PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

ESCUELA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

TÍTULO:

"ESTÁNDARES DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN APLICABLES AL E-COMMERCE "

LÍNEA DE INVESTIGACIÓN:

GOBIERNO DE TI

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR:

JAHIRO FALCONES ESTRADA

ASESOR:

MGT. CESAR GODOY

ESMERALDAS, ABRIL 2018

Trabajo de tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de grado de la PUCESE previo a la obtención del título de INGENIERO DE SISTEMAS Y COMPUTACIÓN.

Presidente Tribunal de Graduación

Lector 1
ING. SUSANA PATIÑO

Lector 2
ING. KLEBER VERA

ING. XAVIER QUIÑONEZ KU
Director de la Escuela de Sistemas y Computación

Esmeraldas, 10 de Enero del 2018

AUTORÍA

Yo, **Jahiro Falcones Estrada**, portador de la cédula de identidad No. **080289720-7,** declaro que la presente investigación enmarcada en el actual trabajo de tesis es absolutamente original, auténtica y personal.

En virtud que el contenido de esta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCESE.

Jahiro Falcones Estrada
C.I.: 080289720-7

CERTIFICACIÓN

Mgt. Cesar Godoy, docente investigador de la PUCE-Esmeraldas, certifica que:
La tesis de grado realizada por JAHIRO JAVIER FALCONES ESTRADA bajo el título "ESTANDARES DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION APLICABLES AL E-COMMERCE", reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final las sugerencias realizadas, en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargado de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, 6 de abril del 2018.

Mgt. Cesar Godoy
Asesor

AGRADECIMIENTOS

A Dios por rodearme de personas maravillosas que han aparecido a lo largo de esta mi gran meta.

A mis padres por su paciencia, entrega y apoyo incondicional.

A mi tía Wendy, por todo su apoyo en el transcurso de mi vida.

A mi maestro, tutor y amigo que creyó en mí y que con paciencia y sabiduría supo guiarme.

A todos mis familiares y amigos que estuvieron pendientes y motivándome a no decaer, porque todo en la vida se puede lograr si te aferras a ese sueño.

Gracias totales, es una bendición tenerlos en mi vida.

DEDICATORIA

El presente trabajo de investigación está dedicado a Dios, a mi madre y mi padre que siempre añoraron que cumpliera esta meta, me motivaron a seguir batallando, mis ejemplo a seguir, todos mis logros son suyos.

A mi familia, para que al igual que yo luchen por todos sus sueños.

Jahiro Falcones

ÍNDICE DE CONTENIDOS

AUTORÍA iii
CERTIFICACIÓN iv
AGRADECIMIENTOS iii
DEDICATORIA iv
ÍNDICE DE CONTENIDOS v
LISTA DE FIGURAS vii
LISTA DE TABLAS viii
RESUMEN ix
ABSTRACT x
INTRODUCCIÓN 1
Presentación del tema de investigación 1
Planteamiento del problema 2
Justificación 3
OBJETIVOS 4
CAPÍTULO I: MARCO TEÓRICO 5
1.1. Bases teóricas científicas 5
1.1.1. Estándares de Seguridad y Confidencialidad 5
1.1.2. Protocolos de Seguridad 7
1.1.3. Sistemas de encriptación 9
1.1.4. Web 10
1.1.5. Herramientas Web de diseño involucradas en el comercio electrónico. 11
1.1.6. Componentes de programación web utilizados en el e-commerce 12
1.1.7. E-Commerce 14
1.1.8. Tiendas Virtuales 15
1.1.9. Formas de Pago 19
1.1.10. Ataques y Seguridad en el E-Commerce 21
1.2. Antecedentes 23
1.3. Marco Legal 25
1.3.1. Bases Legales. 25
CAPÍTULO II: MATERIALES Y MÉTODOS 29
2.1. Área de Estudio. 29
2.1.1. Descripción del lugar 29
2.1.2. Tipo de investigación 29
2.2. Recolección de Datos 30

2.2.1. Población 30
2.3. Métodos y técnicas. 30
2.4. Descripción del instrumento 31
2.5. Descripción de las técnicas de procesamiento y análisis 31
2.6. Normas éticas 31
CAPÍTULO III: RESULTADOS 32
3.1. Análisis de dos de las principales tiendas virtuales utilizadas a nivel mundial con builtwith.com e investigación bibliográfica. 32
CAPÍTULO IV: DISCUSIÓN 36
CAPÍTULO V: CONCLUSIONES 39
CAPÍTULO VI: RECOMENDACIONES 40
CAPÍTULO VII: ANEXOS 41
BIBLIOGRAFÍA 42

LISTA DE FIGURAS

Figura 1. Criptografía de clave simétrica. 9
Figura 2. Criptografía de clave asimétrica. 9
Figura 3. Arquitectura del servicio web 11
Figura 4. Codificación tienda Online con PHP, MySQL HTML5 CSS3. 13
Figura 5. Codificación Carrito de Compras con PHP, MySQL HTML5 CSS3 14
Figura 6. Logo de Amazon. 17
Figura 7. Logo de EBay 17
Figura 8. Logo de Mercado Libre 18
Figura 9. Logo de Yaestá.com. 19

LISTA DE TABLAS

Tabla 1. Estándares de Seguridad 6
Tabla 2. Protocolos de Seguridad 7
Tabla 3. Comparación de sistemas de seguridad 35

RESUMEN

En la actualidad las empresas se han visto obligadas a crear nuevos medios de comunicación con sus clientes que le permitan obtener el volumen de ventas necesario para tener ganancias, es por esto que el e-commerce es una herramienta invaluable para el departamento de ventas de las empresas. Ante el alto crecimiento tecnológico a pesar de las ventajas que representa este avance se ha incrementado también el riesgo de sufrir estafas, daños y robos por medio de la tecnología.

Mediante al uso de entrevistas e investigaciones bibliográficas esta investigación ha logrado determinar los estándares y protocolos de seguridad y confidencialidad de la información, con lo cual se reduce para los usuarios los riesgos de fraude informático en el comercio electrónico.

Así se puede no solo conocer los principales riesgos existentes en el desarrollo del comercio electrónico, sino también los componentes de varias plataformas utilizadas para desarrollo de esta actividad y los métodos más seguros para ser llevada a cabo.

Se han analizado en este trabajo investigativo también varios trabajos presentados con anterioridad que han servido de guía y método de discusión para llegar a conocer los cambios significativos realizados en el e-commerce, en la web y las diferentes plataformas base para su desarrollo, por ende se puede decir que esta investigación despeja gran cantidad de dudas en cuanto a la seguridad necesaria para llevar a cabo el e-commerce además de presentar herramientas útiles para mejorar este importante aspecto.

Palabras Clave: Comercio Electrónico, seguridad electrónica, protección de fraudes informáticos, protocolos de seguridad.

ABSTRACT

At present, companies have been forced to create new means of communication with their clients that allow you to obtain the volume of sales necessary in order to take profits, it is for this reason that e-commerce is an invaluable tool for the sales department of the companies. Before the high technological growth in spite of the advantages that represents this advance has also increased the risk of fraud, damage and theft through technology.

Through the use of interviews and bibliographic research this research has succeeded in establishing the standards and protocols of security and confidentiality of the information, thereby reducing the risks for users of computer fraud in electronic commerce.

So you can not only know the main risks in the development of e-commerce, but also the components of several platforms used for development of this activity and the most secure methods to be carried out.

Have been analyzed in this research paper also several papers previously submitted that have served as a guide and discussion method to get to know the changes made in the e-commerce, on the web and the different platforms as the basis for its development, therefore it can be said that this research clears a lot of doubts as to the security necessary to carry out the e-commerce in addition to useful tools for improving this important aspect.

Key words: Electronic Commerce, Electronic security, protection of computer fraud, security protocols.

INTRODUCCIÓN

Presentación del tema de investigación

Esta investigación se basa en estándares de seguridad y confidencialidad de la información aplicable al e-commerce, con la finalidad de proteger los datos transferidos por los usuarios a través de los pagos por internet, generando una forma más segura a la hora de realizar transferencias o pagos, en las tiendas virtuales este aspecto es fundamental para ejecutar operaciones en línea utilizando sistemas seguros para adquirir algún producto o servicio. En este estudio se analizarán los estándares más conocidos, funcionales y seguros que deben utilizarse en la web.

En estos días, la manera de comprar y vender productos mediante el internet en diversas páginas web que se basan exclusivamente para el e-commerce, es un hecho del día a día por los diferentes usuarios, tanto en personas particulares y empresas que se dediquen a la venta de diferentes productos y servicios a través del internet. La evolución del internet ha hecho que vender de forma presencial sea algo del pasado puesto que el internet es una vía más rentable en lo económico y así mismo cubre un territorio más extenso.

A nivel mundial los líderes en comercio electrónico son Estados Unidos, Europa y Japón aunque la idea de ventas por internet se ha posicionado en el mercado como método de adquisición de productos, en América del sur el uso de plataformas web para comercializar se hace cada vez más popular logrando mover 60 000 y 70 000 millones de dólares anualmente (Diario El Comercio) .

Uno de los países que encabeza la lista competitiva de comercio electrónico es Brasil seguido por Argentina, según investigaciones anteriores ¨Brasil no solo lidera la región en cuanto a la generación de productos y servicios, sino que ocupa el 59% de las operaciones de comercio electrónico de toda América Latina¨ (Pueyrredon, 2015, pág. 19)

Los estándares de seguridad y confidencialidad de la información son un factor fundamental que se debe tener en cuenta al momento de crear páginas web que se dediquen al e-commerce, porque al obtener la seguridad de los datos que se manejan en las diferentes formas de pago es una manera de generar confianza en los usuarios que decidan obtener productos y servicios por internet sin necesidad de ir hasta el establecimiento o lugar donde se encuentre el producto. Para generar ingresos económicos utilizando el e-commerce es necesario obtener la confianza de los clientes, de lo contrario no habrán movimientos para adquirir productos y es por esto que se deben tener estándares de seguridad y confidencialidad de la información óptimos para proteger la información en las diferentes formas de pago.

Planteamiento del problema

La comercialización tanto de empresas o de cliente-empresa tienen riesgos a la hora de efectuar la adquisición de un producto ya que, así como evoluciona la tecnología también evoluciona el riesgo en seguridad de transferencia de información, la seguridad es fundamental a la hora de utilizar herramientas web para el uso del e-commerce y es prevenir riesgos como el acceso no autorizado a información personal de los clientes y el uso no autorizado de esa información.

En la actualidad existen diversos tipos de protocolos y estándares de seguridad para la protección de la información que se maneja al utilizar herramientas para el comercio electrónico, y de esta forma se pueda realizar transacciones entre los interesados del producto en el que fluye información confidencial. Para evitar riesgos de pérdida de información o fraude en las transacciones, existe un protocolo de nombre SET (SECURE ELECTRONIC TRANSACTIONS), este protocolo aplica estándares de seguridad y confidencialidad en la autentificación de diversos tipos de pagos y/o transferencias bancarias. (Garcia y Rodriguez, 2015)

El mercado mundial del comercio se ha caracterizado por el constante intercambio y venta de productos o por un marcado incremento en la demanda de los mismos. En estos tiempos se pueden observar cientos de herramientas para el e-commerce, pero por el contrario, es difícil encontrar una herramienta que tenga la seguridad necesaria para poder utilizarla sin temor a fraude o intenciones maliciosas, el comercio

electrónico ha colocado al sector al borde de la saturación ya que a cada momento se crean nuevas empresas con el fin de globalizarse con la ayuda del internet.

La seguridad es un tema primoridial y el objetivo de esta se centra en que los clientes confien en dar su informacion utilizando el internet.

En el Ecuador el tema del comercio electrónico no ha tenido mucha acogida por diversos factores como la falta de conocimiento sobre el tema, la inseguridad al realizar la transacción y el temor al mal uso de la información personal.

Justificación

El aumento considerable de tecnología en la actualidad ha permitido la evolución de las formas para comprar productos, tanto, que existen diversas herramientas web para soportar tales cambios en el comercio electrónico. Esto lleva a enfocarse en la obtención de productos a un nivel más globalizado como es el uso del internet, estos cambios darán un impacto mayor en la comercialización entre empresas o como también entre clientes y empresas.

La seguridad de las transacciones se consigue a través de mecanismos que favorecen la confidencialidad de las comunicaciones o la autenticación de los intervinientes. Para ello, los extremos de la comunicación tienen que estar dotados de los mecanismos técnicos que posibiliten el uso de la criptografía y de los certificados. (Gómez, 2014)

El comercio a gran escala no tendría un impacto favorable en su crecimiento como tal sin la ayuda de la tecnología o el internet en todas sus funciones. El uso del internet en el comercio es el eje principal de esta sociedad para el intercambio de información y comunicación, por el cual, el estar presente a la hora de obtener un producto o pagar por ello ha quedado un poco en lo que se podría llamar antigüedad.

El comercio electrónico ha impactado significativamente en el área empresarial y en el desarrollo normal del comercio, ya que los clientes se han visto pueden experimentar los beneficios de las amplias alternativas que ofrece este tipo de comercio para la compra y venta de productos y servicios de una manera más accesible. Además ha impulsado la competitividad de las empresas y por ende el

crecimiento del mercado puesto que las pequeñas empresas pueden acceder a una opción diferente para la comercialización de sus productos disminuyendo de esta manera os costes de publicidad y transporte (Murillo, R, 2009).

Es importante que las empresas que quieran actualizar sus métodos de ventas y utilizar aplicaciones web para expandir su alcance y maximizar ganancias se enfoquen en realizar un análisis de cómo asegurar la experiencia de sus clientes en cuando a la compra por internet.

El propósito de esta investigación se basa en la desconfianza de los usuarios que utilizan el comercio electrónico a la hora de realizar compras por internet, de esta manera se pretende cumplir los objetivos planteados para beneficiar al sector del comercio electrónico y brindar a los usuarios mayor conocimiento sobre los estándares de seguridad utilizados en los sitios web presentados como tiendas virtuales, además de ayudar a reforzar la seguridad de dichos mecanismos.

OBJETIVOS

Objetivo General

Determinar los estándares de seguridad y confidencialidad de la información que se aplica en las herramientas web del e-commerce.

Objetivos Específicos

- Describir las herramientas web más utilizadas en la creación de tiendas virtuales aplicables al e-commerce.
- Establecer los estándares de seguridad y confidencialidad que aplican las herramientas web.
- Analizar los protocolos de seguridad que se utilizan en las tiendas virtuales del e-commerce a nivel local.

CAPÍTULO I: MARCO TEÓRICO

1.1. Bases teóricas científicas

1.1.1. Estándares de Seguridad y Confidencialidad

Norma ISO 27001

Es una normativa Estándar de control y seguridad en el comercio electrónico, "contiene los requisitos del sistema de gestión de seguridad de la información. Tiene origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones." Presenta los objetivos de control a los que deben someterse las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles las organizaciones deben argumentar sólidamente la no aplicabilidad de los controles no implementados (www.iso27000.es)

La norma ISO 27000 es certificable. Es decir que las empresas pueden solicitar una auditoria a una entidad certificadora acreditada y de ser aprobada obtener la certificación, previo a la solicitud de la auditoría las empresas deben contar con un Sistema de Gestión de Seguridad de la Información (SGSI) (Ladino, Villa & López 2011).

Norma PCI-DSS (Payment Card Industry Data Security Standard)

Es una norma que deben cumplir todas las entidades que almacenan, procesan o tramitan información de tarjetas de crédito y débito; en Latinoamérica sólo hay 5 empresas certificadoras. La norma PA-DSS es aquella que debe ser cumplida por las compañías o casas de software que desarrollan aplicaciones que manejan información de cuentas y están involucradas en procesos de autorización y conciliación; únicamente hay dos empresas certificadoras para Latinoamérica en ésta norma. El PCI Security Standard Council fue fundado por Visa Internacional, MasterCard Worldwide, American Express, JCB, Discover Financial Services.

Generalmente estos protocolos en e-commerce se aplican principalmente en el login y checkout, asegurando las comunicación (Yaesta.com, 2017).

En e-commerce las diferentes entidades financieras utilizan pasarelas de pago que cumplen con las normas PCI, en el país las más utilizadas son Alignet y Payclub, que no son las más óptimas para utilizar por su bajo nivel de confiabilidad, pero debido a la falta de oferta, y a la necesidad de aceptar tarjetas de crédito para mejorar la conversión, se las debe implementar, cabe destacar que, actualmente hay start-ups que están ingresando en este sector, teniendo como ejemplo a Kushki, el cual a diferencia de las pasarelas anteriores, tiene la capacidad de emular el comportamiento del manejo de tarjetas que utiliza Amazon, es decir, permite almacenar las diferentes tarjetas del cliente, acelerando el proceso de pago, ya que no es necesario volver a ingresar los datos de pago (Yaesta.com, 2017).

A continuación se detalla otros estándares de seguridad:

Estándar	Acciones que realiza
SET (Secure Electronic Transaction)	Estandariza las transacciones seguras con tarjetas de créditos a través de internet
S/MIME (Secure MIME)	Garantiza la transacción seguro, almacenaje, autenticación y transmisión de información secreta en la capa de aplicaciones
SSL & TLS (Secure Sockets Layer & Transport)	Habilitan un "canal seguro" entre dos aplicaciones para la transmisión segura de datos y la autentificación segura mutua.
Sistema de Gestión de Seguridad de la Información (SGSI)	Basándose en la Norma UNE-ISO/IEC 27001, es parte del sistema de gestión general establecido para crear

	implementar y mejorar la seguridad de la información. Tomando el control sobre lo que sucede en los sistemas de información y sobre la información que maneja en organización. El SGSI incluye la organización, políticas, planificación, responsabilidades, prácticas, procedimientos, procesos y recursos para dar soporte a las tareas que realiza (Fernández, L. G., & Álvarez, A. A., 2012).

Tabla 1. Estándares de seguridad

1.1.2. Protocolos de Seguridad.

La palabra protocolo hace referencia al conjunto de reglas que deben seguirse para lograr un fin determinado. Con el fin de obtener vías seguras para el intercambio de información sobre redes abiertas se han establecido diferentes protocolos de seguridad:

Protocolo	Acciones que realiza
CDPC (Cellular Digital Packet Data)	Este es un protocolo estándar diseñado que permite a los clientes el envío de datos de computadora sobre las existentes redes celulares.
DNSSEC (Domain Name System Security Extensions)	Es un protocolo para la distribución segura de servicios de nombres como Hostname y Direcciones IP.
DOCSIS (Data Over Cable Service Interface Specification)	Estandariza el cable modem para la transmisión segura de datos con protección hacia la negación y robo de servicios, así como la protección de la

	privacidad de los clientes.
IEEE 802.11	Es un protocolo estándar para la seguridad de redes de área local del tipo inalámbricas
IPSec (IP Security Protocolo)	Es un protocolo para los servicios de autenticación basada en servicios de: criptografía, integridad y confidencialidad en la capa de datagramas de IP.
PPTP (Point-to-Point Tunneling Protocol)	Este protocolo es usado para crear comunicaciones entres redes virtuales privadas a través de internet bajo la tecnología de protocolos en "conductos"; trabaja en la capa de datagramas de IP.
SSH (Secure Shell)	Este protocolo permite accesos remotos seguros de computadora a computadora a través de una red.

Tabla 2. Protocolos de seguridad

Fuente: (García & Rodriguez)

Estudios realizados en la empresa YaEsta.com sobre el E- commerce, uno de los aspectos más relevantes es la seguridad, lo cual evita comprometer los datos de los clientes. Se deben implementar ciertas normativas que aseguren los datos que se manejan a través de la plataforma de e-commerce, entre los cuales destacan:

El protocolo HTTPS, el cual cifra los datos entre el cliente y el servidor, utiliza un cifrado basado en SSL/TLS, apropiado para el tráfico de información crítica, a diferencia del protocolo HTTP, consigue que la información sensible permanezca segura (Yaesta.com, 2017).

1.1.3. Sistemas de encriptación

El proceso de codificación o encriptación consiste en transformar la información expresada en un lenguaje a otro con reglas distintas, dicha información no puede ser interpretada sin ser debidamente desencriptada por quien conoce el correcto manejo de sistema, el proceso descrito se lleva a cabo mediante a algoritmos de encriptación (Sastre, 2009).

Encriptación simétrica: Se lleva a cabo mediante a un algoritmo de codificación con una clave única de cifrado, el tamaño de esta clave se cuenta en bits. De esta manera el mensaje codificado solo puede ser decodificado por quien conozca la clave (López, Mata, & Domínguez, 2009); (Chou, 2002)

GRÁFICO 3: CRIPTOGRAFÍA DE CLAVE SIMÉTRICA

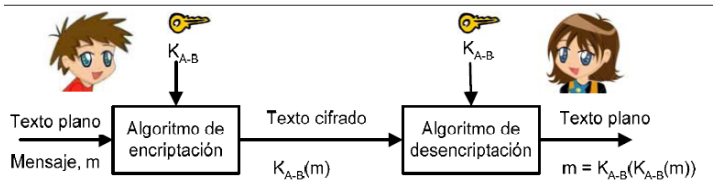


Fig. 1. Criptografía de clave simétrica

Fuente: (López, Mata, & Domínguez,

Encriptación asimétrica: Este método de encriptación consiste en dos claves complementarias, una pública y otra privada. Las dos partes de la comunicación poseen sus propias claves, la clave pública es de conocimiento de ambos usuarios, mientras la privada es de conocimiento exclusivo del propietario, de esta manera de hace visible la clave pública solo a los usuarios con quienes se desee establecer una transferencia de datos de forma segura (López, Mata, & Domínguez, 2009); (Chou, 2002).

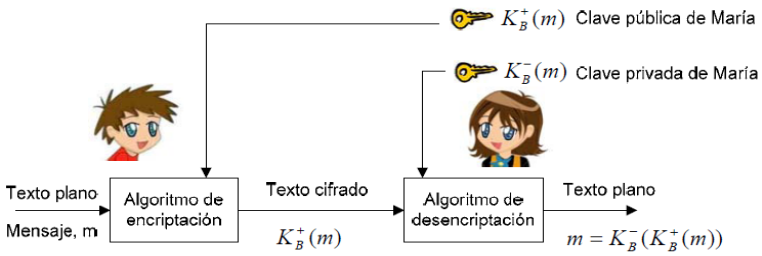


Fig. 2. Criptografía de clave asimétrica

Fuente: (López, Mata, & Domínguez, 2009)

Sistema de protección de datos CRM: Consiste en un sistema de registro de datos, manejo de información y monitoreo de comportamiento de los usuarios para uso interno de la empresa, de esta manera no solo se puede llevar un registro de los clientes que acceden a la plataforma, sino también se pueden generar estadísticas sobre los intereses futuros de los usuarios y clasificar a los mismos en grupos por los intereses manifestados en sus anteriores interacciones virtuales (Martínez, J. 2007)

1.1.4. Web

Un entorno web es aquel en el que el usuario intercambia información haciendo uso del internet mediante un protocolo de transporte, mediante la web se puede compartir diversa información, por ejemplo: Imágenes, sonidos, archivos, aplicaciones entre otros. El protocolo más utilizado es el protocolo HTTP (Hypertext Transfer Protocol) y la forma para referenciar los contenidos es mediante una URL, que en ingles se denomina Universal Resource Locator (Balsas, Ruiz, y Rivas, s.f)

El Hypertext Transfer Protocol más comúnmente llamado HTTP utiliza el concepto de referencia proporcionado por el identificador de recurso universal (URI) como una ubicación (URL) o nombre (URN), para indicar el recurso en el que se va a aplicar un método. Cuando se compone un hipervínculo HTML, la URL (Uniform Resource Locator) es de la forma general http: // host: número de puerto / ruta / archivo.html. Más generalmente, una referencia de URL es del tipo servicio: //host/archivo.extension y de esta manera, el protocolo HTTP puede subsumir los servicios de Internet más básicos (Gauchat, 2017)

Para que un entorno web funcione se necesitan varios elementos uno de ellos es el servidor web.

> ¨Un servidor web será aquel que recoja y procese la petición del cliente, bien devolviendo información, bien llevando a cabo algún proceso. Existe infinidad de software distinto para procesar las distintas peticiones.¨ (Hidalgo, 2014).

El servidor web está a la espera de las peticiones que realice el cliente y se ejecutan en un computador.

Se puede definir al cliente como un navegador o una aplicación que consuma el servicio, para lograr la interacción entre el cliente y el servidor se necesita llegar a una conexión la cual se basa en diversos tipos de protocolos.

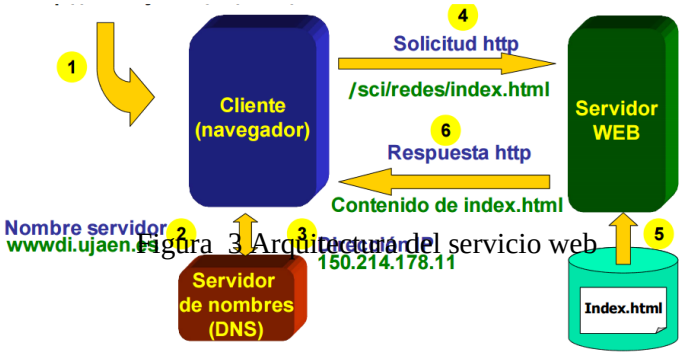


Figura 3 Arquitectura del servicio web

Fuente: (Balsas, Ruiz, & Rivas, s.f)

1.1.5. Herramientas Web de diseño involucradas en el comercio electrónico.

La Web se ha convertido en la principal herramienta del comercio electrónico en los últimos diez años y requiere que las empresas de Internet proporcionen servicios personalizados mediante el seguimiento y el análisis de los patrones de visita de los usuarios.

Según (Thushara & Ramesh, 2016) una de las técnicas orientadas a ayudar al e-commerce es La minería web, este investigador afirma que: “La minería de Web es el término de aplicar técnicas de minería de datos para descubrir y extraer automáticamente información útil de los documentos y servicios de World Wide Web”. Aunque la minería de la Web pone las raíces profundamente en la minería de datos, no es equivalente a la minería de datos. La característica no estructurada de los datos Web desencadena una mayor complejidad de la minería Web. La investigación de la minería de la tela es realmente un área convergente de varias comunidades de la investigación, tales como base de datos, recuperación de la información, inteligencia artificial, y también psicología y estadística también. La minería de la tela implica el análisis de los registros del servidor de Web de un Web site.

Perteneciente a las primeras generaciones del internet, DobleClick ofrece el software como un servicio, presenta una competencia básica de gestión de datos y se ha presentado como un pionero en web services. Utilizados a nivel publicitario mediante a la incentivación de sitios web individualmente (Santiago & Navaridas, 2012).

A diferencia de DoubleClick, ¡Yahoo! Search Marketing y Google AdSense se caracterizan por brindar servicios a miles de publicistas, la clave de su éxito se basa en el poder colectivo de los sitios web pequeños que forman gran parte del contenido de la web y en la accesibilidad de publicidad prácticamente en cualquier página web (Santiago & Navaridas, 2012).

Otra herramienta muy común es Adobe Ilustrador CS6, que corresponde a un editor de gráficos vectoriales que contiene las herramientas necesarias para la creación artística. Esta herramienta creada por Adobe permite crear ilustraciones para cualquier formato y es utilizada para el diseño inicial de las aplicaciones web 3D (Borja & Silvana, 2016).

Dentro de las herramientas de diseño es muy común encontrar también Blender, que es un software libre multiplataforma que proporciona herramientas para modelado, animación y creación de gráficos tridimensionales. Permite modelar objetos 3D además de importar múltiples formatos (Borja & Silvana, 2016). Y Python HTTP server; es un servidor web http basado en el lenguaje de programación Python. Permite el uso diseño de tiendas virtuales y su manejo usando las herramientas de este lenguaje de programación (Borja & Silvana, 2016).

WebGL es una multiplataforma utilizada para crear gráficos 3D en un navegador (Borja & Silvana, 2016).

1.1.6. Componentes de programación web utilizados en el e-commerce

Entre los componentes de programación más utilizados en el e-commerce destacan algunos que hemos podido observar en las páginas web estudiadas. Uno de ellos es la última versión de HTML con nuevos elementos, atributos y comportamientos.

Unifica las tecnologías involucradas en el desarrollo web. De esta manera se obtiene la participación de HTML, CSS y Java Script, integrándolos y cambiando el desarrollo web totalmente (Gauchat, 2017).

También podemos encontrar el CSS3, que al ser la última evolución del lenguaje de las Hojas de Estilo en Cascada (Cascading Style Sheets) pretende ampliar la versión CSS2.1. Permitiendo la integración de cambios como: esquinas redondeadas, sombras, gradientes, transformaciones 2D y 3D. Además se presenta como un lenguaje flexible que implica mejora progresiva y degradación elegante. (Beati, 2016).

Otro lenguaje y herramienta básica de programación es el PHP, que presenta un lenguaje de código abierto adecuado para el desarrollo web y que puede ser incrustado en HTML. Se distingue por su código que es ejecutado en el servidor, generando HTML y enviándolo al cliente. El servidor web puede ser configurado incluso para que procese todos los ficheros HTML con PHP. (Heurtel, 2015).

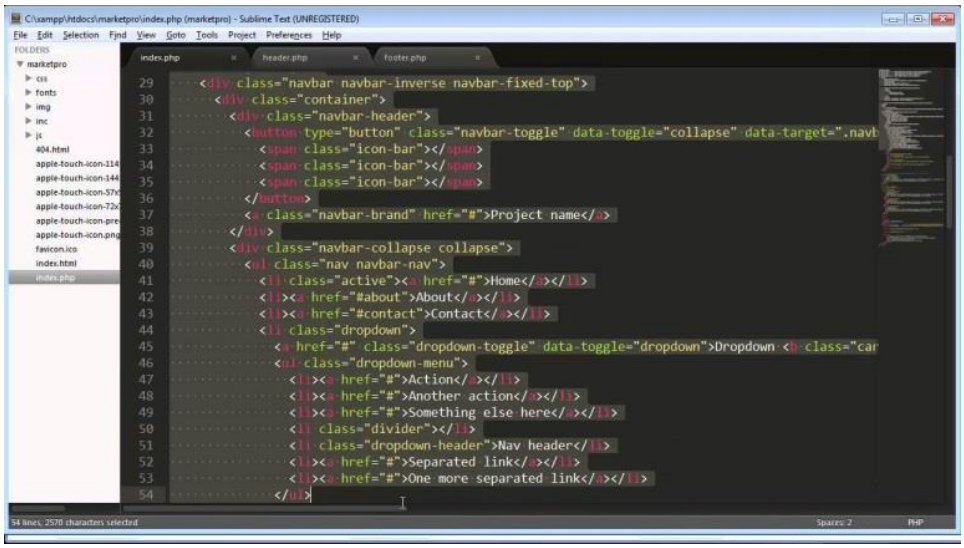


Figura 4. Codifiación tienda Online con PHP, MySQL HTML5 CSS3

Fuente: (Pixelpro Cursos, 2014)

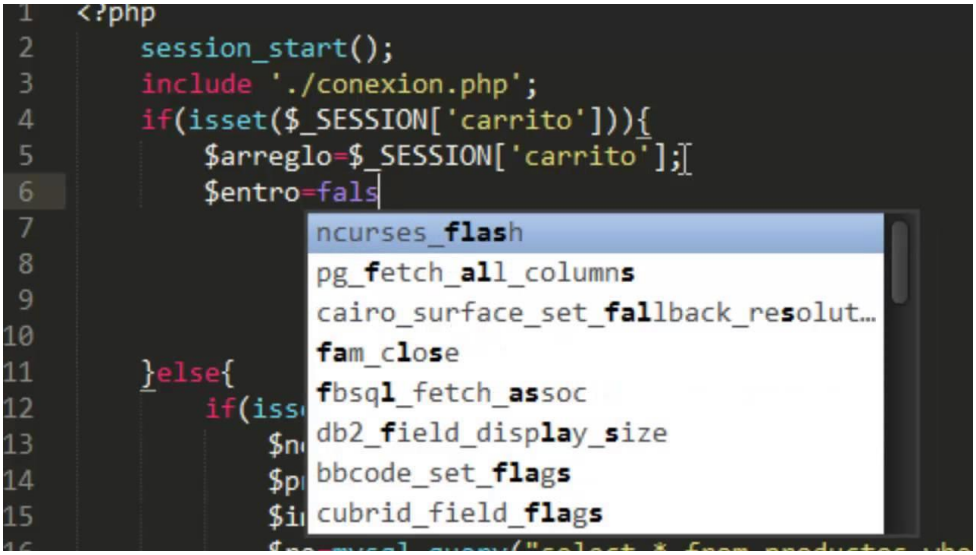


Figura 5. Codifiación Carrito de Compras con PHP, MySQL HTML5 CSS3

Fuente: (Pixelpro Cursos, 2014)

Conocido por las siglas RWD del inglés Responsive Web Design, tiene como objetivo adaptar la apariencia de las páginas web al dispositivo que se esté utilizando para visualizarla. Esta tecnología pretende que con un solo diseño web se tenga una visualización adecuada en cualquier dispositivo (Rodríguez, Blanco, Adán & Pérez, 2016). Y finalente encontramos Bootstrap; este framework front-end desarrollado y liberado por twitter, permite agilizar el desarrollo de los diseño web, además de utilizar una completa colección de elementos como plugins de javascript opcional. Es compatible con la mayoría de los navegadores modernos web y móviles (Rodríguez, Blanco, Adán & Pérez, 2016).

1.1.7. E-Commerce

El comercio electrónico o e-commerce consiste en el uso de las tecnologías de la informática y comunicación (TIC) a favor del comercio, valiéndose del desarrollo tecnológico para facilitar en mayor medida los procesos llevados a cabo en las transacciones básicas de esta importante rama económica (Bernal Jurado & Rodríguez Cohard, 2003).

De esta manera el e-commerce ha logrado simplificar las operaciones de compra y venta de bienes y servicios a nivel mundial mediante a las tiendas virtuales, acercando a los usuarios de manera rápida y efectiva a los objetivos comerciales planteados (Lara-Navarra & Martínez-Usero, 2002).

Además el e-commerce es un procedimiento renovado que se basa en elevar la satisfacción del usuario, promoviendo estrategias eficientes, como asignar promociones en los productos, reducir tiempo de ciclo, mejorar la calidad y el valor percibido por los clientes cumpliendo cada uno de sus requisitos (Hernández, 2012).

El comercio electrónico engloba tres tipos: el comercio entre empresas (Business to Business, B2B); el comercio empresa - consumidor (Business to Consumer, B2C) y el comercio en el que interviene la Administración, englobando las transacciones entre empresas y/o particulares con la Administración (Business to Administration, B2A) (Sellers Rubio & Azorín Escolano, 2001).

Según la Diputación Provincial de Sevilla, su sociedad Sevilla Siglo XXI S.A, y la Federación Andaluza de Municipios y Provincias (FAMP), el comercio electrónico se puede definir, en un sentido amplio, como cualquier forma de transacción o intercambio de información comercial y de productos o servicios basada en la transmisión de datos sobre redes y sistemas que permiten hacer negocio todos los días del año, las 24 horas del día, con total seguridad y privacidad y, sin la presencia física de las partes y, que se está consolidando en muchos sectores económicos.

En este sentido, el concepto de comercio electrónico no sólo incluye la compra y venta electrónica de bienes, información o servicios abarcando también el uso de la red para actividades pre o post venta.

1.1.8. Tiendas Virtuales

Todas las personas que deseen realizar la actividad del comercio por internet necesitan tener claro el concepto de tienda virtual según Headways Media, 2016, una tienda virtual es:

Una tienda virtual es una página web o aplicación en donde se ofertan una variedad de artículos, en un sentido general se puede decir que una tienda online es muy

similar a una tienda física convencional puesto que se cumple la misma función, transacciones comerciales o intercambio económico donde se oferta un bien o servicio por lo que se considere es su valor, pero en este caso todo se realiza mediante el internet y por lo general el cliente comprador utiliza tarjetas de crédito, no obstante, se pueden utilizar otros medios de pago como transferencias bancarias o algunas veces PayPal, etc. Una gran mayoría de los sitios de ventas online requieren que sus usuarios se registren.

De forma general una tienda virtual es un espacio digital o sitio diseñado para vender algún tipo de producto o brindar un servicio a cambio de objetos que representen beneficios económicos para el dueño del espacio (Hoyos, Castro & de Plata, 2015).

Las tiendas virtuales forman parte esencial del comercio electrónico porque estas sirven de base o medio de contacto entre el usuario y el vendedor y estas han tomado cada vez más importancia en los últimos años. Empresas como EBay, MercadoLibre y Amazon han logrado la fidelidad de miles de personas a nivel mundial y el movimiento de millones de dólares, la principal ventaja de este tipo de tienda es que la inversión es muy baja si se compara con una tienda convencional o física. (Avila, 2013)

Lógicamente las tiendas virtuales potencian la idea principal de las tiendas normales que es tener un lugar en donde realizar la transacción, a más de eso en una tienda virtual se tiene más ventajas competitivas, como los hechos de llegar a todo el mundo, poder mostrar la cantidad de productos que se desee, menor coste en publicidad y lo mejor de todo una tienda abierta todo el día, 24 horas, todos los días a la semana, sin pagarle a personal administrativo.

Amazon

Amazon fue creada en Estados Unidos, en la ciudad de Seattle, en el estado de Washington. Empresa pionera en ventas a través del internet, en sus inicios se limitaba a la venta de libros (Club Planeta, s.f)

La logística de Amazon ayuda a aumentar el volumen de las ventas internacionalmente porque facilita envíos, servicio al cliente, y la garantía de ser una tienda reconocida a nivel mundial (Amazon, 2017)

Fue una de las principales compañías en vender bienes en línea a escala mundial. Tras iniciar como una librería en línea, logró expandirse en el medio del e-commerce vendiendo todo tipo de bienes y productos, además de ser identificada como una potencia mundial en el medio del comercio electrónico (Collins Patrick, 2001).



Figura 6. Logo de Amazon.

Fuente: (Amazon, 2017)

EBay

EBay es una corporación multinacional de comercio electrónico que facilita las ventas en línea de consumidor a consumidor y de empresa a consumidor. Tiene su sede en San José, California. EBay fue fundada por Pierre Omidyar en 1995, y se convirtió en una notable historia de éxito de la burbuja de puntocom. Hoy es un negocio multimillonario con operaciones en unos 30 países (Ebay, s.f.)



Figura 7. Logo de EBay.

Fuente: (Ebay, s.f.)

MercadoLibre

Mercado libre es una plataforma para realizar intercambios económicos creados en argentina, mercado libre se dedica al comercio entre los usuarios inscritos y otros usuarios.

MercadoLibre más que como una tienda virtual se presenta como una plataforma de negocios en la que convergen vendedores y compradores para intercambio de bienes y servicios (Arias & Castillo, 2011).

El protocolo de seguridad utilizado por esta popular plataforma consiste en la aplicación de un Digital ID y Secure Server ID que permite proteger datos confidenciales. Además de mostrar la información sobre certificados digitales, logos y textos descriptivos del producto comercializado (Bezos, J., 2015).



Figura 8. Logo de Mercado Libre

Fuente: (Mercado Libre, s.f.)

YaEsta.com

Alejandro Freund y Martin son los creadores de la empresa Yaesta.com tras un año de larga lucha pusieron el concepto de una empresa dedicada cien por ciento a la venta de productos por medio del internet en marcha. A la fecha la empresa ya cuenta con un stock bastante variado con más de 100 proveedores y alrededor de 1500 productos disponibles para la compra (Diario El Universo, 2015)

Esta plataforma de compra virtual nace tras la idea de acercar al país al desarrollo tecnológico mundial. Tuvo su inicio con 21 productos y 4 proveedores, posicionándose como la primera tienda virtual de origen nacional, con el paso del

tiempo ha incrementado su oferta a diversos departamentos brindando acceso a productos nacionales e impulsando la industria local (El Universo, 2015)

Uno de los grandes beneficios que destaca a esta alternativa del e-commerce es que garantiza tanto la recepción como la calidad del producto, haciéndose cargo directamente en caso de reclamos y no siendo solo intermediario de la compra (Tutivén & Anahí, 2017)



Figura 9. Logo de Yaestá.com

Fuente: (Yaesta.com, 2017)

1.1.9. Formas de Pago

Un sistema de pago electrónico facilita la aceptación del cliente ofreciendo nuevos canales de distribución: transferencias bancarias, tarjetas de crédito, cheques. Mientras se amplíe las posibilidades y se logre disminuir los procedimientos para cumplir los pagos, mayor será la aprobación. El compromiso es aumentar la seguridad e inspirar confianza.

Existe una diversidad de niveles de seguridad y de procedimientos de compra que debe utilizar según la tienda virtual que desee. El sistema de pago escogido será clave para que la clientela potencial compre por Internet, en este sentido, las entidades financieras, están invirtiendo cantidades millonarias en generar protocolos seguros y sistemas para enlazar una aplicación integral de comercio electrónico on-line como las pasarelas de pagos de VISA, MasterCard.

Tarjetas de Crédito.

Una tarjeta de crédito suele ser un instrumento emitido por un banco, que cuenta con un respaldo monetario y permite realizar ciertas operaciones, como por ejemplo la compra de un bien o el pago de un servicio. Una tarjeta de crédito es uno de los medios de pago más habituales entre los usuarios de internet para realizar compras, por lo general esta siempre es una opción en la mayoría de los sitios web. La tarjeta de crédito suele ser considerada como un servicio seguro para realizar pagos en Internet ya que con este objeto se protege la información de los usuarios, la página o aplicación web y el banco porque ofrecen mecanismos de autentificación de quien realizara la compra (Ramírez & Ramos, 2008).

Cartera Digital.

La cartera digital al igual que la tradicional guarda los datos de la tarjeta e información del propietario y envía esos datos automáticamente a la hora de la compra. Uno de los sitios que utiliza este medio es Amazon. (Ramírez & Ramos, 2008).

Cheques y órdenes de pago electrónicas.

En el caso del comercio entre empresas el pago mediante tarjeta de crédito es mucho menos usual, por lo que un sistema como SET parece claramente menos adecuado que en el escenario anterior. Entre empresas, en particular Pymes, es frecuente el pago mediante cheques. Los sistemas de pago basados en cheques electrónicos pueden reducir considerablemente el coste de procesar los cheques y minimizar el fraude.

Este sistema utiliza una tarjeta codificada, tipo tarjeta de crédito, que hace las veces de talonario electrónico.

Dinero y Monederos Electrónicos

El Sistema de Dinero Electrónico consiste en un conjunto de operaciones, mecanismos y normativas para facilitar el flujo, almacenamiento y transferencia de

dinero entre agentes económicos mediante a dispositivos electrónicos (Valencia, 2015).

De esta manera se utiliza un equivalente al valor monetario de la moneda de curso legal en el país para ser expresado mediante a este sistema a través de dispositivos electrónicos móviles, este tipo de moneda virtual, es reconocido por todos los agentes económicos del país con poder de libre circulación (Moncayo & Reis, 2016).

Los sistemas anteriores sirven para realizar transacciones electrónicas (cargo en una tarjeta de crédito, orden de pago a una cuenta corriente, etc.) sobre dinero no electrónico.

Existe otro grupo de sistemas en los que se maneja directamente dinero electrónico, por ejemplo almacenado en una tarjeta inteligente (con un chip incorporado) que hace de monedero electrónico.

1.1.10. Ataques y Seguridad en el E-Commerce

El aspecto de seguridad se vuelve muy importante y delicado, sobre todo al involucrar información referente a movimientos económicos e información confidencial. La seguridad es una de las mayores trabas que enfrenta el E-commerce, ya que aunque se mejora cada día las tecnologías de seguridad informática se observa un continuo crecimiento de amenazas para este sector de la mano con el avance tecnológico (Don, 2016).

Fraudes y amenazas.

Con la expansión de la tecnología en el entorno empresarial se dio un alto incremento en los delitos de carácter económico llevados a cabo mediante a fraude informático (López, Antonio & Rodríguez, 2017).

La generalización del internet en los años noventa incluyó el término delitos informáticos como cualquier conducta que terminen en daños económicos a través de falsificación de información por medio de un ordenador.

Los fraudes informáticos corresponden a engaños, manipulación de programas malignos o uso de datos falsos para dañar, perjudicar u obtener información confidencial de usuarios en la red (Gómez & Espinoza, 2015).

Los datos falsos son alteraciones de la información que se procesa en la red, son utilizados para generar transacciones falsas que permiten acceder a la información otorgada simulando procesos reales, es uno de los tipos de fraude más utilizados a nivel informático por su fácil manejo (Acurio Del Pino, 2006).

Entre los programas malignos presentes en los delitos informáticos que actúan sobre el área de transacciones económicas también se encuentran los "Caballos de Troya" que son ejecutados por criminales con conocimiento informático, pues consisten en la invasión del código principal de una aplicación o programa para introducir y modificar líneas de código que ejecutan funciones no autorizadas de manera incógnita a la par de funciones normales reconocidas por el usuario (Azevedo, 2016).

Basándose en los Caballos de Troya se conocen técnicas variadas presentes en el fraude informático, una de ellas es conocida como la técnica del salami, que consiste en tomar valores muy pequeños de las transacciones financieras realizadas y transferirlos a cuentas diferentes al destino principal, de esta manera se pueden robar grandes cantidades sin ser notoria la falta de las mismas de manera inmediata (Rosello, 2014).

Mediante al robo de información, que consiste en el hecho de que una persona se apodere de la identidad de otra utilizando las computadoras para acceder por ejemplo a los usuarios y contraseñas de sus cuentas, se pueden llevar a cabo diversos falsificaciones informáticas, un tipo de fraude que viola la seguridad de los documentos guardados en digital dentro del ordenador, con el equipo informático también pueden realizarse falsificaciones como cambios en la información de los documentos o incluso generar nuevos documentos a partir de otros reales a tal nivel que solo un experto podría identificar (Rodríguez, 2014).

Otra técnica muy común es el Pishing, que basándose en ingeniería social permite obtener datos confidenciales captando información bancaria de un usuario electrónico a través de la imagen de una entidad financiera que los usuarios comúnmente consideran sitios seguros (Seguridadpc.net, 2012).

Según (OVH Innovation is Freedom, 2017) “El objetivo de un ataque DDoS es inhabilitar un servidor, un servicio o una infraestructura sobrecargando el ancho de banda del servidor o acaparando sus recursos hasta agotarlos” (p. 3). En el ataque DDoS múltiples puntos de red envían peticiones al mismo tiempo para desestabilizar el servicio o, para inhabilitarlo.

1.2. Antecedentes

Según el trabajo realizado por (Martínez López, Mata Mata, & Rodríguez Domínguez, 2009) el comercio electrónico se expandió a finales de los 90 convirtiéndose en una forma popular a la hora de realizar alguna transacción económica, transformándose en un elemento prometedor con visión al futuro, pero en la actualidad esta visión de cambio en la mentalidad de la sociedad consumidora no se ha logrado a cabalidad, gracias a la falta de herramientas que aseguren una compra segura por medio del internet. Gracias al avance de las tecnologías y sistemas de pagos electrónicos, la seguridad integral se ha mejorado dando un poco más de fiabilidad a los usuarios pero de todas formas la seguridad sigue siendo un tema importante que no permite maximizar el alcance del comercio electrónico.

En la investigación “Solución integral de seguridad para las pymes mediante un UTM” se tiene como finalidad brindar un enfoque teórico que sirva como base para la implementación de una mejora a la seguridad informática modular para de esta manera integrar las funcionalidades requeridas más comunes, como son los firewall, antivirus y control de contenido o UTM por sus siglas en inglés Unified Threat Management que se traduce como Gestor Unificado de Amenazas.

Para Gómez & Espinoza (2015) las seguridad en la red y los datos almacenados se ven seriamente comprometidos con el desarrollo de la tecnología, por ende la finalidad de su investigación es desarrollar técnicas que apoyándose en los protocolos y estándares de seguridad permitan tanto prevenir como protegerse de los delitos informáticos.

Este proyecto de investigación tiene como finalidad disminuir los ataques de seguridad por ordenador a los que se enfrentan las Pymes y que están más comúnmente relacionados a un escaso control de malware y poca protección

mediante firewall, los autores de esta investigación vieron como herramienta para neutralizar estos ataques la implementación de un UTM (Flórez Wilmar, 2012)

En la investigación Sistemas de Pagos seguros se hace una revisión a los tres protocolos de pagos más utilizados que son el SSL, el SET y el 3D Secure con la finalidad de que el usuario despeje sus dudas y el usuario desarrolle más confianza al realizar compras usando el internet (Martínez López, Mata Mata, y Rodríguez Domínguez, 2009, págs. 63-76)

Según los autores, Gutiérrez, Fernández-Medina y Piattini en la investigación "Seguridad En Servicios Web" afirma que las primeras medidas a tomar cuenta para el intercambio de mensajes SOAP mediante HTTP es el uso de SSL/TLS. Estos protocolos sirven para garantizar la integridad de los mensajes entre un punto y el otro pero por sí solo no son suficientes IBM expresa, "cuando los datos son recibidos y reenviados por un intermediario por encima de la capa de transporte, tanto la integridad de los datos como cualquier otro tipo de información que contenga, podría perderse. Esto fuerza a que cualquier procesador de mensajes posterior confíe en las evaluaciones de seguridad hechas por los intermediarios previos y, a que tenga confianza plena en la forma en que éstos últimos hayan manipulado el contenido de los mensajes"(IBM & Microsoft, 2002a).

Como se puede observarse en el trabajo de Gutiérrez, Fernández Medina y Piattini, XML Digital Signature es una recomendación W3C ya que determina como proceder con el tema de las firmas digitales.

Las firmas digitales son un medio para mantener la integridad de la información y sirve como una evidencia de forma legal. Una de las tecnologías para firmas digitales es la tecnología RSA PKCS #7 la cual sirve para firmal digitalmente cualquier documento pero hasta la llegada de la Seguridad en Servicios Web no se podía contar con una representación basada en XML de una firma digital y mucho menos firmar parcialmente un XML, también habían métodos que dan la posibilidad de asociar firmas digitales con otros elementos como es el caso de la especificación (S/MIME), Secure Multipurpose Internet Mail Extensions la cual brinda un mecanismo para unir una firma digital con su respectivo e-mail. De la misma forma con XML Encryption se necesitan herramientas adicionales para estandarizar el

intercambio de información entre servicios web. (Gutierrez, Fernandez, & Piattini, 2005).

1.3. Marco Legal

1.3.1. Bases Legales.

Según el Código Orgánico Integral Penal (COIP) publicado en el Suplemento del Registro Oficial No. 180 de 10 de febrero del 2014 el 10 de agosto del 2014, se establecen varios artículos importantes para el comercio electrónica, entre esos artículos destacan los siguientes:

Art. 49.- Consentimiento para el uso de medios electrónicos

De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,

b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;

2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;

3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,

4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Art. 36.- Organismo de promoción y difusión.

Para efectos de esta Ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

El comercio electrónico también se rige a una ley que establece las formas de interacción económica en la red, de ella se expresan los artículos de mayor relevancia para el tema investigado.

Art. 1.- Objeto de la Ley.-

Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Art. 9.- Protección de datos.-

Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

Art. 20.- Certificado de firma electrónica.-

Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Art. 21.- Uso del certificado de firma electrónica.-

El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento.

Artículo 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.

La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica.

-Será sancionada con pena privativa de libertad de uno a tres años.

-Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

- La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.

La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad.

Artículo 500.- Contenido digital

El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.

Artículo 559.- Uso de dispositivos electrónicos

Para garantizar el cumplimiento efectivo de las medidas señaladas, la o el juzgador Código Orgánico Integral Penal 211 contará con la ayuda de la Policía Nacional y en los casos de los numerales 2 y 3 del artículo anterior, podrá ordenar a la persona procesada el uso de dispositivos electrónicos.

Artículo 190.- Apropiación fraudulenta por medios electrónicos.

La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones.

Artículo 229.- Revelación ilegal de base de datos.

La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas.

Artículo 232.- Ataque a la integridad de sistemas informáticos

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen.

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1. Área de Estudio.

2.1.1. Descripción del lugar

Esta investigación se la realizó mediante el análisis de las tiendas virtuales más utilizadas a nivel mundial, nacional y local; estableciendo los estándares de seguridad y confidencialidad que se aplican en las herramientas web del e-commerce a través de un estudio técnico.

2.1.2. Tipo de investigación

Las ciencias sociales y naturales son las principales ramas de las ciencias y del saber, en términos generales, estas ramas se enfocan en el comportamiento de las personas basándose en la percepción del investigar. Este tipo de investigación entrega resultados descriptivos y es denominada investigación cualitativa (Mayan, 2001) afirma que:

La investigación cualitativa busca analizar datos de las personas, datos que muchas veces son transmitidos como experiencias de la vida, este tipo de investigación es también llamada naturalísima porque se usa para estudiar los fenómenos de la naturaleza. Es por esta razón que quien analiza solo es un observador y no cambia nada en el ambiente que está investigando.

Es notable el uso del tipo de investigación cualitativa en este estudio, ya que la palabra cualidad hace referencia a la descripción de características de un objeto. La investigación cualitativa surge de observaciones y análisis profundos y brinda la oportunidad de interpretar los datos recogidos para basados en eso dar un criterio.

Según la RAE, el termino observar significa, examinar atentamente algo de interés lo cual se ajusta los objetivos del trabajo realizado, los cuales se centraron en extraer los mejores estándares para la seguridad y confidencialidad de la información que se

aplican en las herramientas web del E-commerce a través de un estudio de las tiendas virtuales.

2.2. Recolección de Datos

2.2.1. Población

La población de este estudio se determinó acorde al alcance investigativo y a la disponibilidad global de la información, por tanto, se analizó las tiendas virtuales más utilizadas a nivel mundial, entre las que se destacan; Amazon, EBay, MercadoLibre y las empresas que manejan comercio electrónico a nivel local: Yaesta.com y Tame.

2.3. Métodos y técnicas.

Para entender el razonamiento inductivo se debe primero comprender el razonamiento lógico, el cual usa el entendimiento y raciocinio para pasar de premisas de las que ya se tiene conocimiento a lo desconocido. El razonamiento inductivo es uno de los más comunes a la hora de realizar investigaciones ya que está asociado comúnmente al análisis y la observación de patrones según investigaciones realizadas:

Uno de los atributos de este método es que se basa en la razón para sacar conclusiones, y estos van desde acciones específicas o particulares que son tomadas para llegar a conclusiones generales. Este método empieza desde la observación y análisis de cada parte del fenómeno que se quiera investigar, se compara y experimenta hasta sacar principios, conclusiones o leyes generales (Universidad Nacional Autónoma de México, 2008)

De forma general, se puede indicar que el método inductivo va desde observaciones y medidas específicas, comenzando por la identificación de patrones y se termina con la formulación de las hipótesis tentativas, para poder desarrollar las conclusiones o teorías generales.

En esta investigación se utilizó el método inductivo, el cual se ajusta al tipo de estudio aplicado, a raíz de que este método brindó la posibilidad de analizar la

información recolectada, se lo hizo de lo específico a lo general, puesto que, cada tienda virtual estudiada tiene diferentes características y diferentes formas de proceder a la hora de realizar sus actividades, pero el objetivo en general fue establecer los mejores estándares para la seguridad en la transmisión de datos.

2.4. Descripción del instrumento

Para esta investigación se utilizaron cuestionarios (véase anexo1) y fichas de observación bibliográfica. Se realizó entrevistas a especialistas en la creación de tiendas virtuales en las que se aplican herramientas de e-commerce, entre ellos: la empresa Yaesta.com y Tame.

Se utilizó la aplicación gratuita builtwith.com para conocer la estructura de las páginas web mencionadas a continuación.

2.5. Descripción de las técnicas de procesamiento y análisis

Las técnicas de procesamiento utilizadas en esta investigación se basaron en entrevistas sobre el e-commerce a especialistas con experiencia en la utilización de herramientas web en las cuales se pretende describir los estándares de seguridad y confidencialidad que utilizan las empresas a nivel nacional e internacional.

Además se llevó a cabo un análisis técnico de exploración de biografías de las tiendas virtuales tales como la empresa Yaesta.com con la cual se determinó los componentes web en las tiendas virtuales del e-commerce.

2.6. Normas éticas

La información recolectada en esta investigación tendrá usos de carácter académico y no será usada de forma ilegítima por parte del investigador, también se respetarán las normas de citación contenidos.

CAPÍTULO III: RESULTADOS

3.1. Análisis de dos de las principales tiendas virtuales utilizadas a nivel mundial con builtwith.com e investigación bibliográfica.

Las entrevistas e investigación bibliográfica llevadas a cabo han arrojado luces sobre el manejo, funcionamiento y desarrollo de las principales tiendas virtuales a nivel mundial y local. Es así que se ha podido identificar varios protocolos de seguridad manejados por las tiendas, los estándares bajo los que operan estos organismos del e-commerce y la funcionalidad que pretenden brindar a los usuarios. Incluso ha permitido despejar la gran interrogante acerca de cómo perciben la seguridad informática los usuarios.

A continuación se presenta un análisis individual de dos grandes tiendas virtuales a nivel mundial.

Amazon.com

El crecimiento y desarrollo del e-commerce, el fácil acceso a la información y el incremento tecnológico contribuyen en el aumento de los riesgos operacionales derivados del comercio electrónico. Como ejemplo de cadena de suministro segura y productiva se considera Amazon, ya que su crecimiento, versatilidad y capacidad de expansión ha evidenciado su buen uso de prácticas de seguridad y logística en las transacciones llevadas a cabo (ESTUDIOS, 2015).

Revolucionando su modelo de negocio con una amplia variedad de productos Amazon se ha convertido en la tienda virtual básica a nivel mundial, una de las claves para el desarrollo del e-commerce (Mosquera C., 2016).

Utilizando el Fullifiment Web Services, Amazon.com integra al sistema de logística internacional un portafolio de protección de información como requisito indispensable en la gestión de seguridad empresarial, de esta manera maneja los datos de los clientes; estos estándares de seguridad han permitido a la empresa

patentar controles propios de seguridad y mantener la estabilidad de su cadena de suministro (González, 2015).

Mercado Libre

Aunque en esta plataforma no cuenta con productos propios posee un amplio y variado catálogo en el que los usuarios pueden encontrar opciones para generar transacciones de su interés. Esta plataforma no solo es utilizada por usuarios que desean comprar y vender artículos específicos, sino que a menudo la usan grandes compañías para vender productos en exceso de inventario o liquidaciones (Ruiz, Villegas & Hernández, 2012).

El problema con esta plataforma es que la empresa solo sirve como un portal intermediario en la que los datos que posee son únicamente los ingresados por el vendedor en la página de registro, además de no responsabilizarse por resultados negativos de las transacciones, explicando que "la seguridad en el proceso de compra, específicamente en la devolución de dinero en caso de no quedar satisfecho y el seguimiento de paquetes, depende del medio de pago seleccionado y acordado entre usuarios" (Ruiz, Villegas & Hernández, 2012).

MercadoLibre garantiza en gran medida transacciones seguras mediante la tecnología altamente avanzada basada en autenticación digital; así permite comunicación entre usuarios por canales privados. Los certificados digitales utilizados por esta plataforma generan información encriptada que viaja por la red de forma privada y segura, manejando también el protocolo de comunicación SSL que se encarga de encriptar, protege y certifica los datos que son proporcionados por los usuarios para su protección creando permisos de acceso de los que depende las transacciones a llevarse a cabo (Luna, 2014).

3.2. Análisis de dos de las principales tiendas virtuales utilizadas a nivel local con entrevistas a especialistas en manejo y creación de sitios web para comercio electrónico

Yaesta.com

Yaesta.com maneja el sistema de encriptación utilizado por los bancos, guardando los datos en servidores seguros y evitando así que sean almacenados por el sitio web, de esta manera garantiza la seguridad del cliente y resguarda su información (Mosquera C., 2016). Las tecnologías utilizadas por los bancos en cuanto a sistemas de seguridad están basadas en la clave pública (PKI), en protocolos SSL y SET; ya que se ha comprobado que son las únicas que cubren carencias de seguridad, protegiendo en mayor medida la información que fluye en internet (Tarrats, J. & Jordán, F., 2000).

La tecnología de clave pública también se aplica en sistemas de banca virtual para garantizar la seguridad en transacciones bancarias, procesos de compra y venta, y gestiones de cuenta (Guzmán, V., & Natali, R. 2012).

De esta manera Yaesta.com ha generado una amplia acogida en el sector comercial a nivel nacional, es cierto que hace falta una amplia evolución de la cultura de compra y venta electrónica dentro del país pero se puede evidenciar el gran interés por incrementar la seguridad en el desarrollo del e-commerce mediante a esta plataforma.

Tame Ecuador

Las agencias de viaje en la actualidad también han incursionado en el acercamiento tecnológico que permite el e-commerce, mismo que para su correcto desarrollo implica la ejecución tanto de una buena estrategia comercial como de un protocolo de seguridad confiable para los usuarios. Al implementarse esta alternativa comercial en el sector turístico tuvo una gran acogida a pesar de brindar un servicio intangible (Lewer, 2009).

La tecnología como un recurso de avance para las aerolíneas genera un incremento de clientes interesados en la adquisición de servicios mediante aplicaciones de compra y venta electrónica, desde la comodidad de donde se encuentran. La responsabilidad de brindar un servicio mediante a una tienda virtual crea un riesgo

muy alto tanto para las empresas como para los usuarios de estas, poniendo en la balanza la necesidad de sistemas de protección de la información que se maneja en la red (Still, 2015).

"TAME posee diferentes programas planteados en su Plan Estratégico para el periodo 2009-2018, a causa de la aplicación de los aspectos de este planeamiento, la mayoría de sus clientes adquieren sus pasajes a través de las agencias de viajes. Señaló que un 50% de sus clientes realizan compras por medio del sitio web, usando el E-Commerce y que la otra mitad estante lo realiza a través de canales indirectos" (Zúñiga, M. E. G., Aguilar, M. T. G., & Freire, E. M. G. 2017).

La empresa maneja un sistema de protección de datos CRM en el que se lleva registro del cliente y su comportamiento de compra, para uso interno de la empresa. Del mismo modo ha implementado el sistema de encriptación simétrica de datos mediante al protocolo SET, sobre todo este protocolo es usado en las transacciones en las que realiza pagos con tarjeta ya que son los utilizados por las instituciones bancarias para brindar mayor seguridad a sus usuarios (Chiriboga, G., & Vanessa, Y. 2016).

Análisis comparativo.

Luego de las entrevistas y análisis realizados se ha desplegado un amplio campo de herramientas necesarias para el uso del e-commerce. En ambas empresas se emplean diferentes mecanismos de seguridad electrónica además de tener un concepto diferente sobre las necesidades que plantean las transacciones económicas realizadas mediante a la web.

A continuación se presenta una tabla comparativa de estándares de seguridad en las empresas analizadas:

Protocolos y sistemas de seguridad / Empresa	Sistema de clave pública PKI	Protocolo SSL	Protocolo SET	Sistema de protección CRM
Yaesta.com	**X**	**X**	**X**	
Tame			**X**	**X**

Tabla 3. Comparación de sistemas de seguridad

CAPÍTULO IV: DISCUSIÓN

El intercambio de bienes y servicios entre personas ha sido una de las actividades básicas en el desarrollo de las sociedades desde el principio de la vida humana, la actividad de comprar y vender no solo ha prevalecido durante los siglos, sino que ha evolucionado constantemente con el crecimiento del medio (Paul R., Krugman, Obstfeld, M., & Marc J., Melitz, 2012).

El aumento y avance desmedido de la tecnología ha abierto las puertas a nuevos intereses comerciales, convirtiéndose de esta manera en una clave para llevar a cabo el comercio, convirtiendo la actividad de compra y venta personal en algo del pasado gracias a las alternativas accesibles, rentables y económicas que ofrece el internet, ofreciendo diversas herramientas web para el comercio electrónico (Liberos, del Poyo, Rabadán, Merino & Somalo, 2010).

Se planteó esta investigación con la finalidad de conocer los estándares de seguridad aplicados en el e-commerce, mejorar los protocolos existentes y proteger los datos transferidos por los usuarios a través de internet al realizar una compra. La seguridad que ofrezcan las tiendas virtuales a sus clientes en las transacciones realizadas influye considerablemente en la confianza y fidelidad que generen para próximas transacciones (Liberos et al. 2010). En este estudio se analizan los estándares más conocidos funcionales y seguros que deben utilizarse en la web.

El propósito de esta investigación se basa en la inseguridad y desconfianza de los usuarios que utilizan el comercio electrónico, mejorado su confianza mediante a herramientas que garanticen la fiabilidad de las transacciones y la completa protección de la información brindada por ellos a las tiendas virtuales.

En los años setenta gracias a la expansión de las computadoras en el entorno empresarial una gran parte de los delitos que afectan a la economía fueron delitos involucrados a fraude informático (Hérnandez, 2009). Con el avance de la tecnología se ha evidenciado no solo el incremento de formas de comercio, sino también el riesgo de fraudes informáticos y fallas en la seguridad de la información (Laudon et al. 2009)

Con la intención de disminuir dichos ataques de seguridad relacionados directamente a ataques con malware esta investigación permitió la identificación de protocolos de seguridad utilizados en el e-commerce para la protección de información que se maneja en las herramientas web que permiten el comercio electrónico, y de esta forma realizar transacciones en las que fluye información confidencial de una manera segura y confiable.

En estos tiempos se pueden observar cientos de herramientas para el e-commerce, mas es difícil encontrar una herramienta que tenga la seguridad necesaria para poder utilizarla sin temor a fraude o intenciones maliciosas.

En el Ecuador el comercio electrónico no ha tenido gran acogida por diversos factores como la falta de conocimiento sobre el tema, la inseguridad al realizar la transacción y el temor al mal uso de la información personal.

Habiendo estudiado, definido e identificado más a fondo los conceptos planteados en la investigación "Solución integral de seguridad para las pymes mediante un UTM", se obtuvo un enfoque no solo teórico sino más abierto para mejorar la seguridad informática y de esta manera implementar dichos contenidos a los sistemas involucrados en protección y seguridad necesarios para el comercio electrónico.

Los datos almacenados en la red se encuentran altamente comprometidos, dado que el avance de la tecnología abre puertas a favor y en contra de la seguridad informática, de esta manera Gómez & Espinoza (2015) plantearon la prevención de los crímenes informáticos más comunes mediante a técnicas desarrolladas con el apoyo de protocolos de seguridad, con referencia a estas técnicas podemos identificar que el uso de los UTM no es lo suficientemente confiable ni cumple totalmente con los estándares de seguridad que garanticen una completa protección de la información.

Cabe recalcar que ningún protocolo, red o servidor es completa y totalmente invulnerable, pero se puede asegurar que con el uso correcto de protocolos actualizados necesarias para protección de información como se ha demostrado en este estudio se pueden disminuir en mayor medida la efectividad de los ataques informáticos y fraudes electrónicos.

Mientras los UTM brindan protección local y un poco más abierta, los protocolos de seguridad con altos estándares de efectividad mostrados por la investigación “Sistemas de Pagos seguros” tales como: el SSL, el SET y el 3D Secure han demostrado ser los más efectivos, utilizados por las tiendas y aceptados por los usuarios gracias a su comprobada efectividad al momento de proteger la transferencia de información y valores.

Existen algunas barreras en el comercio electrónico, pero a nivel de seguridad se puede considerar que la implementación adecuada de los protocolos existentes además de una correcta certificación ISO27001 tienen la alta capacidad de otorgar seguridad en el e-commerce, además de ser esto una ventaja debe considerarse como un incentivo para su aplicación la confiabilidad que se presta a los usuarios que finalmente son el principal motor de este tipo de comercio.

CAPÍTULO V: CONCLUSIONES

Al terminar este estudio se puede aseverar que los objetivos planteados se han cumplido de forma completa y satisfactoria, habiendo observado las herramientas web más utilizadas como son Doble Clic, Adobe ilustrador CS6 e incluso Python HTTP server; componentes de programación como: HTMAL, CSS y Java Script; además de estándares de seguridad que intervienen en el comercio electrónico poder identificar los mejores y más recomendados para cumplir la función en cuanto a seguridad brindada en la web principalmente en las tiendas virtuales. Sobre todo se ha evidenciado la gran necesidad del cumplimiento de la Norma ISO 27001, para un excelente manejo de la seguridad en la web.

Se ha determinado los estándares y protocolos de seguridad que intervienen en el e-commerce, infiriendo que el protocolo de seguridad SSL fue de mayor aceptación, funcionalidad y protección ante fraudes presenta según lo analizado es el SSL, ya que permite establecer comunicaciones seguras y al no ser exclusivo del comercio electrónico permite todo tipo de comunicación por internet segura, incluso las transacciones económicas.

Además utilizar el sistema de certificados digitales permite garantizar la seguridad de la información manejada, siendo un complemento válido para protegerse de fraudes informáticos y evitar robos de información. Otra nueva tecnología de protección que son las firmas digitales, las mismas que son consideradas las más seguras para manterer la integridad de la información y conservar la legalidad de un documento que viaja a través de la web.

Las empresas analizadas, Yaesta.com y Tame, demostraron no solo su alto nivel de compromiso en la seguridad de la información manejada, sino que se pudo observar que ambas utilizan el Protocolo de seguridad SET, mismo que como vimos durante e estudio representa un alto alcance e seguridad a nivel informática.

CAPÍTULO VI: RECOMENDACIONES

Además del sistema de seguridad SSL se propone implementar las transacciones basadas en SET mediantes a las cuales las grandes agencias bancarias a nivel mundial han desarrollado un protocolo que simula a la forma de pago electrónica usando certificados y firmas digitales para compra y venta de bienes y servicios.

Como complemento establecer una estructura de clave pública permite garantizar los procesos antes mencionados como último filtro de seguridad. De esta manera se cifran los datos que se emitirán por la red utilizando el sistema de encriptación simétrica.

Los conceptos estudiados y presentados sirven como aliciente para recomendar el uso de SGSI, mismo que está directamente ligado a la implementación y manejo de la Normativa Estándar ISO 27001 que regula los procesos de seguridad informática.

El manejo correcto de las herramientas y componentes de programación que intervienen en la creación de tiendas virtuales, aplicaciones y plataformas relacionadas con el e-commerce aunado al correcto seguimiento de los estándares de calidad y protocolos de seguridad existentes garantizan que no solo los objetivos planteados a nivel de seguridad informática se cumplan sino de que el comercio electrónico reciba una mayor acogida de parte de los usuarios brindándoles seguridad y calidad, por esto es importante que se realice una inversión profunda en cuanto a temas de seguridad electrónica dentro de las empresas que utilizan el e-commerce.

CAPÍTULO VII: ANEXOS

1. ¿Cuáles son las principales herramientas utilizadas en este sitio web?

_____

_____

_____

2. ¿Cuáles con los estándares y protocolos de seguridad que se sigue para la aplicación de e-commerce?

_____

_____

_____

3. ¿A nivel de tienda virtual, cuáles son las mayores amenazas presenciadas por usted?

_____

_____

_____

4. ¿Qué forma de pago permite este sitio de comercio virtual?

_____

_____

_____

5. Expliquenos alguno de los componentes de programación existentes en el desarrollo de este sitio web.

_____

_____

_____

6. ¿Cuáles son las ventajas en cuanto a condiciones de seguridad ofrecidas por ustedes con referencia a la competencia?

_____

_____

Anexo 1. Entrevista a Especialistas.

BIBLIOGRAFÍA

Acurio Del Pino, S. (2006). Delitos Informáticos: Generalidades. PUCE.

Amazon. (2017). Amazon. Obtenido de https://services.amazon.com/amazon-business.html/ref=asus_b2b_fnav

Arias Arciniegas, C. M., & Castillo Builes, E. (2011). La educación para el emprendimiento y empresarismo virtual: potencialidades. Revista Virtual Universidad Católica del Norte, (32).

Avila, E. (2013). Importancia de las tiendas virtuales y como conseguir una a un dolar. Haciendo negocios por internet de forma fácil y segura.

Azevedo, A. H. F. (2016). Burlas informáticas: modos de manifestação (Doctoral dissertation).

Balcazar, P., Gonzales, N., Gurrola, G., & Moysén, A. (2013). Investigación Cualitativa. Mexico DF: UAEM.

Balsas, J., Ruiz, J., & Rivas, V. (s.f.). Universidad de Jaen. Obtenido de Universidad de Jaen: http://www10.ujaen.es/sites/default/files/users/sinformatica/guiaspracticas/cursopaginasweb.pdf

Beati, H. (2016). HTML5 y CSS3-Para diseñadores. Alfaomega Grupo Editor.

Bernal Jurado, E., & Rodríguez Cohard, J. C. (2003). Las regiones Objetivo 1 españolas en la sociedad de la información: el comercio electrónico como elemento de desarrollo. Revista de Estudios Regionales, (67).

Bezos, J. Amazon. Recuperado el 01 de Febrero de 2008, de http://www.amazon.com. (1995).

Borja, M., & Silvana, G. (2016). Desarrollo de una aplicación 3D para una tienda virtual en webgl (Bachelor's thesis, Quito: UCE).

Brocardo, M. L., Rolt, C. R. D., Dias, J. D. S., Custodio, R. F., & Traore, I. (2017). Privacy information in a positive credit system. International Journal of Grid and Utility Computing, 8(1), 61-69.

Camargo, C., Sáenz, J., & Rosas, N. F. (2014). Implementación de un sistema de seguridad en medidores inteligentes (Smart Grids). Ingenium Revista de la facultad de ingeniería, 15(30), 28-38.

Chiriboga, G., & Vanessa, Y. (2016). Análisis de compras por internet a través de Tarjetas de crédito en ECUADOR (Master's thesis, Universidad de Guayaquil).

Chou, W. “Inside SSL: the secure sockets layer protocol”, IEEE Computer Society, vol. 4, p. 4, pp. 47-52. 2002.

Club Planeta. (s.f.). Historia de Amazon.com. Club Planeta.

Collins, Patrick. Amazon.com una tienda de comercio electrónico. 2001

Diario El Comercio. (s.f.). Comercio electrónico mueve entre USD 60 000 y 70 000 millones en América Latina. Ecuador.

Diario El Universo. (23 de Noviembre de 2015). El Universo. Obtenido de http://www.eluniverso.com/vida-estilo/2015/11/23/nota/5257425/yaestacom-otro-portal-comprar-web

Diario El Universo. (s.f.). YaEsta.com, otro portal para comprar en la web. Ecuador. 2015

Don, G. E. (2016). Comercio electrónico: Tienda virtual e-shell(Doctoral dissertation).

ESTUDIOS, P. D. R. I. Y. La seguridad y la logística en la cadena de suministro: Amazon. com un ejemplo exitoso. 2015.

Ebay. (s.f.). Ebay. Obtenido de http://www.ebay.es/

Fernández, P., & Pértegas , D. (2002). Investigación cuantitativa y cualitativa. Coruña: Unidad de Epidemiología Clínica y Bioestadística. Complexo Hospitalario-Universitario Juan Canalejo. .

Flórez R., W., Arboleda, C., & Cadavid, J. (2012). Solución Integral de seguridad para las PYMES mediante un UTM. Medellin.

Flórez Wilmar, A. C. (2012). SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN.

Garcia, P., & Rodriguez, F. (s.f.). El Comercio Electrónico y la seguridad en sus transacciones. Investigación y Ciencia. 2015.

García, B., Gómez, A., Conde, R., Hernández, Y., & Valero, M. Á. (2015). Breaking the web barriers of the e-Administration using an accessible digital certificate based on a cryptographic token. Advances in Software Engineering, 2015, 3.

Gauchat, J. D. (2017). HTML5 para Mentes Maestras, 2da Edición: Cómo aprovechar HTML5 para crear sitios web adaptables y aplicaciones revolucionarias. JD Gauchat.

Gomez, E. C. F., & Espinoza, H. A. C. (2015). Cómo responder a un Delito Informático. Ciencia Unemi, 7(11), 43-50.

Gomez, E. C. F., & Espinoza, H. A. C. (2015). Cómo responder a un Delito Informático. Ciencia Unemi, 7(11), 43-50.

González Serrano, L. F. (2015). El impacto del desarrollo de proveedores en la cadena de suministros (Bachelor's thesis, Universidad Militar Nueva Granada).

Gutierrez, C., Fernandez, E., & Piattini, M. (2005). Seguridad en Servicios Web.

Guzmán, V., & Natali, R. (2012). Framework de Seguridad para el Comercio electrónico (e-Commerce) en Cuenca (Bachelor's thesis, Universidad del Azuay).

Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Asociación Española de Normalización y Certificación.

Gómez, F. (2014). La Seguridad es las transacciones. Revista Información Comercial Española.

Headways Media. (2016). Headways. Obtenido de ttps://www.headways.com.mx/glosario-mercadotecnia/palabra/tienda-virtual/

Hernández García, Á. (2012). Desarrollo de un modelo unificado de adopción del comercio electrónico entre empresas y consumidores finales. Aplicación al mercado español (Doctoral dissertation, Telecomunicacion).

Heurtel, O. (2015). PHP 5.6: desarrollar un sitio web dinámico e interactivo. Ediciones ENI.

Hidalgo, L. (Junio de 2014). Core. Obtenido de https://core.ac.uk/download/pdf/29406798.pdf

Hoyos, M. M., Castro, L. V., & de Plata, D. P. (2015). Tienda virtual: social market Colombia. Multiciencias, 14(3).

ISO/IEC 27000 Obtenido de: http:/www.iso27000.es/iso27000.html/

Ladino, M. I., Villa, P. A., & López, A. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica, 17(47).

Lara-Navarra, P., & Martínez-Usero, J. Á. (2002). Del comercio electrónico a la administración electrónica: tecnologías y metodologías para la gestión de información. El profesional de la información, 11(6), 421-435.

Lewer, a. (2009). Estrategias comerciales y financieras (E-commerce). estrategias económicas para todo empresario , (pp. 10-15). Quito.

Luna, D. (2014). Implementación y Adaptación de Módulos de Oscommerce en la Creación de una Tienda Virtual.

López, L. M., Mata, F. M., & Domínguez, R. M. R. Sistemas de pago seguro. Seguridad en el comercio electrónico. Revista de estudios empresariales. Segunda época, 2009.

Martínez López, L., Mata Mata, F., & Rodríguez Domínguez, R. (2009). Sistema de Pago Seguro Seguridad en el comercio elecctronico. Revista de Estudios Empresariales. Segunda época. , 63 - 76 .

Martinez, J. A. S. (2007). CRM¿ Filosofía o Tecnología? Mitos y realidades de la orientación al cliente. Pecvnia, (5), 209.

Mayan, M. (2001). Una Introducción a los métodos cualitativos. Iztapalapa: International Institute for Qualitative Methodology. .

Mercado Libre. (s.f.). Mercado Libre. Obtenido de https://www.mercadolibre.com/

Moncayo, J., & Reis, M. (2016). Un análisis inicial del Dinero Electronico en Ecuador y su impacto en la inclusión financiera.

Mosquera Castro, L. K. (2016). Los retos del marketing online frente a los prosumidores. Análisis de las estrategias de mercadeo en el marco de la cibercultura (Bachelor's thesis, Quito: UCE).

Murillo, R. S. (2009). Beneficios del Comercio Electronico. Perspectivas, (24), 151-164.

OVH Innovation is Freedom. (2017). OVH Innovation is Freedom. Obtenido de https://www.ovh.com/us/es/anti-ddos/principio-anti-ddos.xml

Pachano, J. (2013). Comercio electrónico en el Ecuador: análisis de ventajas y desventajas. Quito: Ubiversidad San Francisco de Quito.

Paul R.. Krugman, Obstfeld, M., & Marc J.. Melitz. (2012). Economía international: Teoría y política. Pearson.

Pixelpro Cursos. (2014, Enero 29). Tienda Online con PHP MySQL HTML5 CSS3 jQuery 3. Recuperado de https://www.youtube.com/watch?v=_XOIlf2RTvw

Pueyrredon, M. (2015). Instituto Latinoamericano de Comercio Electrónico. Obtenido de Instituto Latinoamericano de Comercio Electrónico: http://www.einstituto.org/marketing/2015/einstituto/Estado-Situacion-Comercio-Electronico-Am.pdf

Rodríguez Altamirano, H. J., Blanco, R., Adán, C., & Pérez Sánchez, D. E. (2016). Desarrollo de una aplicacíon Web publicitaria con implementación de Yii framework y PostgreSQL(Doctoral dissertation)

Rodríguez Arbeláez, J. D. (2014). Análisis de los delitos informáticos presentes en l as redes sociales en Colombia para el año 2011 y su regulación.

Rosello, R. H. (2014). BREVE ANALISIS Y ALGUNAS OBSERVACIONES AL DELITO INFORMATICO. NOUS, 5(5),99.

Ruiz, A., Villegas, M. L., & Hernández, H. A. Estudio de Usabilidad en Aplicaciones de Comercio Electrónico B2C–Amazon–Dell–MercadoLibre. Universidad del Quindío, Quindío-Colombia.[citado 15 de abril 2014] Disponible en línea: http://www. uniquindio. edu. co/uniquindio/revistadyp/backup20121214/archivo/edificio n_5/Articulos/5ta% 20Edicion/q. pdf. 2012.

Santiago Campión, R., & Navaridas Nalda, F. (2012). LA WEB 2.0 EN ESCENA. Píxel-Bit. Revista de Medios y Educación, (41).

Sastre, M. G. Comercio Electrónico, Seguridad y Sistemas de Pago en la Red, httD. Dersonales. com/esDana/leon/tristan.

Seguridadpc.net. (2012). Seguridadpc.net. Obtenido de http://www.seguridadpc.net/phishing.htm

Sellers Rubio, R., & Azorín Escolano, A. (2001). EL COMERCIO ELECTRÓNICO YEL FUTURO DEL CANAL DE DISTRIBUCIÓN TURÍSTICO. Investigaciones Europeas de Dirección y Economía de la Empresa, 7(1), 13-36.

Still, M. (5 de abril de 2015). Beneficios del E-commerce.

Tarrats, J. B., & Jordán, F. (2000). La seguridad de las transacciones bancarias en Internet. Informes SEIS, 133.

Thushara, Y., & Ramesh, V. (2016). A Study of Web Mining Application on E-Commerce using Google Analytics Tool. International Journal of Computer Applications.

Torroba, R., & Ramírez, J. F. B. (2015). Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta. Revista de la Academia Colombiana de Ciencias Exactas, Físicas y Naturales, 39, 55-60.

Tutivèn, R., & Anahi, M. (2017). FACTORES LIMITANTES EN LA IMPLEMENTACIÒN DEL COMERCIO ELECTRÒNICO EN LAS MIPYMES DEL SECTOR MIRAFLORES DE LA CUIDAD DE GUAYAQUIL (Bachelor's thesis).

Universidad Nacional Autónoma de México. (2008). Profesores.fi-b.unam . Obtenido de http://profesores.fi-b.unam.mx/jlfl/Seminario_IEE/Metodologia_de_la_Inv.pdf

Valencia, F. (2015). Sistema de Dinero Electronico, un medio de pago al alcance de todos. Boletín, 60 (4), 255, 269.

Weaver, A.C. “Secure Sockets Layer”, IEEE Computer Society, vol. 39, nº 4, pp. 88- 90. 2006

Yaesta.com. (2017). Informe General de la empresa. Quito.

Zúñiga, M. E. G., Aguilar, M. T. G., & Freire, E. M. G. (2017). Análisis del E-commerce como estrategia comunicacional de las aerolíneas. Un comparativo entre TAME y LATAN. Observatorio de la Economía Latinoamericana, (228).