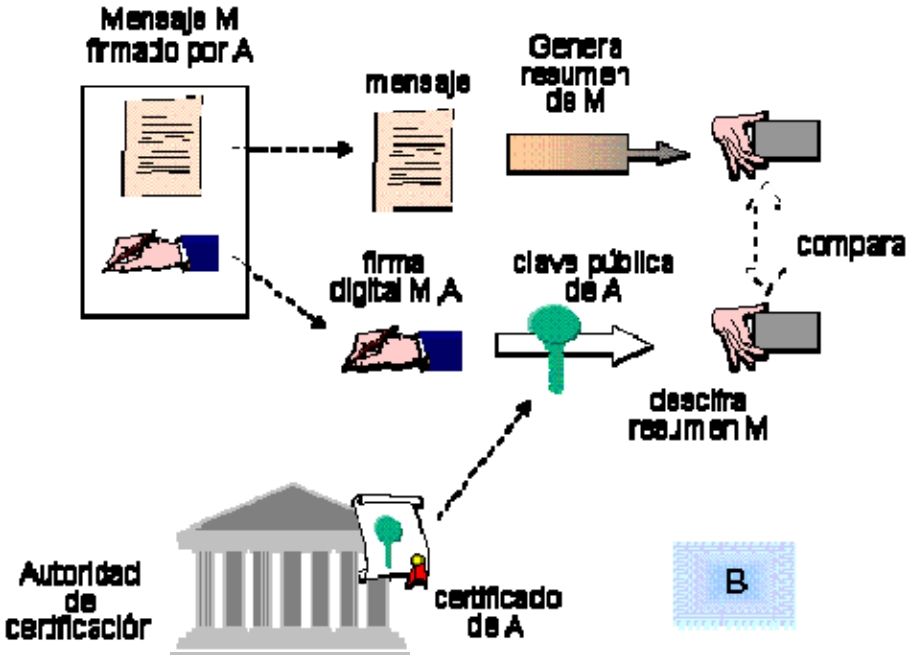
Apub, Apriv: claves pública y privada de A; Bpub, Bpriv: claves pública y privada de B

Anexo 1.7.d

Generación de la firma digital de un mensaje



Comprobación de una firma digital



ANEXO 2.1:
LISTA DE EMPRESAS QUE REALIZAN COMERCIO ELECTRÓNICO.

Nº	EMPRESA	PAGINA WEB	GIRO O ACTIVIDAD
1	ALMACENES SIMAN	www.siman.com	Venta de Artículos varios
2	AQUITEMANDO.COM	www.aquitemando.com	Venta de productos para el consumo y el hogar
3	CLUBCOMPRAFACIL.COM	www.clubcomprafacil.com	Comercio de artículos varios para el hogar
4	COEX CAFE	www.coexcafe.com	Venta de café
5	COFFE NEST	www.coffenest.com	Comercio y exportación de café
6	DATA POINT	www.data-point.com	Venta de equipo de computo
7	EQUIPOS ELECTRÓNICOS VALDÉS	www.eevales.com	Venta de equipo informático
8	ESTUDIOS RAF	www.raf.com.sv	Industrias fotográficas
9	FARMACIA SAN NICOLÁS	www.farmaciasannicaolas.com	Cadena de farmacias
10	FLORISTERÍA BELLA FLOR	www.mercaditos.com/floristeriabellaflor	Venta de arreglos florales
11	FLORISTERÍA TAMARA	www.floristeriatamara.com	Venta de arreglos florales
12	GEVESA	www.gevesa.com	Venta de automóviles y accesorios
13	GRUPO TV OFFER	www.grupotvoffer.com	Venta de artículos varios
14	LA CURACAO	www.curacaonet.com	Venta de electrodomésticos
15	LIBRERÍA FEPADE	www.fepade.com/libros	Ventas de libros

16	MERCADITOS.COM	www.mercaditos.com	Tienda virtual
17	MESA DE REGALOS	www.mercaditos.com/mesaderegalos	Venta de artículos varios
18	OFERTON	www.oferton.com	Venta de equipo informatico
19	PANADERÍA SANTA EDUVIGIS	www.santaeduvigies.com	Venta de pan
20	PARAELHOGAR.COM	www.paraelhogar.com	Venta de alimento
21	PASTELERÍA SWEETE	www.mercaditos.com/pasteleriasweet	Venta de pasteles
22	PULGOTIENDA.COM	www.pulgotienda.com	Venta de artículos usados
23	REGALIUX.COM	www.regaliux.com	Venta de regalos para el hogar y familia
24	RESTAURANTES PIZZA HUT	www.elsalvadorpizza.com	Venta de alimentos
25	TU CANASTERIA.COM	www.tucanasteria.com	Venta de canasta con productos comestibles
26	TU TIENDONA.COM	www.tutiendona.com	Venta de productos para el hermano lejano
27	VIVERO LA MASCOTA	www.mercaditos.com/viverolamascota	Venta de plantas

ANEXO 2.2. PROCESAMIENTO DE LA INFORMACIÓN

ÁREA: CONOCIMIENTO DEL NEGOCIO

MACRO – OBJETIVO: Conocer de manera general el volumen de operaciones de comercio electrónico que realizan las empresas, a través de un canal virtual o tienda virtual. Con el fin de determinar la materialidad y la importancia relativa de las operaciones de las empresas.

1. ¿Cuántos empleados tiene la empresa?

OBJETIVO: Tener un conocimiento aceptable del negocio en cuanto a su tamaño, de tal forma que se pueda acceder a una comprensión mas adecuada de sus operaciones.

NUMERO DE EMPLEADOS QUE POSEE LA EMPRESA		
N° de Empleados	**Frecuencia Absoluta**	**Frecuencia Relativa**
0 - 10	7	41.18%
11 - 20	2	11.76%
21 - 30	1	5.88%
31 - 40	0	0.00%
41 - 50	1	5.88%
Mas de 50	6	35.29%
Total	17	100.00%

Análisis

Se puede observar que la mayoría de empresas que se dedican a efectuar operaciones de comercio electrónico, poseen diez empleados o menos representando un 41.18% de las empresas

encuestadas. Esto afirma la tesis que las empresas dedicadas únicamente al comercio electrónico (tiendas virtuales) funcionan con una utilización mínima de recursos, ya que por la inherencia de sus transacciones (automatizadas), no requieren en gran medida de la intervención de la mano del hombre; esto se debe también a que las actividades de reparto, entre otras, son subcontratadas. No obstante a lo antes mencionado, se puede verificar que una buena proporción de las empresas en cuestión (35.29%) tienen mas de 50 empleados. La explicación a este fenómeno es que, estas empresas son las que poseen un canal virtual, como uno de los muchos medios de comercialización de sus productos, es decir, no son enteramente tiendas virtuales, las cuales tienen una organización robusta y una estructuración tradicional.

2. **¿A cuánto Asciende el promedio de ingresos mensuales del comercio electrónico o canal virtual?**

OBJETIVO: Conocer el volumen de operaciones de las empresas dedicadas al comercio electrónico, que se ve reflejado en el promedio mensual de ingresos.

PROMEDIO DE INGRESOS MENSUALES DEL COMERCIO ELECTRÓNICO O CANAL VIRTUAL		
Ingresos	**Frecuencia Absoluta**	**Frecuencia Relativa**
De 0 a $1,000	9	52.94%
De $1,000 a $2,000	2	11.76%
De $2,000 a $3,000	1	5.88%
De $3,000 a $4,000	0	0.00%
De $4,000 a 5,000	1	5.88%
De $5000 a $6000	0	0.00%
De $6000 a $7000	0	0.00%
De $7000 a $8000	0	0.00%
De $8000 a 9000	0	0.00%
De $9000 a 10,000	0	0.00%
De $10,000 a 11,000	0	0.00%
Mas de $11,000	1	5.88%
No contestaron	3	17.65%
Total	**17**	**100.00%**

Análisis

En el cuadro anterior se puede verificar que la mayoría de empresas encuestadas obtienen un promedio de ingreso mensual de dos mil dólares o menos, a través de las transacciones de comercio electrónico representando un 64% de la muestra. Con esto se confirma que las tiendas virtuales comienzan a despegar en el país, ya que sus ingresos provenientes de esta actividad son relativamente pequeños.

En el otro extremo se puede observar que un 5.88% de las empresas, tienen ingresos mayores de $11,000, esto se debe a que dicho porcentaje representa a las empresas que poseen un canal virtual que ya están muy bien posesionadas en el mercado, por su imagen, prestigio y tradición; es decir son empresas que inspiran confianza al consumidor.

3. ¿A cuánto asciende el promedio de pedidos recibidos durante el día?

OBJETIVO: Conocer el volumen de operaciones de las empresas dedicadas al comercio electrónico, que se ve reflejado en el número de pedidos recibidos durante un día.

PEDIDOS PROMEDIO RECIBIDO DURANTE 24 HORAS		
Pedidos	Frecuencia Absoluta	Frecuencia Relativa
De 0 a 10	15	88.24%
De 11 a 20	0	0.00%
De 21 a 30	0	0.00%
De 31 a 40	0	0.00%
De 41 a 50	1	5.88%
Mas de 50	0	0.00%
No contestaron	1	5.88%
Total	17	100.00%

Análisis

Se puede observar que en un 88.24% de las empresas encuestadas reciben diez pedidos o menos, en lapso de veinticuatro horas. Esto confirma que el volumen de operaciones es relativamente pequeño en relación a otro tipo de empresas. Sin embargo este factor depende del tipo de producto y la temporada en que se comercializan, ya que hay artículos que se venden en periodos estacionarios como por ejemplo: flores, libros, arreglos, etc.

Por otro lado hay un 5.88% de empresas que reciben entre 41 a 50 pedidos en el transcurso de veinticuatro horas, esto en congruencia con el resultado de la pregunta anterior, son los comercios que están muy bien posesionadas del mercado por los factores mencionados anteriormente.

ANÁLISIS GENERAL DEL ÁREA EVALUADA: CONOCIMIENTO DEL NEGOCIO

En relación a los resultados de las respuestas a las preguntas hechas sobre esta área, se puede decir que la mayoría de las empresas que se dedican a operaciones de comercio electrónico se clasifican en pequeñas o medianas, atendiendo a los parámetros de medición utilizados para tal efecto, como lo son: Numero de empleados, que realmente no es un factor preponderante para distinguir dicha clasificación, no obstante da alguna noción del mismo; promedio de ingresos mensuales, que da un enfoque muy amplio del volumen de transacciones y promedio de pedidos diarios, que básicamente es un parámetro especifico del volumen de operaciones realizadas por las empresas en cuestión.

Atendiendo a la materialidad o importancia relativa, esto responde al tipo de empresas y al área evaluada, por ejemplo, para este estudio no importa el volumen de las transacciones realizadas y por ende la clasificación de las mismas, ya que la medición no es cuantitativa si no cualitativa es decir importa o es material la actividad a la cual se dedican las empresas, puesto que ésta es el objeto de la evaluación.

Hay que aclarar, que la mayoría de tiendas virtuales son empresas pequeñas, entre tanto que las empresas con canales virtuales; son medianas o grandes y se encuentran ya posicionadas en el mercado, y como consecuencia dan mayor seguridad a los clientes.

ÁREA: LOGÍSTICA DE OPERACIONES

MACRO – OBJETIVO: Conocer la capacidad instalada que poseen las empresas para hacer frente a las exigencias de este modelo de negocios, así mismo determinar el flujo de los productos y la logística de operaciones al recibir una orden de pedido. Todo esto incluye el tiempo de respuesta para cada orden, los pedidos rechazados durante un lapso de tiempo, el momento de facturación y los medios de pago aceptados.

4. ¿Cuál es el tiempo promedio de respuesta a los pedidos en horas?

OBJETIVO: Determinar la capacidad instalada que posee la empresa para poder responder a las necesidades de los clientes de recibir sus pedidos en el tiempo menor posible.

TIEMPO PROMEDIO DE RESPUESTA A LAS ORDENES DE PEDIDOS / HORA		
Horas	**Frecuencia Absoluta**	**Frecuencia Relativa**
De 0 a 3	3	17.65%
De 3 a 6	5	29.41%
De 6 a 9	0	0.00%
De 9 a 12	3	17.65%
De 12 a 15	1	5.88%
De 15 a 18	1	5.88%
De 18 a 21	0	0.00%
De 21 a 24	0	0.00%
De 24 a 27	0	0.00%
Mas de 27	2	11.76%
No contestaron	2	11.76%
Total	**17**	**100.00%**

Análisis

Un 29.41% de las empresas encuestadas tardan de 3 a 6 horas en dar respuesta a cada orden de compra o pedido recibido, esto quiere decir que después de haber recibido dicha orden demoran entre 3 a 6 horas para echar andar el aparato logístico, a fin de dar respuesta a la misma. Un 17.65% de empresas tarda tres horas o menos, otro 17.65% tarda de 9 a 12 horas, mientras que un 11.76% tarda más de 27 horas.

Estos tiempos de respuesta son muy importantes, puesto que miden la eficiencia de la logística en las operaciones implementadas por las empresas, la cual da un alto grado de confiabilidad y satisfacción a los clientes.

Muchas empresas poseen políticas de entrega "justo a tiempo" en la cual se estipula un período de tiempo para la entrega del producto, eso depende de la región o país del cliente, después de ese periodo prefijado el producto es gratis.

5. ¿Cuál es el promedio de pedidos (en porcentajes) rechazados por el cliente en el mes?

OBJETIVO: Determinar un rango aceptable de rechazo de pedidos por parte del cliente para conocer los orígenes o causales de los mismos, ya sea por la empresa o por subjetivismo del cliente.

PORCENTAJE PROMEDIO DE PEDIDOS RECHAZADOS POR MES		
Promedio	**Frecuencia Absoluta**	**Frecuencia Relativa**
0%	9	52.94%
1%	5	29.41%
2%	0	0.00%
3%	0	0.00%
4%	0	0.00%
5%	1	5.88%
6%	0	0.00%
7%	0	0.00%
8%	0	0.00%
9%	0	0.00%
10%	0	0.00%
Mas del 10%	0	0.00%
No contestaron	2	11.76%
Total	**17**	**100.00%**

Análisis

Como se puede observar en el cuadro de resultados en la mayoría (52.94%) de empresas no son rechazados los pedidos realizados durante un mes. En un 29.41% de empresas se rechaza el 1% de órdenes al mes y en un 5.88% se rechaza un 5%. Lo cual indica que en este sentido las empresas son eficaces en la logística de operaciones.

6. ¿En qué momento se factura el pedido del cliente?

OBJETIVO: Conocer la logística y políticas en cuanto a la facturación de pedidos, que poseen las empresas dedicadas al comercio electrónico, para determinar el manejo y los sistemas de control utilizados en relación al despacho de la mercadería.

MOMENTO EN QUE SE FACTURA EL PEDIDO		
Facturación	**Frecuencia Absoluta**	**Frecuencia Relativa**
Cuando se recibe el pedido	2	11.76%
Cuando se recibe el pago	4	23.53%
Cuando se entrega el producto	0	0.00%
Cuando se envía el producto	9	52.94%
Al Confirmar el pedido	1	5.88%
No contestaron	1	5.88%
Total	**17**	**100.00%**

Análisis

Según el cuadro anterior se puede apreciar que el 52.94% de las empresas encuestadas facturan el producto cuando se envía, un 23.53% lo hacen cuando se recibe el pago y un 11.76% facturan cuando se recibe el pedido. En realidad en las transacciones electrónicas confluyen dos momentos simultáneamente en la transacción: la recepción del pago y la recepción del pedido, sin embargo esto dependerá de la arquitectura del comercio electrónico.

7. ¿Qué medios de pagos acepta la empresa?

OBJETIVO: Conocer las diferentes formas de pago que se dan en los negocios en línea, por los bienes comercializados.

MEDIOS DE PAGO ACEPTADOS POR LAS EMPRESAS		
Medios de Pago	**Frecuencia Absoluta**	**Frecuencia Relativa**
Tarjeta de Crédito	3	17.65%
Tarjeta de Crédito y Debito	1	5.88%
Tarjeta de Crédito y transferencia Bancaria	1	5.88%
Contra reembolso y financiación	1	5.88%
Tarjeta de Crédito, Transferencia bancaria y tarjeta Credisiman	1	5.88%
Tarjeta de Crédito, debito, Contra reembolso y Transferencia Bancaria	1	5.88%
Tarjeta de crédito, debito, transferencia bancaria y otros	7	41.18%
Tarjeta de crédito, contra reembolso y transferencia bancaria	1	5.88%
No contestaron	1	5.88%
Total	**17**	**100.00%**

MEDIOS DE PAGO MAS UTILIZADO POR LAS EMPRESAS		
Medios de Pago	**Frecuencia Absoluta**	**Frecuencia Relativa**
Tarjeta de crédito	15	31.91%
Tarjeta de debito	9	19.15%
Contra reembolso	3	6.38%
Transferencia bancaria	11	23.40%
Financiación	1	2.13%
Otros	8	17.02%
Total	**47**	**100.00%**

Análisis

De esta interrogante se han derivado dos cuadros de respuesta: el primero, la combinación de medios de pago aceptados por la

empresa y el segundo el medio de pago con mayor aceptación por parte de Ellas.

En el primero de los casos se puede observar que, un 41.18% de la empresas encuestadas aceptan tarjeta de crédito, tarjeta de debito, transferencia bancaria y otros; un 17.65% acepta solamente tarjetas de crédito; mientras que el resto tiene una combinación diferente.

Por otro lado se puede verificar que el medio de pago con mayor aceptación por el comercio, son las tarjetas de crédito con un 31.91%, le siguen las transferencias bancarias con un 23.40%, las tarjetas de debito con un 19.15%. Un dato curioso e importante es que, el medio de pago contra reembolso representa un porcentaje relativamente pequeño en relación con los demás, esto quiere decir que tiene poca materialidad, por lo que efectivamente las evidencias de auditoría resultan en las operaciones virtuales realizadas al momento de la transacción (pago con tarjeta de crédito o débito que ambas representan un 51.06% de los medios de pago mas aceptados), y esto a la vez da pie a inferir el tipo de arquitectura del comercio electrónico, implementado por la mayoría de empresas.

ANÁLISIS GENERAL DEL ÁREA EVALUADA: LOGÍSTICA DE OPERACIONES

La logística en las operaciones tanto en el manejo de inventarios "justo a tiempo" como en el reparto de la mercadería, es un aspecto muy importante a considerar en la evaluación al comercio electrónico, pues forma parte de los aspectos de seguridad y confiabilidad que debe ser generada en los clientes, ya que esto se vuelve uno de los detonantes importantes en la satisfacción o insatisfacción de los consumidores. Los compradores en línea, además de la preocupación por la seguridad en la red, también se preocupan por que el pedido efectuado tenga una eficaz respuesta, es decir, que llegue en el menor tiempo posible; además que el producto cumpla con la calidad mostrada a través del escaparate virtual y que al momento del pago el comercio tenga instalado una estructura que le permita aceptar cualquier medio y forma de pago en línea, al menos los más usuales (tarjetas de crédito y débito), todos estos aspectos mencionados entre otros confluyen en el andamiaje construido para determinar la logística idónea en las operaciones de comercio electrónico. En este sentido se puede observar que una buena parte de las empresas encuestadas, poseen indicadores aceptables sobre su desempeño en esta área, para citar algunos, se tiene que, un 47.06% posee una capacidad de respuesta a los pedidos de 6 horas o menos, los productos que se transan a través de la red cumplen con las expectativas de los clientes ya que el 52.94% de las empresas no

tienen rechazo en los productos enviados y el 88.24% de las empresas encuestadas tiene alguna infraestructura que les permite aceptar cuando menos alguna tarjeta de crédito.

ÁREA: SEGURIDAD EN LA RED (INTERNET)

MACRO – OBJETIVO: Conocer si las empresas dedicadas al comercio electrónico tienen la capacidad de proveer un canal seguro para el tráfico de información confidencial, de los clientes para con el comercio y viceversa y del comercio para un tercero.

---

8. ¿Se puede garantizar a los clientes la autenticidad del sitio Web donde se tiene instalado el canal virtual?

OBJETIVO: Conocer, en un primer momento, si se posee un sitio web seguro para la transmisión de datos.

EMPRESAS QUE TIENEN AUTENTICADO SU SITIO WEB		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	17	100%
No	0	0%
Total	**17**	**100%**

Análisis

Ante la pregunta efectuada las empresas responden en unanimidad que sí tienen autenticado su sitio web, sin embargo esta interpelación va entrelazada con las interrogantes

subsiguientes, las cuales comprobaran la veracidad de esta respuesta.

9. ¿Se posee un certificado de seguridad emitido por una compañía autorizada?

OBJETIVOS: Conocer si se posee un sitio web seguro para la transmisión electrónica de datos, y para verificar la veracidad de la respuesta anterior.

EMPRESAS QUE POSEEN CERTIFICADO DE SEGURIDAD		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	14	82.35%
No	2	11.76%
No responden	1	5.88%
Total	**17**	**100.00%**

Análisis

Se puede observar que un 82.35% de las empresas encuestadas poseen certificado de seguridad, mientras que el resto no tiene. Por tanto, en contraste con la respuesta a la pregunta anterior, no todas las empresas pueden garantizar la autenticidad de su sitio web.

La mayoría de empresas encuestadas no poseen un servidor propio (*tal como se comprobará en la respuesta a la pregunta N° 19*) por lo que no se puede decir que dichas empresas tengan autenticado su sitio web a través de un certificado de seguridad, en este caso quienes lo tienen autenticado son las que prestan los servicios de alojamiento y validación.

10.¿Se posee firma digital?

OBJETIVO: Conocer los estándares de seguridad que las empresas dedicadas al comercio electrónico poseen y aplican para transmitir datos de los clientes y de si mismos.

EMPRESAS QUE POSEEN FIRMA DIGITAL		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	4	23.53%
No	13	76.47%
Total	**17**	**100.00%**

Análisis

La respuesta a esta pregunta viene a confirmar lo comentado en el análisis anterior, ya que un 76.47% de las empresas encuestadas respondieron que no tienen firma digital.

Por supuesto, sólo pueden tener firma digital los comercios con sitios web debidamente autentificados por una compañía autorizada para tal efecto, lo cual se materializa en un certificado de seguridad, que proporciona un par de claves: pública y privada, que les permite firmar digitalmente los mensajes.

11.¿Se puede proveer un canal seguro de transmisión de información a los clientes?

OBJETIVO: Conocer la seguridad que las empresas dedicadas al comercio electrónico poseen para que los clientes les transmitan datos de una manera confiable y segura.

EMPRESAS QUE POSEEN UN CANAL SEGURO PARA LA TRANSMISIÓN DE INFORMACIÓN POR LA RED		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	15	88.24%
No	0	0.00%
No responden	2	11.76%
Total	**17**	**100.00%**

Análisis

En base al cuadro de respuesta se puede observar que el 88.24% de los comercios encuestados respondieron que si poseen un canal seguro para la transmisión de la información, mientras que un 11.76% no respondieron a tal interrogante.

Esta pregunta esta relacionada con la pregunta N° 9 y se puede constatar que las respuestas afirmativas tienen un porcentaje similar, por lo que persiste la coherencia en las respuestas, ya que solamente las empresas que poseen un certificado de seguridad pueden proporcionar un canal seguro para la transmisión de información a través de la red.

12. ¿Qué protocolo de seguridad se posee para una transmisión segura de datos?

OBJETIVO: Conocer el protocolo de seguridad que las empresas dedicadas al comercio electrónico tienen instalado en su servidor para que los clientes les transmitan datos de una manera confiable, y asi mismo, para verificar la veracidad de la respuesta anterior(que no haya contradicción).

PROTOCOLO DE SEGURIDAD UTILIZADO POR LAS EMPRESAS EN LA TRANSMISIÓN DE DATOS		
Protocolo	**Frecuencia Absoluta**	**Frecuencia Relativa**
Secure Sockets Layer (SSL)	14	82.35%
Secure Electronic Transactions (SET)	0	0.00%
No responden	3	17.65%
Total	17	100.00%

Análisis

El 82.35% de las empresas encuestadas utilizan el protocolo de seguridad para transmisión y recepción de datos Secure Socket Layer (SSL), que sólo puede ser empleado cuando se posee un sitio web seguro, congruentemente con la respuesta a la pregunta N° 9 y N° 11.

ANÁLISIS GENERAL DEL ÁREA EVALUADA: SEGURIDAD EN LA RED

La seguridad en la transmisión de datos a través de una red pública como lo es Internet, en los países subdesarrollados y

algunos desarrollados, reviste una gran importancia en la generación de seguridad y confiabilidad a los clientes.

Es por ello que se han diseñado a través de técnicas criptográficas, herramientas para proporcionar dicha certeza y confiabilidad, como lo son los certificados y los protocolos de seguridad.

En este sentido, tal como se ha podido observar, la mayor parte de empresas que se dedican hacer transacciones y validaciones en línea, ya sea por cuenta propia o por cuenta de terceros, poseen un certificado de seguridad, lo cual proporciona la certeza razonable que poseen un sitio web seguro y por lo tanto brindan un canal seguro para la transferencia de información en cualquier vía.

ÁREA : SEGURIDAD Y CONFIDENCIALIDAD CON LA INFORMACIÓN ALMACENADA DE LOS CLIENTES

MACRO – OBJETIVO: Conocer si los comercios cuentan con el debido cuidado en el manejo de la información recabada de los clientes a tal grado que puedan garantizar la seguridad, integridad y confidencialidad de la misma de tal manera que no se vaya hacer un uso abusivo o fraudulento con dicha información.

13.¿Qué tipo de información se almacena de los clientes?

OBJETIVO: Conocer que tipo de información se almacena de los clientes, para determinar si no existe un mal manejo de la misma.

INFORMACIÓN DE LOS CLIENTES ALMACENADA POR LAS EMPRESAS		
Información	**Frecuencia Absoluta**	**Frecuencia Relativa**
Nombre, correo electrónico y domicilio	3	17.65%
Nombre, correo electrónico y N° de Tarjetas de crédito	1	5.88%
Nombre, correo electrónico, información de negocios y Domicilio	1	5.88%
Nombre, correo electrónico, información personal, información del negocio, domicilio y N° de tarjetas de crédito	11	64.71%
No contestaron	1	5.88%
Total	**17**	**100.00%**

INFORMACIÓN MAS UTILIZADA POR PARTE DE LAS EMPRESAS		
Información	**Frecuencia Absoluta**	**Frecuencia Relativa**
Nombres y correo electrónico	16	24.24%
Información personal	11	16.67%
Información de Negocio	12	18.18%
Domicilio	15	22.73%
N° de Tarjetas de crédito	12	18.18%
Total	**66**	**100.00%**

Análisis

De esta interrogante se han derivado dos cuadros de respuestas: el primero agrupa las combinaciones de los tipos de información de los clientes, solicitadas y almacenada por parte del comercio, y el segundo muestra el tipo de información más solicitada y almacenada.

En el primer cuadro de respuestas se puede constatar que el 64.71% de las empresas encuestadas almacena: nombre, correo electrónico, información personal, información del negocio, domicilio y números de tarjetas de crédito del consumidor; mientras que un 17.65% solo almacena nombre, correo electrónico y domicilio, estas son las empresas que no efectúan transacciones ni validación en línea, congruentemente con las respuestas negativas y las abstenciones de las preguntas N° 9 y 12.

En el segundo cuadro se puede observar que la información más solicitada y almacenada por las empresas son los nombres y correo electrónico con un 24.24%, seguido por el domicilio con un 22.73%, números de Tarjetas de crédito con un 18.18%, Información de Negocio con 18.18% e Información personal con un 16.67%.

14.¿Para qué se utiliza La base de Datos con la información de los Clientes?

OBJETIVO: Determinar el uso que se le da a la información almacenada de los clientes, cuáles son los fines que se persiguen al almacenarla y conocer si no existe un mal manejo de esa información.

UTILIZACIÓN DE LA BASE DE DATOS DE LOS CLIENTES POR PARTE DE LA EMPRESA		
Utilización	**Frecuencia Absoluta**	**Frecuencia Relativa**
Hacer análisis estadísticos	1	5.88%
Enviar publicidad y/o ofertas, hacer análisis estadísticos	2	11.76%
Enviar publicidad y/o ofertas, establecer nichos de mercado	1	5.88%
Enviar publicidad y/o ofertas y otros	1	5.88%
Enviar publicidad y/o ofertas, hacer análisis estadísticos y establecer nichos de mercado	10	58.82%
Enviar publicidad y/o ofertas, hacer análisis estadísticos, establecer nichos de mercado y otros	1	5.88%
No respondieron	1	5.88%
Total	**17**	**100.00%**

UTILIZACIÓN DE LA BASE DE DATOS DE LOS CLIENTES POR PARTE DE LA EMPRESA		
Utilización	**Frecuencia Absoluta**	**Frecuencia Relativa**
Enviar publicidad y/o ofertas	15	34.88%
Para hacer análisis estadísticos	14	32.56%
Cooperación y alianzas con otras empresas	0	0.00%
Establecer nichos de mercado	12	27.91%
Otros	2	4.65%
Total	**43**	**100.00%**

Análisis

De la respuesta a la pregunta anterior se pueden derivar dos cuadros: el primero muestra las diferentes combinaciones de uso de información de los clientes por parte del comercio y el segundo muestra los usos mas frecuentes de la información proporcionada por el consumidor.En el primer cuadro se puede observar que la mayoría de comercios utilizan la información de los clientes para: enviar publicidad y/o ofertas, hacer análisis estadísticos y establecer nichos de mercado con un 58.82%, mientras que un 11.76% la usa para enviar publicidad y/o ofertas y hacer análisis estadísticos solamente.En el segundo cuadro se constata que un 34.88% de la información se utiliza para enviar publicidad y/o ofertas, un 32.56% se usa para hacer análisis estadísticos y un 27.91% la utiliza para establecer nichos de mercado.En base a esto, se deduce que la información de los clientes es aprovechada, en un primer momento, para formarse un perfil del consumidor, ya que de esta manera se pueden enviar correos electrónicos conteniendo publicidad y/o ofertas, de acuerdo al perfil diagramado.

Un caso bastante peligroso en cuanto al uso que se le da a este tipo de información, es cuando existen acuerdos con otras empresas, en los cuales se establece intercambio de información de los compradores, sin embargo en base a las respuestas no se tiene esta situación en los comercios encuestados.

15.¿Tiene la empresa políticas de seguridad y confiabilidad con la información de los clientes?

OBJETIVO: Determinar si la información de que se posee de los clientes, tiene un tratamiento seguro, oportuno y eficaz, a través de políticas de acceso, manejo, distribución y confiabilidad de los datos; por parte de la empresa.

EMPRESAS QUE TIENEN POLÍTICAS DE SEGURIDAD Y CONFIDENCIALIDAD CON LA INFORMACIÓN DE LOS CLIENTES		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	16	94.12%
No	0	0.00%
No responden	1	5.88%
Total	**17**	**100.00%**

Análisis

Se puede verificar que la mayoría de empresas respondió afirmativamente a esta pregunta, es decir, que si cuentan con políticas de seguridad y confidencialidad con la información de los clientes (94.12%), no obstante un 5.88% se abstuvieron a responder, lo que da entender que no cuentan con estas políticas o que no guardan ninguna información de los consumidores, lo cual es bastante difícil, sin embargo en base a los resultados de las preguntas N° 13 y N° 14 así parece ser, ya que dicho porcentaje se repite.

Estos datos se confirmara con las respuestas a las preguntas subsecuentes.

16.¿Pueden personas externas a la empresa tener acceso a alguna información de los clientes?

OBJETIVO: Determinar si la información de que se posee de los clientes, tiene un tratamiento seguro, oportuno y eficaz, a través de políticas de acceso, manejo, distribución y confiabilidad de los datos; por parte de la empresa y así mismo, para verificar la veracidad de la respuesta anterior (que no haya contradicción).

EMPRESAS QUE TIENE LA POSIBILIDAD DE ACCESO EXTERNO A LA INFORMACIÓN DE LOS CLIENTES		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	8	47.06%
No	8	47.06%
No responden	1	5.88%
Total	**17**	**100.00%**

Análisis

Se puede constatar que un 47.06% de las empresas tienen una infraestructura de comercio electrónico que asegura que ningún tercero ajeno a la empresa, pueda acceder a las bases de datos que contienen la información de los clientes, mientras que en otro 47.06% de los comercios, terceros ajenos a ellos puede tener acceso a la mencionada información, lo cual demuestra una debilidad en sus políticas de seguridad y confiabilidad. Generalmente las empresas que tienen acceso externo son las que no cuentan con servidor propio para el alojamiento de su sitio web, ya que el administrador de dicho servidor puede tener acceso irrestricto a cualquier información alojada en él. Todo

esto como ya se mencionó anteriormente tiene que ver con la infraestructura de comercio electrónico instalada.

17.¿Qué personal de la empresa tiene acceso a la información de los clientes?

OBJETIVO: Determinar si la información que la empresa posee de los clientes es tratada de manera segura y confidencial, a tal grado que existen políticas restrictivas al acceso de la misma, para que únicamente personal autorizado acceda a ella. Además se quiere verificar la veracidad de la respuesta anterior (que no haya contradicción).

PERSONAL CON ACCESO A LA INFORMACIÓN DE LOS CLIENTES		
Personal	**Frecuencia Absoluta**	**Frecuencia Relativa**
Personal administrativo	1	5.88%
Personal de informática	2	11.76%
Personal de ventas y Personal administrativo	7	41.18%
Personal de ventas, personal de informática	2	11.76%
Personal administrativo y personal de informática	3	17.65%
Personal de ventas, Personal administrativo y personal de entrega y reparto	1	5.88%
No respondieron	1	5.88%
Total	**17**	**100.00%**

PERSONAL CON ACCESO A LA INFORMACIÓN DELOS CLIENTES		
Personal	**Frecuencia Absoluta**	**Frecuencia Relativa**
Personal de ventas	10	33.33%
Personal administrativo	12	40.00%
Personal de entrega y reparto	1	3.33%
Personal de informática	7	23.33%
Total	**30**	**100.00%**

Análisis

De esta interrogante se derivan dos cuadros de respuesta: el primero muestra las combinaciones de personal con acceso a información de los clientes en las empresas y el segundo el personal con mayor acceso a dicha información.

En el primer cuadro se puede observar que en un 41.18% de las empresas encuestadas los que tienen acceso a la información son: el personal de ventas y personal administrativo, en un 17.65% el personal administrativo y personal de informática, en un 11.76% el personal de ventas y personal de informática y en un 11.76% el personal de informática.

En el segundo de los cuadros se puede constatar que el personal con mayor acceso a la información es el personal administrativo con un 40%, el personal de venta con un 33.33%, el personal de informática con un 23.33% y el personal de entrega y reparto con un 3.33%.

ANÁLISIS GENERAL DEL ÁREA EVALUADA: SEGURIDAD Y CONFIDENCIALIDAD CON LA INFORMACIÓN ALMACENADA DE LOS CLIENTES

Otro de los componentes esenciales en la seguridad del comercio electrónico es el manejo o uso de la información de los clientes, ya que, ésta es la preocupación más grande en estos días de cataclismos mundiales, en donde el que tiene la información tiene el poder. En consecuencia los consumidores se preocupan por que su información personal no sea divulgada ni sea objeto de comercialización, además que sus números de tarjetas de crédito almacenados no salgan por ningún motivo del comercio, y es más, que un número muy reducido de empleados confiables y honestos sean los que puedan acceder a dicho compendio.

Para lograr la seguridad y confiabilidad en el manejo de la información, las empresas deben montar todo un aparataje que asegure el buen uso de la misma, esto tiene que ver con: qué tipo de información se almacena de los consumidores, para qué se utiliza esta información, las políticas de seguridad y confiabilidad adoptadas y establecidas por las empresas para lograr este cometido, evitar el acceso externo y limitar el acceso interno a un número muy reducido de personas, entre otros.En este caso en concreto, se puede verificar que las empresas almacenan información muy importante de la vida del consumidor, como lo es: su nombre y su numero de tarjeta de crédito, estos datos son muy importantes para el cliente, por

las implicaciones económicas y jurídicas que esto trae (usurpación de identidad). Un 70.59% de los comercios encuestados almacenan los números de las tarjetas de crédito y un 94.12% almacena el nombre completo del consumidor. Otro factor importante dentro de este análisis es el uso que se le da a los datos de los clientes, un 87.92% de las empresas los utilizan para hacerse un perfil del cliente, ya que de ésta manera pueden enviar ofertas y/o publicidad, ajustado a las necesidades perfiladas, lo cual si se hace un uso irrestricto y abusivo de este medio de publicidad puede causar molestias al consumidor. Un aspecto bastante preocupante es la arquitectura de comercio electrónico montada por algunas empresas (47.06%) ya que personas externas y fuera del ámbito de control de ellas, puede tener acceso a la información del consumidor, siendo esto una amenaza no sólo para el consumidor, sino también para la imagen del comercio.

ÁREA : SEGURIDAD FÍSICA Y LÓGICA INTERNA

MACRO – OBJETIVO: Conocer si las empresas poseen una infraestructura física, lógica y segura; de comercio electrónico; como base para realizar transacciones en línea, que provean confianza al consumidor.

18.¿Alguna vez han sido victimas de fraude?

OBJETIVO: Conocer la seguridad del sistema para evitar y detectar operaciones internas y externas a la empresa, que pueden dar inicio a actividades fraudulentas.

EMPRESAS QUE HAN SIDO VICTIMAS DE OPERACIONES FRAUDULENTAS		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	2	11.76%
No	14	82.35%
No responden	1	5.88%
Total	**17**	**100.00%**

Análisis

Tal como se observa en el cuadro de respuestas un 82.35% de las empresas encuestadas afirman que nunca han sido victimas de algún fraude u operación fraudulenta, mientras que un 11.76% dice lo contrario, es decir, que efectivamente, han sido alguna vez victimas de fraude u operaciones fraudulentas en lo referente al comercio electrónico.

El hecho de haber sido o no, victimas de fraude, refleja la robustez de la infraestructura del comercio electrónico, con todo lo que ello implica. Estos fraudes se dieron especialmente a lo largo del año 2003, en donde se puso de moda la clonación de tarjetas de crédito y la usurpación de identidad, para contrarrestar este problema, los comercios implementaron nuevas medidas de seguridad en cuanto a la validación de datos, para comprobar si el clientes es en verdad quien dice ser. Es

importante aclarar que estas operaciones fraudulentas no tienen nada que ver con la seguridad en línea.

19.¿Se posee servidor propio en donde se encuentra la información y se muestra el sitio web de la empresa?

OBJETIVOS: Determinar si la empresa posee su propio servidor para poder mostrar su sitio Web en la red y de esta manera evitar que personas externas a la empresa, accedan a información confidencial o reservada sin su consentimiento.

EMPRESAS QUE POSEEN SERVIDOR PROPIO		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	7	41.18%
No	9	52.94%
No responden	1	5.88%
Total	**17**	**100.00%**

Análisis

Según el cuadro de respuestas se pueda apreciar que un 52.94% de comercios no poseen un servidor propio para alojar su comercio electrónico con su sitio web, es decir, prestan los servicios de un tercero intermediario al comercio, mientras que un 41.18% si tienen su propio servidor. Este factor es importante para determinar si personas ajenas al comercio pueden tener acceso a la información del mismo.

20. ¿Se poseen planes de contingencia en caso de daños en el equipo que posee el comercio electrónico, que le imposibiliten estar conectado a la red o por cualquier falla en el proveedor del servicio, tales como: Cierre del servidor, Clausura del servidor donde se tiene alojado el sitio web del comercio electrónico, entre otros.

OBJETIVO: Conocer si la empresa posee planes contingentes como parte de sus políticas de seguridad físicas y lógicas de redes, dándose a si misma y a sus clientes certeza y confiabilidad de su estructura.

EMPRESAS QUE POSEEN PLANES DE CONTINGENCIA		
Respuestas	**Frecuencia Absoluta**	**Frecuencia Relativa**
Si	7	41.18%
No	9	52.94%
No responden	1	5.88%
Total	**17**	**100.00%**

Análisis

Según la respuesta a esta pregunta, se puede observar que un 52.94% de las empresas, no tienen previsto un plan para hacerle frente a contingencias que puedan interferir e incluso cancelar el comercio electrónico, mientras que un 41.18% si tienen un plan para hacerle frente a estas eventualidades futuras.

ANÁLISIS GENERAL DEL ÁREA EVALUADA: SEGURIDAD FÍSICA Y LÓGICA

En esta área se ha evaluado la seguridad interna en aspectos físicos y lógicos, es decir, comprobar la robustez de la infraestructura instalada, ello implica: saber si la empresa posee un servidor propio, de ser así, de esta condición se derivan otros aspectos secundarios, como lo es, la estructura de la red interna y su seguridad física, los software utilizados para administrar (sistemas operativos) y proteger la red(cortafuegos o Firewall), los diferentes niveles de acceso a la información, entre otros. Si los comercios no tienen su propio servidor, esto puede ser una ventaja por la disminución de costos en su gestión, ya que la seguridad es costosa, no obstante ello puede ser una gran debilidad, ya que prácticamente no controla ningún factor de seguridad en la red (Internet) o seguridad física y lógica interna, lo cual queda a dispensas del proveedor del servicio, como ya se dijo anteriormente, el que tiene la información tiene el poder.

Lo mencionado en los párrafos precedentes está relacionado, obviamente, con el hecho del aseguramiento de las contingencias, por parte del comercio, ya que es necesario que cuenten con un plan que prevenga cualquier circunstancia dañosa al comercio electrónico, entre las cuales se puede mencionar las mas comunes: clausura del servidor que provee el servicio de Internet o de alojamiento, caídas constantes del servicio, disminución en la eficiencia del mismo, aspectos legales,

ataques de virus peligrosos y potentes que destruyan la información, entre otros.

En estos aspectos fundamentales van dirigidas las interrogantes hechas a las empresas, puesto que de las respuestas de las mismas se derivan una serie de condiciones importantes para la evaluación, las cuales a groso modo ya han sido mencionadas.

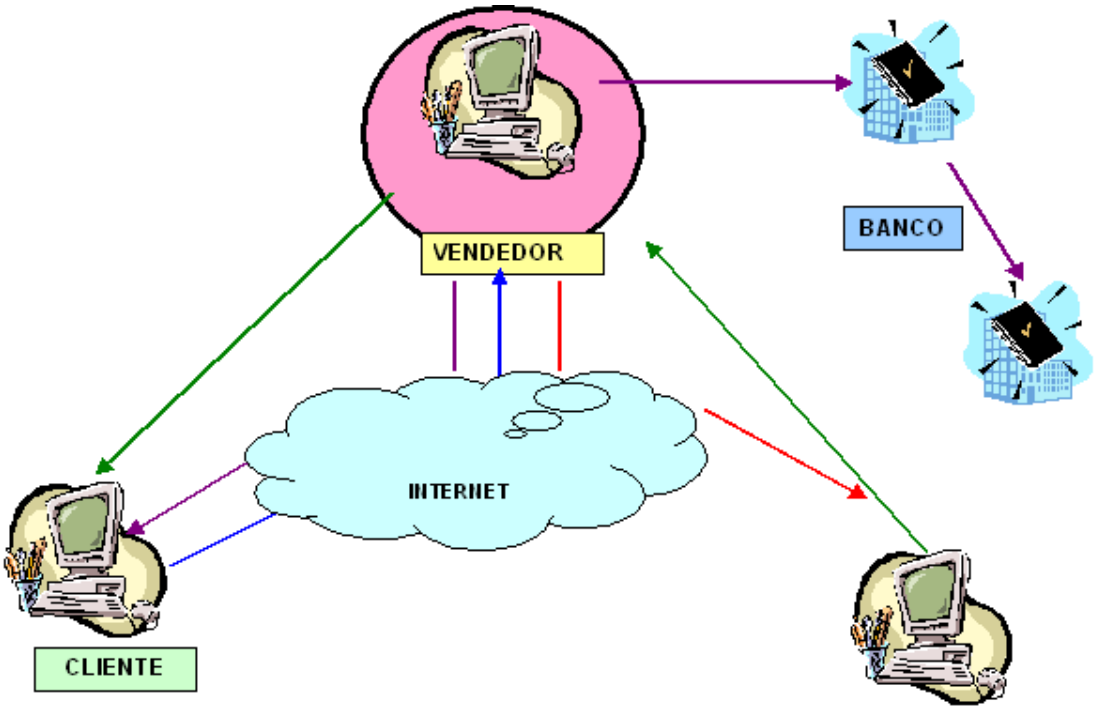
Anexo 2.3.

BASE DE DATOS DE EMPRESAS DEDICADAS AL COMERCIO ELECTRÓNICO A TRAVÉS DE UN CANAL O TIENDA VIRTUAL

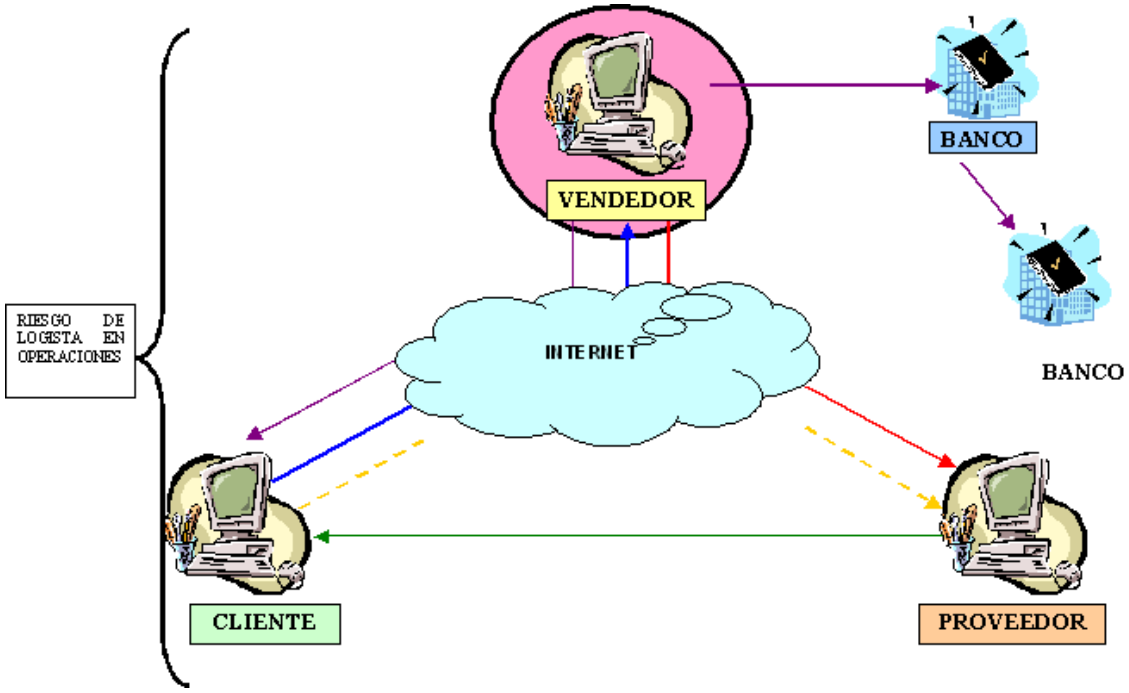
N°	CONOCIMIENTO DEL NEGOCIO			LOGÍSTICA DE OPERACIONES				SEGURIDAD EN LA RED (INTERNET)				
	1	2	3	4	5	6	7	8	9	10	11	12
	Numero de Empleados	Ingresos Promedios Mensuales	Pedidos Promedios Diarios	Tiempo Promedio de Respuesta / Horas	Pedido Promedio Rechazado por Mes	Momento de Facturación del Pedido	Medios de Pago Aceptados	Autenticidad del Sitio Web	Certificado de Seguridad	Firma Digital	Transmisión Segura de Datos	Protocolo de Seguridad
1	6	12	5	6	1	2	146	1	1	2	1	1
2	2	3	1	1	1	4	1246	1	1	1	1	1
3	6	1	1	4	2	4	134	1	2	2	1	
4	1	5	1	10		2	1234	1	1	1	1	1
5	6		1	1	2	1	1	1	1	2	1	1
6	1	2	1	4	1	2	14	1	1	2		1
7	1	2	1	1	6	1	35	1	2	2	1	
8	1							1	1	1	1	1
9	6	1	1	2	2	4	1246	1	1	2	1	1
10	6	1	1	10	1	4	1246	1	1	2	1	1
11	1	1	1	2	1	4	1246	1	1	2	1	1
12	1	1	1	2	2	4	1246	1	1	2	1	1
13	3	1	1	4	1	4	1246	1	1	2	1	1
14	5	1	1	5	1	4	1	1	1	2	1	1
15	2	1	1	2	1	4	1246	1	1	2	1	1
16	6		1		1	4	1	1		2		
17	1	1	1	2	2	2	12	1	1	1	1	1

SEGURIDAD DE LA INFORMACIÓN DE LOS CLIENTES					SEGURIDAD LÓGICA Y FÍSICA INTERNA		
13	14	15	16	17	18	19	20
Información Almacenada de los clientes	Utilización de la Base de los Clientes	Políticas de seguridad y confiabilidad de Inf. de Clientes	Acceso Externo a la Inf. de los Clientes	Personal con acceso a la Inf. De Clientes	Victima de Fraude	Servidor Propio	Planes de Contingencia
12345	124	1	2	4	1	1	1
12345	1245	1	2	24	1	1	1
14	15	1	2	4	2	1	1
14	124	1	2	24	2	1	1
15	12	1	2	14	2	1	1
14	2	1	2	2	2	2	2
134	14	1	2	123	2	2	2
12345	12	1	2	24	2	1	1
12345	124	1	1	12	2	2	2
12345	124	1	1	12	2	2	2
12345	124	1	1	12	2	2	2
12345	124	1	1	12	2	2	2
12345	124	1	1	12	2	2	2
12345	124	1	1	12	2	2	2
12345	124	1	1	12	2	2	2
12345	124	1	1	14	2	1	1

ANEXO 3.1. DIAGRAMA DEL PROCESO DE VENTA EN UNA TIENDA VIRTUAL EN SENTIDO ESTRICTO: COMO VENDEDOR



ANEXO 3.2. DIAGRAMA DEL PROCESO DE VENTA EN UNA TIENDA VIRTUAL EN SENTIDO AMPLIO: COMO INTERMEDIARIO



ANEXO 3.3: CORRIDA DE PROGRAMA DE FACTORES TÉCNICOS FUNDAMENTALES DEL ÁREA DE SEGURIDAD EN RED.

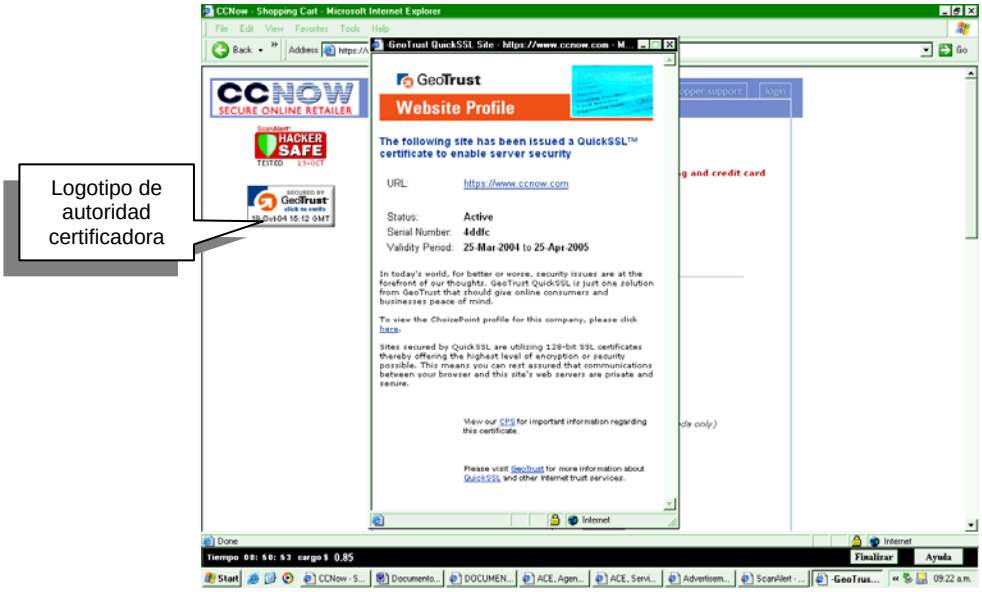
A continuación se procederá a desarrollar algunos aspectos técnicos que se consideran relevantes, de la lista de verificación propuesta, para que sirva como ejemplo para el auditor, al ejecutar la evaluación de esta área.

5. Ingresar al sitio Web del comercio evaluado.

En este procedimiento lo único que se tiene que hacer es digitar la dirección o nombre de dominio del E-commerce, donde se desplegara la página Web respectiva (el escaparate virtual).

6. Verificar la existencia de un logotipo de alguna autoridad certificadora.

Tal como se menciona en el programa, todo servidor que este certificado, en su página Web debe mostrar un logotipo, el cual es el sello digital de la autoridad certificadora.



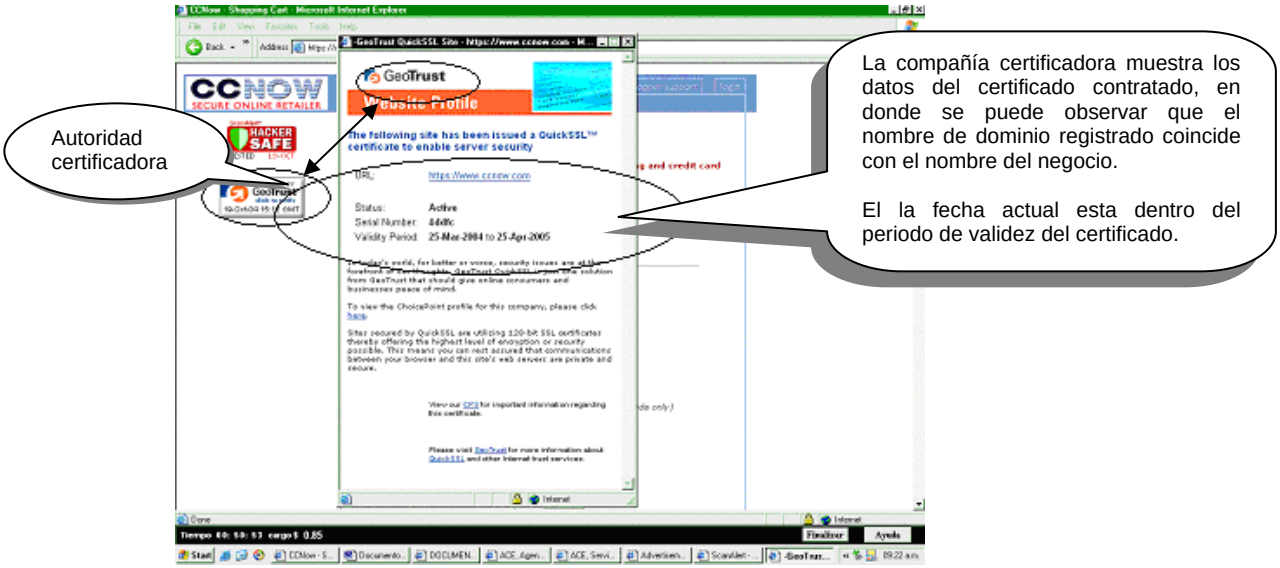
7. Dar clic a dicho logotipo y verificar:

c) Que los datos de identificación del certificado tales como, denominación o razón social de la empresa y nombre de dominio, coincidan con los datos reales del comercio.

d) Que la fecha actual este dentro del periodo de validez del certificado.

Este procedimiento se debe efectuar para comprobar la autenticidad del sitio Web del negocio, ya que un certificado de

seguridad es un contenedor de información tal como la que mencionan los literales a) y b) de este procedimiento.

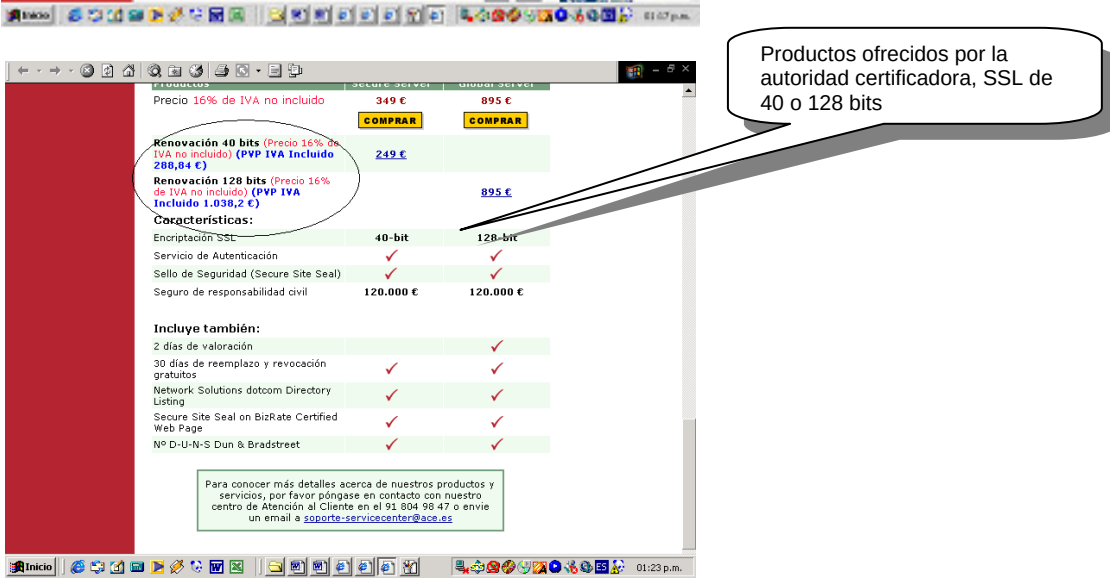


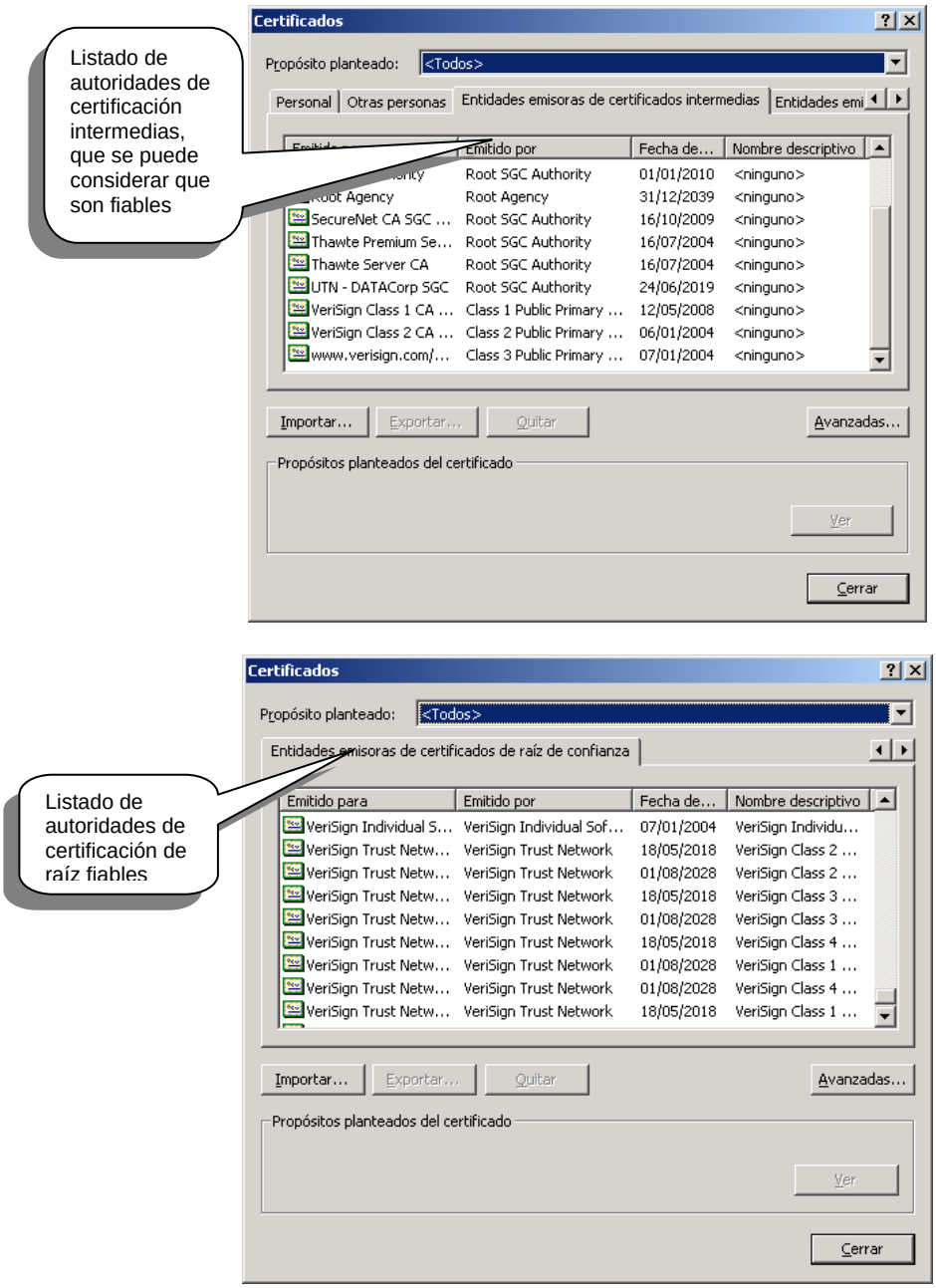
9. **Ingresar al sitio Web de la autoridad certificadora y verificar:**

   c) El servicio contratado por la empresa (SSL de 40 o 128 bits)

   d) Si dicha entidad certificadora es fiable, si es de raíz o intermedia, puede tomar como parámetro para dicha evaluación, las compañías proporcionadas por Microsoft Internet Explorer mas reciente, en el menú de Herramientas, submenú opciones de Internet ficha de contenido, opción certificados. Esto no obsta que hayan muchas más compañías fiables en Internet que las proporcionadas en dicha lista.

Para ejemplificar este procedimiento se tomará la Agencia de Certificaciones Electrónicas, filial de Verisign en España.

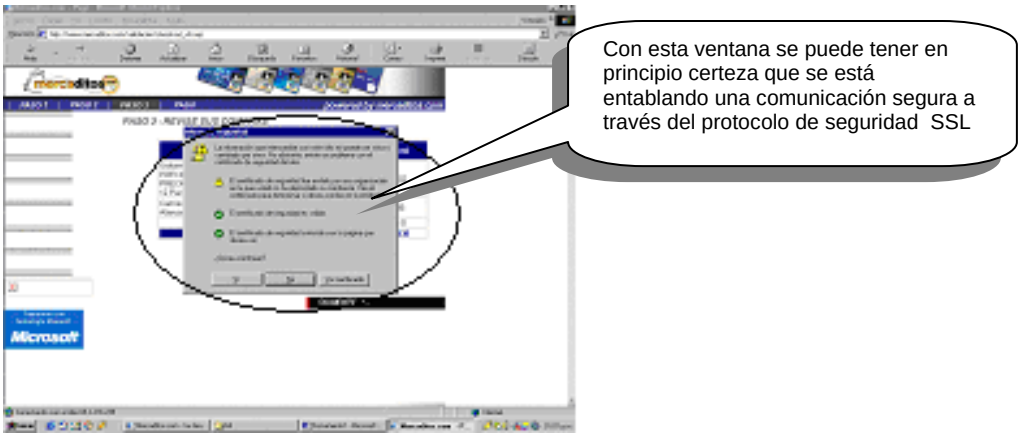




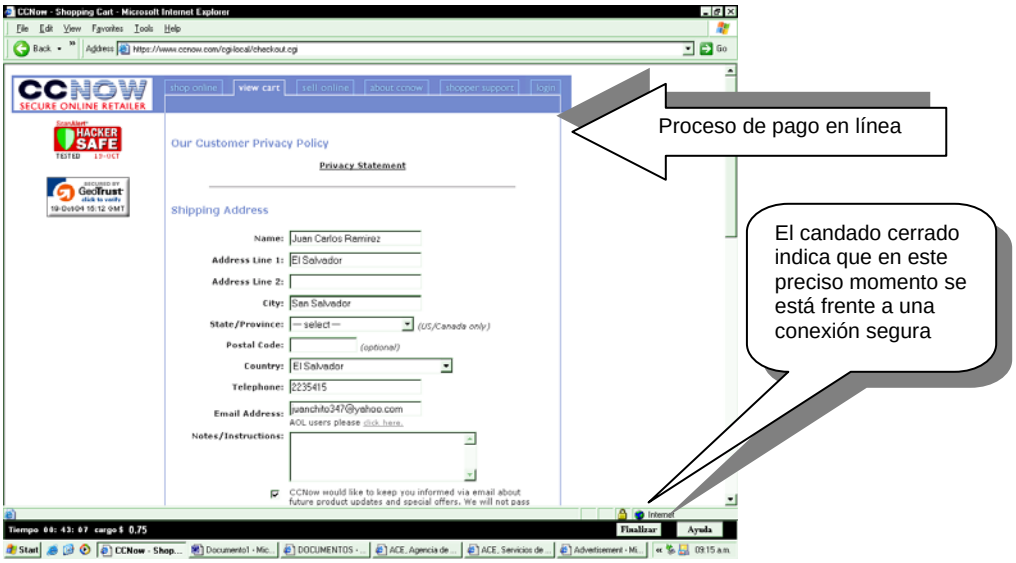
9. Simular un proceso de compras, y documentarlo paso a paso por medio de captura de pantallas y comprobar los siguientes acontecimientos en momentos cruciales:

a) En el momento de enviar los datos personales tales como: nombre, dirección, teléfono, numero de tarjeta de crédito,

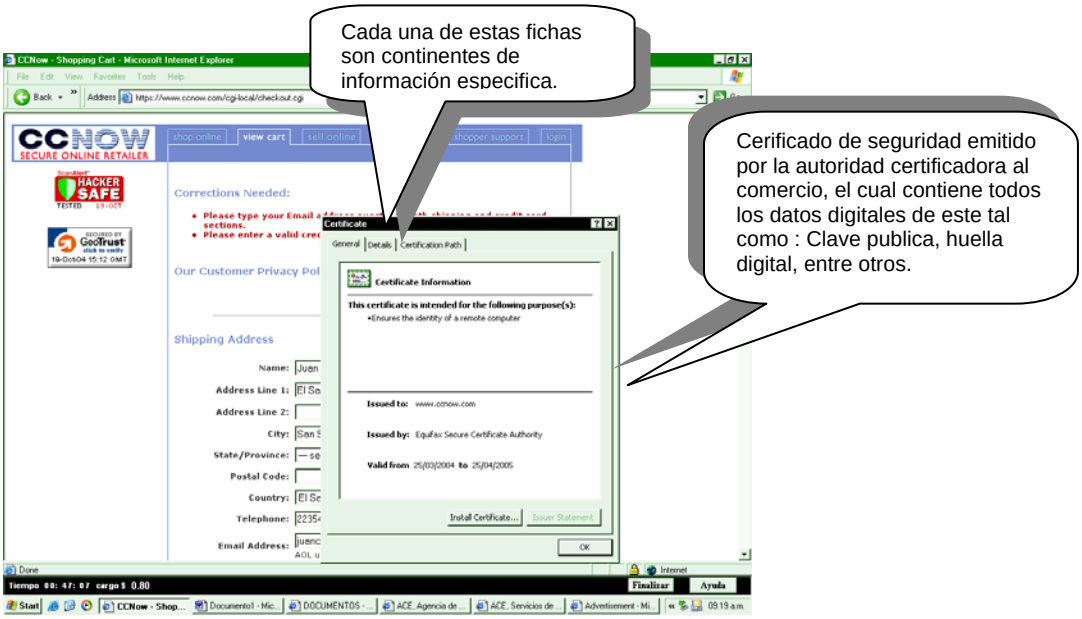
en el proceso de pago en línea, verificar que el explorador (si se esta trabajando con Microsoft Explorer), despliegue una ventana donde diga que la información que se intercambie con este sitio no puede ser vista o cambiada por otros, en dicha ventana, se estipula si se tiene o no confianza en el certificado, si el certificado es válido, si el certificado coincide con la página que se desea ver. Tal como se muestra en la siguiente pantalla.



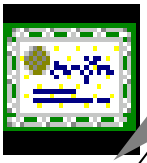
b) Corroborar que en la parte inferior derecha del Navegador, aparezca un candado cerrado, el cual indica que la comunicación entablada con el sitio Web es segura, esto debe ser en el momento del proceso de pago. Es importante aclarar que muchas veces el Navegador no despliega la ventana señalada en el literal a), sino solamente el candado cerrado en la parte inferior derecha.



c) Dar clic sobre el candado cerrado, y verificar el certificado de seguridad, en el cual aparecen datos tales como: El propósito del certificado, nombre del comercio al cual ha sido emitido, nombre de la autoridad certificadora, período de validez, el algoritmo hash utilizado para la firma digital, la clave pública y su extensión, la huella digital, entre otros datos de importancia.

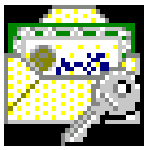


d) Extraer dicho certificado, copiándolo a un medio de almacenamiento flexible, tal como un disco magnético, una memoria flash o un disco óptico.



Este archivo contiene todos los datos del certificado, incluyendo la clave pública, el cual puede ser almacenado en cualquier medio removible.

CERTIFICADO.cer



Este archivo contienen todos los datos del certificado del comercio al igual que el archivo anterior con la diferencia, que en este además de la clave publica se almacena la clave privada, para lo cual su tratamiento requiere de muchas medidas de seguridad tal como el uso de contraseñas.

CERTIFICADO.pfx

Con los ejemplos anteriores, se ha suministrado una guía objetiva, sobre los aspectos técnicos, que requieren mayor elucidación sobre el desarrollo material del programa o guía de verificación proporcionada, para la evaluación del área de seguridad en red, estos ejemplos también serán referenciados en las propuestas de evaluación de las demás áreas.

ANEXO 3.4. INSTRUMENTOS DE EVALUACIÓN EN UNA AUDITORIA DE SEGURIDAD PARA EL COMERCIO ELECTRÓNICO

ANEXO 3.4.1. Guía de Evaluación para el Conocimiento del Negocio

GUÍA PARA EL CONOCIMIENTO DEL NEGOCIO

Cliente: _____
Periodo de auditoria: _____

Factor de riesgo: Conocer apropiadamente el negocio, el tipo de arquitectura de comercio electrónico, determinación de riesgos asociados en las distintas áreas de seguridad.

Objetivo de la evaluación: Conocer de manera general el volumen de operaciones de comercio electrónico que realizan las empresas, a través de un canal virtual o de tienda virtual (arquitectura del e-commerce). Con el fin de determinar la materialidad y la importancia relativa de las operaciones y áreas de seguridad de las empresas

REF	Actividad que será Evaluada	Procedimiento de Auditoria	Herramienta que serán utilizadas	Observación
	Determinar condiciones económicas que afectan al negocio	Determinar las empresas de comercio electrónico que son la principal competencia del cliente. Determinar los productos que ofrece el cliente.	❑ Revisión: de los Sitios Web que ofrecen productos similares ❑ Revisión: del Sitio Web de la Empresa, realizando una lista de los productos ofertados. ❑ Inspección: de los Artículos ofrecidos	

	Evaluar la administración y propiedad de la entidad	Determinar el tipo de empresa en base a lo mercantil. Conocer quienes son los dueños y cómo esta compuesto el patrimonio de la empresa. Conocer la estructura organizacional de la empresa.	❑ Revisión Documental de: Escritura de Constitución y Organigrama. ❑ Entrevista con Funcionarios de la empresa, corroborando niveles Jerárquicos	
	Evaluar la Actividad de administración y gestión de la tienda virtual o canal virtual.	Solicitar la visión, misión, objetivos, metas de la administración. Evaluar la existencia, congruencia y apego a la estructura organizacional. Evaluar la existencia y aplicación del perfil de puestos para la selección y promoción del personal del área. Evaluar la división adecuada del trabajo y departamentalización de las funciones y actividades del personal. Evaluar las relaciones personales y de trabajo entre los directivos y empleados.	❑ Entrevista: con el Gerente General de la Empresa ❑ Revisión de Organigrama y Manual de Puestos de la Empresa. ❑ Observación Participativa ❑ Revisión de Manual de Procedimientos. ❑ Entrevista con empleados del área de ventas (e-commerce)	

		Evaluar la suficiencia o carencia de personal o recursos informáticos para cumplir con la actividades del área		
	Determine el número de empleados de la empresa	Solicitar al gerente el número de empleados que laboran en la empresa y luego Contrastar la respuesta solicitando la planilla de pago	❑ Entrevista: con el Gerente ❑ Revisión Documental de la planilla de pago ❑ Observación Participativa	
	Determinar el promedio de ingresos mensuales del comercio electrónico	Solicitar al encargado de ventas el monto de las ventas del comercio electrónico del mes anterior. Verificar dicho dato, con el encargado de contabilidad	❑ Revisión Documental: de las Ventas e- commerce.	
	Determinar la naturaleza del E-commerce: estructura o arquitectura	Determine si posee inventarios la empresa Determine si corre los riesgos de envió e imagen. Determine si los clientes conocen a los proveedores de la empresa	❑ Inspección de los Inventarios ❑ Revisión Documental de: Políticas de Venta y Envío la Empresa. ❑ Entrevista a Clientes	

	Evaluar la existencia de inventarios de la empresa	Conocer si poseen inventarios físicos Determinar el sistema de inventarios que utilizan Evaluar la eficiencia y eficacia del manejo de sus inventarios	❑ Revisión de la Arquitectura del e-commerce ❑ Inspección de los Inventarios Físicos que la empresa posee. ❑ Entrevista: para conocer las Políticas. ❑ Revisión de tarjetas de Inventarios	
	Determinar los proveedores importantes de la empresa	Solicitar la lista de los proveedores usuales de la empresa. Realizar la confirmación de algunos de ellos. Determinar las competencias del proveedor con respecto al pedido.	❑ Revisión Documental de Lista de proveedores, entregada por área: e-commerce. ❑ Confirmación por escrito a Proveedores. ❑ Revisar los Contratos existentes con Proveedores.	
	Determinar el número de pedidos que recibe cada día	Realizar una evaluación durante un día, verificando todos los pedidos que se efectúan, realizar este proceso por lo menos dos veces más en un período	❑ Observación Participativa, en el proceso de pedidos por día. ❑ Revisión documental de	

		corto. Solicitar al Gerente de Ventas la cantidad promedio de ventas recibido por día, según temporada	Ventas por Cliente	

Anexo 3.4.2. Cuestionario de Control Interno

CUESTIONARIO PARA LA EVALUACIÓN
DE LA SEGURIDAD DEL COMERCIO ELECTRONICO

Cliente: _____
Periodo de auditoria: _____

ÁREA: EN LA LOGISTICA DE OPERACIONES

Factor de riesgo: Satisfacción de las expectativas del cliente en cuanto a la eficiencia del tiempo de entrega del producto y eficacia de las especificaciones del producto, así como del proceso logístico de venta.

Objetivo de la evaluación: Conocer la capacidad instalada que poseen las empresas para hacer frente a las exigencias de este modelo de negocios, así como para asegurar que la logística de operación de venta al recibir un pedido u orden de compra es eficiente y eficaz. Todo esto incluye el tiempo de respuesta para cada orden, los pedidos rechazados durante un lapso de tiempo, el momento de facturación, los medios de pago aceptados, el proceso de envió del producto y políticas de devolución.

N°	Preguntas	Si	No	N/A	Comentarios
1	¿En el sitio Web los productos tienen especificaciones claras de los mismos?				
2	¿Estos detalles o especificaciones se pueden conocer antes de haber adquirido o cancelado el producto?				
3	¿Se puede seguir agregando productos al “carrito de compras” hasta que se esté listo para pagar?				
4	Cuando un cliente tiene duda acerca de un producto o acerca de cómo llenar un formulario de datos personales, ¿Puede dirigirse a la empresa y ésta le responde eficientemente?				
5	¿A cuánto asciende el promedio de pedidos recibidos durante el día (24 horas)? ❑ 0-10 ❑ 11-20 ❑ 21-40 ❑ 41-60 ❑ 61 o más				

6	¿El tiempo promedio de respuesta a los pedidos se hace de manera inmediata?				
7	¿Se confirma el pedido realizado a través de un correo electrónico o llamada telefónica al cliente?				
8	¿Qué medios de pago acepta la empresa? ❑ Tarjeta de Crédito ❑ Tarjeta de Debito ❑ Contra reembolso ❑ Transferencia bancaria ❑ Financiación				
9	Si el pago es a través de tarjetas de crédito, ¿Cuándo se recibe el número de la misma? el proceso de pago es: ❑ Convencional con el Sistema POS, y la notificación se hace de manera mediata ❑ El servidor esta conectado con la red de pagos y automáticamente se hace la notificación.				
10	¿Cuándo se confirma el pago es cuando se envía la orden de venta a bodega o a los proveedores?				
11	¿Qué tipo de arquitectura de comercio electrónico posee la empresa? ❑ Tienda Virtual en sentido estricto o Canal Virtual ❑ Tienda Virtual en sentido Amplio				
12	Dependiendo del tipo de arquitectura del comercio electrónico: ❑ <u>Tienda Virtual en sentido Estricto o Canal Virtual</u>: Cuándo se confirma el pago, ¿Es cuando se envía la orden de venta a los proveedores o a bodega para que envíen en producto a despacho? ❑ <u>Tienda Virtual en sentido Amplio</u>: Cuándo se confirma el pago, ¿Es cuando se envía la orden a los proveedores para que envíen en producto a los clientes?				

13	Dependiendo del tipo de arquitectura del comercio electrónico: ❑ <u>Tienda Virtual en sentido Estricto o Canal Virtual</u>: ¿La empresa utiliza su propio personal para la entrega del producto? ¿La empresa posee una subcontratación para entregar el producto y disminuir riesgos de envío? ❑ <u>Tienda Virtual en sentido Amplio</u>: ¿Existe un contrato con el proveedor donde establezca la cláusula en la cual éste último se compromete a entregar un producto de manera eficiente (tiempo de entrega) y eficaz (calidad del producto).				
14	¿Cuál es el tiempo de entrega de los productos? ❑1 día ❑2 días ❑3 días ❑4 días ❑5 días o más				
15	¿ Todos los productos se ofrecen con envío sin restricciones de lugar o país? (debe existir una cláusula o información acerca de esto en la página Web)				
16	¿En qué momento se factura el pedido del cliente? ❑Cuando se recibe el pedido ❑Cuando se recibe el pago ❑Cuando se envía el producto ❑Cuando se entrega el producto ❑				
17	En caso de consultas sobre envíos específicos ¿Puede el cliente dirigirse, esperando una solución o respuesta, a la tienda o canal virtual?				
18	¿Posee la empresa una política de posventa?				

19	Si posee dicha política ¿a través de qué medio hace la confirmación del producto? ❑ Correo electrónico ❑ Confirmación escrita ❑ Llamada telefónica				
20	¿El cliente tiene la posibilidad de devolver el producto si no le gusta o le sale defectuoso?				
21	¿La devolución del producto consiste en remplazar el producto?				
22	¿Existe la posibilidad de rembolsar el dinero obtenido del cliente, del producto devuelto?				
23	¿El número de pedidos rechazados o devueltos en el mes por el clientes es aceptable o bajo?				
24	¿Cuál es el promedio de pedidos (en porcentaje) rechazados por el cliente en el mes? ❑ 0-10 ❑ 11-25 ❑ 25-50 ❑ 50 o mas				
25	¿Es la tienda o canal virtual la responsable de cualquier reclamo o devolución por parte del cliente?				

ÁREA: TRANSFERENCIA DE INFORMACIÓN A TRAVÉS DE INTERNET Y LA AUTENTICIDAD DEL SITIO WEB

Factor de riesgo: Transmisión de información confidencial a través de una red pública y
autenticidad del Sitio Web

Objetivo de la evaluación: Determinar si el E-commerce posee una canal seguro para el tránsito de información entre el comercio y el cliente, y comprobar la autenticidad de Sitio Web (Si el Comercio es quien dice Ser)

N°	Preguntas	Si	No	N/A	Comentarios
26	¿Existe una persona encargada de velar por la seguridad de la red (vigilante) tanto interna como externa (Internet)?				

27	¿Se tienen políticas de seguridad para la transferencia segura de datos a través de Internet?				
28	¿Se puede garantizar a los clientes la autenticidad del sitio Web donde se tiene instalado el canal virtual?				
29	¿Se posee un certificado de seguridad emitido por una compañía autorizada?				
30	¿Cuál es el nombre de la compañía que ha emitido el certificado de seguridad?				
31	¿El certificado de seguridad esta vigente a la fecha?				
32	¿Se tiene un certificado de seguridad robusto?				
33	¿Cuántos bits tiene la longitud de clave en el proceso de encriptación (según el servicio contratado con la autoridad certificadora)?				
34	¿La autoridad certificadora es reconocida en el mercado?				
35	¿De qué nivel es la compañía certificadora?				
36	¿Se posee firma digital?				
37	¿Se puede proveer un canal seguro de transmisión de información a los clientes?				
38	¿Qué protocolo de seguridad se posee para una transmisión segura de datos?				
	En el caso de los comercios en sentido amplio preguntar adicionalmente lo siguiente:				
39	¿Se prestan servicios de Hosting para la independización de los comercios, de tal manera que ellos tengan la administración completa de su Sitio Web desde el diseño, la información en él contenida hasta que				

	la validación del pago se haga por las mismas empresas independientes o terceras contratadas por estas, diferente al comercio?				
40	¿Para cada nombre de domino de los hosting en el servidor del comercio, se tiene un certificado de seguridad (para cada uno).				
41	¿Es el comercio (prestador del servicio) o la empresa alojada (prestataria) quien tiene la obligación de contratar un certificado de seguridad?				

ÁREA: SEGURIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN PROPORCIONADA POR LOS CLIENTES

Factor de riesgo: Seguridad, confidencialidad e integridad de la información proporcionada por el consumidor

Objetivo de la evaluación: Determinar si el E-commerce posee medidas y políticas para un uso y manejo seguro, confiable, confidencial e íntegro de la información proporcionada por los clientes

N°	*Preguntas*	Si	No	N/A	Comentarios
42	¿Qué tipo de información se recolecta de los clientes?				
43	¿Se tienen políticas de privacidad para el uso y manejo de los datos proporcionados por el cliente?				
44	¿Si se tienen políticas de privacidad, estas son comunicadas a los clientes a través de un link en el sitio Web del comercio?				
45	¿Para que se utiliza la información proporcionada por el consumidor?				
46	¿Personas externas al comercio pueden acceder a dicha información?				
47	¿Quién recolecta la información? ¿La empresa o un tercero?				

48	¿Se tienen alianzas con otros comercios en cuanto al intercambio de información?				
49	¿El cliente puede tener acceso a su propia información y eliminarla por completo de la base de datos del comercio?				
50	¿Se envía publicidad constantemente a los clientes, en relación al perfil formado por medio de sus datos almacenados?				
51	¿Se utilizan Cookies en el ordenador del cliente para publicitar los productos proporcionados por el E-commerce?				
52	¿Qué personal dentro de la empresa puede tener acceso a la información?				
53	¿Existe un responsable directo de la custodia, gestión y distribución de datos?				
54	¿Se tiene algún reglamento o documento de seguridad, en donde se implemente la normativa de seguridad de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información que los gestionan?				
55	¿Se tienen implementados procedimientos de identificación y autenticación que establecen de forma inequívoca y personalizada la identificación de todo aquel usuario que intente acceder al sistema de información y la verificación de que está previamente autorizado?				
56	¿Sólo el personal autorizado podría tener acceso a los locales donde se encuentren ubicados los sistemas de información que gestione los datos de carácter personal?				
57	¿Se lleva un inventario y registro de la gestión de los soportes informáticos que puedan contener datos de carácter personal de los Usuarios?				

58	¿Se tiene algún procedimiento de notificación y gestión de incidencias (anomalías que afecten o pudieran afectar a la seguridad de los datos) y un procedimiento de recuperación de los datos y de gestión de copias de respaldo?				
59	¿Se posee un software robusto y suficiente para manejar, asegurar y gestionar la información de los clientes?				
60	¿Los ficheros o base de datos contenedores de los datos personales de clientes, son accesibles en línea por el personal autorizado desde un punto remoto?				
61	¿Se posee servidor propio donde se encuentre alojado el E-commerce?				
62	¿Se contrata servicio de hosting para mantener el E-commerce (en caso de no tener servidor propio)				
63	¿El Sitio Web está publicitado en otro portal ajeno al E-commerce, en donde, por medio de él se realicen transacciones de venta, de tal manera que, éste pueda contener bases de datos propias donde almacena información de los clientes del comercio?				
64	¿Se utiliza cifrado en aquellos caso en que: (a) la información a transferir sea sensible y (b) la transmisión se realice en canales abierto de comunicaciones?				
65	¿Se llevan a cabo operaciones de interfuncionamiento entre sistemas de información altamente seguros y otros menos seguros (como por ejemplo un servidor seguro con encriptación de 128 bits con un ordenador con navegador que soporta una encriptación menor de 40 bits)				

ÁREA: SEGURIDAD FÍSICA Y LÓGICA INTERNA

Factor de riesgo: La existencia de Garantías de Seguridad, en cuanto a las medidas y políticas que se tengan para salvaguardar el Hardware y Software.

Objetivo de la evaluación: Conocer si las empresas poseen una infraestructura física, lógica y segura de comercio electrónico; como base para realizar transacciones en línea, que provean confianza al consumidor.

N°	Preguntas	Si	No	N/A	Comentarios
66	¿Existe un único responsable de implementar la política de autorizaciones de entrada al lugar donde se encuentra el equipo informático vital para el funcionamiento del E-commerce.				
67	¿Quiénes saben cuales son las personas autorizadas?				
68	¿Se tienen alguna medida de seguridad tal como uso de tarjetas magnéticas o contraseña, para ingresar al lugar donde se tiene el equipo informático importante (el servidor)?				
69	¿Existe control de acceso al Centro de Cómputo?				
70	¿Existe una persona encargada de evaluar y velar por la seguridad de la red interna y externa (Internet)?				
71	¿Existe en la empresa un gerente de tecnología diferente al del área de informática?				
72	¿Existe en la empresa alguien capaz de solucionar problemas críticos de la red y del comercio electrónico, tales como?: • Ataques de piratas informáticos (Hacker) • Ataques de virus • Daño físico de la red o del servidor, entre otros				
73	¿Se le explica al usuario todo lo que				

	está permitido en cuanto al uso de la maquina, y todo lo que expresamente no esté permitido está prohibido?				
74	¿Se posee servidor propio en donde se encuentra la información y se muestra el sitio Web de la empresa?				
75	¿Cuántas personas tienen acceso de administrador al servidor?				
76	¿Cuáles son los niveles de acceso que posee el servidor y cuál es el número de personas en cada nivel de acceso?				
77	¿Existen niveles escalonados de acceso al sistema?				
78	¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?				
79	¿Se ha instruido los usuarios sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?				
80	¿Se tienen políticas de contraseña, en cuanto a?: • La longitud mínima y máxima • El periodo de vigencia de la misma				
81	¿Se posee una red interna de información administrada por un servidor?				
82	¿El servidor que administra la red interna esta conectado a Internet?				
83	¿Qué tipo de conexión se posee?				
84	¿Cuál es la velocidad de la conexión?				
85	¿Cuántas veces se cae el servicio de Internet en el mes (Estimado)?				
86	¿Cuál es el promedio de tiempo sin servicio de Internet en cada caída del servicio (Estimado)?				
87	¿Cuál es la velocidad de respuesta del				

	proveedor del servicio de Internet en caso de falla?				
88	¿Se poseen planes de contingencia en caso de daño en el equipo que posee el comercio electrónico que lo imposibiliten a estar conectado a la red o por cualquier falla en el proveedor del servicio, tales como?: • Cierre del servidor • Clausura del servidor donde se tiene alojado el sitio Web del comercio electrónico, entre otros				
89	¿Se poseen políticas en cuanto al uso del software y del hardware?				
90	¿Qué sistema operativo tiene instalado el servidor?				
91	¿El sistema operativo con el que cuenta su servidor, le permite llevar un registro o bitácora de todos los sucesos surgidos en la red que administra?				
92	¿Se tiene la política de realizar auditoria al sistema operativo por lo menos una vez cada semana?				
93	¿Qué tipo de auditoria se realiza? 4) Auditoría de cuentas de usuario: • Inicio y cierre de sesión. • Acceso a ficheros, directorios o impresoras. • Ejercicio de los derechos de un usuario. • Seguimiento de procesos. • Inicio, reinicio y apagado del sistema. 5) Auditoría del sistema de archivos: • Rastrea sucesos del sistema de archivos • Los sucesos que se pueden auditar • *Cambio de permisos* y *Toma de posesión*. 6) Auditoría de impresoras: • Registro de sucesos de aplicaciones.				

	• Registro de sucesos de seguridad. • Registro de sucesos del sistema				
94	¿Existe una sola persona con el cargo de administrador del servidor?				
95	¿Alguna vez su servidor ha sido atacado por un pirata informático (hacker)?				
96	¿Alguna vez su servidor a sido atacado por algún virus lanzado desde Internet?				
97	¿Alguna vez han sido víctimas de Fraude?				
98	¿Se tienen instalados Firewall (Cortafuego) en su equipo, que le provean certeza en cuanto a la infiltración de datos o personas no autorizadas a la red?				
99	¿Se tienen programas antivirus con actualización contínua capaz de detectar a priori cualquier tipo de virus que se introduzca a la red?				
100	¿Se tienen registrados a nombre de la empresa todo el software de desarrollo, de plataforma y de utilidades del comercio electrónico?				
101	¿Se lleva un inventario del software utilizado por la empresa?				
102	¿Las aplicaciones o software de soporte y utilitarios para el E-commerce son: • Desarrollados por la empresa • Adquirido en el mercado • Mandados hacer a la medida				
103	¿Existe una persona responsable de la Seguridad del hardware?				
104	¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?				
105	¿El Hardware y Software posee la capacidad necesaria para realizar operaciones e- commerce?				

106	¿Se han adoptado medidas de seguridad en el departamento de sistemas de información, tales como: reguladores de voltaje que adecuen la energía eléctrica para dicho departamento, UPS, extinguidotes, entre otros?				
107	¿Son adecuadas las instalaciones para el buen funcionamiento del equipo informático?				
108	¿Se tienen rutinas de mantenimiento preventivo?				
109	¿Se tiene inventariado cada uno de los dispositivos componentes del Hardware, tales como, ordenadores con sus características individuales (Disco duro, Motherboard, Micro procesador, memoria RAM, CD-Rom u otros dispositivos), periféricos, enrutadores, entre otros.				
110	¿Se cuenta con un plan de actualización de hardware a medida que van surgiendo los avances tecnológicos, de tal manera que se adecúa a las nuevas exigencias de los clientes en cuanto a eficiencia?				

3.4.3. Programa de Auditoria

PROGRAMA DE AUDITORIA
PARA EVALUAR LA SEGURIDAD EN EL COMERCIO ELECTRONICO

Cliente: _____
Periodo de auditoría: _____

ÁREA: LOGÍSTICA DE OPERACIONES

Factor de riesgo: Satisfacción de las expectativas del cliente en cuanto a la eficiencia del tiempo de entrega del producto y eficacia de las especificaciones del producto, así como del proceso logístico de venta.

Objetivo de la evaluación: Conocer la capacidad instalada que poseen la empresa para hacer frente a las exigencias de este modelo de negocios, así como para asegurar que la logística de operación de venta al recibir un pedido u orden de compra es eficiente y eficaz. Todo esto incluye el tiempo de respuesta para cada orden, los pedidos rechazados durante un lapso de tiempo, el momento de facturación, los medios de pago aceptados, el proceso de envió del producto y políticas de devolución.

N°	PROCEDIMIENTO	ejec.	Hecho	Fecha	Refer.
1	Solicitar el catálogo de productos que ofrece la tienda y Revisar si cada producto posee especificaciones claras y precisas.				
2	Si no existe un catálogo de productos ofertados en el sitio Web: e) Entrevistarse con el gerente de ventas o e-commerce y hacer una narrativa en donde se pueda identificar las razones por las cuales no se ha elaborado. f) Comparar lo expuesto por el gerente ventas con lo que expresa el				

	encargado de despacho o bodega				
3	Ingresar al sitio Web de la empresa y simular una compra y antes de pagar: ❑ Verificar si los productos ofrecidos tienen detalles o especificaciones claras. Leer detalles y capturar una pantalla. ❑ Verificar si se puede seguir comprando o seleccionando productos. capturar pantalla ❑ Verificar si existen indicaciones acerca de aclaraciones o dudas de productos o algún procedimiento. Capturar pantalla				
4	Realizar Punto Fijo: Observación participativa, durante un día completo (dicho día debe ser considerado normal, en una temporada normal) en el servidor de la entidad con el fin de : ❑ Verificar cuántos pedidos se reciben durante un día y documentarlo a través de una narrativa. ❑ Verificar el tiempo promedio que se tarda la empresa en confirmar el pedido a sus clientes. ❑ Verificar el medio utilizado por la empresa para confirmar el pedido a sus clientes.				
5	Ingresar al sitio Web de la empresa y simular una compra : ❑ Al momento de pagar, observe el medio o				

	medios de pago que acepta la empresa. Capture la Pantalla ❑ Si se puede pagar con tarjeta de crédito, determine si dicho pago se notifica de manera inmediata, ❑ Observe si la confirmación de la compra se hace antes, durante o después del pago. Utilice una Narrativa				
6	Inspeccione en la empresa si se posee un Sistema POS para validar la operación de pago				
7	Dependiendo de la Arquitectura de comercio electrónico que posee la empresa, Observe : ❑ <u>Tienda Virtual en sentido Estricto o Canal Virtual</u>: Verifique si cuando se confirma el pago, es cuando se envía la orden de venta a los proveedores o a bodega para que envíen el producto a despacho. Documente a través de una narrativa ❑ <u>Tienda Virtual en sentido Amplio</u>: Verifique si cuándo se confirma el pago, es cuando se envía la orden a los proveedores para que envíen el producto a los clientes. Documente a través de una narrativa.				
8	Dependiendo de la Arquitectura de comercio electrónico que posee la empresa, Observe :				

	❑ Tienda Virtual en sentido Estricto o Canal Virtual: 4. Solicite a la empresa sus políticas de envió, y determine cual es la forma para realizarlo. 5. Si fuere realizado dicho envió, a través del personal de la empresa, solicitar los manuales de descripción de puestos, para determinar las funciones y responsabilidades de los empleados con el fin de disminuir los riesgos adheridos a dicha función de envío. 6. Si fuere bajo subcontrataciones, solicite una copia del contrato para determinar las competencias y responsabilidades de dichas entidades que prestan el servicio de courier ó ❑ Tienda Virtual en sentido Amplio: Solicite el contrato para verificar las cláusulas en donde se compromete el proveedor a entregar el producto en el tiempo mínimo previsto y en condiciones según especificaciones determinadas				
9	Sin importar la estructura del comercio electrónico, verifique, cuál es el tiempo promedio de entrega				

	de los artículos, para esto: ❑ Ingrese a la página Web de la empresa y busque la sección de políticas de envío, en la cual debe especificar el tiempo de entrega según productos y localidad. Capture la pantalla ❑ Entreviste al gerente de la empresa para solicitar información, basada en la experiencia, de cuanto es el tiempo de entrega de productos al cliente, ya sea que lo realice la misma empresa, subcontratantes o sus proveedores. ❑ Envié una confirmación a varios clientes seleccionados al azar, para corroborar el período de entrega de productos.				
10	Desarrolle el mismo procedimiento anterior para determinar si existen restricciones de envíos de productos en base a su localidad o país.				
11	Realizar una entrevista con el encargado de ventas o e-commerce para consultar el momento específico en que se factura el pedido. Las razones del porque ese momento. Redacte una Narrativa para sustentar. Verifique la respuesta del encargado de ventas, por				

	medio de observar el proceso que sigue al recibir un pedido escogido al azar. Redacte una Narrativa para sustentar.				
12	Solicitar el manual de políticas y procedimientos de la empresa y verificar la existencia de políticas de postventa, en la cual se establece, entre otras: ❑ El mecanismo para confirmar la satisfacción del cliente con el producto vendido ❑ Evaluar la eficiencia de la empresa en el envió del producto				
13	Solicitar el manual de políticas y procedimientos de la empresa y verificar la existencia de políticas de devolución, en la cual se establece, entre otras: ❑ Si existe la posibilidad de devolver productos ❑ Cuáles son las causas que proceden para una devolución de productos ❑ Qué efectos tiene la devolución del producto, el reemplazo del artículo o el reembolso del dinero ❑ Si la empresa es la responsable de dicho reclamo o si traslada la responsabilidad al proveedor. Redacte una narrativa de dicho procedimiento				

14	Realice un procedimiento similar al anterior, solamente que a través de una Entrevista al encargado de e-commerce. Redacte una narrativa de dicho procedimiento				
15	Ingresar al sitio Web de la empresa y:: ❑ Verificar si existen las políticas de devolución escritas en la página Web. Capturar pantalla ❑ Si dichas políticas coinciden con la descrita en el manual de políticas de la empresa u opinión del encargado de e-commerce				

ÁREA: SEGURIDAD ENTRANSFERENCIA DE INFORMACIÓN A TRAVÉS DE INTERNET Y LA AUTENTICIDAD DEL SITIO WEB

Factor de riesgo: Transmisión de información confidencial a través de una red publica y
autenticidad del Sitio Web

Objetivo de la evaluación: Determinar si el E-commerce posee una canal seguro para el tránsito de información entre el comercio y el cliente, y comprobar si se tiene un mecanismo para la autenticidad de Sitio Web donde se encuentra el Comercio Electrónico (Si el Comercio es quien dice ser.)

N°	PROCEDIMIENTO	Eje.	Hecho por	Fecha	Ref.
16	Preguntar si existe una persona encargada de vigilar la seguridad de la red tanto interna como externa, y: e) Establecer contacto con dicha persona f) Entrevistarlo, y hacer una				

	narrativa de sus funciones. g) Preguntar las políticas y medidas de control que se tienen e implementan para lograr una seguridad en red satisfactoria h) Establecer un perfil de idoneidad para el cargo que ostenta.				
17	Solicitar el manual de políticas y procedimientos de la empresa y verificar la existencia de políticas y medidas especificas para la seguridad en las transacciones efectuadas a través de Internet (transferencia de información).				
18	Si no existen políticas y procedimientos de control escrito: g) Entrevistarse con el gerente general y hacer una narrativa en donde se pueda identificar las líneas generales establecidas por éste en cuanto a la seguridad en red. h) Comparar lo expuesto por el gerente general con lo que expresa el encargado de la seguridad (si lo hay).				

19	Desde cualquier ordenador, con las siguientes requerimientos mínimos a la fecha de este trabajo, sin embargo con el avance continuo y acelerado de la tecnología en un futuro cercano pueden ser mayores: d) Hardware • Pentium III 1 GHZ, Celeron 1 GHZ, AMD Duron 1500, Athlon 2600 u otras equivalentes. • Memoria de 256 MB • Disco duro de 10 GB e) Software • Windows 98 o equivalente (Linux, UNIX) • Navegador Microsoft Internet Explorer 4.0 o Netscape Navigator 4.0 f) Conexión a Internet • Con MODEM 56 kbps, preferiblemente conexión a través de cable de 128 kbps o más. Realizar las siguientes pruebas:				
20	Ingresar al sitio Web del comercio evaluado				
21	Verificar la existencia de un logotipo de alguna autoridad certificadora				
22	Dar clic a dicho logotipo y verificar: a) Que los datos de identificación del certificado tales como, denominación o razón social de la empresa y nombre de dominio, coincidan con los datos reales del comercio. b) Que la fecha actual este dentro del periodo de validez del certificado.				
23	Ingresar al sitio Web de la autoridad certificadora y				

	verificar: a) El servicio contratado por la empresa (SSL de 40 o 128 bits) b) Evaluar si dicha entidad certificadora es fiable, si es de raíz o intermedia, puede tomar como parámetro para dicha evaluación, las compañías proporcionadas por Microsoft Internet Explorer mas reciente, en el menú de Herramientas, submenú opciones de Internet ficha de contenido, opción certificados. Esto no obsta que hayan muchas más compañías fiables en Internet que las proporcionadas en dicha lista.				
24	Simular un proceso de compras, y documentado paso a paso por medio de captura de pantallas y comprobar los siguientes acontecimientos en momentos cruciales: b) En el momento de enviar los datos personales tales como: nombre, dirección, teléfono, número de tarjeta de crédito, en el proceso de pago en línea, verificar que el explorador (si se esta trabajando con Microsoft Explorer), despliegue una ventana donde diga que la información que se intercambie con este sitio no puede ser vista o cambiada por otros, en dicha ventana, se estipula si se tiene o no confianza en el certificado, si el certificado es válido, si el certificado coincide con la pagina que se desea ver. c) Corroborar que en la parte inferior derecha del				

	Navegador, aparezca un candado cerrado, el cual indica que la comunicación entablada con el sitio Web es segura, esto debe ser en el momento del proceso de pago. Es importante aclarar que muchas veces el Navegador no despliega la ventana señalada en el literal a), sino solamente el candado cerrado en la parte inferior derecha. d) Dar clic sobre el candado cerrado, y verificar el certificado de seguridad, en el cual aparecen datos tales como: El propósito del certificado, nombre del comercio al cual ha sido emitido, nombre de la autoridad certificadora, período de validez, el algoritmo hash utilizado para la firma digital, la clave publica y su extensión, la huella digital, entre otros datos de importancia. e) Extraer dicho certificado, copiándolo a un medio de almacenamiento flexible, tal como un disco magnético, una memoria flash o un disco óptico.				
25	En el caso de los comercios en sentido amplio adicionalmente a lo anterior corroborar los siguiente: d) Si la empresa presta servicios de hosting independientes a otras empresas diferentes de los proveedores definidos, para lo cual se debe preguntar al gerente general y al encargado de informática. e) Si los proveedores definidos, son realmente proveedores o un comercio independiente, para lo cual se debe ingresar				

	a un 10% de las paginas de los proveedores albergados en el servidor del comercio y simular un proceso de compras en cada uno de ellos en donde se debe verificar, que en el momento de pago, quien valide la transacción, sea el comercio y no otra empresa. f) Si los proveedores son una empresa independiente, que solamente ha contratado un servicio de hosting (albergue) en el servidor del comercio, verificar que posea su propio certificado de seguridad.				

ÁREA: SEGURIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN PROPORCIONADA POR LOS CLIENTES

Factor de riesgo: Seguridad, confidencialidad e integridad de la información proporcionada por el consumidor

Objetivo de la evaluación: Determinar si el E-commerce posee medidas y políticas para un uso y manejo seguro, confiable, confidencial e integro de la información proporcionada por los clientes

N°	PROCEDIMIENTO	Eje.	Hecho por	Fecha	Ref.
26	Desde un ordenador con las especificaciones proporcionadas en el área de seguridad en red Ingresar al Sitio Web del comercio y realizar los siguiente procedimientos: g) Efectuar el proceso de compras desde el inicio hasta el fin, documentándolo a través de la captura de pantallas. h) Algunos comercios solicitan registro del socio, para que éste pueda acceder a utilizar el E-commerce como tienda virtual, documentar dicha situación capturando las pantallas correspondientes.				

	i) Cerciorarse que quien pida la información sea el E-commerce y no un tercero. j) Corroborar que en el momento de ingresar y enviar cualquier tipo de información personal, ya sea en el momento de registro o de pago, se esté en un canal de comunicación seguro (tal como se ha establecido en el área de seguridad en red) k) Si fuese posible ingresar al sitio Web con un navegador Internet Explorer o Netscape versión 1.0 o menor, y comprobar si se puede establecer una conexión segura (Debido que estos navegadores no soportan el protocolo de seguridad SSL) l) Verificar y documentar el tipo de información solicitada por el comercio.				
27	Durante el transcurso de diez días después de haber efectuado el procedimiento anterior verificar las siguientes situaciones: e) Ingresar al correo electrónico proporcionado en el momento de enviar los datos solicitados por el comercio, y determinar: ❑ Si se ha recibido Spam publicitarios ❑ La frecuencia con que se recibe dicha publicidad por día. ❑ Documentar las situaciones anteriores por medio de: captura de pantallas y narrativas taxativas de las observaciones realizadas. f) Ingresar periódicamente al sitio Web del comercio y observar: ❑ Si en el momento de cargar la pagina Web del				

	E-commerce, automáticamente aparecen ventanas, del comercio o de terceros con contenido publicitario. ❑ Si estas páginas publicitarias son propiedad del comercio. ❑ ¿Cual es el contenido de las referidas páginas?, ya que muchas veces, pueden ser link a sitios pornográficos. ❑ Documentar las situaciones anteriores por medio de: captura de pantallas y narrativas taxativas de las observaciones realizadas g) Si confluyen los aspectos señalados en el literal anterior es por que el comercio está haciendo uso de Cookies, para verificar los Cookies implantados en el ordenador del cliente, realizar los siguientes procedimientos: ❑ Ingresar al menú de herramientas del navegador, y escoger opciones de Internet, dentro de esta acceder a la opción de configuración, y seleccionar “ver archivo”, allí se le mostrará una lista de Cookies almacenados en su ordenador, buscar los relativos a las ventanas observadas en el momento de cargar las páginas Web de E-commerce (si se utiliza Internet Explorer). ❑ Documentar las situaciones anteriores por medio de: captura de pantallas y narrativas				

	taxativas de las observaciones realizadas h) Determinar y evaluar si existe o no exceso en el uso de estas técnicas publicitarias (Spam y Cookies), en relación a las observaciones hechas al respecto, lo cual quedará a criterio del auditor, sin embargo, dicho aspecto se debe documentar en una narrativa razonada del criterio adoptado.				
28	Entrevistarse con el Gerente General, y preguntar si existen políticas de privacidad, si existieren, solicitar el documento escrito, y revisar lo siguiente: e) Las cláusulas relativas, a la privacidad, confidencialidad, seguridad e integridad de los datos f) Los usos, fines y manejo de la información g) Preguntar al gerente si se está ligado a algún código de ética en cuanto a la protección, manejo y uso de datos, tal como el de garantía de protección de datos de la AECE en Europa. h) Evaluar y hacer una narrativa, sobre los aspectos antes mencionados, soportándolo con la copia de las políticas de privacidad si están escritas, de lo contrario inferirlas acorde a la entrevista suscitada con el gerente y corroborarla con otro personal de la empresa.				
29	Dentro del sitio Web del comercio verificar que: e) En cualquier proceso, ya sea de pago o de registro, exista un link perfectamente visible				

	para desplegar la página que contiene las políticas de privacidad. f) En los procesos mencionados en el literal anterior, se pida consentimiento al cliente, sobre el uso y manejo de la información recavada. g) Exista algún logotipo como sello de garantía, de la adhesión del E-commerce a algún código de ética que regule lo relativo a la protección, uso y manejo de los datos del usuario. h) El cliente o usuario pueda tener acceso a su información personal para eliminar su registro.				
30	Solicitar al gerente un reglamento donde se encuentren plasmadas normas prohibitivas e imperativas que vinculen directamente a los empleados responsables del tratamiento de los datos, así como a cualquier otro, aunque no esté directamente ligado a dicha responsabilidad. Dicho documento debe contar con sanciones por contravenciones a las normas previstas. c) Hacer una narrativa sobre el contenido de dicho documento, evaluándolo y comparándolo con los parámetros antes mencionados y con el juicio razonable del auditor. d) De no existir dicho documento expresarlo y documentarlo a través de la narrativa correspondiente.				
31	Observar el proceso del flujo de la información, desde que se recaba y almacena hasta que utiliza para cualquier fin previsto, como por ejemplo, para: procesar y enviar el pedido, notificar el envió, hacer				

	estudios internos (estadísticos, demográficos, gustos y preferencias, etc.), el envió de publicidad, etc. y determinar: d) El personal que interviene en el proceso en cuanto: ❑ La existencia de un responsable general, en cuanto a la guardia, distribución y manejo de la información. ❑ Los departamentos o áreas del negocio usuarios de la información ❑ La cantidad de personas en cada departamento que acceden a los datos para los fines antes mencionados. ❑ Los niveles de acceso a dicha información dependiendo el departamento o área y la persona. ❑ Hacer una narrativa y un flujograma de lo observado. e) Para ejecutar los cometidos antes mencionados, se debe realizar lo siguiente: ❑ Observar por un tiempo prudencial las labores ejecutadas por cada persona relacionada con el procesamiento de los datos de los clientes. ❑ Pedir una muestra de las labores ejecutadas por cada persona vinculada al procesamiento de la información de los clientes. ❑ Capturar las pantallas donde se muestren, los accesos y el tipo información procesada por el empleado respectivo. f) En el caso de las tiendas				

	virtuales ya sea en sentido estricto o amplio, se vuelve mucho mas sencillo la ejecución de los procedimientos antes señalados, debido que la organización es menos compleja, no así con los comercios que poseen un canal virtual, sin embargo esto no obsta para obviar su ejecución. Lo que se tiene que tener mas en cuenta en este prototipo de negocios, son los niveles de acceso que cada empleado, departamento o área tiene a la información en cuestión.				
32	Solicitar al encargado principal de la guardia, y manejo de la información, que le proporcione el ordenador de trabajo de él, y realice las siguientes pruebas: d) Tratar de ingresar a la base de datos que contiene la información de los clientes. e) Pedir al encargado que ingrese a dicho fichero y observar, su nombre de usuario. f) Documentar lo realizado anteriormente mediante la captura de pantallas. Realizar el mismo procedimiento anterior, con una muestra significativa de personas con acceso a la información de los clientes.				
33	Solicitar al administrador del servidor que le proporcione una lista, de los accesos a la base de datos o fichero que contiene la información del consumidor, durante el período en el cual se corrió el procedimiento anterior y verificar: d) Que se haya registrado los accesos denegados así como				

	todos los accesos no denegados. e) Corroborar que coincidan con los nombres de usuarios muestreados. f) Documentar estos procedimientos a través de narrativas y captura de pantallas.				
34	Elaborar un inventario del software que se encarga de gestionar, manejar y asegurar los datos de los clientes.				
35	Pedir al encargado de informática que muestre la copia de respaldo de los datos almacenados en el servidor.				
36	En el caso que cualquier información almacenada en el servidor del E-commerce, fuere accesible por personal autorizado desde un punto remoto, verificar: c) La seguridad en cuanto a la transferencia de información a través de Internet (Seguridad en Red) d) La seguridad en cuanto a las claves y niveles de acceso.				
37	Corroborar, que se tenga servidor propio y que en éste se encuentre alojado el E-commerce, esto se hace mediante una inspección física, y la consecuencia de los procedimientos anteriores lo indica. De no contar con servidor propio es obvio que personas ajenas a la empresa pueden acceder a cualquier tipo de información relacionada con el comercio electrónico, en este caso el prestador de servicio de Hosting.				
13	Los procedimientos adicionales a cerca de la seguridad física				

	(Hardware) y lógica (software) se detallaran en el área que para tal efecto se tiene segregada.				

ÁREA: LA SEGURIDAD FÍSICA Y LOGICA INTERNA

Factor de riesgo: La existencia de Garantías de Seguridad, en cuanto a las medidas y políticas que se tengan para salvaguardar el Hardware y Software.

Objetivo de la evaluación: Conocer si las empresas poseen una infraestructura física, lógica y segura; de comercio electrónico; como base para realizar transacciones en línea, que provean confianza al consumidor.

N°	PROCEDIMIENTO	Ejec	Hecho	Fecha	Ref.
37	Entrevistarse con el gerente general del E-commerce y preguntarle los siguientes aspectos: ❑ Quién es responsable especifico de el área de informática. ❑ Quién es el responsable de autorizar a los usuarios en cuanto al acceso al equipo informático y al software especifico. ❑ Cuéles son las políticas y medidas de seguridad generales adoptadas por la empresa en cuanto a la seguridad del equipo informático en todos sus aspectos. ❑ Si existe un manual de políticas y procedimientos por escrito donde se detalle taxativamente las políticas y procesos que debe cumplir y seguir cada empleado. ❑ Si existe un manual de inducción para cada empleado en cuanto a las labores que ejecuta. ❑ Hacer una narrativa de lo expuesto por el gerente general.				

38	Entrevistarse con cualquier empleado del departamento de informática del E-commerce y preguntar lo siguiente: ❑ Quién es su jefe superior inmediato. ❑ Quién le ha autorizado su acceso al equipo y al software. ❑ Si se le ha explicado todo lo que está permitido y prohibido en lo referente a la utilización del software y hardware. ❑ Si se le ha hecho una descripción taxativa de sus funciones. ❑ Si conoce las políticas y procedimientos. ❑ Y en general si ha recibido un adiestramiento en lo referente a su trabajo.				
39	Solicitar el manual de políticas y procedimientos y el manual de descripción de funciones y de puesto en lo referente al área de informática.				
40	Solicitar al encargado de informática que le muestre él o los servidores que administran y gestionan la información y verificar lo siguiente: ❑ Capacidad de procesamiento. ❑ Capacidad de almacenamiento. ❑ Capacidad de memoria. ❑ Velocidad de conexión a la red. ❑ Documentar dicha información.				
41	Solicitar al administrador del servidor que le permita ingresar al sistema operativo y verificar lo siguiente: ❑ Los grupos y usuarios que tienen acceso al sistema operativo. ❑ Cantidad de usuarios que				

	tienen acceso de administradores. ❑ Si los usuarios ordinarios tienen acceso restringido. ❑ En base a lo anterior, indagar cuál es el nivel de acceso de los programadores y analistas.				
42	Comprobar que los sistemas utilizados para manejar la información vital del E-commerce tales como aplicaciones, tendientes a gestionar y manipular bases de datos posean seguridad de acceso a través del uso de nombres de usuario y contraseñas.				
43	Cerciorarse que las bases de datos que contienen información valiosa para el E-commerce principalmente datos de clientes, proveedores e información financiera, estén debidamente protegidas contra el acceso no autorizado, a través de claves o que sus datos se encuentren cifrados o inteligibles. Para lo cual se debe extraer una base de datos y tratar de ingresar a ella, si es necesario, solicitar la colaboración de un experto para realizar este procedimiento.				
44	Preguntar al encargado de autorizar los accesos a los sistemas la política de contraseñas en lo referente a: ❑ Longitud mínima y máxima. ❑ Periodo de vigencia.				
45	Solicitar el listado de todos los usuarios con su respectiva longitud de contraseñas y sus períodos de vigencia.				
46	Cerciorarse que exista una verdadera y eficaz rotación de contraseñas y que los períodos de validez de la misma no sean muy largos o prolongados como máximo 90 días.				

47	Solicitar la diagramación de la red interna y corroborar si el servidor principal que la administra, esta conectado a Internet.				
48	Confirmar el tipo de conexión que posee el E-commerce, en lo referente a: a) Medios de comunicación de la red interna con Internet. ❑ Satelital. ❑ Cable. ❑ Modem con conexión a línea telefónica. d) Velocidad de conexión. e) Hacer una evaluación en cuanto a la idoneidad de la conexión y su velocidad en cuanto al volumen de transacción de E-commerce (Vistas por días al sitio Web).				
49	En el transcurso del período de auditoría ingresar al sitio Web del comercio por lo menos unas tres veces al día, distribuido de forma aleatoria con intervalos prudenciales, durante cuatro días a la semana y observar: ❑ Que el sitio Web se cargue correctamente, es decir que no presente errores de página. ❑ Que el servidor se encuentre funcionando durante las 24 horas del día. ❑ Que la velocidad en la exploración y la realización de las operaciones sea razonable. ❑ Que se encuentre en pleno trabajo todas las funciones y servicios proporcionados en la página Web.				
50	Revisar los contratos de servicio de Internet y verificar las garantía que ofrece el proveedor del servicio en caso de fallas o				

	clausura de éste.				
51	Solicitar los planes de contingencia que poseen en caso de cualquier contingencia que imposibilite parcial o totalmente el funcionamiento del E-commerce, y evaluar la razonabilidad y factibilidad material de los mismos.				
52	Solicitar un inventario de todo el software que posee el comercio (aplicaciones y utilitarios) y realizar los siguientes procedimientos: ❑ Verificar que cada uno de ellos este registrado a nombre de la empresa (los que no son gratuitos). ❑ Realizar un muestreo del 5% y corroborar su existencia así como su pleno funcionamiento. ❑ Corroborar que se encuentre almacenados en el ordenador indicado según el inventario.				
53	Ingresar al servidor principal y corroborar el sistema operativo que posee (Windows 2000, Windows 2000 Server, Windows NT, UNÍX, LINUX, entre otros)				
54	Dependiendo el sistema operativo así serán los sistemas y rutinas de seguridad que posean, sin embargo éstos deben contar con componentes básicos de seguridad, por tanto, revisar que el sistema posea: ❑ Bitácora de todos los sucesos surgidos en la red que administra. ❑ Auditorias del sistema en cuanto a rastreo de sucesos y procesos.				
55	Cerciorarse que se estén realizando auditorias a la red o al sistema, en lo referente, a cuentas de usuario, sistemas de archivo e				

	impresoras.				
56	Corroborar la existencia de cortafuegos. Hacer una lista de los mismo describiendo su función principal y verificar su última actualización.				
57	Enlistar los antivirus que se poseen tanto en el servidor como en cada estación de trabajo. Verificar su última actualización.				
58	Verificar que se estén haciendo copias de respaldo de la información importante periódicamente, ya sea a través de medios de almacenamiento óptico, magnéticos, o backup de servidor en otras regiones.				
59	Solicitar el inventario de las copias de seguridad, y cerciorarse que se encuentren en un lugar distinto al establecimiento del comercio.				
60	Solicitar la colaboración de un experto para evaluar si el hardware y software de la compañía tiene la capacidad necesaria para soportar E-commerce con un volumen de transacciones cuantioso.				
61	Solicitar el inventario de Hardware y verificar a través de una muestra razonable: ❑ La existencia. ❑ La obsolescencia. ❑ El buen funcionamiento. ❑ Que se encuentren ubicados, según inventario.				
62	Observar y evaluar si las instalaciones físicas son idóneas para resguardar el equipo informático, para lo cual se debe verificar que: ❑ Exista una temperatura apropiada para el				

	mantenimiento del sistema (Aire acondicionado). ❑ Las instalaciones sean herméticas en cuanto a la humedad. ❑ Existan sistemas de alarma contra incendios y suficientes extinguidores. ❑ Se tenga una adecuada tensión eléctrica. ❑ Se posean polarizaciones en los tomacorrientes donde se conecta el equipo. ❑ Se tengan reguladores de voltaje y UPS. ❑ En el lugar donde se encuentra el equipo principal tal como el servidor sea de acceso restringido, solo para personal autorizado y que cuente con las medidas de seguridad tendientes a cumplir con estas condiciones, tal como la utilización de cerraduras eléctricas, donde el personal autorizado posea claves de acceso o tarjetas magnéticas.				