Resumen

El presente trabajo realiza un estudio del comercio electrónico a nivel general y luego su implementación para realizar transacciones de manera segura a través de una tienda virtual. Consta de seis capítulos de los cuales el primero realiza una introducción sobre el comercio electrónico: Conceptos, ventajas, desventajas, modelos de negocios. En el segundo capítulo se habla sobre los mecanismos de seguridad que se deben implementar para disponer de un comercio electrónico seguro, la utilización de la criptografía, los protocolos de seguridad y los medios de pago. En el capítulo tercero se hace un estudio de las herramientas de comercio electrónico de libre distribución para luego seleccionar una que será utilizada para su implementación.

En los capítulos cuarto y quinto se realiza un estudio a profundidad del software seleccionado para su implementación, en este caso Opencart, con sus respectivas modificaciones y recomendaciones para que se convierta en una tienda virtual de comercio electrónico seguro tanto desde el punto de vista de transmisión de datos como de la parte de pago que es el punto crítico para el usuario que realiza una compra, así como también la seguridad para proteger los datos de los clientes que se encuentran almacenados.

Por último, en el capítulo seis se documentan las conclusiones y recomendaciones que se han encontrado a lo largo del desarrollo de este trabajo.

Palabras Claves:
Criptografía simétrica

Criptografía asimétrica

Certificados Digitales

Firmas Digitales

SSL

Protocolos de seguridad

Tienda Virtual

Prestashop

Magento

Abstract

The present work carries out a study from the electronic commerce to general level and then its implementation to carry out transactions in a secure way through a virtual store. It consists of six chapters of which the first one carries out an introduction on the electronic commerce: Concepts, advantages, disadvantages, models of business. In the second chapter it is talked about the mechanisms of security that should be implemented to have a secure electronic commerce, the use of the cryptography, the protocols of security and the payment means. In the chapter third a study of the tools of electronic trade of free distribution is made it for then to select one that will be used for its implementation.

In the chapters four and five are carried out a study to depth of the selected software for their implementation, in this case Opencart, with their respective modifications and recommendations so that it becomes a virtual store of electronic commerce so much insurance from the point of view of transmission of data like of the payment part that is the critical point for the user that carries out a purchase, as well as the security to protect the data of the clients that are stored.

Lastly, in the chapter six the conclusions and recommendations are documented that have been along the development of this work.

Índice del contenido.

CAPITULO 6: Conclusiones, recomendaciones y líneas futuras de investigación

UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

MAESTRIA EN TELEMATICA

"IMPLEMENTACION DE UN PROTOTIPO DE TIENDA VIRTUAL SOBRE PLATAFORMA LINUX PARA REALIZAR TRANSACCIONES DE COMERCIO ELECTRONICO SEGURO"

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGISTER EN TELEMÁTICA

AUTOR: ING. JORGE PATRICIO BARROS PICÓN

DIRECTOR: DR. DIEGO ARTURO PONCE VÁSQUEZ

CUENCA-ECUADOR

30 DE JULIO DEL 2010

DEDICATORIA

Este trabajo de tesis lo dedico a mi esposa Rocío, y a mis tres hijos Jorge, Anabel y Gabriel. A mi madre y a la memoria de mi padre quienes siempre me apoyaron en todo lo que yo emprendiera.

AGRADECIMIENTO

Al Dr. Diego Ponce Vásquez, director de este trabajo de tesis de máster, por su gran colaboración y asistencia prestada durante el desarrollo del mismo.

A todos los profesores de la maestría por compartir sus conocimientos y experiencias muy valiosos.

A mi esposa por el apoyo y comprensión que siempre me brindó durante todo el tiempo desde el inicio de esta maestría.

A todas las personas que no nombro, pero que de una u otra manera colaboraron para que el presente trabajo se haga realidad.

Introducción

El comercio electrónico permite tanto a los consumidores como a los proveedores de bienes físicos y digitales así como servicios realizar transacciones en forma sencilla y económica. Los consumidores finales pueden consultar fácilmente los productos de varias compañías y realizar sus transacciones desde cualquier lugar y en cualquier momento y realizarlo en el menor tiempo.

La red Internet es una red abierta que dispone de una serie de mecanismos para garantizar que dichas transacciones se realicen de forma segura. Aunque en todos los casos es importante que se realicen las transacciones de forma segura, es indudable que en el caso del pago es imprescindible ya que compromete no solo transacciones económicas, sino también los datos personales o comerciales y la privacidad de los hábitos de consumo del usuario.

Antecedentes

Con la llegada del Internet se ha creado un nuevo concepto de negocios, donde existe la posibilidad de comprar y vender productos a través de portales o tiendas virtuales. En la práctica las empresas están usando Internet como un nuevo canal de ventas, sustituyendo las visitas personales y el teléfono por pedidos electrónicos, ya que realizar un pedido por Internet cuesta menos que hacerlo por vías tradicionales. Nace entonces el comercio electrónico como una alternativa de reducción de costos y una herramienta fundamental en el desempeño empresarial, todo esto en un mercado global.

Estado del Arte:

Realidad Mundial

El comercio electrónico es una tecnología madura que se sustenta sobre la criptografía y teoría de números ampliamente desarrollada durante las guerras mundiales y la guerra fría, hoy se utiliza habitualmente en el mundo y existe gran cantidad de transacciones comerciales en Internet.

En la actualidad, a nivel mundial, podemos encontrar una amplia variedad de portales y tiendas virtuales dedicadas al comercio electrónico de todo tipo de productos (tanto bienes como servicios), basados en la implementación de algún modelo de comercio electrónico.

Situación Nacional

A pesar de que a nivel mundial existe un notable desarrollo del comercio electrónico, en Ecuador la aplicación de esta tecnología ha sido muy reducida, esto se debe principalmente a la falta de una base legal sólida y al desconocimiento de las herramientas tecnológicas para poder realizar negocios de forma segura en Internet. En la actualidad, a nivel Nacional existen muy pocas empresas que han implementado el comercio electrónico, recientemente están disponibles las primeras autoridades de certificación pese a los evidentes beneficios tales como la reducción de gastos de ventas, cobertura a nivel mundial y, por lo tanto, incremento en volumen de ventas e ingresos.

Descripción del Problema

Hoy en día vivimos en un mundo sumergido en un constante y acelerado crecimiento de las tecnologías de comunicación y computación, y esto lo podemos constatar con la constante demanda de Internet por parte de los usuarios.

Cada día se incrementa el número de personas que realizan transacciones comerciales vía Internet de productos que se ofertan a través de tiendas virtuales de otros países.

El problema que se presenta en el Ecuador es que no existen desarrollos de comercio electrónico, por lo que los empresarios ecuatorianos carecen de una guía que les muestre sus ventajas, desventajas y los requerimientos para implementarla dentro de sus empresas, para que de esta manera puedan tener una base que les ayude a decidir si les conviene o no invertir en la adopción de esta tecnología.

Justificación del tema de tesis

La aplicación del comercio electrónico en el Ecuador está en su fase de nacimiento, por lo que sería de gran importancia que la Universidad de Cuenca cuente con una tesis de maestría sobre este tema. Al desarrollarse un prototipo, éste contribuirá para que los alumnos de la Universidad dispongan del mismo y puedan tener una idea mucho más clara de los requerimientos para la implementación de una tienda virtual.

Además, este trabajo puede ser de gran importancia para las empresas, ya que en el mismo se realizará un análisis comparativo de las mejores herramientas de libre distribución.

Objetivos

Generales

El objetivo principal del presente proyecto es definir un modelo de tienda virtual y desarrollar un prototipo tal que provea los mecanismos de seguridad criptográfica y los mecanismos electrónicos de pago para vender por Internet, aprovechando para ello software de libre distribución.

Específicos

- Realizar un análisis de las diferentes herramientas requeridas para el desarrollo e implementación de una tienda virtual en un entorno seguro, con el fin de determinar las fortalezas y debilidades de cada una de ellas.
- Desarrollar un prototipo de tienda virtual que provea los mecanismos de seguridad criptográfica, basada en software de libre distribución y adaptarla a las leyes ecuatorianas.
- Instalar y configurar la infraestructura de hardware y software necesaria, en un ambiente de laboratorio, para la implementación del prototipo propuesto.

Alcance del proyecto

El presente proyecto cubrirá los siguientes aspectos:

1. **Estudio Teórico.**

   Introducción al comercio electrónico

   Aspectos de seguridad

   Aspectos legales

   Análisis de herramientas base y software de comercio electrónico de libre distribución.

2. **Desarrollo del prototipo**

   Análisis, diseño e implementación del prototipo.

   Análisis de resultados.

Principales características del prototipo propuesto:

- Será montado sobre plataforma LINUX en un ambiente de laboratorio (sobre un PC de escritorio), utilizando para ello herramientas de libre distribución (servidor WEB seguro, base de datos, lenguaje de programación, librerías criptográficas).
- Tendrá como mínimo 5 categorías diferentes de productos de la tienda virtual, cada una de ellas con 10 productos.
- El usuario (cliente) podrá navegar por los productos y realizar el pedido de acuerdo con la disponibilidad de los mismos. Además, el sistema permitirá realizar una búsqueda independiente de productos, sin necesidad de navegar por las diferentes categorías.
- Una vez que el cliente haya terminado de realizar el pedido, se mostrará el listado de los productos a comprar y se permitirá quitar aquellos que el cliente no desee adquirirlos.
- Al ser una tienda virtual en línea, luego de confirmado el pedido se procederá a la actualización de las existencias de los productos.

Se mantendrá un registro de los clientes y sus transacciones con el fin de disponer de un historial que puede ser usado posteriormente, en futuras

implementaciones, para poder ofertar productos en función de sus preferencias de compra y dar un seguimiento al cliente.

Método de trabajo

La metodología que se usará para la elaboración del presente trabajo se indica a continuación:

Paso1: Estudio e investigación teórica de aspectos de comercio electrónico y seguridad.

Paso 2: Búsqueda y preselección de herramientas de software de comercio electrónico de libre distribución.

Paso 3: Análisis de las mejores herramientas de software libre para comercio electrónico.

Paso4: Instalación de las herramientas base sobre las que se realizará el desarrollo del prototipo (Linux, Apache, Módulos de Seguridad requeridos, Lenguajes de programación, Bases de Datos).

Paso 5: Modificación y acoplamiento del código acorde a las leyes y tributación de impuestos ecuatorianos.

Paso 6: Implementación de mecanismos de seguridad y de pago.

Paso 7: Pruebas del prototipo, medición y análisis de resultados.

I. INTRODUCCION AL COMERCIO ELECTRONICO

1.1 Introducción

El comercio electrónico permite tanto a los consumidores como a los proveedores de bienes físicos y digitales así como servicios realizar transacciones en forma sencilla y económica. Los consumidores finales pueden consultar fácilmente los productos de varias compañías y realizar sus transacciones desde cualquier lugar y en cualquier momento y realizarlo en el menor tiempo.

La red Internet es una red abierta que dispone de una serie de mecanismos para garantizar que dichas transacciones se realicen de forma segura. Aunque en todos los casos es importante que se realicen las transacciones de forma segura, es indudable que en el caso del pago es imprescindible ya que compromete no solo transacciones económicas, sino también los datos personales o comerciales y la privacidad de los hábitos de consumo del usuario.

El comercio electrónico se convierte en una necesidad estratégica dentro de los negocios, tanto en los sectores privados como públicos, constituyéndose en un factor clave para reducir los costos, incrementar la competencia, y enfrentar la alta velocidad de demanda de los consumidores. Las empresas que lo miren como un "complemento" a su forma habitual de hacer negocios, obtendrán sólo beneficios limitados, siendo el mayor beneficio para aquellas que sean capaces de cambiar su organización y sus procesos comerciales para explotar completamente las oportunidades ofrecidas por el comercio electrónico.

1.2 Definición.

Definido de una forma muy amplia e ideal, comercio electrónico o *e-commerce* es una moderna metodología que da respuesta a varias necesidades de empresas y consumidores, como reducir costes, mejorar la calidad de productos y servicios, acortar el tiempo de entrega o mejorar la comunicación

con el cliente. Más típicamente se suele aplicar a la compra y venta de información, productos y servicios a través de redes de ordenadores.

Existen varias definiciones formales de comercio electrónico pero voy a mencionar 2 que me parecen más apropiadas:

1.- "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)[1]

2.- "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" [2]

Analizando estas definiciones podemos decir que el comercio electrónico es una metodología moderna para hacer negocios que permite a las empresas, comerciantes y consumidores reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los mismos. Por lo tanto, no debe seguirse contemplando el comercio electrónico como una tecnología, sino que es el uso de la tecnología para mejorar la forma de llevar a cabo las actividades empresariales, de tal forma que éstas resulten transparentes a las personas que lo utilizan dentro de las empresas.

El comercio electrónico es el medio de llevar a cabo dichos cambios dentro de una escala global, permitiendo a las compañías ser más eficientes y flexibles en sus operaciones internas, para así trabajar de una manera más cercana con sus proveedores y estar más pendiente de las necesidades y expectativas de sus clientes. Además permiten seleccionar a los mejores proveedores sin importar su localización geográfica para que de esa forma se pueda hacer negocios en un mercado global.

[1] BT Electronic Commerce Innovation Center, "An Introducction to Electronic Commerce", University of Cardiff, UK.

[2] Halchmi, Z., Hommel, K., y Avital., O., 1996. "Electronic Commerce", The Technion-Israel Institute of Technology.

1.3 Tecnologías empleadas en comercio electrónico.

Existe un amplio rango de tecnologías que utiliza el comercio electrónico, entre ellas son:

- Intercambio Electrónico de datos (EDI- Electronic Data Interchange)
- Transferencia Electrónica de Fondos (EFT- Electronic Funds Transfer)
- Aplicaciones Internet: Web
- Aplicaciones de Voz: Buzones, Servidores
- Transferencia de Archivos
- Multimedia
- Videoconferencia
- Tableros Electrónicos de Publicidad

Para este proyecto nos centraremos en la tecnología de Aplicaciones de Internet, particularmente el Web, ya que éste puede utilizarse como un medio comercial ofreciendo ventajas importantes tanto para los clientes como para las empresas.

1.4 Ventajas y desventajas del comercio electrónico

Ventajas:

- Permite el acceso a más información. Al tratarse de un entorno Web permiten búsquedas profundas que son iniciadas y controladas por los clientes, por lo tanto las actividades de mercadeo mediante el Web están más impulsadas por los clientes que aquellas proporcionadas por los medios tradicionales.

- Facilita la investigación y comparación de mercados. La capacidad del Web para acumular, analizar y controlar grandes cantidades de datos

especializados permite la compra por comparación y acelera el proceso de encontrar los artículos.

- Baja en los costos y precios. Conforme aumenta la capacidad de los proveedores para competir en un mercado electrónico abierto se produce una baja en los costos y precios, de hecho tal incremento en la competencia mejora la calidad y variedad de los productos y servicios.

- Mejoras en la distribución. El Web ofrece a ciertos tipos de proveedores (industria del libro, servicios de información, productos digitales) la posibilidad de participar en un mercado interactivo, en el que los costos de distribución o ventas tienden a cero. Por poner un ejemplo, los productos digitales (software) pueden entregarse de inmediato, dando fin de manera progresiva a la intermediación. De igual forma se puede disminuir el tiempo que se tardan en realizar las transacciones comerciales, incrementando la eficiencia de las empresas.

- Comunicaciones de mercadeo. La naturaleza interactiva del Web ofrece beneficios conducentes a desarrollar las relaciones con los clientes. Este potencial para la interacción facilita las relaciones de mercadeo así como el soporte al cliente, hasta un punto que nunca hubiera sido posible con los medios tradicionales. Un sitio Web se encuentra disponible las 24 horas del día bajo demanda de los clientes. Las personas que realizan el mercadeo pueden usar el Web para retener a los clientes mediante un diálogo asincrónico que sucede a la conveniencia de ambas partes. Esta capacidad ofrece oportunidades sin precedentes para ajustar con precisión las comunicaciones a los clientes individuales, facilitando que éstos soliciten tanta información como deseen. Además, esto permite que los responsables del área de mercadeo obtengan información relevante de los clientes con el propósito de servirles de manera eficaz en las futuras relaciones comerciales.

- Beneficios operacionales. El uso empresarial del Web permite mayor facilidad para entrar en mercados nuevos, especialmente en los geográficamente remotos, y alcanzarlos con mayor rapidez. Todo esto se debe a la capacidad de contactar de manera sencilla y a un costo menor a los clientes potenciales, eliminando demoras entre las diferentes etapas de los subprocesos empresariales.

Desventajas:

- Desconocimiento de la empresa. No conocer la empresa o persona que vende es un riesgo del comercio electrónico, ya que muchas veces ni siquiera están constituidas legalmente en su país y no se trata más que de gente que esta "probando suerte en Internet" o tratando de estafar.

- Desconfianza en los medios electrónicos. La mayoría de los usuarios no confía en la Web como canal de pago ya que desconocen que existen mecanismos y protocolos que proveen seguridad en la transmisión, autenticación, privacidad e integridad de los datos.

- Aspectos legales, políticos y sociales. Existen algunos aspectos abiertos en torno al comercio electrónico: validez de la firma electrónica, no repudio, legalidad de un contrato electrónico, violaciones de marcas y derechos de autor, pérdida de derechos sobre las marcas, pérdida de derechos sobre secretos comerciales y responsabilidades. Por otra parte, deben considerarse las leyes, políticas económicas y censura gubernamentales.

1.5 Riesgos del Comercio Electrónico.

El comercio electrónico puede resultar de mucho beneficio para las organizaciones y sus negocios, y crear oportunidades en nuevos y mejores servicios a los clientes. Sin embargo, los sistemas electrónicos y la infraestructura que le da soporte al comercio electrónico son susceptibles de situaciones de abuso cuando por desconocimiento no utiliza protocolos seguros ni los mecanismos existentes para este fin, mal uso y fallas en algunas de sus formas. Un gran perjuicio puede ocurrir a cualquiera de las partes que intervienen en las transacciones por comercio electrónico, incluyendo a comerciantes, entidades financieras, proveedores de servicios, y clientes particulares.

Como consecuencias más comunes del abus
o, el mal uso y las fallas, pueden incluir:

- *Pérdidas financieras como resultado de un fraude:* alguien puede transferir fondos, en forma fraudulenta, de una cuenta a otra, o destruir importantes registros financieros, valiéndose para ello de un método llamado Phishing que es la suplantación de identidad.

- *Pérdidas de información confidencial de valor y/o utilización no autorizada de los recursos:* un ataque externo puede generar acceso a los recursos no autorizados, y hacer uso de la información para el beneficio propio, resultando en un daño muy importante. Para poder vulnerar el servidor los atacantes generalmente se valen de los fallos de seguridad que se descubren en los sistemas operativos.

- *Pérdida de confidencia o respeto del cliente:* una organización puede sufrir pérdidas significativas como resultado de la publicidad negativa de una intrusión o falla. Si un atacante logró vulnerar las seguridades de un servidor de una empresa, ésta será desprestigiada por las noticias que se divulgarán sobre el ataque a la misma lo que dará como resultado la pérdida de credibilidad en dicha empresa.

Algunas de estas consecuencias pueden ser minimizadas por prácticas adecuadas en los controles internos de la tecnología informática dentro de la organización. Un ejemplo: para disminuir las posibles pérdidas por discontinuidad de servicios, podría ser tomar medidas de planificación de contingencias y de seguridad física. No obstante, el escenario en el cual se desenvuelven las transacciones del comercio electrónico es global, va mas allá de los entornos de las organizaciones involucradas, y los riesgos no siempre pueden ser minimizados con los tradicionales métodos de seguridad y/o prevención.

1.6 Usos del Comercio Electrónico.

El comercio electrónico puede utilizarse en cualquier entorno en el que se intercambien documentos entre empresas: compras o adquisiciones, finanzas, industria, transporte, salud, legislación, cobro de impuestos, etc.

Actualmente la mayoría de compañías utilizan el comercio electrónico para desarrollar los aspectos siguientes:

- Creación de canales nuevos de mercadeo y ventas.
- Acceso interactivo a catálogos de productos, listas de precios y folletos publicitarios.
- Venta directa e interactiva de productos a los clientes.
- Soporte técnico ininterrumpido, permitiendo que los clientes encuentren por sí mismos, y fácilmente, respuestas a sus problemas mediante la obtención de los archivos y programas necesarios para resolverlos.

Mediante el comercio electrónico se intercambian los documentos de las actividades empresariales entre socios comerciales. Los beneficios que se obtienen en ello son: reducción del trabajo administrativo, transacciones comerciales más rápidas y precisas, acceso más fácil y rápido a la información, y reducción de la necesidad de reescribir la información en las computadoras.

1.7 Modelos de Negocio.

En el Comercio Electrónico participan 3 tipos principales de actores: las empresas, los consumidores y las Administraciones Públicas. Así, se distinguen los siguientes modelos de negocio:

· Entre empresas (*B2B, Business to Business*).
· Entre empresa y consumidor (*B2C, Business to Consumer*).
· Entre empresa y Administración (*B2A, Business to Administration*).
· Entre ciudadano y Administración (*C2A, Citizen to Administration*).
· Entre ciudadanos (*C2C, Citizen to Citizen*).

Las empresas intervienen como usuarias (compradoras o vendedoras) y como proveedoras de herramientas o servicios de soporte para el Comercio Electrónico: servicios de certificación de claves públicas, instituciones financieras, etc. Un ejemplo de la categoría empresa-empresa sería una compañía que usa una red para ordenar pedidos a proveedores, recibiendo los cargos y haciendo los pagos. Esta modalidad está establecida desde inicios de los años 1980, usando en particular Intercambio Electrónico de Datos (EDI,

ElectronicData Interchange) sobre redes privadas o de valor añadido, pero ha experimentado un gran auge en estos últimos 15 años.

El modelo de negocio entre empresa y consumidor (B2C, Business to Customer) se ha expandido con la llegada de la Word Wide Web. Hay ahora galerías comerciales sobre Internet ofreciendo todo tipo de bienes tanto tangibles como bienes digitales. Entendiéndose por bienes tangibles todos aquellos que requieren de un proceso de entrega posterior, es decir que se trata de bienes físicos (Ropa, perfumes, hardware, libros, electrodomésticos, etc); en tanto que los bienes digitales se refieren a cualquier bien que puede ser transportado a través de líneas de comunicación como Internet tales como software, libros digitalizados, películas, servicios bancarios, etc.

Las Administraciones Públicas actúan como agentes reguladores y promotores del Comercio Electrónico y como usuarias del mismo, por ejemplo en los procedimientos de contratación pública o de compras por la Administración.
El modelo de negocio Negocio-Administración (B2A) cubre todas las transacciones entre las empresas y las organizaciones gubernamentales. Por ejemplo, en EE.UU. las disposiciones gubernamentales se publicitan en Internet y las compañías pueden responder electrónicamente. Además, las administraciones pueden ofrecer también la opción del intercambio electrónico para transacciones como determinados impuestos y el pago de tasas corporativas.
Los consumidores pueden participar en dos formas adicionales de Comercio Electrónico además del B2C: por una parte, el Comercio Electrónico directo entre consumidores (venta directa entre particulares) y, por otra, las transacciones económicas entre ciudadano y la Administración.
El modelo de negocio Administración-Ciudadano abarca transacciones entre ciudadanos y organizaciones gubernamentales, es usada para áreas tales como los pagos de pensiones, declaraciones de impuestos, consultas de trámites legales, etc.

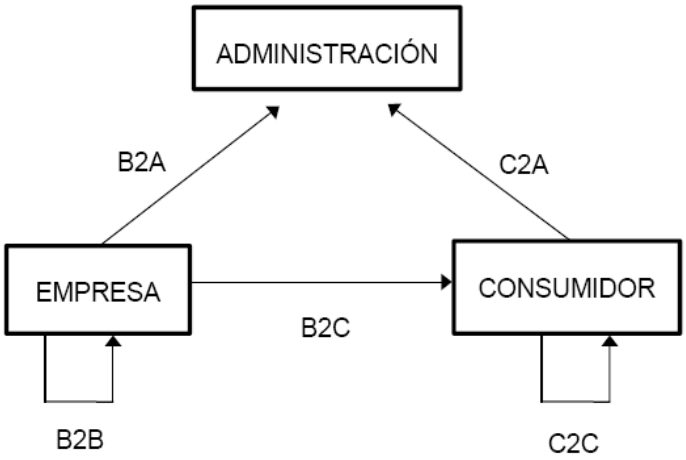

Gráfico 1: Modelo de negocios de comercio electrónico

II. SEGURIDAD EN EL COMERCIO ELECTRONICO

2.1 Introducción

La seguridad en el comercio electrónico y específicamente en las transacciones comerciales es un aspecto de suma importancia. Para ello es necesario disponer de un servidor seguro a través del cual toda la información confidencial es *cifrada* y viaja de forma segura, esto brinda confianza tanto a proveedores como a compradores que hacen del comercio electrónico su forma habitual de negocios.

Al igual que en el comercio tradicional existe un riesgo en el comercio electrónico, al realizar una transacción por Internet, el comprador teme por la posibilidad de que sus datos personales sean interceptados por "alguien", y suplante así su identidad; de igual forma el vendedor necesita asegurarse de que los datos enviados sean de quien dice serlos.

Por tales motivos se han desarrollado sistemas de seguridad para transacciones por Internet como: Encriptación, Firma Digital y Emisión de Certificados, los mismos que garantizan la confidencialidad, integridad y autenticidad respectivamente.

Los algoritmos criptográficos empleados para los procesos de cifrado, emisión de certificados y generación de firmas digitales son de doble naturaleza. Por un lado, se define un algoritmo de clave privada, de fortaleza contrastada y excelente rendimiento: DES (Data Encryption Standard), en uso desde 1977. Por otro lado, se hace imprescindible contar con un algoritmo que permita el intercambio de claves en una red pública, con total seguridad, entre múltiples participantes sin ninguna relación previa; un algoritmo como el descrito se define de clave pública, y generalmente se usa RSA (diseñado por Rivest, Shamir y Adleman), cuyas iniciales componen su nombre.

Cada algoritmo criptográfico permite la implementación de una función determinada. DES se emplea para garantizar la confidencialidad de los mensajes transmitidos; RSA se emplea para garantizar la integridad de los

datos y la autenticidad de los participantes. RSA desempeña todavía una función adicional, posible gracias a su definición como algoritmo de clave pública o algoritmo asimétrico: permite la distribución y utilización de una clave secreta entre participantes sin ninguna relación previa y, lo que es más importante, sobre *canales* (vínculos de comunicación) no seguros.

2.2 Terminología.- Antes de comenzar el estudio de las técnicas criptográficas, es necesario definir una serie de conceptos básicos que se requieren usar durante el resto del documento.

Criptografía: Es un conjunto de técnicas que permiten enviar un mensaje desde un emisor a un receptor sin que nadie que intercepte el mensaje en el camino pueda interpretarlo.
Criptógrafos: Son las personas que estudian y usan la criptografía. El objetivo de los criptógrafos es poder enviar mensajes de forma segura, es decir, sin que ninguna otra persona pueda descubrir qué mensaje es el que se está enviando por un canal inseguro como Internet.
Criptoanálisis: Es una técnica que busca poder descifrar mensajes cifrados. A las personas que realizan el criptoanálisis se les llama **criptoanalistas**.
Criptología: Es la rama de la matemática que se encarga de estudiar tanto la criptografía como el criptoanálisis. Los **criptólogos** son las personas que realizan esta tarea.

El siguiente gráfico resume los elementos que intervienen en un sistema criptográfico:

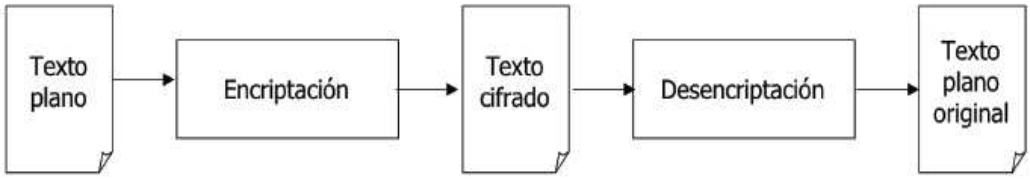

Gráfico 2: Elementos de un sistema criptográfico.

El **texto en claro (plaintext)** es el mensaje que queremos transmitir de forma confidencial. El cifrado es el proceso de transformar el texto en claro en un texto que nadie pueda interpretar. El **descifrado** es el proceso de volver a transformar el texto cifrado en el texto en claro original.

Al **texto cifrado** se le llama también **texto encriptado** que significa que no se puede acceder a él. Sin embargo, en los libros se usa con más frecuencia el término "cifrado" (ciphertext).

Normalmente al texto en claro se le representa con una M (Mensaje) o una P (Plaintext), y al texto cifrado por una C (Cifrado).

El proceso de la encriptación (cifrado) se representa con una función E() de forma que:

C = E(P)

Al proceso del descifrado se le representa como una función D() de forma que:

P = D(C)

Para que un sistema criptográfico sea correcto, tiene que cumplirse la propiedad:

P = D(E(P))

La criptografía se divide en dos grandes ramas, la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica, **DES** pertenece al primer grupo y **RSA** al segundo.

2.3 Criptografía Simétrica o de clave privada.

La criptografía de clave privada (o criptografía simétrica) se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía es conocida también como criptografía de clave privada o criptografía de llave privada.

Existe una clasificación de este tipo de criptografía en tres familias: cifrado de bloques (block cipher), cifrado de flujo (stream cipher) y cifrado de funciones resumen (hash functions).

La criptografía simétrica ha sido la más usada en toda la historia, ésta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, **DES**.

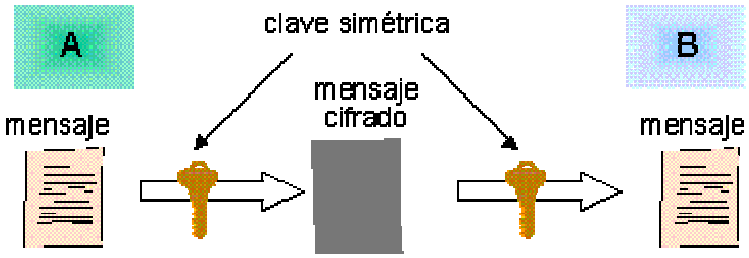

Gráfico 3: Cifrado/descifrado simétrico

2.3.1 Algoritmo DES.

El algoritmo DES toma como entrada un bloque de 64 bits del mensaje y este se somete a 16 interacciones, con una clave de 56 bits. Este sistema fue tomado como estándar y ha sido uno de los más conocidos, usados y estudiados.

DES opera con una llave de longitud de 56 bits, en la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usado como de paridad, pero en sí la clave solo tiene 56 bits de longitud. Dependiendo de la naturaleza de la aplicación, DES tiene 4 modos de operación para poder implementarse: **ECB** (**E**lectronic **C**odebook **M**ode) para

mensajes cortos, de menos de 64 bits, **CBC** (**C**ipher **B**lock **C**haining **M**ode) para mensajes largos, **CFB** (**C**ipher **B**lock **F**eedback) para cifrar bit por bit ó byte por byte y el **OFB** (**O**utput **F**eedback **M**ode) el mismo uso pero evitando propagación de error.

En la actualidad no se ha podido romper el sistema **DES** desde la perspectiva de poder deducir la clave simétrica a partir de la información interceptada, sin embargo con un método a fuerza bruta, es decir, probando todas las 2^56 posibles claves se ha podido romper **DES** a mediados de 1998. Lo cual quiere decir que, es posible verificar todas las claves posibles en el sistema **DES** en un tiempo corto, lo que lo hace inseguro para propósitos de alta seguridad.

A pesar de su caída, DES sigue siendo ampliamente utilizado en multitud de aplicaciones, como por ejemplo las transacciones de los cajeros automáticos. De todas formas, el problema real de DES no radica en su diseño, sino en que emplea una clave demasiado corta (56 bits), lo cual hace que con el avance actual de las computadoras los ataques por la fuerza bruta comiencen a ser opciones realistas. Mucha gente se resiste a abandonar este algoritmo, precisamente porque ha sido capaz de sobrevivir durante veinte años sin mostrar ninguna debilidad en su diseño, y prefieren proponer variantes que, de un lado evitarían el riesgo de tener que confiar en algoritmos nuevos, y de otro permitirían aprovechar gran parte de las implementaciones por hardware existentes de DES.

La opción que se ha tomado para poder reemplazar a **DES** ha sido usar lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave, esto a tomado la forma de un nuevo sistema de cifrado que se conoce actualmente como triple-DES o TDES.

2.3.2 Algoritmo TDES.

El funcionamiento de **TDES** consiste en aplicar 3 veces **DES** de la siguiente manera: la primera vez se usa una clave **K1** junto con el bloque B0, de forma ordinaria **E** (de Encryption), obteniendo el bloque B1. La segunda vez se toma a B1 con la clave **K2**, diferente a **K1** de forma inversa, llamada **D** (de

Desencryption) y la tercera vez a B2 con una clave **K3** diferente a **K1** y **K2**, de forma ordinaria **E** (de Encryption), es decir, aplica de la interacción 1 a la 16 a B0 con la clave **K1**, después aplica de la 16 a la 1, a B1 con la clave **K2**, finalmente aplica una vez mas de la 1 a la 16 a B3 usando la clave **K3**, obteniendo finalmente a B3.

Explicado de otra forma podemos decir que TDES responde a la siguiente estructura:

$$C = E_{k1}(E_{k2}^{-1}(E_{k1}(M)))$$

Es decir, codificamos con la subclave k1, decodificamos con k2 y volvemos a codificar con k1. La clave resultante es la concatenación de k1 y k2, con una longitud de 112 bits.

Este sistema **TDES** usa entonces una clave de 168 bits, aunque se ha podido mostrar que los ataques actualmente pueden romper a **TDES** con una complejidad de 2^112, es decir efectuar al menos 2^112 operaciones para obtener la clave a fuerza bruta, además de la memoria requerida.

En los últimos 30 años se han diseñado una gran cantidad de sistemas criptográficos simétricos, entre algunos de ellos están: RC-5, IDEA, FEAL, LOKI'91, DESX, Blowfish, CAST, GOST**,** etc. Sin embargo no han tenido el alcance de **DES**, a pesar de que algunos de ellos tienen mejores propiedades.

2.3.3. Algoritmo AES (Rijndael)

AES es el nuevo estándar de encriptación de datos propuesto por el NIST en octubre de 2000. Es el sustituto de DES.

Este estándar ha sido desarrollado para sustituir a DES, cuya longitud de clave (56 bits), hoy en día resulta ineficiente. Este estándar goza de más confianza que su predecesor, DES, ya que ha sido desarrollado y examinado de forma pública desde el primer momento.

AES es un algoritmo simétrico de encriptación desarrollado para cifrar bloques de longitudes de 128, 192 o 256 bits utilizando claves de longitud de 128, 192 o 256 bits.

Puede ser utilizado en cualquiera de las combinaciones posibles de bloque/longitud.
Es fácilmente extensible a múltiplos de 32 bits tanto para la clave como para la longitud de bloque.
Según sus autores, es altamente improbable que existan claves débiles o semidébiles en AES, debido a la estructura de su diseño, que busca eliminar la simetría en las subclaves. También se ha comprobado que es resistente a criptoanálisis tanto lineal como diferencial. En efecto, el método más eficiente conocido hasta la fecha para recuperar la clave a partir de un par texto cifrado–texto claro es la búsqueda exhaustiva, por lo que podemos considerar este algoritmo como uno de los más seguros en la actualidad. Otro hecho que viene a corroborar la fortaleza de AES es que en junio de 2003 fue aprobado por la NSA para cifrar información clasificada como alto secreto.

2.4 Criptografía Asimétrica o de clave pública.

Los algoritmos asimétricos o de clave pública han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet).
La criptografía asimétrica es aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Hellman proponen una forma para hacer esto, sin embargo no fue hasta que el popular método de Rivest Shamir y Adleman RSA publicado en 1978, cuándo toma forma la criptografía asimétrica; su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

Actualmente la Criptografía asimétrica es muy usada, sus dos principales aplicaciones son precisamente el intercambio de claves privadas y la firma digital. Una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica se basan en la teoría de números.

En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias, según el problema matemático del cual basan su seguridad. La primera familia la que basa su seguridad en el Problema de Factorización Entera PFE, los sistemas que pertenecen a esta familia son, el sistema RSA y el de Rabin Williams RW. La segunda familia es la que basa su seguridad en el Problema del Logaritmo Discreto PLD, a esta familia pertenece el sistema de Diffie Hellman DH de intercambio de claves y el sistema DSA de firma digital. La tercera familia es la que basa su seguridad en el Problema del Logaritmo Discreto Elíptico PLDE, en este caso hay varios esquemas tanto de intercambio de claves como de firma digital que existen como el DHE (Diffie Hellman Elíptico), DSAE, (Nyberg-Rueppel) NRE, (Menezes, Qu, Vanstone) MQV, etc.

Aunque a las familias anteriores pertenecen los sistemas asimétricos más conocidos, existen también tipos de sistemas que basan su seguridad en otro tipo de problema como por ejemplo en el Problema del Logaritmo Discreto Hiperelíptico, sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, aunque necesita una longitud de clave considerable. Otros algoritmos son los de ElGamal y Rabin.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos —si exceptuamos aquellos basados en curvas elípticas— se recomiendan claves de al menos 2048 bits. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado simétrico. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

2.4.1 Algoritmo RSA.

Es el algoritmo público más utilizado y seguramente el más sencillo tanto para comprender, como para implementar. Debe su nombre a sus tres inventores: Rivest Ron, Shamir Adi y Adleman Leonard

Este algoritmo basa su seguridad en la factorización de números primos grandes.

En una forma muy resumida el modo de funcionamiento de RSA es el siguiente:

a) A cada usuario se le asigna un número entero *n*, que funciona como su clave pública

b) solo el usuario respectivo conoce la factorización de *n* (o sea *p,q*), que mantiene en secreto y es la clave privada.

c) existe un directorio de claves públicas

d) si alguien quiere mandar un mensaje *m* a algún usuario entonces elige su clave pública *n* y con información adicional también pública puede mandar el mensaje cifrado **c**, que solo podrá descifrar el usuario correspondiente, el mensaje *m* convertido a número (codificación) se somete a la siguiente operación.

$$c = m^e \bmod n$$

e) Entonces el mensaje *c* puede viajar sin problema por cualquier canal inseguro

f) Cuando la información cifrada llega a su destino el receptor procede a descifrar el mensaje con la siguiente fórmula

$$m = c^d \bmod n$$

g) Se puede mostrar que estas formulas son inversas y por lo tanto dan el resultado deseado, (*m, e*) son públicos y se pueden considerar como la clave pública, la clave privada es la pareja (*p, q*) o equivalentemente el número *d*. La relación que existe entre *d* y *e* es que uno es el inverso multiplicativo del otro módulo $\lambda(n)$ donde $\lambda(n)$ es el mínimo común múltiplo de *p*-1 y *q*-1.

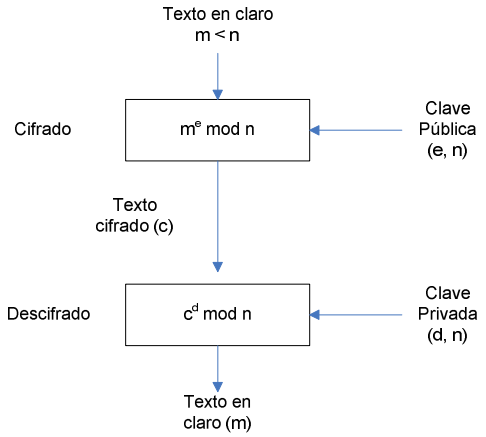

Gráfico 4: Esquema de funcionamiento del algoritmo RSA.

En términos muy generales es así como funciona el sistema **RSA**. Sin embargo en la realidad existen dos formas que son las más comunes, estas formas dependen de la aplicación y se llaman el esquema de firma y el esquema de cifrado.

2.5 Funciones Resumen.

Una función resumen (hash en inglés), proporciona una secuencia de bits de pequeña longitud que va asociada al mensaje aunque contiene menos información que éste, y que debe resultar muy difícil de falsificar. Existen 2 clases de funciones resumen:

a) Funciones MAC (Message Authentication Code) las mismas que emplean en sus cálculos una clave adicional y,

b) Funciones MDC (Modification Detection Codes) que son aquellas que no usan clave adicional para sus cálculos.

Sabemos que un mensaje m puede ser autentificado codificando con la llave privada Kp el resultado de aplicarle una función resumen, EKp(r(m)). Esa información (que denominaremos firma del mensaje m) sólo puede ser generada por el poseedor de la clave privada Kp. Cualquiera que tenga la llave pública correspondiente estará en condiciones de decodificar y verificar la firma. Para que sea segura, la función resumen r(x) debe cumplir además ciertas características:

- r(m) es de longitud fija, independientemente de la longitud de m.
- Dado m, es fácil calcular r(m).
- Dado r(m), es computacionalmente intratable recuperar m.
- Dado m, es computacionalmente intratable obtener un m0 tal que r(m) = r(m0).

Estas propiedades son válidas tanto para los MDC como para los MAC, con la dificultad añadida para estos últimos de que el atacante deberá averiguar además la clave correspondiente. De hecho, conocida la clave, un MAC se comporta exactamente igual que un MDC.

2.5.1 Estructura de una función MDC.

En general, los MDC se basan en la idea de funciones de compresión, que dan como resultado bloques de longitud fija ***a*** a partir de bloques de longitud fija ***b***, con $a < b$.

Estas funciones se encadenan de forma iterativa, haciendo que la entrada en el paso i sea función del i-ésimo bloque del mensaje (mi) y de la salida del paso i - 1 (ver el siguiente gráfico). En general, se suele incluir en alguno de los bloques del mensaje m – al principio o al final -, información sobre la longitud total del mensaje. De esta forma se reducen las probabilidades de que dos mensajes con diferentes longitudes den el mismo valor en su resumen.

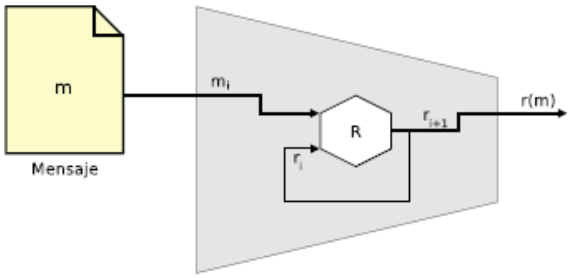

Gráfico 5: Estructura iterativa de una función resumen. R representa la función de compresión, m es el mensaje completo, *mi* el i-ésimo trozo de m, y *ri* la salida de la función en el paso i.

2.5.2 Algoritmo SHA-1.

La familia **SHA** (*Secure Hash Algorithm*, Algoritmo de *resumen* Seguro) es un sistema de funciones *hash* criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el *National Institute of Standards and Technology* (NIST). El primer miembro de la familia fue publicado en 1993 y se lo llamó oficialmente **SHA**. Sin embargo, ahora se le llama **SHA-0** para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de **SHA-1**. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: **SHA-224**, **SHA-256**, **SHA-384**, y **SHA-512** (llamándose **SHA-2** a todos ellos).

En 1998 se detectó un ataque a SHA-0, pero no fue reconocido para SHA-1, se desconoce si fue la NSA quien lo descubrió pero aumentó la seguridad del SHA-1.

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. No obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de *hash* con una estructura similar a SHA-1; lo que ha planteado dudas sobre la seguridad a largo plazo de SHA-1.

SHA-0 y SHA-1 producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 2^{64} bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.

En el 2005, la seguridad del algoritmo SHA-1 se ha visto comprometida por un equipo de investigadores chinos, compuesto por Xiaoyun Wang, Yiqun Lisa Yin y Hongbo Yu (principalmente de la *Shandong University* en China), quienes han demostrado que son capaces de romper el SHA-1 en al menos 2^{69} operaciones, unas 2000 veces más rápido que un ataque de fuerza bruta (que requeriría 2^{80} operaciones). Los últimos ataques contra SHA-1 han logrado debilitarlo hasta 2^{63}.

Según el NIST:

«Este ataque es de particular importancia para las aplicaciones que usan firmas digitales tales como marcas de tiempo y notarías. Sin embargo, muchas aplicaciones que usan firmas digitales incluyen información sobre el contexto que hacen este ataque difícil de llevar a cabo en la práctica.»

A pesar de que 2^{63} suponen aún un número alto de operaciones, se encuentra dentro de los límites de las capacidades actuales de cálculos, y es previsible que con el paso del tiempo romper esta función sea trivial, al aumentar las capacidades de cálculo y al ser más serios los ataques contra SHA-1.

La importancia de la rotura de una función *hash* se debe interpretar en el siguiente sentido: Un *hash* permite crear una huella digital, teóricamente única, de un archivo. Una colisión entre *hashes* supondría la posibilidad de la existencia de dos documentos con la misma huella digital.

A pesar de que el NIST contempla funciones de SHA de mayor tamaño (por ejemplo, el SHA-512, de 512 bits de longitud), expertos de la talla de Bruce Schneier abogan por, sin llamar a alarmismos, buscar una nueva función hash estandarizada que permita sustituir a SHA-1. Los nombres que se mencionan al respecto son Tiger, de los creadores de Serpent, y WHIRLPOOL, de los creadores de AES.

2.6 Gestión de Claves.

La gestión de claves son un conjunto de técnicas destinadas a generar, intercambiar, almacenar y destruir claves.

En el mundo real la gestión de claves es la parte más complicada de la criptografía: diseñar un algoritmo criptográfico seguro es relativamente menos

complicado que mantener una clave en secreto; esto es así porque es más fácil encontrar puntos débiles en las personas que en los algoritmos criptográficos. ¿De qué vale montar un sistema criptográfico muy avanzado en una organización, si luego hay empleados fáciles de corromper?

A continuación vamos a comentar varios aspectos fundamentales relacionados con la gestión de claves.

2.6.1 Generación de Claves.

La seguridad de todo el sistema depende de la clave, si un espía descubre la clave, de nada sirven todos los demás esfuerzos. Sin embargo, hay una serie de factores que influyen negativamente en la seguridad de la clave:

a) Pobre elección de la clave: Para evitar estos ataques, una técnica muy usada es recomendar a los usuarios utilizar **passphrases** en lugar de passwords, que es una frase a la que se hace un hash para obtener la clave.

b) Espacios de claves reducidos: Muchas veces sólo se aceptan subconjuntos del juego de caracteres como claves lo que implica que es fácil de romper la clave por fuerza bruta.

c) **Defectos en la generación de claves aleatorias**. Cuando se usan claves binarias (p.e. clave de sesión, o par de claves pública/privada), hay que tener cuidado de que el algoritmo que usemos realmente genere claves aleatorias. Muchos sistemas se han atacado aprovechando que la clave que generaba el sistema era predecible. Por ejemplo, las primeras implementaciones de SSL de Netscape generaban una clave de sesión en función de la hora, un espía podía predecir la clave de sesión que iba a generar el programa si sabía la hora del reloj del host donde se estaba ejecutando Netscape. Esta hora además la mandaba Netscape en sus cabeceras, y aunque no se supiera la hora exacta bastaba con saber la hora aproximada para hacer un ataque por fuerza bruta.

Un estándar para generación de claves muy conocido es ANSI X9.17.

2.6.2 Transferencia de claves.

Otro problema es el de cómo se ponen de acuerdo A y B en la clave a usar.

Una solución es que A y B se reúnan en un lugar físico y acuerden la clave que van a utilizar, pero esto no siempre es posible.

Otra posible solución es que partan la clave en trozos y envíen cada trozo por un canal distinto (correo, telegrama, teléfono, Internet), así el supuesto espía tendría que espiar todos los canales.

La técnica más usada para el intercambio seguro de claves se basa en la criptografía de clave pública y la veremos a continuación:

Básicamente consiste en que A y B usan criptografía asimétrica para acordar una clave de sesión que luego usan con su algoritmo simétrico para comunicarse; el protocolo es el siguiente:

1. B envía a A su clave pública.
2. A genera una clave de sesión aleatoria (binaria), la cifra usando la clave pública de B, y se la envía a B.
3. B descifra el mensaje enviado por A, usando su clave privada, y recupera la clave de sesión.
4. Ambos se comunican cifrando sus mensajes con la clave de sesión.

Pero este protocolo es vulnerable al ataque de “Man in the Middle” por lo que veremos a continuación el intercambio seguro de claves con firmas digitales.

2.6.2.1 Intercambio seguro de claves con firmas digitales

Podemos usar firmas digitales para evitar el man in the middle attack. Para ello necesitamos un árbitro que firme las claves públicas de A y B.

Una vez que A y B tienen sus claves públicas firmadas por el árbitro, el atacante no puede cambiar las claves de A y B, ya que no sabe firmarlas con la firma del árbitro.

Ahora, lo más que puede hacer el atacante activo es impedir que A y B se comuniquen, pero no puede escuchar la comunicación.

2.6.3 Almacenamiento de claves.

Las claves binarias (p.e. una clave privada) no las puede memorizar una persona, sino que hay que almacenarlas en disco, pero su almacenamiento en disco es peligroso porque alguien podría acceder a ellas. Para evitarlo las claves se almacenan cifradas con un password o passphrase.

Ahora la seguridad de la clave depende de dos factores:

1. Las posibilidades que tiene el espía de acceder al fichero (p.e en una máquina UNIX, si un usuario desactiva el permiso r de un fichero, los demás usuarios no pueden ver sus ficheros, pero el superusuario de la máquina sí que puede acceder a él).
2. La fuerza del password o passphrase que se usó para cifrar el fichero.

Otra alternativa consiste en almacenar las claves en tarjetas USB destinadas a este fin, de forma que las claves nunca permanecen en disco y si el espía quiere nuestra clave debería quitarnos la tarjeta. Esta solución tiene la ventaja de que podemos estar seguros de si alguien tiene acceso al sistema o no, ya que siempre podemos saber si tenemos la tarjeta en el bolsillo, o no.
Recuérdese que, un posible ataque que puede lanzar el espía para acceder a nuestra clave consiste en estudiar el fichero de memoria virtual del sistema. Este ataque es posible porque los sistemas operativos modernos paginan los programas de RAM a disco sin avisar, y nosotros nunca sabemos si la clave no se ha paginado a disco en mitad de la ejecución del programa.

2.6.4 Previsión de pérdida de claves

Imaginemos que A trabaja en una empresa que le obliga a cifrar todos sus ficheros. Y supongamos que A muere, entonces todos sus datos se pierden para siempre.
Para evitarlo podemos usar el algoritmo de compartición de secreto: A reparte su clave entre otros empleados de forma que un empleado, por sí solo, no puede acceder a los datos de A, pero si es necesario se pueden reunir todos los empleados y reconstruir la clave de A.

2.6.5 El ciclo de vida de una clave

Normalmente, no se recomienda mantener una clave durante mucho tiempo, ya que esto aumenta la probabilidad de que alguien la descubra, y si la descubre mayor será la cantidad de información a la que podrá acceder. Además la tentación que tiene el atacante por descubrirla será mayor si la clave no se cambia muy a menudo que si se cambia diariamente.

Por el contrario, los usuarios suelen ser reacios a cambiar regularmente sus claves, con lo que una solución de compromiso podría ser la **actualización automática de claves**, que consiste en que el sistema cambia periódicamente las claves como un hash de la clave anterior.

2.7 Firmas Digitales.

La firma digital es una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

Las firmas digitales, al igual que las firmas normales, se usan para conseguir básicamente cuatro objetivos:

1. **Integridad**. Una vez que el documento se firma, si luego se modifica se detecta el cambio.
2. **Autenticidad**. La firma convence al receptor del documento de que está firmado por quien aparece como firmante.
3. **Irreutilizabilidad**. Nadie puede copiar la firma de un documento a otro documento, y si lo hace la firma se detecta como inválida.
4. **Irrepudiabilidad**. El firmante no puede luego alegar que él no firmó el documento.

2.7.1 Firma de documentos con criptografía de clave secreta y árbitro

Se puede implementar un sistema de firmas digitales usando sólo criptografía de clave secreta y un árbitro.

Supongamos que A quiere firmar un documento y enviárselo a B. También supongamos que el árbitro comparte una clave secreta KA con A y otra clave secreta KB con B.

En este escenario, el protocolo para firmar documentos digitalmente podría ser:

1. A cifra el mensaje que quiere enviar a B firmado usando KA y se lo envía al árbitro.
2. El árbitro descifra el mensaje usando KA y lo guarda en su base de datos.

3. El árbitro cifra el mensaje plano usando KB y se lo envía a B.

4. B descifra el mensaje con KB.

El árbitro sabe que el mensaje proviene de A porque es el único que comparte la clave secreta KA con él.

B está seguro de que el documento recibido es auténtico ya que se lo ha enviado cifrado el árbitro, que es el único que (además de él mismo) conoce KB.

Este protocolo cumple con los cuatro objetivos que se consiguen con un protocolo de firma digital:

1. **Integridad**. Si el mensaje se modifica al enviarlo de A al árbitro o del árbitro a B, el proceso de descifrado falla.

2. **Autenticidad**. Como B confía en el árbitro, y es el único que comparte con el KB, sabe que el mensaje procede de A.

3. **Irreutilizabilidad**. Si B muestra mensajes firmados que A dice no haber firmado, pueden ir al árbitro que resuelve la disputa consultando su base de datos.

4. **Irrepudiabilidad**. Si A alega no haber firmado un documento que sí ha firmado, B puede ir al árbitro que determina que el documento sí que está en la base de datos.

Si B quiere demostrar a C la autenticidad de un documento firmado por A pueden seguir el siguiente protocolo:

1. B cifra el mensaje con KB y se lo envía al árbitro indicándole que quiere demostrar a C que el documento fue firmado por A.

2. El árbitro descifra el mensaje y comprueba en su base de datos que el documento fue firmado por A.

3. El árbitro vuelve a encriptar el mensaje con KC y se lo envía a C.

4. C desencripta el mensaje.

C confía en el árbitro, y sabe que el mensaje es auténtico porque sólo C y el árbitro conocen la clave secreta KC.

Como acabamos de ver, este protocolo funciona pero presenta dos inconvenientes:

• Debe existir un árbitro en el cual deben confiar todos.

• El árbitro se convierte en un cuello de botella.

Estos problemas los van a resolver los algoritmos criptográficos de firma con clave pública que vamos a ver a continuación.

2.7.2 Firma de documentos con criptografía de clave pública

La criptografía de clave pública es la técnica que se suele usar para generar firmas digitales. Tiene básicamente dos ventajas respecto a la técnica anterior:

• No necesita un árbitro.

• La clave privada, a diferencia de la clave secreta, no la tenemos que compartir con nadie.

Para firmar digitalmente un documento con técnicas de criptografía asimétrica, tal como se muestra en la siguiente tabla, se utiliza la clave privada para firmar, y la clave pública para comprobar la firma.

	Clave privada	**Calve Pública**
Confidencialidad	Descifrar	Cifrar
Firma digital	Firmar	Verificar

Tabla 1: Uso de las claves públicas/privadas para confidencialidad y firma digital

Realmente firmar es equivalente a cifrar con la clave privada, y verificar es equivalente a descifrar con la clave pública, con lo que a veces al proceso de firmar se le llama "cifrar con clave privada", y al de verificar "descifrar con la clave pública".

El protocolo que se sigue para firmar digitalmente un documento es:

1. A cifra el documento con su clave privada, dando lugar al documento firmado.
2. A envía el documento original y su firma a B.
3. B descifra el documento usando la clave pública de A, y verifica el documento, para ello el documento firmado descifrado debe ser igual al documento original. Es decir, si S(KprivadaA,M) es la firma (sign) del mensaje M usando la clave privada de A (KprivadaA), y V(KpúblicaA,M) es la verificación del documento M usando la clave pública de A, se cumple que:

V(KpúblicaA, S(KprivadaA,M)) = M

D(KpúblicaA, E(KprivadaA,M)) = M

Siendo E() la función de encriptación (cifrado) y D() la función de desencripción (descifrado).

Obsérvese que este protocolo, al igual que el anterior, también satisface los cuatro objetivos de las firmas digitales:

1. **Integridad**. Si se modifica el documento, la firma no coincide con la del documento y se detecta el cambio. Es decir, si un atacante modifica el documento tendría que modificar también su firma para evitar que se detecte el cambio, pero el atacante no conoce la clave privada necesaria para recalcular la firma.
2. **Autenticidad**. El receptor sabe que el documento está firmado por quien dice que lo ha firmado porque es el único que conoce la clave privada.
3. **Irreutilizabilidad**. Nadie puede copiar la firma de un documento a otro documento, y si lo hace la firma se detecta como inválida.
4. **Irrepudiabilidad**. El firmante no puede luego alegar que él no firmó el documento, porque él es el único que conoce la clave privada.

Respecto a las principales aplicaciones que tienen hoy en día las firmas digitales, vamos a comentar cuatro de ellas:

1. **Firmar e-mails**. Con S/MIME o PGP podemos firmar e-mails usando una clave privada, y luego el receptor del e-mail puede comprobar su autenticidad usando una clave pública.
2. **Firmar un contrato**. La mayoría de países (incluido Ecuador) ya ha introducido la firma digital como válida para firmar contratos.
3. **Crear servidores seguros**. Podemos diseñar servidores que firmen la información que sirven con el fin de que un atacante no la pueda modificar. Por ejemplo, los servidores DNS seguros firman los nombres DNS que resuelven.
4. **Identificación de usuarios frente al servidor**. Una forma más segura que la identificación por password es que el usuario al mandar una petición al servidor la firme digitalmente.

2.7.3 Algoritmos de firmas digitales más usados

Existen varios algoritmos para firmas digitales, pero los más usados son:

1. RSA, que además de usarse para criptografía de clave pública se puede usar también para firmar digitalmente.
2. DSA (Digital Signature Algorithm), que es un algoritmo propuesto en 1991 por el NIST (National Institute for Standards and Technology). DSA se diseñó con el fin de que sólo se pudiera usar para firmar, pero no para cifrar.

Una diferencia que hay entre RSA y DSA está en lo que respecta a la velocidad: DSA es más rápido para generar la firma que RSA, pero RSA es más rápido validando la firma. Como una firma se valida más veces que lo que se crea, de acuerdo a este criterio sería mejor RSA.

2.8 Protocolos de seguridad.

Un protocolo de seguridad es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica.

Existen varios protocolos de seguridad, entre ellos los más conocidos son:

- **SSL** (**S**ecure **S**ockets **L**ayer) (que vemos integrado en la mayoría de los navegadores (Netscape, Internet Explorer, Mozilla Firefox, etc.) y hace su aparición cuando el candado de la barra de herramientas se cierra y también si la dirección de Internet cambia de http a https.
- **PGP** es un protocolo libre ampliamente usado en intercambio de correo electrónico seguro
- **SET** que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito.
- **IPsec** que proporciona seguridad en la conexión de Internet a un nivel mas bajo.

Todos los protocolos de seguridad procuran resolver los problemas de la seguridad como la integridad, la confidencialidad, la autenticación y el no repudio (o no rechazo), mediante sus diferentes características

Por ejemplo sobre la seguridad por Internet se deben considerar las siguientes tres partes:

- Seguridad en el navegador (Netscape, Internet Explorer, etc)
- Seguridad en el Web server (el servidor al cual nos conectamos) y,

- Seguridad de la conexión.

2.8.1 Protocolo SSL.

SSL es el protocolo de comunicación seguro más conocido y usado actualmente, SSL se sitúa en la capa de aplicación, directamente sobre el protocolo TCP, y es como un túnel que protege a toda la información enviada y recibida.

Con **SSL** se pueden usar diferentes algoritmos para la encriptación, por ejemplo usa DES, TDES, RC2, RC4, MD5, SHA-1, DH y RSA.

El procedimiento que se lleva acabo para establecer una comunicación segura con **SSL** es el siguiente:

1) El cliente (browser) envía un mensaje de saludo al Servidor “ClientHello”
2) El servidor responde con un mensaje “ServerHello”
3) El servidor envía su certificado
4) El servidor solicita el certificado del cliente
5) El cliente envía su certificado: si éste es válido, continua la comunicación, caso contrario se suspende, o sigue la comunicación sin el certificado del cliente
6) El cliente envía un mensaje “ClientKeyExchange” solicitando un intercambio de claves simétricas si es el caso
7) El cliente envía un mensaje “CertificateVerify” si se ha verificado el certificado del servidor, en caso de que el cliente este en estado de autenticado.
8) Ambos cliente y servidor envían un mensaje “ChangeCipherSpec” que significa el comienzo de la comunicación segura.
9) Al término de la comunicación ambos envían el mensaje “finished” con lo que termina la comunicación segura, este mensaje consiste en un intercambio del hash de toda la conversación, de manera que ambos están seguros que los mensajes fueron recibidos intactos.

La versión más actual de **SSL** es la v3, existen otro protocolo parecido a **SSL** que es desarrollado por **IETF** que se denomina **TLS** (Transport Layer Security) y difiere en que usa un conjunto más amplio de algoritmos criptográficos. Por otra parte existe también **SSL** plus, un protocolo que extiende las capacidades de **SSL** y tiene por mayor característica que es interoperable con **RSA**, **DSA/DH** y **CE** (**C**riptografía **E**líptica).

Gráficamente, el procedimiento para establecer una comunicación segura con SSL es el siguiente:

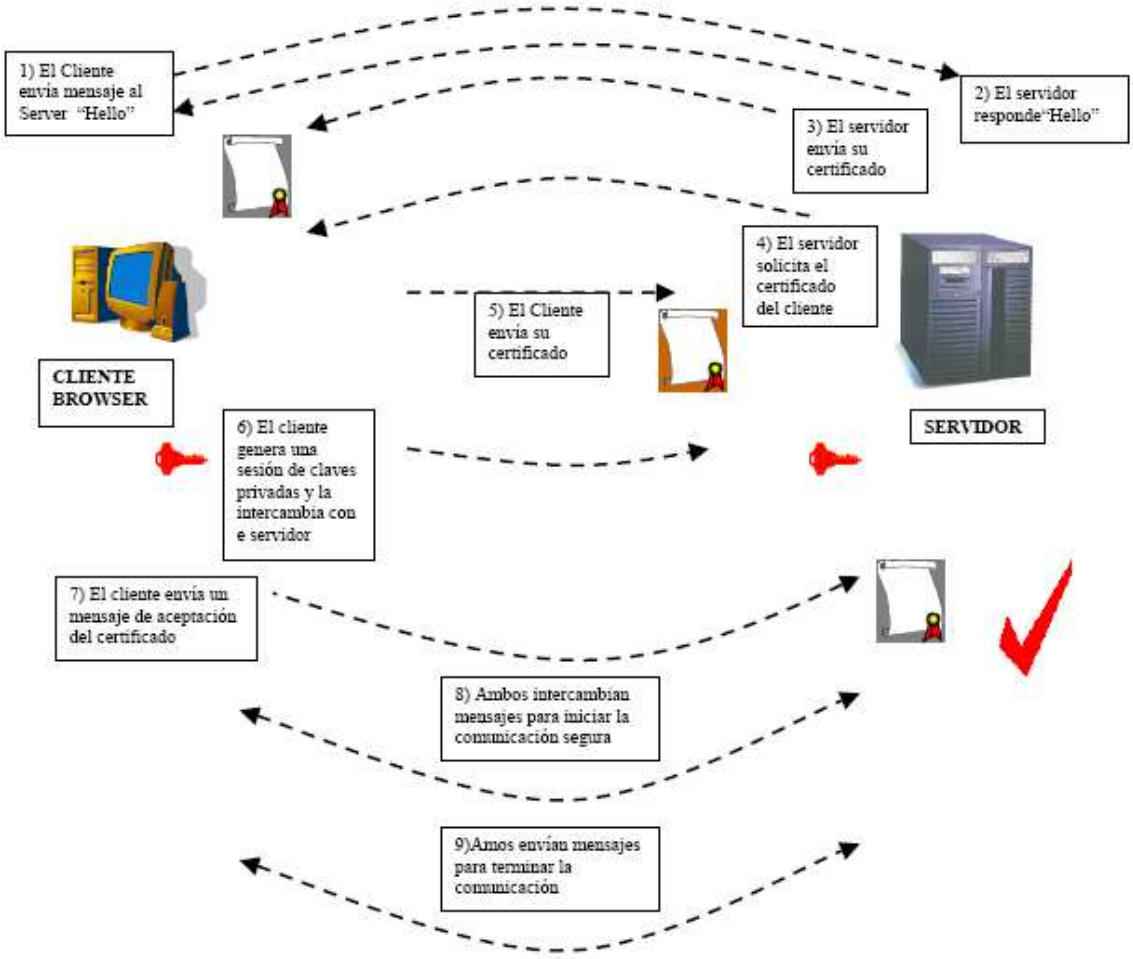

Gráfico 6: Establecimiento de comunicación con el protocolo SSL

2.8.2 Protocolo SET.

En 1985 las compañías Visa y MasterCard junto con otras empresas del sector tecnológico como RSA, IBM, Netscape, VeriSign, Microsoft, entre otras,

decidieron desarrollar un protocolo respaldado por la industria y estandarizado desde el primer momento. El propósito de este protocolo es favorecer las transacciones electrónicas con tarjetas de crédito a través de redes electrónicas.

SET trata de cubrir los agujeros de seguridad dejados por SSL. Por ejemplo con **SSL** solo se protege el número de tarjeta cuando se envía del cliente al comerciante, sin embargo no hace nada para la validación del número de tarjeta, para chequear sí el cliente esta autorizado a usar ese número de tarjeta, para ver la autorización de la transacción del banco del comerciante etc. Todas estas debilidades son cubiertas por **SET**, éste permite dar seguridad al cliente, al comerciante, al banco emisor de la tarjeta y al banco del comerciante.

El proceso de **SET** es el siguiente:

1) **El cliente inicializa la compra**: consiste en que el cliente usa el navegador para seleccionar los productos a comprar y llena la forma de orden correspondiente. **SET** comienza cuando el cliente hace clic en “pagar” y se envía un mensaje de iniciar **SET**.
2) **El cliente usando SET envía la orden y la información de pago al comerciante**: el software **SET** del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.
3) **El comerciante pasa la información de pago al banco**: el software **SET** del comerciante genera un requerimiento de autorización, éste es

comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.

4) **El banco verifica la validez del requerimiento**: el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.
5) **El emisor de la tarjeta autoriza la transacción**: el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.
6) **El banco del comerciante autoriza la transacción**: una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.
7) **El servidor del comerciante complementa la transacción**: el servidor del comerciante da a conocer que la transacción con la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.
8) **El comerciante captura la transacción**: en la fase final de SET el comerciante envía un mensaje de “captura” a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.
9) **El generador de la tarjeta envía el aviso de crédito al cliente**: el cargo de SET aparece en el estado de cuenta del cliente que se le envía mensualmente.

2.9 Sistemas o Medios de pago.

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

En este ámbito el comercio electrónico presenta una problemática semejante a la que plantea en otros sistemas de compra no presencial, 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.
- 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.

Se observa que al tratar los medios de pago en el comercio electrónico, se abordan fundamentalmente los temas de seguridad, garantía y acreditación.

Aún queda un requerimiento respecto a los medios de pago de cualquier tipo de comercio:

- El costo por utilizar un determinado medio de pago debe ser aceptable para el comprador y el vendedor.

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 micropagos.

Para realizar estos micropagos los sistemas suelen ser de uno de estos dos tipos:

1. El comprador adquiere dinero anticipadamente (prepago) para poder gastarlo en pequeños pagos.
2. 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.

Todo pago electrónico debe cumplir con los siguientes requisitos de seguridad:

- Autenticación
- Integridad
- Confidencialidad
- No repudio

2.9.1 Medios de pago más utilizados.

A continuación abordaremos algunos de los Medios de Pago con mayor uso en la Internet.

Tarjeta de crédito

La tarjeta de Crédito es el Medio de Pago más usado entre los ciberconsumidores. Esto se debe básicamente a su fácil uso, característica esencial de este medio de pago, y por la seguridad que brinda tanto al vendedor, ya que existe alguna entidad financiera que respalda al consumidor, así como para el consumidor ya que frecuentemente las Tarjetas de Crédito se encuentran amparadas por seguros. Asimismo, existe la confianza generalizada que las operaciones que se realizan utilizando Tarjetas de Crédito, están más que probadas y cuentan con todas las garantías.

Es fundamental tener en cuenta que para que la Tarjeta de Crédito tenga validez, ésta debe contener la denominación de la empresa que emite la tarjeta, así como el sistema de tarjeta de crédito al que pertenece; numeración codificada de la tarjeta; nombre del usuario de la tarjeta y su firma; fecha de vencimiento y la indicación expresa del ámbito geográfico de validez.

Tarjeta de débito:

Son tarjetas plásticas, magnetizadas y numeradas, que sirven para realizar compras de bienes y/o servicios a través de la Internet, en las tiendas virtuales en las que se permita el uso de estas tarjetas.

Estas tarjetas se encuentran asociadas a una cuenta de ahorros, que no genera intereses a favor del cliente ni gastos de mantenimiento, es decir a diferencia de la Tarjeta de Crédito, la entidad emisora no abre una línea de crédito, sino lo que va a responder por las obligaciones asumidas son los ahorros que se posean en una cuenta.

Para realizar la compra, se debe digitar el número de la tarjeta y la fecha de vencimiento de la misma, previa verificación que la tienda acepte este tipo de tarjetas y que sea una zona segura.

Dinero electrónico o digital:

El Dinero Electrónico o Digital es un sistema para adquirir créditos de dinero en cantidades relativamente reducidas. Este sistema consta de unidades o símbolos de valor monetario, debidamente cifrado que representa cantidades de dinero, que asumen forma digital; unidades que pueden ser convertidas en dinero físico. Este dinero electrónico se almacena en la computadora y se transmiten a través de redes electrónicas para ser gastado al hacer compras electrónicas a través de Internet.

Teóricamente, el Dinero Electrónico o Digital podría utilizarse para cancelar compras por montos pequeños, hasta décimas de centavo de dólar o menos. Sin embargo, la mayoría de los comerciantes que aceptan dinero electrónico hasta el momento, lo emplean como una alternativa a otras formas de pago de adquisiciones de precio un tanto superior.

El Dinero Electrónico funciona de la siguiente manera (para el consumidor):

El primer paso es afiliarnos a un banco que ofrezca este sistema de Dinero Electrónico, luego debemos suscribir un contrato con alguna empresa proveedora del sistema, la cual nos proporcionará el software para instalarlo en la computadora. Este software permite bajar el dinero electrónico al disco duro de la computadora. La adquisición inicial de dinero se realiza contra nuestra cuenta bancaria o una tarjeta de crédito.

Una vez instalado el software en la computadora, procederemos a realizar nuestras compras en la red, para lo cual debemos simplemente hacer click en el botón de pago y el software de la tienda generará una solicitud de pago describiendo la mercancía, el precio, la fecha y la hora.

Una vez generada la solicitud y siempre que aceptemos, el software resta la cantidad del precio y crea un pago que es enviado al banco, verificado y luego depositado en la cuenta de la tienda virtual. Una vez que se ha concluido este proceso se notifica a la tienda virtual y ésta envía la mercancía que hemos comprado.

Entre los sistemas de dinero electrónico o digital más usados en la actualidad tenemos el CyberCash, pariente de CyberCoin, E-cash y el sistema DigiCash.

Tarjetas inteligentes o smarts cards

Las tarjetas inteligentes son tarjetas de plástico similares en tamaño y otros estándares físicos a las tarjetas de crédito que llevan estampadas un circuito integrado. Este circuito puede ser de sola memoria o contener un microprocesador con un sistema operativo que le permite una serie de tareas como: almacenar, cifrar información y leer y escribir datos, como un ordenador.

Como mecanismo de control de acceso las tarjetas inteligentes hacen que los datos personales y de negocios solo sean accesibles a los usuarios apropiados, esta tarjeta asegura la portabilidad, seguridad y confiabilidad en los datos.

Entre sus características más importantes encontramos:

1 Inteligencia: Es capaz de almacenar cualquier tipo de información, además es autónoma en la toma de decisiones al momento de realizar transacciones.
2 Utiliza clave de acceso o PIN: Para poder utilizarse es necesario digitar un número de identificación personal, es posible además incorporar tecnología más avanzada como identificación por técnica biométrica, huella digital o lectura de retina.
3 Actualización de cupos: Después de agotado el cupo total de la tarjeta inteligente es posible volver a cargar un nuevo cupo.

Tarjeta relacionista:

Es una tarjeta que posee un microcircuito que permite la coexistencia de diversas aplicaciones en una sola tarjeta, es decir que funcione como tarjeta de crédito, tarjeta de débito, dinero electrónico, etc. Esta tarjeta presentará en un sólo instrumento la relación global entre el cliente y su banco.
Actualmente, VISA tiene como proyecto la creación de esta tarjeta, pues para esta firma la tarjeta relacionista expresa perfectamente la idea que poseen sobre la tarjeta del futuro.

Monederos electrónicos y dinero electrónico:

Son tarjetas prepago que contienen un fondo de pago materializado en un chip que tienen incorporado, en el que se almacenan elementos o unidades de valor que previamente se han incorporado con cargo a la cuenta propia o mediante su carga con efectivo, y siempre por un importe determinado que permite ir pagando hasta que dicho importe se agote, pudiendo ser recargable o desechable; con lo cual, y por sus propias características, están diseñadas para pequeños pagos en efectivo.

Para el consumidor tiene la ventaja de no tener que pagar ni recibir continuamente cambio en monedas

Cada vez será más habitual en la sociedad de la información tener instalado en el ordenador o en aparatos técnicos (como terminales de televisión digital) tarjetas monedero, en alguna de las modalidades arriba descritas, para realizar pequeñas compras, pues el importe de éstas no puede superar el de la tarjeta, no existiendo por ello, al igual que ocurre con las tarjetas de débito, riesgo de impago.

Por otra parte, con el software adecuado, existe ya la posibilidad de transferir dinero de la cuenta bancaria particular al propio disco duro del ordenador, a través de una red de comunicación, consiguiendo así tener dinero para su uso posterior.

Actualmente, el dinero electrónico se enfrenta a algunas cuestiones desanimadoras, debido a que para poner este sistema de pago en funcionamiento, los consumidores han de instalar en su computadora programas específicos; que representan un costo adicional a corto plazo. Asimismo, existen pocas tiendas virtuales que poseen estos programas, con lo cual no se puede utilizar en toda la red; además de provocar una acumulación de pequeñas facturas que no es del agrado de la mayoría de los consumidores.

Pago mediante móvil

La generalización del teléfono móvil en los últimos años ha llevado a algunas empresas telefónicas a desarrollar sistemas basados en el teléfono móvil. La primera experiencia europea se produjo en Italia de la mano de la compañía Omnipay (http://www.omnipay.it).

El usuario de este medio de pago puede optar por dos opciones:

a) Un sistema de pago basado en tarjetas prepago (a imagen de las populares tarjetas telefónicas).

b) Otro, en cargo indirecto a la tarjeta de crédito del usuario, previa confirmación telefónica del pago.

2.9.2 Tecnología.

Un entorno seguro debe basarse en el uso intensivo de la firma electrónica avanzada. De esta forma se aúnan aspectos tecnológicos y legales para resolver los requisitos necesarios que garanticen la seguridad de las transacciones en la red: Autenticación, confidencialidad, no-repudio e integridad de los datos.

Tecnológicamente estos requisitos se resuelven mediante una infraestructura compuesta por un conjunto de políticas, prácticas, estándares y leyes que emergen de tecnología de clave pública. Esta tecnología, se basa en la criptografía asimétrica, donde se emplean un par de claves electrónicas: Una para la codificación y la otra para la decodificación de documentos. La infraestructura se completa con la figura de la Autoridad de Certificación (CA) de quien es responsabilidad asegurar la autenticidad de las claves públicas.

III. ANALISIS DE HERRAMIENTAS DE COMERCIO ELECTRONICO DE LIBRE DISTRIBUCION.

3.1 Introducción

Hoy en día, en la red Internet, existen a disposición muchas herramientas de comercio electrónico tanto de libre distribución como comerciales, cada una con sus diferentes particularidades y niveles de complejidad, por lo que en el presente trabajo lo que se ha pretendido es realizar un análisis de las herramientas de libre distribución más populares y de entre ellas seleccionar la más adecuada de acuerdo a criterios importantes como facilidad de uso, buena administración, velocidad y, algo sumamente importante, de fácil mantenimiento que es de vital importancia para su implementación y adaptación a las necesidades propias de cada empresa o persona que lo adopte.

3.2 Análisis de software de comercio electrónico open source.

En la actualidad, son cada vez más los comerciantes y emprendedores interesados en el comercio electrónico. Afortunadamente, hoy en día es muy fácil encontrar gran cantidad de software de comercio electrónico open source para hacer una tienda en línea y así ofrecer productos y servicios a potenciales clientes ubicados en cualquier parte del mundo. A continuación se presenta una lista muy resumida de dicho software con sus principales características:

osCommerce: Este es sin duda el más conocido de todos los programas para tiendas en línea y ha servido de inspiración a una gran cantidad de sucesores. Está dando vueltas en el mundo de la Internet desde el año 2000. Su creador es Harald Ponce de Leon. La comunidad que lo respalda es bastante numerosa, superando los 200.000 miembros. Debido al tiempo que tiene en el mercado, cuenta con mucha documentación, módulos (más de 5.000), ayuda y tutoriales en numerosos foros y páginas Web que se dedican al tema. Tiene una gran madurez lo que hace que sea muy robusto y confiable. El punto débil es que se ha rezagado con respecto a los estándares actuales. El diseño está basado en tablas, lo cual está en desuso y hace que cambiar la apariencia de

la tienda sea un tanto difícil. También parece que entró como en una especie de abandono, ya que la última versión estable 2.2 RC 2a (que no es exactamente una versión final, sino una Release Candidate) es de Enero del 2008, y la versión sustituta 3.0, que contempla una re-escritura del código para incorporar un sistema de plantillas que permita cambiar el aspecto de la tienda fácilmente, un re-diseño del panel de administración y uso de programación orientada a objetos, apenas va por la versión Alpha 5, y no ha habido cambios desde Marzo de 2009. Pero sin duda, sigue siendo una referencia a tomar en cuenta, y actualmente existen una gran cantidad de tiendas en línea que funcionan usando osCommerce.
Página Oficial: http://www.oscommerce.com
Página Demo: http://www.oscommerce.com/shops/demonstration

Requisitos:

- Apache
- PHP 3.0 o superior
- MySQL 4.0 o superior

Magento: Aplicación desarrollada por la empresa estadounidense Varien, fue lanzada oficialmente el 31 de Marzo de 2008. Su arquitectura se basa en el modelo MVC (Modelo, Vista, Controlador) y utilizaron Zend Framework para su programación. A pesar de que el 15 de Abril de 2009 presentaron la versión Enterprise, que tiene un costo bastante elevado, podemos tener acceso totalmente gratuito a la versión Community. La diferencia entre ambas radica en ciertas funcionalidades añadidas a la versión Enterprise, además del soporte y garantía con las que esta última cuenta. Pero el núcleo (*core)* como tal es el mismo para ambas. Lo que llama la atención de este software de tienda virtual son todas las funcionalidades que tiene. Además, tiene la particularidad de que permite crear diseños innovadores debido a su sistema de *layouts*, pudiéndose asignar *vistas* distintos a productos o categorías específicos. En la actualidad cuenta con una comunidad que supera los 180.000 miembros registrados, foros en distintos idiomas y más de 1.700

extensiones (entre gratuitas y comerciales), que pueden ser instaladas de forma muy sencilla, para agregar alguna característica adicional que se necesite. A eso le podemos sumar una gran campaña de marketing desarrollada por Varien, lo cual hace que Magento sea muy dinámico y esté en constante renovación.

Su punto débil es que requiere de un servidor bastante potente, ya que la aplicación consume muchos recursos. Otra desventaja es su extrema complejidad (la última versión 1.4.0.0 pesa casi 55MB, tiene más de 9.000 archivos ubicados en más de 3.000 carpetas y la base de datos tiene 273 tablas), por lo que no es nada sencillo realizar modificaciones al mismo. Claro que esto mejora a medida que uno se familiariza con su estructura, pero definitivamente la curva de aprendizaje es mucho mayor en comparación con otras opciones disponibles que veremos a continuación.

Página Oficial: http://www.magentocommerce.com

Página Demo: http://www.magentocommerce.com/demo

Requisitos:

- Apache
- PHP 5.0 o superior
- MySQL 5.0 o superior

Prestashop: Fue creado por un grupo de estudiantes de informática franceses en 2005. Más adelante, el proyecto toma mayor seriedad cuando en Agosto de 2007 lanzan la primera versión estable. Está basado en el motor de plantillas Smarty, y también se hace uso de AJAX. Es un script muy liviano, por lo que no exige demasiado en cuanto a servidor se refiere. Cuenta con un buen número de funcionalidades, que lo convierte en una opción muy completa para hacer una tienda en línea. Modificar su código fuente es relativamente sencillo, y además se pueden instalar módulos adicionales (gratuitos o comerciales) para ampliar sus funcionalidades. Su comunidad va en constante ascenso, contando actualmente con más de 50.000 miembros. Igualmente tiene un foro con

distintos idiomas, en los que sus lectores pueden aclarar dudas y compartir experiencias.
Página Oficial: http://www.prestashop.com
Página Demo: http://www.prestashop.com/es/showcase_demo/

Requisitos:

- Apache
- PHP 5.0 o superior
- MySQL 5.0 o superior

OpenCart: Es un proyecto relativamente joven, pero no por eso deja de ser interesante. Al igual que Magento, su arquitectura se basa en el modelo MCV (Modelo Vista Controlador), pero es muchísimo más sencillo y liviano que éste. Fue creado por el inglés Daniel Kerr. Además que su instalación es muy sencilla, es notable su sencillez y rapidez, combinadas con suficientes funcionalidades como para poder crear una tienda en línea bastante completa.
Al igual que la mayoría de software de tiendas virtuales, se pueden agregar módulos para añadir características adicionales. Cuenta con una aceptable documentación y un foro para aclarar dudas y compartir conocimientos. La comunidad es un tanto pequeña aún (unos 6.000 miembros), pero va en constante aumento. Al igual que en la mayoría de software aquí analizado, se pueden instalar módulos adicionales (gratuitos o comerciales) para ampliar sus funcionalidades.
Respecto a la organización de productos por categorías y la introducción de artículos son sus puntos fuertes, con grandes facilidades, sencillos editores donde podremos añadir todas las características de nuestro artículo y una buena galería de fotos del producto para ayudar a que el comprador tenga toda la información a su disposición.
Este software se destaca por su sencillez de manejo tanto en la tienda como en el módulo de administración, siendo además su código bastante bien estructurado, lo cual ha hecho que me incline por este Software para realizar un estudio más detenido del mismo. Su última versión estable es la versión 1.4.

3.3 Estudio de Opencart.

Como ya mencioné en las líneas anteriores, este software opensource es uno de los mejores si comparamos velocidad, estructura, facilidad de manejo y curva de aprendizaje para su mantenimiento. Su página oficial es http://www.opencart.com, además, se puede acceder a una demostración en línea de sus funcionalidades en la siguiente dirección:
http://www.opencart.com/index.php?route=information/demonstration
Existe también un sitio web de opencart en español: www.opencartspanish.com desde el cual se puede obtener acceso a cierta información en español así como la posibilidad de bajarse el software.

3.3.1 Requisitos:

- Apache 2.0 o superior, o Internet Information Server (IIS)
- PHP 5.0 o superior
- MySQL 5.0 o superior
- Sistema Operativo: cualquiera en donde se pueda instalar los 3 requisitos anteriores.

3.3.2 Características:

OpenCart está diseñado con unas características muy completas, fácil de usar, potente, rápida y con un interfaz visualmente atractivo. Hoy en día según muchas valoraciones y estadísticas que hay en Internet es quizás la mejor (o una de las mejores) de entre todas las existentes de código abierto, comparando rapidez, sencillez y eficacia. Sus principales características son:

- Fácil instalación y administración
- Estructura totalmente abierta
- Soporta SSL
- Categorías Ilimitadas
- Artículos Ilimitados
- Fabricantes Ilimitados
- Múltiples Monedas

- Múltiples Lenguajes (18), entre ellos: Inglés, Español, Francés, Chino, Italiano.
- Comentarios en artículos
- Valoración de artículos
- Código abierto Open Source
- Documentación Gratis (Inglés), aunque no muy extensa.
- Plantillas intercambiables
- Redimensionado de Imágenes
- Múltiples formas de pago (más de 25)
- Varios medios de transporte (más de 8)
- Ampliación de módulos.

3.3.3 Estructura: Opencart consta de 2 módulos claramente definidos:

a) Front End (Tienda en línea) y,
b) El módulo de administración de la misma.

Opencart usa un patrón de diseño denominado MVC(+L) (Model, View, Controller o Modelo, Vista y Controlador) (+Lenguaje), el mismo que fue diseñado para reducir el esfuerzo de programación necesario en la implementación y mantenimiento de sistemas. Sus características principales son que los Modelos, las Vistas y los Controladores se tratan como entidades separadas.

El Modelo se encarga de todo lo que tiene que ver con la persistencia de datos. Guarda y recupera la información del medio persistente que utilicemos, ya sea una base de datos, ficheros de texto, XML, etc.

La Vista presenta la información obtenida con el modelo de manera que el usuario la pueda visualizar.

El Controlador, dependiendo de la acción solicitada por el usuario, es el que pide al modelo la información necesaria e invoca a la plantilla (de la vista) que corresponda para que la información sea presentada.

Así, para cada página del producto en la parte de vista al público (frontend), hay 4 ficheros maestros:

M: \catalog\model\catalog\product.php

V: \catalog\view\template\product\product.tpl

C: \catalog\controller\product\product.php

L: \catalog\language\english\product\product.php

De modo similar, en la parte del administrador (backend), para el mantenimientote los productos por ejemplo, serán necesarios 4 ficheros que se distribuyen de la siguiente manera:

M: \admin\model\catalog\product.php

V: \ admin \view\template\product\product.tpl

C: \ admin \controller\product\product.php

L: \ admin \language\english\product\product.php

3.3.4 Análisis comparativo:

Una vez realizado el estudio de los principales programas para tiendas virtuales disponibles, es conveniente resumir en una tabla las características más relevantes de cada uno de ellos, sobresaliendo en algunos aspectos el software Opencart, motivo por el cual me ha llevado a realizar un estudio más profundo del mismo y a tomar como base para implementar los cambios requeridos para generar una factura acorde a las leyes ecuatorianas.

	OpenCart	osCommerce	PrestaShop
Open Source	SI	SI	SI
Documentación	SI*	SI	SI*
Categorías Ilimitadas	SI	SI	SI
Productos Ilimitados	SI	SI	SI
Fabricantes Ilimitados	SI	SI	SI
Templates Intercambiables	SI	NO	SI
Multi Lenguaje	SI	SI	SI
Multi Moneda	SI	SI	SI
Comentarios en Productos	SI	SI	NO
Valoración de Productos	SI	SI	NO
Descarga de productos	SI	SI	NO
Autoredimensionado de imágenes	SI	NO	SI
Productos Relacionados	SI	NO	NO
Cálculo de peso de envío	SI	SI	SI
Sistema de cupones de descuento	SI	NO	SI
Optimización Motores de búsqueda	SI	NO	SI
Sistema de módulos	SI	SI	SI
Copia/Restauración de Base de Datos	SI	SI	SI
Reportes de Ventas	SI	SI	SI

Tabla 2: Cuadro comparativo de software de tiendas virtuales

* Existe documentación básica pero no suficiente.

3.3.5 Instalación: La instalación de la tienda virtual es muy simple, solamente hay que seguir un pequeño procedimiento, el mismo que explicaré más adelante.

Antes de comenzar la instalación es requisito indispensable tener instalado y funcionando toda la plataforma sobre la cual se va a montar la tienda virtual, esto es:

- Apache
- PHP 5.0 o superior
- MySQL 5.0 o superior

Procedimiento: El procedimiento a seguir para la instalación es similar tanto para Linux como para Windows.

1. Subir todos los archivos y carpetas que se encuentran en la carpeta "Upload" a un directorio en donde va a funcionar la tienda virtual.

Se puede ubicar la tienda en el directorio principal o en el subdirectorio que se elija. Ejm.: /public_html/tienda o /wwwroot/tienda

2. Asegurarse de que las siguientes carpetas tienen permiso de escritura.

    image/
    image/cache/
    cache/
    download/
    config.php
    admin/config.php

3. Asegurarse que se haya creado una Base de datos MySQL con un usuario asignado a la misma.

4. Dentro de un navegador, dirigirse a la página principal de la tienda. Ejm.: http://localhost/tienda

5. Proceder a la instalación siguiendo las instrucciones que le aparecen en pantalla.

6. Borrar completamente el directorio install.

Las imágenes del proceso de instalación son las siguientes:

1. Pantalla de licencia: Solicita aceptación de los términos de la licencia.

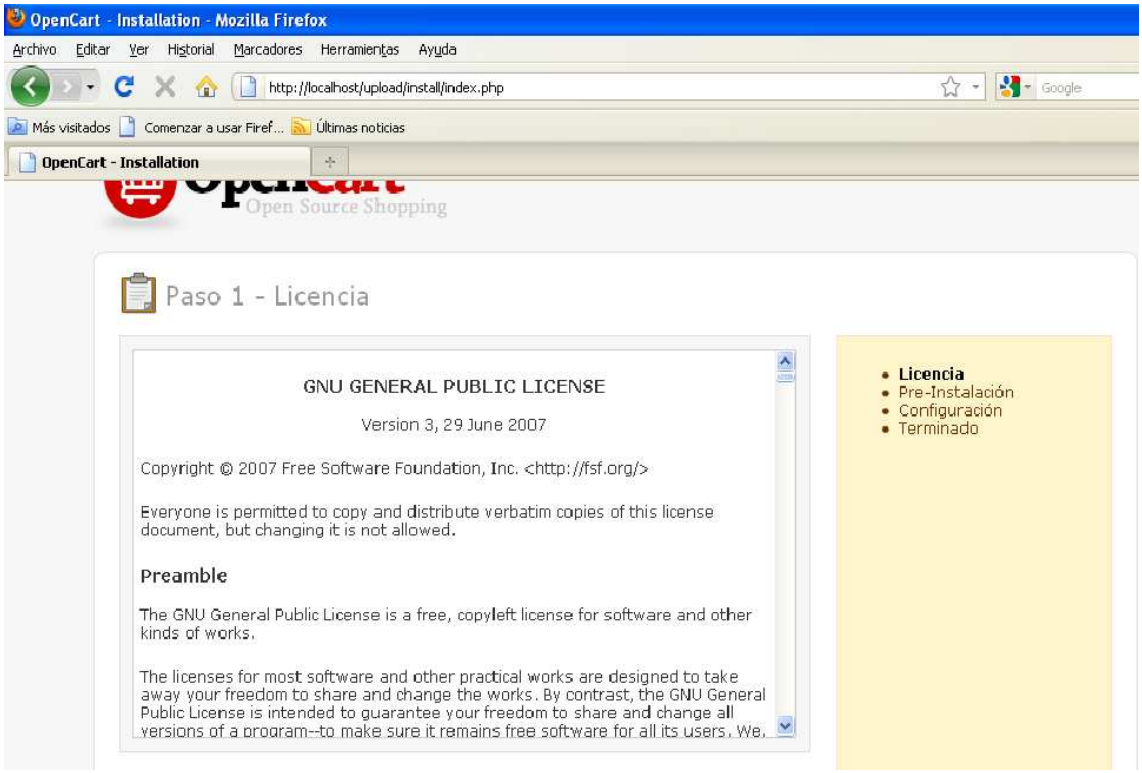

Gráfico 7: Instalación de OpenCart – Paso 1

2. Preinstalación: Muestra el estado de los prerrequisitos.

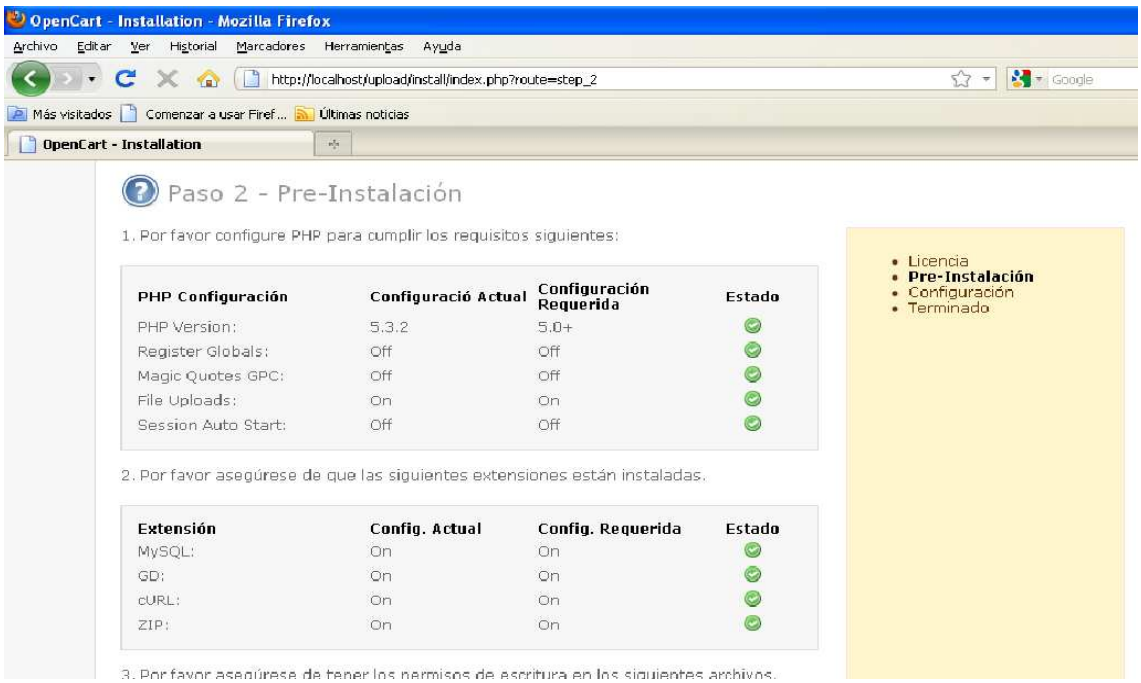

Gráfico 8: Instalación de OpenCart – Paso 2

3. Configuración: Permite especificar datos de la conexión con la base de datos, así como usuario y clave para la administración de la tienda.

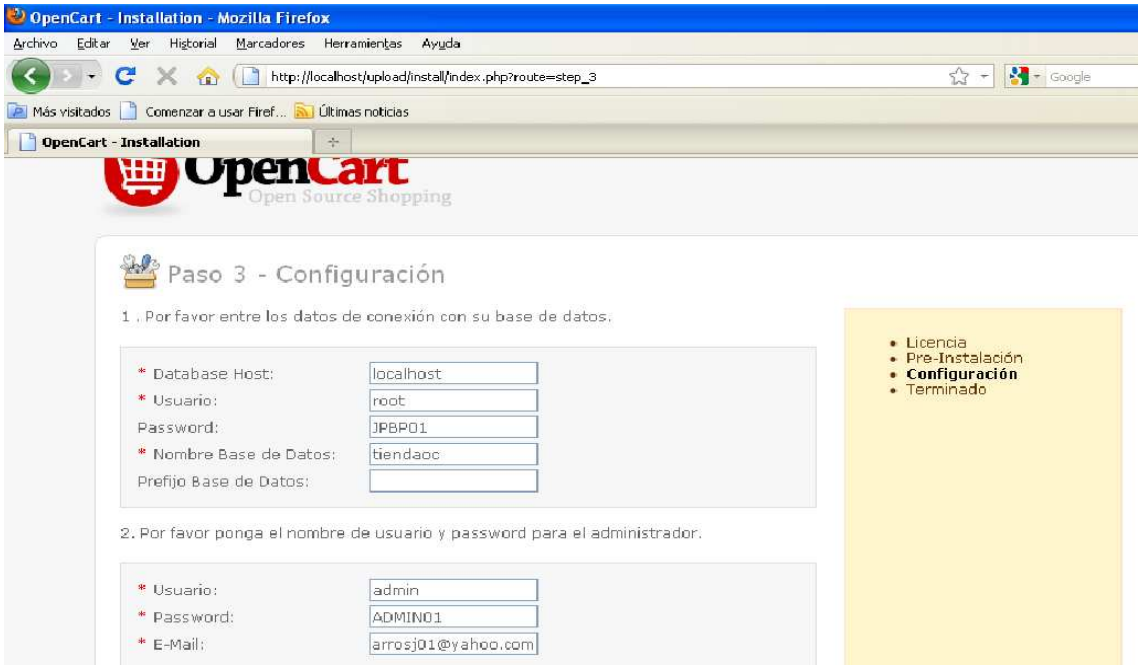

Gráfico 9: Instalación de OpenCart – Paso 3

4. Finalización. Pantalla que nos informa que la instalación se ha completado y permite ingresar ya sea al módulo de administración o a la tienda virtual.

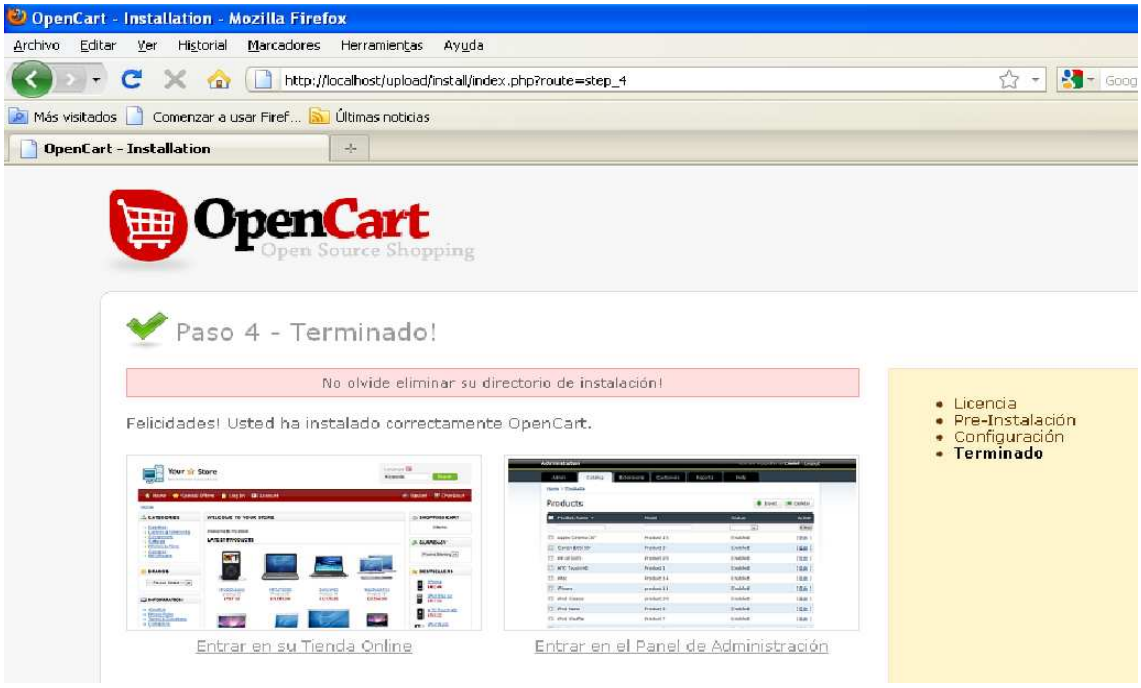

Gráfico 10: Instalación de OpenCart – Paso 4

3.3.6 Configuración y administración: Una vez instalada la aplicación, es necesario realizar la configuración correspondiente para que quede acorde a los requerimientos (Datos de la tienda, Localización, ajustes extras). Dicha configuración se lo debe realizar desde el módulo de Administración. Ejm: http://localhost/upload/admin/index.php dentro de la cual se debe autenticar con la información proporcionada al instalar la aplicación, así: usuario: admin, contraseña: ADMIN01.

Dentro de la opción de configuración existen 6 pestañas para dejar a punto la tienda antes de su funcionamiento:

1. Tienda: datos referentes a la tienda (Nombre, Título, Dirección, Propietario, etc)
2. Local: Aquí se definen los datos referentes a la localidad en donde se encuentra la tienda, además de moneda, idioma, medida, peso.
3. Opción: Permite definir varias opciones como permitir vender sin stock, actualizar stock al vender, mostrar stock, permitir comprar como invitado, etc.
4. Imagen: Presenta opciones para definir el logotipo, cambiar tamaños de las imágenes de productos, categorías, carrito de compras.
5. Correo: Para digitar la configuración correspondiente al correo (Protocolo, servidor, usuario, contraseña, puerto).
6. Servidor: Definir si se usa SSL, digitar clave de encriptación para pedidos, nivel de compresión, registro de errores.

Una vez llenados estos datos estamos listos para realizar compras en línea a través de la tienda virtual.

3.3.7 Navegación por la tienda virtual.

Ahora solo nos queda navegar por la tienda virtual, para lo cual, en nuestro caso, entramos en: http://localhost/upload/index.php.

De aquí en adelante únicamente debemos navegar por los productos que deseamos comprar y agregar al carrito de compras (Cesta) para realizar el pedido.

IV. DISEÑO E IMPLEMENTACION DEL PROTOTIPO.

4.1 Elementos básicos que intervienen en un sistema de tienda electrónica.

Antes de describir el prototipo, es conveniente presentar los principales elementos que intervienen en un sistema de tienda electrónica:

4.1.1 Catálogo de productos

El catálogo de productos y servicios es la carta de presentación a los clientes. Por tanto se debe prestar mucha atención y cuidado a la hora de seleccionar qué productos y servicios se van a ofrecer, y cómo se los va a mostrar y destacar.

La presentación de los productos es muy importante ya que debe transmitir confianza y seriedad a los clientes. El uso de fotografías reales de los productos y una buena descripción del producto, contribuyen a incrementar estos aspectos.

De igual forma, se debe acompañar los productos con información complementaria multimedia (videos, PodCast, otros) o incluso documentos pdf.

4.1.2 Carrito de compra.

La cesta o carrito de compra es un elemento indispensable en la Tienda Online. Este elemento debe ofrecer la posibilidad de añadir, eliminar o modificar los productos que durante la navegación hemos ido seleccionando e incorporando. Es aconsejable, para que el usuario no pierda de vista en ningún momento lo que lleva comprado, que esté visible en todas las páginas de la Tienda Online, o al menos en aquellas donde se puedan seguir añadiendo productos.

De igual forma, se debe dar la posibilidad, con un solo clic, que el cliente pueda visualizar de una forma clara:

- Las referencias comprada (especificando la cantidad).
- Los gastos de envío.
- Impuestos aplicables de forma directa.
- Importe total del pedido

4.1.3 Mecanismos de promoción y ofertas.

Uno de los factores más importantes que atraen a los clientes de una Tienda Online e influyen en la decisión de compra es el precio. El precio de los productos debe estar siempre bien visible.

Pero alrededor de una captación de clientes por el precio tenemos varias estrategias comerciales que pasan por la aplicación de promociones o descuentos especiales sobre los productos.

Las promociones y las ofertas deben comunicarse de una forma clara, resaltando el precio de la oferta y mostrando junto a él, el precio no rebajado.

4.1.4 Motor de búsqueda.

Con la idea de facilitar al cliente encontrar los productos y servicios es indispensable disponer de un potente motor de búsqueda o buscador integrado que permita la búsqueda de productos por diversos criterios y parámetros de búsqueda. Criterios de interés son las búsquedas por palabras clave, precio, categoría, nombre, etc.

El motor de búsqueda siempre debería ofrecer resultados para dar la sensación de robustez y buen funcionamiento. En caso de no poder mostrar resultados exactos a nuestra búsqueda es deseable que el buscador ofrezca otras sugerencias relacionadas con el producto buscado.

De esta forma no comentemos el error de que el buscador parezca que no funciona, o que el catálogo de productos es muy reducido.

4.1.5 Proceso de compra.

Se considera un buen proceso de compra aquel que es directo y se encuentra guiado mediante mensajes de información. Se suele aconsejar que el *registro de usuarios sea opcional*. No es aconsejable que para efectuar una compra obliguemos a los visitantes a registrarse previamente ya que muchos compradores potenciales pueden ser sólo ocasionales. En cualquier caso, la información que solicitemos para que un cliente pueda realizar un pedido en la tienda debe ser la mínima imprescindible.

Idealmente se debe plantear que la duración del proceso de compra implique el menor número posible de pasos y clicks de ratón (5 clicks de ratón o menos es un número idóneo).

Es importante que durante el proceso de compra se muestre *información complementaria* que transmita confianza a los usuarios, y que a éstos al terminar la compra no les quede ninguna duda respecto a la compra que acaban de hacer.

4.1.6 Medios de Pago.

El momento del pago de los artículos que el cliente ha ido añadiendo en el carrito de la compra es uno de los pasos más críticos dentro de los procesos de una Tienda Online pues, estadísticamente, es en ese momento en el que se dan más abandonos.

Para evitar que el cliente abandone el proceso de compra que ha iniciado es fundamental ofrecerle el mayor número de posibilidades y flexibilidad a la hora de seleccionar la forma de pago del pedido que ha realizado.

4.1.7 Impuestos.

Los precios de los productos o servicios que se publiquen en la página web de la Tienda Online deben ser los precios finales completos, incluidos todos los impuestos, tasas y demás gravámenes aplicables.

Asimismo, la Tienda Online debe tener en cuenta e informar de forma clara al consumidor de las posibles tasas, impuestos o gravámenes que puedan ser de aplicación en función del lugar de residencia del consumidor o del lugar de entrega del producto o servicio, antes de la realización del pedido. Finalmente, la tienda online en la factura o en el e-mail de confirmación del pedido deberá señalar el tipo y la cuota del impuesto, tasa o gravamen aplicados.

4.1.8 Logística.

Al igual que los impuestos, la Tienda Online debe ofrecer de forma clara el coste por el envío de la mercancía adquirida. En este sentido, debe permitir configurar una matriz de gastos de envío para cada transportista y ofrecer la

posibilidad de calcular los gastos de envío en función de volumen de compra, peso, etc.

4.1.9 Información Corporativa.

Dentro de una Tienda Online no toda la información deben ser escaparates de productos. Es necesario mostrar al comprador información de la empresa, que entienda la filosofía de negocio, la trayectoria empresarial, etc. Este tipo de información transmite transparencia, fiabilidad y confianza hacia los clientes.
Esta información suele estructurarse en secciones como:

- Quiénes somos
- Qué ofrecemos
- Aviso Legal y Política de Privacidad
- Información de contacto
- Dónde estamos
- Condiciones de compra y contratación
- Preguntas Frecuentes
- Otros

4.2 Descripción General del prototipo.

En vista de que el modelo de tienda virtual escogido para el estudio tiene la mayoría de elementos ya implementados, más que realizar un prototipo, he realizado una revisión profunda de sus diferentes partes y se han hecho modificaciones puntuales, por lo que el software producto del presente trabajo será un producto Opencart modificado y configurado de acuerdo a los impuestos que rigen en el Ecuador (12% IVA, Punto de emisión y serie en impresión de facturas) y con opción a la forma de pago de Paypal configurada para realizar pruebas de pago seguro sin afectar datos reales (Sandbox).
Como ya se mencionó en el capítulo anterior, el software OpenCart puede ser montado sobre cualquier plataforma (Linux, Windows, etc) que soporte Apache, PHP y MySql.
Para guardar coherencia con el tipo de licencia de Opencart (opensource) esta versión modificada será instalada sobre plataforma LINUX y, utilizando para

ello herramientas de libre distribución tales como servidor Web Apache, base de datos MySql y Lenguaje de programación PHP. Sus principales características son:

- El usuario (cliente) podrá navegar por los productos y realizar el pedido de acuerdo con la disponibilidad de los mismos. Además, el sistema permitirá realizar una búsqueda independiente de productos, sin necesidad de navegar por las diferentes categorías.
- Una vez que el cliente haya terminado de realizar el pedido, tendrá la opción de listar los productos a comprar y se permitirá quitar aquellos que el cliente no desee adquirirlos.
- Al ser una tienda virtual en línea, luego de confirmado el pedido se procederá a la actualización de las existencias de los productos.
- Se mantendrá un registro de los clientes y sus transacciones con el fin de disponer de un historial que puede ser usado posteriormente, en futuras implementaciones, para poder ofertar productos en función de sus preferencias de compra y dar un seguimiento al cliente.

El gráfico siguiente ilustra la arquitectura implementada en el presente trabajo:

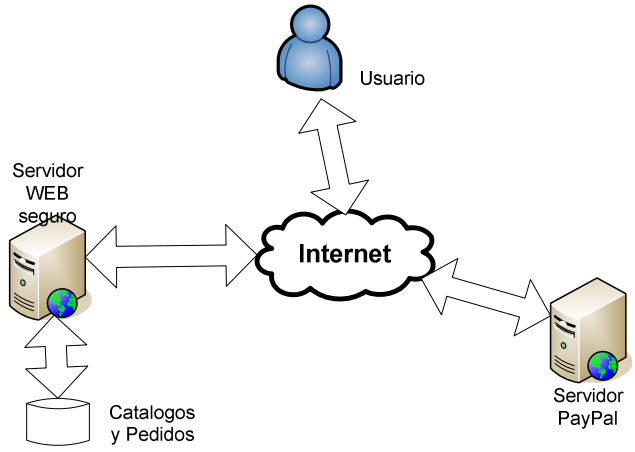

Gráfico 11: Arquitectura de la tienda virtual implementada.

Como podemos ver en el gráfico anterior, la pasarela de pago PayPal actúa de forma independiente tanto con el usuario cuando solicita el pago por la compra de un producto como con el servidor Web de la tienda para obtener los datos de la cuenta donde se acreditará el valor de la transacción.

4.2 Diseño de la base de datos

Al trabajar sobre un software existente y producto de colaboración de miles de usuarios, la estructura de la base de datos ha sido elaborada con muy buen criterio por lo que no fue necesario cambiarla. Cabe destacar que el gran inconveniente de este software es que no existe documentación técnica suficiente sobre la estructura de la base de datos por lo que ha sido una labor bastante grande descifrar y elaborar las relaciones de las tablas.

Para la elaboración del diagrama fue necesario realizar 2 pasos:

1. Probar la aplicación y en función de los datos que se modificaban descubrir sus relaciones y,
2. Revisar a profundidad el código de la aplicación para asegurarse de que las relaciones estén correctas.

A continuación se muestra el diseño de la base de datos con sus 51 tablas que intervienen. Por motivos de facilitar el entendimiento, en el diagrama se muestra cada tabla solamente con los campos de la llave y los campos relacionados. Para obtener la estructura completa de cada una de las tablas es necesario dirigirse a los archivos anexos a esta tesis o hacerlo desde algún software manejador de base de datos de MySql (PhpMyAdmin por ejemplo) y acceder a la base de datos llamada ***tiendaoc***.

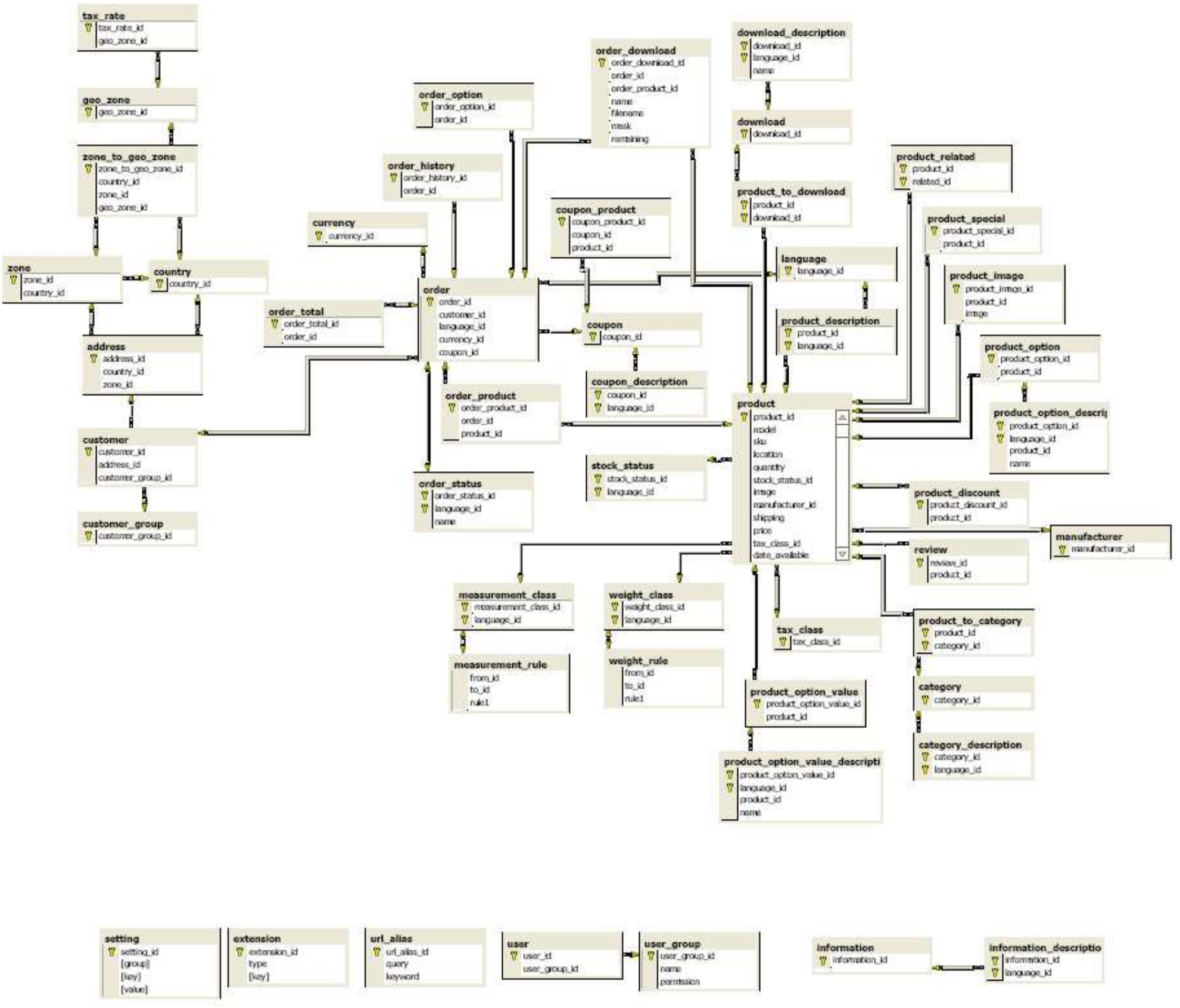

Gráfico 12: Diagrama general de la base de datos para la aplicación

Breve descripción de las tablas:

address: Guarda información de ubicación geográfica de clientes

category: Tabla maestra de categorías de productos

category_description: Guarda las descripciones de las categorías de productos en sus diferentes lenguajes.

country: Tabla de países

coupon: Tabla de cupones de descuentos

coupon_description: Contiene las descripciones de los cupones de descuento en diferentes idiomas.

coupon_product: Guarda información de los cupones de descuento por producto

currency: tabla de monedas (Euro, Dólar).

customer: Tabla con los datos básicos de clientes.

customer_group: Tabla de grupos a los que puede pertenecer un cliente.

download: Tabla de archivos que se pueden descargar.

download_description: Descripción en los diferentes idiomas de los archivos que se pueden descargar.

extension: Opencart maneja extensiones adicionales para su funcionamiento.

geo_zone: Tabla de Zonas para aplicar los impuestos.

information: Tabla de diferentes informaciones que se presenta los clientes (Terminos y Condiciones, Políticas de Privacidad, etc)

information_description: Guarda la descripción de la información de la tabla anterior en diferentes idiomas.

language: Tabla de idiomas.

manufacturer: Tabla de fabricantes.

measurement_class: Tabla de unidades de medida

measurement_rule: tabla de conversión de unidades de medida.

order: Tabla maestra de ordenes de compra de clientes (Pedidos)

order_download: Tabla para registrar los productos descargados con sus respectivas órdenes de compra

order_history: Tabla de información adicional de la orden (comentarios, fecha de creación, etc)

order_option: Guarda información adicional de los productos de la orden (características de cada producto)

order_product: Tabla de registro de los productos por orden.

order_status: Tabla maestra de los posibles estados de las ordenes en su respectivo idioma.

order_total: Tabla de registro de los totales de cada orden (subtotal, envío, impuestos, total neto)

product: Tabla maestra de productos.

product_description: Tabla con descripción de cada productos en los diferentes idiomas.

product_discount: Tabla de descuentos por producto.

product_image: Tabla con las direcciones url de las imágenes de los productos.

product_option: Guarda los posibles datos adicionales que puede tener un producto.

product_option_description: Guarda las descripciones de los datos adicionales en sus diferentes idiomas.

product_option_value: Guarda los valores de los opcionales de los productos (por ejemplo aquí se dirá que se adiciona $50 si compra una memoria adicional de 1GB determinado producto)

product_option_value_description: Guarda la descripción en diferentes idiomas de los opcionales del producto ordenado.

product_related: Tabla de productos relacionados.

product_special: Tabla de productos de promoción.

product_to_category: Tabla de relación de productos con sus categorías

product_to_download: Tabla de relación de los productos y sus descargas.

review: Tabla de estadística de productos revisados por los visitantes.

setting: Tabla muy importante, guarda todas las configuraciones de la tienda virtual.

stock_status: Tabla de posibles estados de inventario de productos (sin stock, con stock, etc) por idioma.

tax_class: Tabla maestra de descripción de impuestos.

tax_rate: Tabla de porcentajes de impuestos.

url_alias: Tabla usada internamente por el sistema.
user: Tabla maestra de usuarios del sistema.
user_group: Tabla maestra de grupos de usuarios y sus permisos de acceso (Administrador, usuario simple, etc)
weight_class: Tabla de descripción de pesos en sus diferentes idiomas.
weight_rule: Tabla de conversión de pesos
zone: Tabla de zonas geográficas por País.
zone_to_geo_zone: Relación entre Zona Geográfica y Zona de impuestos.

4.3 Diseño de la aplicación

La aplicación de tienda virtual tiene 2 componentes claramente identificados:

1. Administración de la tienda (back end).
2. Tienda virtual propiamente dicha (front end).

Para poder realizar modificaciones al software OpenCart original y adaptarlo para utilizar como software de tienda virtual que funcione en Ecuador fue necesario en primer lugar hacer una revisión y estudio profundo de cada uno de los programas que intervienen en la aplicación para luego con una idea clara de cómo se encuentra diseñada la misma proceder a realizar los correspondientes ajustes.
Adicionalmente, al ser Paypal la pasarela de pago seleccionada para utilizar en el presente trabajo, fue necesario implementar un mecanismo para permitir realizar pruebas de pago/cobro a través de este medio sin afectar datos reales de tarjetas de crédito, denominado PayPal Sandbox. Para ello se hizo uso de librerías disponibles en la página Web de Paypal (www.paypal.com) que permite realizar este trabajo.

Además, para que se cierre completamente el proceso de la venta, fue necesario realizar la impresión de la factura de acuerdo a las leyes ecuatorianas, esto significa que en la factura impresa debe constar como mínimo los siguientes datos exigidos por el Servicio de Rentas Internas SRI:

- Datos del contribuyente que emite la factura (Nombres, Ruc, Dirección)

- Establecimiento-Punto de emisión-Número Factura (Ejm: 001-001-1467)
- Datos del cliente (Nombre, Dirección)
- Fecha de emisión de la factura
- Datos de los bienes transferidos (Descripción y precio)
- Subtotal antes de impuestos
- Valor del IVA
- Total Neto
- Número de autorización (otorgado por el SRI).

La aplicación de tienda virtual presentada en el presente trabajo tendrá las siguientes características:

- Soporta múltiples monedas.
- Soporta múltiples lenguajes.
- El catálogo de productos está estructurado de tal forma que cada producto pueda pertenecer a una o más categorías de productos.
- Cada producto puede o no pertenecer a un fabricante.
- En cada producto se podrá especificar su peso, unidad de medida y sus productos relacionados.
- Así mismo dentro de cada producto se puede especificar sus características especiales (por ejemplo cantidad de memoria, tamaño de disco, etc), sus descuentos y sus promociones.
- Soporta varios medios de transporte.
- Soporta varias formas de pago, entre ellas Sandbox de Paypal que permite realizar pruebas de pago antes de entrar en producción, la misma que lo utilizaremos para la demostración de este trabajo.
- Segmentación de clientes a través de grupos.

Para el desarrollo de la aplicación prototipo, se hizo uso de un IDE de libre distribución denominado Netbeans versión 6.9 para PHP.

4.3.1 Ubicación de archivos

Como ya se mencionó en el capítulo anterior, el software OpenCart fue desarrollado usando el modelo MVC con un framework llamado “Zend Framework”, por lo que los directorios de la aplicación se encuentran estructurados de la siguiente manera:

/tienda/catalog/controller: se encuentran todos los programas encargados de la parte de controlador (controla las llamadas a las vistas o a los modelos).

/tienda/catalog/view: en donde se encuentran todos los archivos necesarios para procesar las salidas (visualización de datos).

/tienda/catalog/model: Se encuentran los archivos necesarios para el procesamiento de los datos (registro, consulta, modificación, eliminación).

Además de estos tres directorios principales requeridos por el modelo MVC, al ser un sistema Multilenguaje, es necesario una nueva estructura de directorio la misma que se encuentra en /tienda/catalog/language en el cual se encuentran los archivos necesarios para procesar los mensajes en función del idioma con el que se trabaje.

4.3.2 Dificultades encontradas y soluciones.

Una de las mayores dificultades encontradas en el diseño e implementación de este software fue que no existe información técnica de OpenCart, por lo que fue un gran reto lograr entender gran parte de la programación realizada y, luego, con la ayuda de un software denominado NetBeans IDE poder realizar las modificaciones necesarias para su funcionamiento.

Es muy importante hacer notar que, aunque el software es de libre distribución y se dice que es muy fácil entender su código, se requiere de un nivel alto de conocimientos de programación para llegar a realizar modificaciones en el mismo.

4.3.3 Administración de la tienda.

Para ingresar a la parte de administración de la tienda virtual, dentro del navegador digitaremos la siguiente dirección url: http://192.168.0.2/tienda/admin luego de lo cual nos pedirá un nombre de usuario y contraseña como muestra la siguiente figura:

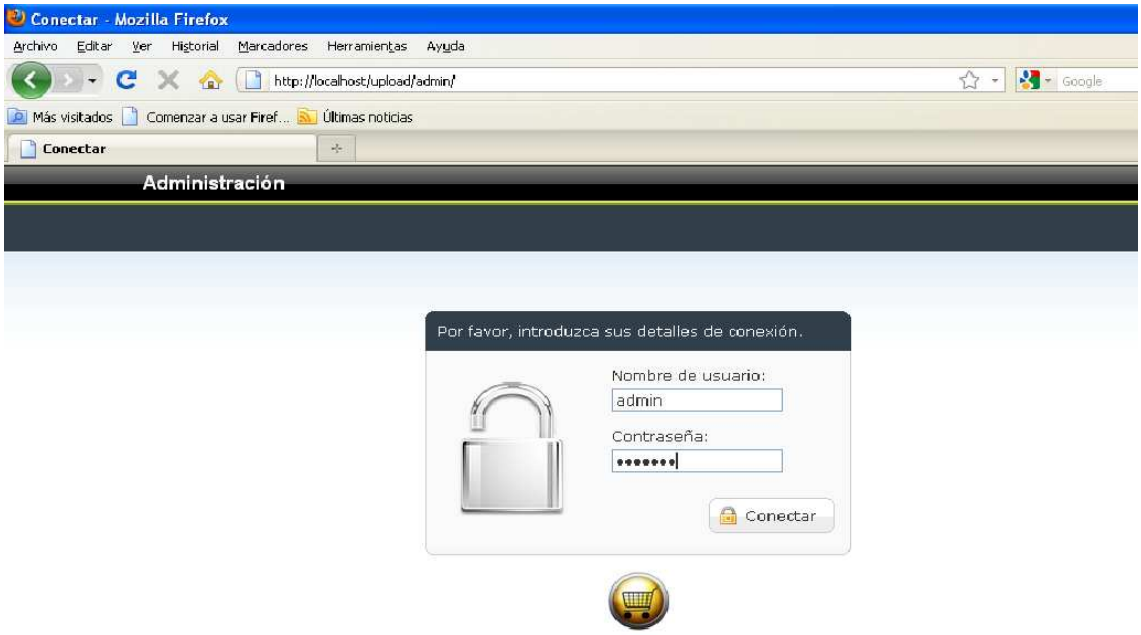

Gráfico 13: Ventana de autenticación para la administración de la tienda

Como nombre de usuario debemos digitar *admin*, y como contraseña la palabra ADMIN01 y luego conectar. Una vez autenticados podemos realizar todas las tareas concernientes a la administración de la tienda, tales como mantenimiento de Categorías de productos, marcas de productos, productos, grupos de clientes, clientes, descuentos, ofertas y todo lo referente a la administración de la tienda propiamente dicha.

4.3.4 Navegación por la tienda.

Para ingresar a la tienda virtual es necesario disponer de un navegador de Internet, que soporte el protocolo seguro https, los más conocidos son Internet Explorer y Mozilla Firefox. La url para acceder a la aplicación es http://192.168.0.2/tienda. Al ingresar a dicha página nos presentará la página web, desde la cual de una forma muy sencilla podemos navegar por las diferentes categorías o productos disponibles y luego realizar la compra de una manera segura.

4.4 Diseño de los mecanismos de seguridad.

Para que una transacción de comercio electrónico sea segura de principio a fin es necesario implementar diferentes mecanismos de seguridad tanto en la parte de la navegación de la tienda para realizar el pedido, como en la parte de procesamiento del pago.

Para la navegación segura se implementó el protocolo https el mismo que permite navegar de una forma segura ya que los datos viajan cifrados y, por lo tanto nadie más que el destinatario del mensaje puede descifrar los mismos, garantizándose de esta manera la confidencialidad e integridad de los datos.

Para poder brindar seguridad a los compradores al momento de realizar el pago, se implementó una forma de pago a través de la pasarela de pago PayPal la misma que trabaja de forma segura tal y como se explica más adelante en este mismo capítulo. Además esta forma de pago está vigente para Ecuador lo cual significa que este trabajo está preparado para funcionar en este País.

Para que una tienda virtual sea confiable, es requisito indispensable que disponga de un certificado digital emitido por una entidad certificadora reconocida, sin embargo, para el presente estudio hemos autogenerado un certificado digital con el único propósito de demostrar que el servidor Web sea validado por el cliente que navega por este sitio, cosa que en la práctica no nos serviría de nada ya que nuestro certificado no será reconocido por navegador alguno.

4.5 Protocolos de seguridad.

Para que los datos viajen seguros a través de una red que por naturaleza es insegura, como lo es el Internet, es necesario implementar protocolos de seguridad para brindar la confianza necesaria a los clientes de la tienda virtual. Para el presente trabajo el protocolo de seguridad implantado es el SSL, estudiado en el capítulo 2, el mismo que se implementa sobre el protocolo TCP en la capa de aplicación.

A través de este protocolo podemos crear certificados digitales con lo cual es posible establecer una conexión segura (ya que los datos viajan cifrados) a partir de una negociación previa (handshake) utilizando dicha clave.

Para montar una conexión segura entre nuestro servidor web y un usuario, necesitamos crear un certificado y configurar dicho servidor para que lo utilice.

La confianza de un certificado se logra gracias a que una Autoridad Certificadora (CA) en la que confiamos (los navegadores cuentan con certificados de Autoridades Certificadoras de confianza) firma nuestro certificado con su clave privada. El navegador puede comprobar que un certificado fue firmado por una CA dada porque cuenta con su clave pública. Una CA de confianza sólo firmará nuestro certificado una vez que compruebe que somos quienes decimos ser.

El formato de los certificados encontrados comúnmente sigue la recomendación X.509 de la serie de recomendaciones X.500 de ITU-T, e incluye:

Versión	Identificador del certificado.
Algoritmo de firma	Algoritmo utilizado para firmar el certificado.
Nombre del emisor	Nombre X.500 de la CA que creó y firmó el certificado.
Período de validez	Consiste en dos fechas que indican el período de validez del certificado.
Nombre de la entidad	Nombre del usuario al que hace referencia el certificado.
Información de la clave pública de la entidad	Clave pública de la entidad junto con un identificador del algoritmo que debe usarse para esta clave.
Identificador único del emisor (opcional)	Identifica unívocamente la CA que firma en el caso que el nombre X.500 se halla reusado para distintas entidades.
Identificador único de la entidad (opcional)	Identifica unívocamente a la entidad en el caso que el nombre X.500 se halla reusado para distintas entidades.
Extensiones	Conjunto de uno o más campos de extensión.
Firma	Cubre todos los otros campos del certificado, ésta contiene el código hash de todos los otros campos, cifrado con la clave privada de la CA. Este campo incluye el identificador del algoritmo usado para firmar.

Tabla 3: Formato de certificado X.509

Para disponer de un certificado es necesario crear un requerimiento que lo enviaremos a la Autoridad Certificadora, la misma que firmará nuestro requerimiento y así obtendremos nuestro certificado.

Las Autoridades Certificadoras más conocidas son las siguientes:

http://www.entrust.net

http://www.geotrust.com

http://www.globalsign.com

http://www.rapidssl.com

http://www.verisign.com/

http://www.thawte.com/

http://www.godaddy.com

El precio que cada una de ellas cobra por emitir el certificado es en función de la confiabilidad en las mismas.
Para nuestro caso, al tratarse de un trabajo de tesis, podemos optar por otra opción que es crearnos nuestro propia CA y firmar el requerimiento con lo que dispondremos de un certificado válido para las pruebas correspondientes.

Los pasos que se realizaron son los siguientes:
1) Generamos una clave para el servidor útil para el algoritmo RSA de 4096 bits:
openssl genrsa -des3 -out server.key 4096

2) Creamos una solicitud de firma de certificado:
openssl req -new -key server.key -out server.csr

Aquí nos pide una serie de datos (unos obligatorios y otros opcionales) que debemos llenar tales como País, Provincia, localidad, Nombre de la Organización, Dirección de correo, entre otros.

3) Procedemos a auto-firmar nuestro certificado con validez de 365 días. Para auto firmarnos necesitamos ejecutar el siguiente comando:
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Con esto obtenemos server.crt el cual es el certificado ya firmado y listo para usar.

4) Una vez que tenemos nuestro certificado firmado, el siguiente paso que se hizo fue configurar el Apache para que vea el certificado y lo utilice.

4.6 Mecanismos de pago.

La tarjeta de Crédito es el Medio de Pago más usado entre los ciberconsumidores. Esto se debe básicamente a su fácil uso, característica esencial de este medio de pago, y por la seguridad que brinda tanto al vendedor, ya que existe alguna entidad financiera que respalda al consumidor, así como para el consumidor ya que frecuentemente las Tarjetas de Crédito se

encuentran amparadas por seguros. Asimismo, existe la confianza generalizada que las operaciones que se realizan utilizando Tarjetas de Crédito, están más que probadas y cuentan con todas las garantías.

Hoy en día existen varias empresas que brindan la facilidad de realizar pagos seguros con tarjetas de crédito, entre ellas se encuentran 2CheckOut, Authorize.net y PayPal que son las más conocidas.

El mecanismo de pago implementado en esta aplicación prototipo es a través de Paypal y Paypal Sandbox.

4.6.1 Descripción de PayPal.

PayPal es una empresa del sector del comercio electrónico, cuyo sistema permite a sus usuarios realizar pagos y transferencias a través de Internet sin compartir la información financiera con el destinatario, con el único requerimiento de que estos dispongan de correo electrónico.

Paypal procesa transacciones para particulares, compradores y vendedores online, sitios de subastas y otros usos comerciales.

¿Cómo funciona PayPal?

El envío de dinero o pagos a través de Paypal es gratuito. El destinatario puede ser cualquier persona o empresa, tenga o no una cuenta Paypal, que disponga de una dirección de correo electrónico.

1. Se elige la opción de pago:
   Con tarjeta de Crédito o Débito.
   Saldo de la Cuenta Paypal.
   Cuenta Bancaria.
2. Paypal realiza el envío del dinero al instante, sin compartir la información financiera con el destinatario.
3. El destinatario recibe el mensaje de Paypal sobre los fondos, y tendrá que crear una cuenta Paypal (en caso de no tener una) para poder retirarlos o transferirlos a una cuenta bancaria propia.

Como abrir una cuenta PayPal

1. Seleccionar el país, idioma y elegir la modalidad de cuenta:
   - Cuenta Personal (Para particulares que compran).
   - Cuenta Premier (Para particulares que compran y venden).
   - Cuenta Business (Para empresas que venden en Internet).

2. Rellenar un formulario de registro con el correo electrónico, una contraseña, nombre, apellidos, dirección postal, teléfono y tipo de tarjeta.

Porqué es PayPal un método seguro para realizar pagos y transferencias de dinero?

PayPal es un método seguro para realizar pagos y transferencias de dinero porque usa tecnología de encriptación SSL de 128 bits para proteger toda la información confidencial y el destinatario nunca recibe datos financieros como el número de tarjeta o cuenta bancaria ni información personal.

Además, ofrece programas de protección, donde el comprador puede pedir la devolución total o parcial de su dinero. PayPal ofrece protección para:

- Artículos no recibidos.
- Artículos muy diferentes a la descripción del vendedor.
- Transacciones no autorizadas realizadas desde tu cuenta Paypal.

4.6.2 Tarifas de Paypal en Ecuador.

Para el cliente que realiza la compra, el servicio no tiene costo.

Para la persona o empresa que recibe de pago de compras (el comerciante) existen 2 tipos de tarifas:

Tarifas de transacciones para pagos Nacionales:

La tarifa estándar para recibir pagos por bienes y servicios es de 3.4% + $0.30 USD.

Si recibe más de $3,000.00 USD por mes, es elegible para solicitar la Tarifa para vendedor de PayPal - que disminuye sus tarifas en la medida que aumenta el volumen de sus ventas, basado en el volumen de ventas del mes anterior.

Ventas mensuales	Precio por transacción
$0.00 USD - $3,000.00 USD	3.4% + $0.30 USD
$3,000.01 USD - $10,000.00 USD	2.9% + $0.30 USD
$10,000.01 USD - $100,000.00 USD	2.7% + $0.30 USD
> $100,000.00 USD	2.4% + $0.30 USD

Tabla 4: Tarifas de transacciones para pagos nacionales con Paypal

Tarifas de transacciones para pagos Internacionales (Recibir pagos de compradores fuera de Ecuador):

Ventas mensuales	Precio por transacción
$0.00 USD - $3,000.00 USD	3.9% + $0.30 USD
$3,000.01 USD - $10,000.00 USD	3.4% + $0.30 USD
$10,000.01 USD - $100,000.00 USD	3.2% + $0.30 USD
> $100,000.00 USD	2.9% + $0.30 USD

Tabla 5: Tarifas de transacciones para pagos internacionales con Paypal

4.6.3 Paypal Sandbox

Para que un programa funcione correctamente es necesario probarlo y depurarlo. En el caso de probar los pagos en una tienda virtual es un tema muy delicado ya que si probamos con datos bancarios reales estaríamos poniendo en riesgo nuestro dinero.

PayPal nos permite hacer pruebas del proceso de pago de nuestra tienda virtual sin tener que usa dinero real ni datos bancarios reales, sino a través de un ambiente de pruebas de PayPal Sandbox que es un duplicado del sitio real de PayPal destinado para este fin.

Los pasos requeridos para crear las cuentas de prueba son los siguientes:

1. Ingresamos en el sitio web de PayPal Sandbox: https://developer.paypal.com
2. Una vez en la página seleccionamos la opción “Sign Up Now” y rellenamos el formulario con los datos solicitados.

3. Una vez registrados nos identificamos en el sistema con el email y la contraseña que proporcionamos en el registro. Dentro del Sandbox podemos crear todas las cuentas ficticias de Paypal que necesitemos y les podemos asignar dinero ficticio, cuentas bancarias ficticias y tarjetas de crédito ficticias.
4. En la opción “Test Accounts” seleccionamos “Create Test Account” para crear las cuentas ficticias.
Para poder realizar las pruebas de pago es necesario crear como mínimo 2 cuentas:
- Una como business (vendedor) para poder cargar el dinero cobrado y,
- Una cuenta como personal (buyer) desde la cual se va a realizar el pago.

Hay que tener presente que para poder realizar el pago desde la tienda virtual debemos estar logados simultáneamente en el Sandbox Test Environment de Paypal para que las pruebas funcionen.

Para el presente trabajo las cuentas creadas son las siguientes:
Cuenta para acceder a Paypal Sandbox: barrosj01@yahoo.com
Cuenta Personal (comprador): com1_1280018521_per@yahoo.com
Cuenta Business (vendedor): jorge_1280016920_biz@yahoo.com

4.7 Políticas de Seguridad.

La seguridad, tanto desde el punto de vista técnico (algoritmos de cifrado, longitud de claves, etc.) como desde el punto de vista de percepción de los usuarios, es un aspecto clave para generar en las empresas y en los consumidores la confianza necesaria para que el comercio electrónico se desarrolle. La necesidad de generar confianza, es especialmente importante debido al hecho de que Internet es una red abierta y a la sensación de inseguridad que este hecho genera en los usuarios.
Sin embargo, la seguridad de la red, en este caso Internet, es solo uno de los factores que intervienen en la seguridad del comercio electrónico en conjunto. La desconfianza de los usuarios a, por ejemplo, enviar los datos de su tarjeta de crédito a través de Internet para efectuar un pago se menciona frecuentemente como una de las barreras iniciales para el crecimiento del

comercio electrónico. En Estados Unidos (donde existe una mayor familiarización con el comercio electrónico y, de hecho, con la venta a distancia en general) se empieza a observar un cambio en las preocupaciones de los usuarios. Más que de la seguridad del pago, los usuarios empiezan a preocuparse sobre todo de problemas como ¿es el vendedor fiable?, ¿podré devolver el producto si no me gusta?, ¿utilizará mis datos personales para enviarme publicidad que no deseo?, ¿cederá esos datos a otras empresas?, en el caso de 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 depende en gran parte de los detalles técnicos, pero además 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.

Por todo lo anteriormente mencionado, es necesario definir políticas de seguridad, que para nuestro caso, vamos a mostrar un ejemplo de una política.

Política de Seguridad.

a) Declaración.

EmpresaVitual.com cifra automáticamente toda información transmitida desde el computador del Usuario a nuestros servidores utilizando el protocolo Secure Sockets Layer (SSL) con 128 bits de longitud de llave. La información que llega a nuestro portal, es almacenada en servidores de un centro de datos que está altamente protegido tanto física como electrónicamente. Los mecanismos estándar de seguridad mantienen los servidores detrás de una barrera electrónica de Firewalls, quedando la información sólo disponible para usuarios válidos. El up time del centro de datos es de 99.9% que es la disponibilidad que este ofrece para acceso al portal. Sin embargo, el usuario declara y acepta que EmpresaVitual.com no puede garantizar la disponibilidad, continuidad y/o calidad del servicio y declara conocer que por o a través del Portal no

necesariamente podrá satisfacer los requerimientos del el usuario para ingresar al mismo.

b) Nombre de Usuario y Clave de Ingreso.

Las cuentas de EmpresaVitual.com están identificadas con un Sistema de Autenticación, a través de un nombre de usuario y clave secreta de ingreso para ser validadas. La Clave Secreta de Ingreso puede ser cambiada en cualquier momento y cuantas veces se desee. Las Claves de Ingreso están cifradas directamente en la base de datos. Series de Claves y llaves de encriptación protegen estos datos de forma segura y le aseguran la total identificación de quien realiza las transacciones o consultas.

Si olvida su Clave, deberá responder la pregunta de seguridad que usted mismo ingresó al momento de registrarse. Si la respuesta es correcta, se enviará a la casilla de correo (e-mail) registrada en la cuenta personal, la Clave temporal, que deberá ser cambiada por usted.

c) Uso de los datos personales por EmpresaVirtual.com

Los datos personales que recolecta EmpresaVirtual.com son usados generalmente para procesar las solicitudes y transacciones del usuario, para proveer servicios de máxima calidad, para comunicar oportunidades, y para entender las necesidades de los usuarios. Por ejemplo, EmpresaVirtual.Com puede usar el número de teléfono de un usuario o su dirección de correo electrónico para: 1) comunicar información relativa a las compras; o 2) comunicar eventuales situaciones de seguridad.

EmpresaVirtual.com no vende, arrienda, comunica o transmite datos personales de sus usuarios a persona alguna, salvo por situaciones excepcionales como por ejemplo en el caso de cumplimiento de órdenes de compra, donde puede ser necesario proveer cierta información a terceras personas para cumplir con un pedido.

d) Seguridad en las Formas de Pago.

En nuestro portal encontrará, básicamente tres formas de pago. Depósito directo en cuenta corriente, Contra reembolso y transferencia electrónica de fondos y con tarjetas de crédito bancario usando para ello la aplicación Paypal.

Todos disponen de una solución que utiliza protocolo de encriptación de la información SSL de 128 bits de longitud de llave, permitiéndoles a los Usuarios enviar sus datos en forma segura y confidencial a través de Internet. EmpresaVitual.com no tiene acceso ni gestiona las transferencias siendo esta operación realizada directamente por el recaudador masivo, en caso de usar Interfaz electrónica.

e**) Consejos de Seguridad.**

Consideramos importante informarle de la existencia de una modalidad de fraude electrónico conocido como "Phishing", cuya finalidad es robar sus datos personales mediante correos electrónicos, mensajes o llamados telefónicos muy convincentes que pueden ser a nombre de EmpresaVitual.com, solicitando datos como nombres de Usuario, Clave, cédula de identidad, entre otros.

Para evitar ser víctima de este tipo de fraudes, tenga siempre presente estos consejos:

Desconfíe. No responda correos electrónicos, mensajes o llamados telefónicos que le soliciten información personal o de sus productos EmpresaVitual.com, o que lo inviten a ingresar a través de un link a nuestra página. EmpresaVitual.com no solicita este tipo de información a sus clientes, un funcionario de EmpresaVitual.com NUNCA le pedirá su Clave personal. Desconfíe de correos electrónicos cuya procedencia desconozca, le sugerimos no abrirlos y eliminarlos de inmediato. Si los lee, recomendamos no abrir archivos adjuntos, ésta es la forma más común de contaminar con virus o software malicioso un computador.

Ingrese a nuestro sitio Web para realizar sus transacciones siempre digitado www.EmpresaVitual.com en la barra de direcciones de su navegador, no lo

haga desde enlaces (vínculos o links) incluidos en correos electrónicos, y evite ingresar desde lugares públicos.

Cuide su Clave de Ingreso. Cuide su Clave de Ingreso, no la use para ingresar a otros sitios web, no la de a conocer a otras personas o incluso a funcionarios de EmpresaVitual.com, y tampoco permita que su PC la guarde para facilitar el ingreso posteriormente. Por seguridad, le sugerimos cambiarla en nuestro sitio cada 2 ó 3 meses. Ante cualquier sospecha de que alguien obtuvo su clave personal, cámbiela inmediatamente.

En caso de dudas o fraude, envíenos un correo a nuestra casilla info@EmpresaVitual.com.

f) Medidas de seguridad y protección de datos personales.

EmpresaVitual.com ha dispuesto estrictas medidas de seguridad para evitar la pérdida, el uso o alteración de los datos personales recolectados. La información personal que EmpresaVitual.com recolecta es almacenada electrónicamente y en su protección se utilizan medidas físicas, administrativas, contractuales y técnicas.

La información de la cuenta es accesible a través de Internet sólo a través del uso del nombre de usuario y la clave de ingreso. Para proteger la confidencialidad de la información personal, el usuario tiene que mantener su clave de ingreso en secreto y no compartirla con otras personas. El usuario es responsable del uso que de EmpresaVitual.com o de su información se haga con su clave o número por cualquier persona.

4.8 Protección de servidores, transacciones, contenidos, y plataforma de pago.

La seguridad en la transmisión de la información es sólo una parte de todo el proceso de seguridad que se debe implementar. Existen otras consideraciones de suma importancia que se deben tomar en cuenta para elevar el nivel de seguridad global.

La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

La información es un recurso que, como el resto de los activos, tiene valor y por consiguiente debe ser debidamente protegida.

Es necesario proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

• **Clasificación y Control de Activos**

Destinado a mantener una adecuada protección de los activos.

• **Seguridad del Personal**

Orientado a reducir los riesgos de error humano, comisión de ilícitos o uso inadecuado de instalaciones.

• **Seguridad Física y Ambiental**

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información.

• **Gestión de las Comunicaciones y las Operaciones**

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

• **Control de Acceso**

Orientado a controlar el acceso lógico a la información.

• **Desarrollo y Mantenimiento de los Sistemas**

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

• **Administración de la Continuidad de las Actividades**

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

4.8.1 Clasificación y Control de Activos

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

4.8.2 Seguridad Personal.

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes.

4.8.3 Seguridad Física y ambiental.

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la Empresa. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones

de servicio. Deben contemplarse tanto los riesgos en las instalaciones del Organismo como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo pero situado físicamente fuera del mismo (“housing”) así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información a la Empresa (“hosting”).

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Organismo y de las instalaciones de procesamiento de información.

Se debe utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, a fin de permitir el acceso sólo al personal autorizado.

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación

civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se deben considerar las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía, se deben contemplar las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas.

c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía.

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra intercepción o daño.

Se debe realizar el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de los Responsables del Área Informática.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

d) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

4.8.4 Gestión de Comunicaciones y operaciones.

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas en producción, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre si, tanto dentro de la empresa como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

Se debe controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan, evaluando el posible impacto operativo de los cambios previstos y verificando su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, deberán estar separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Se deben definir controles de detección y prevención para la protección contra software malicioso.
Es necesario determinar los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.
Se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico.
Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades.

Se deben definir controles para garantizar la seguridad de los datos y los servicios conectados en las redes, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:
a) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
b) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:
a) Almacenar la documentación del sistema en forma segura.
b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario.

4.8.5 Control de Acceso.

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a

los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado.

4.8.6 Desarrollo y mantenimiento de sistemas.

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Es necesario utilizar sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

4.8.7 Administración de la continuidad de las actividades.

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Con el fin de establecer un Plan de Continuidad de las Actividades, se deben contemplar los siguientes puntos:

• Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.

• Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

• Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Todas estas recomendaciones son un resumen del estándar para la seguridad de la información (ISO 17799) publicado en por primera vez en el año 2000.

V. ANALISIS DE RESULTADOS OBTENIDOS.

5.1 Diseño de los mecanismos de seguridad.

En capítulos anteriores se ha mencionado que son cuatro los aspectos básicos de seguridad que conciernen al comercio electrónico: autenticación, confidencialidad, integridad y no repudio.

Autenticación: El presente trabajo permite únicamente la identificación por parte del servidor Web hacia el cliente a través de un certificado digital, que para efectos de pruebas es un certificado autofirmado, pero que en la práctica éste no sería válido sino que habría que adquirirlo a través de una Entidad Certificadora tal como Verisign, Thawte, etc.

Confidencialidad: Debido a que la información viaja cifrada, está garantizada la confidencialidad de la información.

Integridad: la aplicación prototipo brinda integridad ya que las partes intervinientes en la comunicación usan el protocolo SSL y, por lo tanto, en caso de alteración de la información será detectada inmediatamente.

No repudio: La implementación de no repudio no ha sido posible debido a que el usuario de la tienda virtual no se autentica ante el servidor antes de realizar una transacción.

5.2 Protocolos de seguridad.

En la actualidad existen varios protocolos de seguridad, pero para este trabajo se ha utilizado el protocolo SSL el mismo que es el más difundido y usado y, con más implementaciones en plataformas de comercio electrónico.

Este protocolo, como se ha visto en el capítulo 2, no es el mejor en todo, ni el más idóneo para todas las circunstancias, sin embargo, el secreto de su éxito está en su bondad, versatilidad, facilidad de implementación y su oportunidad (o lo que se llama estar en el momento justo y el lugar apropiado).

El estándar SSL no implementa el “No repudio”, sin embargo su soporte sería muy sencillo en el caso de una comunicación SSL en la que ambas partes utilizan certificados con validez para firma electrónica. Basta, en este caso, con que ambas partes firmen todos sus mensajes antes de que sean cifrados con SSL. Las firmas serían comprobadas inmediatamente después de recibir cada

mensaje por la parte opuesta y la sesión SSL sería abortada en caso de recibir una firma inválida en cualquiera de los mensajes. Esta solución sería la ideal, pero al tratarse de una tienda virtual para todo público sería muy difícil de que cada usuario que desee realizar una transacción en la misma requiera tener un certificado.

Desde mi punto de vista, el no repudio aplicado de esta forma sería válido para entornos B2B (Bussiness to Bussiness) en donde la relación va a ser frecuente y sería muy necesario, pero, para el caso del presente estudio en donde el modelo de negocio es B2C (Bussiness to Customer) sería muy difícil, con esta filosofía de firma digital, implementar el no repudio.

5.3 Mecanismos de pago.

El mecanismo de pago usado en la aplicación prototipo es Paypal, con lo que los usuarios de la tienda virtual tienen la posibilidad de pagar con tarjeta de crédito sin realizar complicados trámites o adquirir certificado digital alguno. El único requisito es que el usuario tenga una cuenta de correo electrónico y se suscriba como usuario de Paypal, luego de lo cual puede realizar sus compras y pagar con tarjeta de crédito.

Al ser ésta una forma muy simple y sencilla de realizar compras en Internet, los usuarios se sentirá motivados de realizar compras y pagar con tarjeta de crédito con total seguridad ya que esta empresa Paypal es una de las más difundidas para la recepción de pagos por Internet.

Existen otras posibilidades de pago como transferencia bancaria, cheque bancario o pago contra reembolso que si bien pueden ser interesantes o fáciles de realizar, no sirven para pagos fuera del País y por lo tanto sería una gran limitante sabiendo que el comercio electrónico no tiene límites geográficos.

5.4 Carga útil.

El Cifrado de cualquier forma tiene un costo en el rendimiento – incluido SSL. Si el servidor seguro tiene un alto nivel de tráfico, este puede sufrir una degradación del rendimiento debido a la carga de llevar a cabo el cifrado y descifrado. Esta degradación de rendimiento puede ser abordado de diversas maneras.

La primera posibilidad es la de rediseñar la aplicación para limitar la cantidad de datos que se transfieren a través de SSL. Por ejemplo, una aplicación Web sólo podrá exigir SSL en páginas específicas y, desactivar SSL cuando sea necesario, con lo que el rendimiento del servidor aumentaría. El peligro de este enfoque es la posibilidad de que datos que deben protegerse se puede perder. Sólo un análisis a fondo sobre el flujo de datos puede determinar que datos de la aplicación debe ser protegida mediante SSL.
La segunda solución es cambiar el sistema o arquitectura de red y ejecutar un hardware de aceleración SSL para descargar el trabajo del servidor Web. El acelerador SSL de hardware puede ser instalado en el hardware de servidor o aplicado en la red para realizar todas las operaciones de cifrado y descifrado.

5.5 Escalabilidad

El producto fruto de este trabajo, es una tienda virtual totalmente escalable ya que se encuentra diseñada para crear una cantidad ilimitada de: categorías de productos, productos, marcas, clientes; acepta varias monedas, soporta varios idiomas. Se encuentra diseñada utilizando el modelo MVC lo cual permite el desarrollo de nuevas funcionalidades de una manera ordenada. La única dificultad con la que se puede encontrar es la deficiente información técnica disponible para realizar modificaciones, siendo éste el único pero gran limitante de la aplicación.

En resumen puedo decir que la aplicación prototipo presentada en el presente trabajo cumple con los requisitos básicos de seguridad como son autenticación, confiabilidad e integridad. Además el mecanismo de pago escogido, Paypal, es uno de los más utilizados en el mundo y que brinda seguridad en la transacción. En lo referente a la escalabilidad, es un producto que se puede escalar fácilmente ya que tanto la parte de diseño de la base de datos como de la aplicación están preparados para ello.
Con respecto a la plataforma utilizada como Unix, Apache, MySql y PHP, como todos sabemos son las más difundidas y utilizadas para el desarrollo de este tipo de aplicaciones y además son de libre distribución, lo que permitirá un

crecimiento acorde a las necesidades de todos quienes deseen adoptar este producto para realizar futuras implementaciones.

VI. CONCLUSIONES, RECOMENDACIONES Y LINEAS FUTURAS DE INVESTIGACION.

Conclusiones.

Muchas organizaciones están aprovechando las oportunidades ofrecidas por el comercio electrónico basado en Internet, y se espera que muchas más lo hagan en poco tiempo. Entre estas aplicaciones se encuentran las compras en línea, la banca electrónica, la tele educación, los casinos virtuales, los servicios de pago por visión y vídeo bajo demanda, etc.

Pero aún queda una gran cantidad de empresas, y sobre todo un enorme número de potenciales clientes, que tienen desconfianza de tomar parte en el comercio electrónico, alegando una inadecuación de los servicios de seguridad. Es indudable que no les falta razón, pues las aplicaciones de comercio electrónico presentan una serie de nuevos requisitos que van más allá de los tradicionales requisitos de la Seguridad en Red, el área donde más investigación se ha desarrollado recientemente.

A mi juicio, se hace imprescindible un mayor grado de investigación en estas áreas para poder realizar una implantación a gran escala de las aplicaciones de comercio electrónico.

También se hace necesaria una mayor investigación en otras áreas relacionadas, como, por ejemplo, la de las tarjetas inteligentes, ya que éstas serán el soporte básico en la utilización de la mayoría de las aplicaciones.

Asimismo, será de vital importancia el desarrollo de nuevas técnicas de análisis de protocolos de seguridad, debido a que los protocolos orientados al comercio electrónico presentan características de eficiencia y escalabilidad opuestas a las de los tradicionales protocolos de seguridad, como los de intercambio de claves o los de autenticación de usuarios.

En definitiva, queda aún mucho trabajo por desarrollar y bastantes áreas que requieren un mayor grado de estudio antes de que el comercio electrónico pueda llegar a tener el nivel de implantación que se vislumbra, pero no cabe duda que el camino recorrido hasta el momento es significativo y que la dirección parece ser la correcta.

Se ha dicho que la seguridad en la Web es difícilmente absoluta, pero se puede minimizar el riesgo utilizando medidas de seguridad apropiadas y planes para una recuperación rápida ante un incidente de seguridad. La seguridad Web no es fácil ni barata pero la inseguridad puede ser aún más costosa. La seguridad debe ser parte integral de una organización y por lo tanto, de sus componentes. Poner cuidado en el desarrollo de las políticas de seguridad, posibilita evitar muchos problemas potenciales.

Sabemos que aún existe desconfianza en realizar transacciones a través del Internet, por lo que es necesario dirigir todas las fuerzas a la difusión de la seguridad del comercio electrónico.

Es necesario persuadir a los empresarios de que la recuperación de un incidente es más costosa que la toma de medidas preventivas.
La seguridad del sistema de transacción de datos no debe ser un agregado al comercio electrónico, sino algo que surja desde el propio diseño.
La mayor parte de los problemas de seguridad en los sistemas y por ende en los sistemas de comercio electrónico se debe, a errores de programación por lo que se debe tender a maximizar la seguridad controlando y corrigiendo los mismos. Si bien la seguridad es difícilmente absoluta; existe tecnología, conocimiento y posibilidades suficientes para lograr una gran mejora en la seguridad y una minimización de los riesgos. Es sólo un tema de conciencia de todos los actores de este juego.

A lo largo de este trabajo de tesis se comentaron las diferentes herramientas de protección, las prácticas y arquitecturas que aumentan la seguridad. Las técnicas de identificación digital mediante certificados y firmas. Se habló de la criptografía como base para la protección de los datos, aunque no es sinónimo de seguridad total.
Se hizo hincapié en los principales problemas de seguridad de las máquinas en la actualidad y se encontró que su solución estaba disponible desde hacía mucho tiempo y se basa en los siguientes puntos:

- Definir políticas en tiempo de diseño.

- Prevenir la intercepción de claves de acceso.
- Utilizar las herramientas de seguridad disponibles.
- Evitar fallas y errores de programación.
- Utilizar respaldos
- Restringir el acceso
- Utilizar seguridad física
- Auditar la seguridad

Utilizando medidas de seguridad, buenas prácticas y arquitecturas que pueden asegurar al cliente la integridad y fiabilidad de sus datos se logra la tan anhelada confianza y satisfacción que es el objetivo primordial de cualquier empresa para subsistir en un mercado competitivo.
Las posibilidades que los clientes tienen de protegerse de ataques son muchas. Las responsabilidades en caso de fraude, recaen sobre el prestador del servicio, por negligencia, ya que las herramientas de seguridad existen y son eficientes si se usan con buenas prácticas.
El usuario debe estar al tanto de los riesgos y cómo defenderse ya sea de las formas de prevención como de las posibilidades de reaccionar ante ataques.

En el capítulo 3 se presentó un análisis de las principales herramientas de libre distribución para realizar comercio electrónico, pero estas herramientas son solamente unas pocas de la gran cantidad existente y que se necesitaría de mucho tiempo poder explorarlas y sacar conclusiones más minuciosas de las prestaciones que cada una de ellas ofrece.
Cada una de estas herramientas tienen sus particularidades, sus pro y sus contras, pero de acuerdo a la documentación existente sobre las especificaciones de estos productos y a pruebas online que las mismas ofrecen, se tomó a Opencart como la herramienta para este estudio ya que este proyecto es relativamente nuevo y, por lo tanto ha hecho uso de herramientas más modernas para su implementación tales como Apache2, PHP5, MySql5, además tiene un diseño mucho más limpio que otras que heredaron de su predecesor Oscommerce que si bien en su tiempo fue si no el

único pero si el más popular de los proyectos de tiendas virtuales de libre distribución y con el que se han implementado miles de tiendas alrededor del mundo.

Al ser Opencart un producto desarrollado y mantenido por miles de usuarios en todo el mundo, es un proyecto bastante bien estructurado, pero al mismo tiempo complicado de entender para alguien que ve por primera vez su código fuente y la estructura de su base de datos, por lo que el trabajo realizado sobre el mismo no fue en su mayoría el desarrollo de nuevas características sino más bien el estudio y entendimiento de su estructura en sí y, solamente realizar modificaciones y configuraciones puntuales sobre el mismo.

Finalmente, puede afirmarse que es posible realizar transacciones de comercio electrónico de forma segura gracias a las diferentes herramientas de seguridad disponibles en el mercado. El desarrollo deberá estar orientado hacia la cobertura y la reducción de costos. Además, es necesario el conocimiento de muchas áreas tecnológicas para su correcta implementación.

Como conclusión final debo decir que los objetivos planteados al inicio de este trabajo se han cumplido ya que se logró implementar una tienda virtual que realice transacciones de comercio electrónico de manera segura, utilizando software Open Source como base y los mecanismos de seguridad existentes para tal efecto.

Recomendaciones:

- Se debe incentivar los programas de educación superior en el área de la Telemática y del comercio electrónico, con el fin de que los futuros profesionales se adapten a los cambios y nuevos retos que representa el comercio mundial a través de las redes informáticas y de esta manera contar con personal calificado para que las empresas ecuatorianas puedan entrar en este mundo del comercio electrónico brindando total seguridad y confianza a sus usuarios.
- Deberían crearse más entidades de certificación con el fin de que exista mayor competencia y así bajen los costos de los certificados para que puedan

ser adquiridos por la gran mayoría de personas y de esta manera fomentar el comercio electrónico seguro.

Líneas futuras de investigación.

El comercio electrónico es tan amplio y abarca muchos temas, pero todos ellos apuntan a realizar transacciones de una manera segura, incluyendo los mecanismos de pago, los protocolos de seguridad, por lo que sería de gran utilidad profundizar en ese tema que no ha sido posible cubrir totalmente en el desarrollo de esta tesis, precisamente por su amplitud.

Además, sería de gran importancia realizar una investigación sobre las diferentes librerías criptográficas disponibles para los múltiples lenguajes de programación existentes y de esta manera poder ofrecer toda una biblioteca de funciones con el fin de que sea mucho más fácil escoger e implementar de acuerdo a la plataforma escogida para su desarrollo.

Bibliografía

- Asokan N., Janson Phillipe, Steiner Michael, “The State of the Art in Electronic Payment Systems”, IBM Zurich Resource Laboratory, Septiembre 1997.
- Authentication and Notary Working Group/Electronic Commerce Promotion Council of Japan, “Considerations for Applying Authentication and Notary for Inter-Business Electronic Commerce”, Marzo 1999, versión 0.5.
- Verisign INC, “Building an E-Commerce Trust Infrastructure”, http://www.verisign.com/enterprice/library.
- PayPal Inc. Co., “PayPal Website Payments Standard Checkout Integration Guide”, Agosto 2005.
- López Hernández Fernando, “Seguridad, Criptografía y Comercio Electrónico con JAVA”, Madrid, 2007, www.macprogramadores.org.
- Lucena López Manuel José, “Criptografía y Seguridad en Computadores”, Cuarta Edición, Marzo 2009.
- Stephen Thomas, “SSL And TLS Essentials Securing the Web”, Canada, 2000.
- Siles Peláez Raul, “Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados”, Primera Edición, Junio 2002.
- Morales Vázquez José María, “SSL, Secure Socket Layer y Otros Protocolos Seguros para el Comercio Electrónico”, Primera Edición, 2001.
- Asociación Española de Comercio Electrónico y Marketing Relacional (AECEM), “Libro blanco de comercio electrónico”, 2009.

URLs

- http://www.fsf.org
- http://sourceforge.net
- http://www.gnu.org
- http://www.bce.fin.ec
- http://www.conatel.gov.ec
- http://www.sri.gov.ec
- http://www.verisign.com

- http://www.centos.org
- http://www.opencart.com
- http://www.oscommerce.com
- http://www.prestashop.com
- http://www.magentocommerce.com
- http://php.net
- http://www.apache.org
- http://www.paypal.es

Glosario de términos y abreviaturas

AES = Advanced Encryption Standard

AJAX = Asynchronous JavaScript And XML. *E*s una forma de desarrollo Web para crear aplicaciones interactivas

Apache = Servidor Web ampliamente utilizado

B2A = Business to Administration

B2B = Business to Business

B2C = Business to Consumer.

C2A = Citizen to Administration

C2C = Citizen to Citizen

CA = Autoridad de Certificación

CBC = Cipher Block Chaining Mode

CFB = Cipher Block Feedback

DES = Data Encryption Standard

DNS = Domain Name Service

DSA = Digital Signature Algorithm

E-commerce = Término usado para referirse al comercio electrónico

ECB = Electronic Codebook Mode

EDI = Electronic Data Interchange

HTTP = Hyper Text Transfer Protocol

HTTPs = HTTP que usa protocolos de seguridad

ISO = International Organization for Standardization

MAC = Message Authentication Code

MCV = Model View Controller

MDC = Modification Detection Code

Micropagos = pagos digitales por importes de bajo valor

MIT = Massachusetts Institute of Technology

MySql = Motor de base de datos ampliamente usado conjuntamente con PHP.

NIST = National Institute of Standards and Technology

NSA = National Security Agency

OFB = Output Feedback Mode

Open Source = Aplicaciones que tienen su código fuente liberado.

Passphrase = Secuencia de palabras usada para control de acceso a un sistema de computador.

PayPal = Empresa que permite pagos y transferencias de dinero por Internet

PGP = Pretty Good Privacy

Phishing = Método usado para la suplantación de identidad.

PHP = Lenguaje de programación usado para el desarrollo de aplicaciones Web

RC = Realease Candidate

RSA = Algoritmo asimétrico de Rivest Ron, Shamir Adi y Adleman Leonard.

SET = Secure Electronic Transaction

SHA = Secure Hash Algorithm

SSL = Secure Sockets Layer

TDES = Triple DES

TLS = Transport Layer Security

VeriSign = Empresa que emite certificados digitales

XML = eXtensible Markup Language