MARCO TEÓRICO SOBRE LOS PROTOCOLOS SSL/TLS Y SU APLICACIÓN EN EL SISTEMA DE COMERCIO ELECTRÓNICO

CARLOS FERNANDO ESTÉVEZ MARÍN
YIRISH ARTURO MARTÍNEZ ORTEGA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DETELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2013

MARCO TEÓRICO SOBRE LOS PROTOCOLOS SSL/TLS Y SU APLICACIÓN EN EL SISTEMA DE COMERCIO ELECTRÓNICO

CARLOS FERNANDO ESTÉVEZ MARÍN
YIRISH ARTURO MARTÍNEZ ORTEGA

Proyecto de grado para optar el título de
ESPECIALISTA EN TELECOMUNICACIONES

Director
OSCAR MAURICIO REYES TORRES

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DETELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2013

A mis padres y hermanos con profundo amor.

Yirish.

A Dios Todopoderoso por sus bendiciones y protección.

A mis familiares por su apoyo y compañía incondicional.

A todos los profesores que apotaron sus conocimientos para conseguir este logro.

Carlos Fernando Estévez Marín

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

TITULO: Marco teórico sobre los protocolos SSL/TLS y su aplicación en el sistema de comercio electrónico.[*]

AUTORES: YIRISH MARTINEZ ORTEGA, CARLOS FERNANDO ESTEVEZ MARIN.[**]

PALABRAS CLAVE: Protocolos de seguridad, integridad, confidencialidad, no repudio, criptografia, vulnerabilidades, SSL/TLS, comercio electronico.

DESCRIPCION:

A medida que la sociedad actual crece, paralelamente lo hace el interés por el uso y el conocimiento del internet como medio para interactuar entre los usuarios finales y todos los estamentos de una sociedad (económico, social y político). Ésta interacción sociedad-internet, permite que la información personal, pública ó confidencial pueda llegar a ser intercambiada y circule eventualmente de forma libre por la nube. Partiendo de esto, surge la necesidad de suministrar las pautas y herramientas fundamentales de seguridad para efectuar el intercambio y negociación de la información. Estas pautas permiten velar por la seguridad de la información, la cual se ve reflejada en los niveles de vulnerabilidad, integridad, confidencialidad y autenticidad de la misma. Con ésta monografía, se suministrará información y un análisis que permita realizar una descripción de los protocolos SSL/TSL, su aplicación y aporte en el comercio electrónico B2C (*Bussiness to Consumer*). Igualmente, se proporcionará una descripción y análisis comparativo de la modalidad de comercio electrónico B2C a nivel nacional con respecto al ámbito global. Como complemento, se entregará un análisis de la medida de aceptación y manejo del modelo de comercio electrónico B2C a nivel nacional y el manejo de la seguridad de la información en los últimos 5 años, además, se proveerá un análisis de la medición del uso e implementación de los protocolos SSL/TSL en el comercio electrónico B2C a nivel nacional en el mismo período de tiempo.

[*] Monografia

[**] Facultad de Ingenierias Fisico-Mecanicas. Escuela de Ingenierias Electrica, Electronica y Telecomunicaciones. Especializacion en Telecomunicaciones. Director: Ing. Oscar Mauricio Reyes.

SUMMARY

TITLE: PROTOCOL ON THEORETICAL SSL / TLS AND ITS APPLICATION IN E-COMMERCE SYSTEM.*

AUTHORS: YIRISH MARTINEZ ORTEGA, FERNANDO ESTEVEZ CARLOS MARIN.**

KEYWORDS: Security protocols, integrity, confidentiality, non-repudiation, cryptography, vulnerabilities, SSL / TLS, e-commerce.

DESCRIPTION:

As societygrows, so doestheparallelinterest in the use and knowledge of the internet as a media tointeractwithendusers and alllevels of society (economic, social and political). Thissociety-internet interaction, allows personal information, publicorconfidentialmaybecomeexchanged and eventuallycirculatefreelybythecloud. Fromthis, thereis a needtoprovideguidelines and basic safety toolstomaketheexchange and negotiation of information. Theseguidelinesallowensuringthe security of information, whichisreflected in thelevels of vulnerability, integrity, confidentiality and authenticity of it. Withthismonograph, willprovide information and analysistomake a description of the SSL / TLS, itsapplication and contribution in electroniccommerce B2C (*Business toConsumer*). Similarly, itwillprovideanoverview and comparativeanalysis of the B2C e-commercemodenationwideoverthe global scope. In addition, itwillprovide an analysis of theextent of acceptance and management of B2C e-commercemodelnationally and themanagement of information security in thelastfiveyears, in addition, provides an analysis of the use and measurementimplementation of the SSL / TLS in B2C e-commercenationally in thesame period of time. Thismonographis intended to showa tool availableandwill allowaccess to allusers andmerchants to keepa higher level oftrust and confidencebetween the partiesduring acommercialelectronic transaction, besides, it even pretend toshowone of thesafetysystemssaferinformationthat will helpusersandmerchantsinroads intotelecommunications networksseekingbusiness growththanks to thebreadth ofmarkets, needs, products and services in the world today, leaving aside the fearof providingrelevant informationthroughoursuch networks. With these tools we can find and telecommunications networks and commercial electronic transactions more secure.

*Monograph

**Faculty of Physical-Mechanical Engineerings. School of Electrical Engineering, Electronic and Telecommunication. Specialization in Telecommunications. Director: Eng. Oscar Mauricio Reyes.

INTRODUCCION

En la sociedad actual y con el transcurso del tiempo, el hombre ha buscado que sus actividades diarias y su ritmo de vida aumenten su pragmatismo y hagan mas fácil, dinámica y esencialmente seguro el uso y prestación de servicios, usando como plataforma la Internet, trayendo consigo el intercambio de información confidencial, personal ó simplemente de domino publico y que podrían caer en manos inadecuadas ó también podrían usarse de manera fraudulenta y/ó engañosa. Éste intercambio de información se da comúnmente dentro de la modalidad del comercio electrónico, el cual será objeto de estudio de esta monografia, principalmente en el comercio B2C (bussiness to consumer), que es la modalidad más popular de comercio electrónico. Conociendo la relevancia de la información compartida en una transacción de comercio electrónico se hace necesario buscar mecanismos que aseguren los tres principios de la seguridad informática: Confidencialidad, integridad y Disponibilidad; estos mecanismos se traducen en técnicas y protocolos de seguridad que actúan durante toda la transacción electrónica. Ésta monografia se centra en el análisis y la funcionalidad de la implementación de los protocolos SSL/TLS dentro de la modalidad de Comercio Electrónico en su modalidad B2C como baluarte y herramienta de defensa contra los posibles ataques informáticos en contra de la información que se propaga en la internet, de ésta manera, se atenuarían los riesgos de fraude electrónico y permitirá a los usuarios finales mantener, conocer e implementar un contacto seguro, dinámico y funcional con sus entidades comerciales, bancarias, académicas ó de cualquier otro tipo, así, también se contribuye de manera segura a la convergencia de la sociedad a la internet y en la globalización del mundo moderno.

A medida que la sociedad actual crece, paralelamente lo hace el interés por el uso y el conocimiento de la internet como medio para interactuar entre los usuarios finales y todos los estamentos de una sociedad (económico, social y político),ésta

interacción sociedad-internet permite que información personal, pública ó confidencial sea intercambiada y circule por todos los medios de telecomunicaciones, teniendo esto como primicia, surgió la necesidad de suministrar las pautas y herramientas fundamentales de seguridad para efectuar el intercambio y negociación de la información, éstas pautas velarán por la seguridad de la información, la cual se ve reflejada en los niveles de vulnerabilidad, integridad y confidencialidad de la misma. Con esta monografia, se suministrará información y un análisis que permita realizar una descripción de los protocolos SSL/TLS, su aplicación y aporte en el comercio electrónico B2C, igualmente, se proporcionará una descripción y análisis comparativo de la modalidad de comercio electrónico B2C a nivel nacional con respecto al ámbito global. Como complemento, se entregara un análisis de la medida de aceptación y manejo del modelo de comercio electrónico B2C a nivel nacional y el manejo de la seguridad de la información en los últimos 5 años, además, se proveerá un análisis de la medición del uso e implementación de los protocolos SSL/TSL en el comercio electrónico B2C a nivel nacional durante los últimos 5 años.

Con el surgimiento de las Tecnologías de la Información y Comunicación (TICs), el mundo cada vez se hace más globalizado y las actividades cotidianas como ir al banco, realizar una compra ó comunicarse con alguien que se encuentra a kilómetros de distancia, se puede realizar desde la comodidad del hogar.Para poder alcanzar este nivel de comodidad en estas actividades comunes, se requiere un conjunto de políticas y tecnologías que muchas veces operan invisibles a nuestra experiencia. Estas tecnologías se han venido desarrollando y perfeccionando con el paso del tiempo y con el surgimiento de nuevas necesidades.

La presente monografia se centra en el estudio de protocolos de seguridad como SSL/TLS y su aplicación a los sistemas de Comercio electrónico, así como un análisis comparativo del uso de los medios electrónicos a nivel nacional y regional.

En el capitulo 9 y 10 se hace un marco teórico de cada uno de los dos protocolos de seguridad utilizados en las transacciones electrónicas; su definición, estructura, funcionamiento, versiones, etc. En el capítulo 10 se aborda un número de aplicaciones e implementaciones en las cuales se usan los protocolos anteriormente descritos, en los capítulos 6, 7, 8 y 9 muestra algunas de las vulnerabilidades descubiertas a los protocolos SSL/TLS; se realiza una breve definición de cada una, así como posibles medidas para contrarrestar dichos ataques, adicionalmente, en el capitulo 11 se muestran estadísticas que indican el porcentaje de uso del comercio electrónico B2C y su seguridad en Colombia y Latinoamercia permitiendo ver a groso modo la situación actual del nivel de seguridad y penetración del comercio electrónico B2C presentado por los sitios web y la población en general.

1. COMERCIO ELECTRONICO

En la sociedad actual y con el transcurso del tiempo, el hombre ha buscado que sus actividades diarias y su ritmo de vida aumenten en su pragmatismo y hagan más fácil, dinámica y esencialmente seguro el uso, prestación de servicios ó compraventa de productos, usando como plataforma la Internet y las redes de telecomunicaciones. Lo anterior, lleva implícitamente el intercambio de información confidencial, personal ò simplemente de domino publico y que podrían caer en manos inadecuadas ò también podrían usarse de manera fraudulenta y/ò engañosa. Este intercambio de información se da comúnmente dentro de la modalidad del comercio electrónico ó conocido como e-commerce (electronic commerce), en el cual se enfocara esta monografía. Conociendo la relevancia de la información compartida en una transacción de comercio electrónico, se hace necesario buscar mecanismos que aseguren los tres principios de la seguridad informática: *confidencialidad, integridad y autenticidad*; estos mecanismos se traducen en técnicas y protocolos de seguridad que actúan durante toda la transacción electrónica y generalmente se ejecutan de manera transparente a los usuarios finales.

En la actualidad, se ha observado que el acceso a internet y a las tecnologías de las comunicaciones es mayor y más eficiente en los países desarrollados que en los países que no lo son ò se encuentran en vía de serlo. Aquellos países por sus altosestandares políticos, económicos, sociales y culturales, tienen mejor desarrollo, implementación y divulgación de los planes y estrategias para el acceso a la internet y las TICs en sus comunidades, estos países han conformado un sistema tecnológico sólido y actualizado, lo que ha llevado a que su población tenga una mayor cultura enel uso de la tecnologías de las comunicaciones. Por otro lado, los paísesen vía de desarrollo, como Colombia, han apostado e invertido en mayor medida en la consecución de tecnología de hardware que en los mismos servicios tecnológicos que se ofrecen, algo que ha venido cambiando con el paso

del tiempo y la visión gubernamental. Sin embargo, las mejoras en tal situación han venido cambiando en gran proporción y a ritmo acelerado debido al incremento del uso del comercio electrónico por aquella población ávida e inclinada por las nuevas modalidades en las transacciones electrónicas ofrecidas en la internet, ellos pretenden con estas herramientas ahorrar tiempo y costos en la consecución de un servicio ò producto mediante las tecnologías de las comunicaciones. Paralelamente al incremento del uso de esta modalidad en los medios electrónicos, también se incrementa la necesidad de desarrollar, mantener, actualizar y divulgar estrategias que permitan dar soluciones a las transacciones electrónicas, que proporcionen seguridad y medidas en contra para que aquellas no se transformen en amenazas propias.

Los países en vía de desarrollo como Colombia, ven en el desarrollo de las tecnologías de las comunicaciones una oportunidad para el crecimiento integral de la sociedad, enfocando sus intereses en el control de la información para acceder al conocimiento, comercio, interconexión de las redes e inmiscuirse en la globalización. Los esfuerzos próximos a realizar y desarrollar en el comercio electrónico por parte de las entidades reguladoras de las comunicaciones, el sector comercial e industrial publico y privado es generar y proveer la confidencialidad, integridad y autenticidad de la información, lo que sumará un mayor nivel de confianza en todos los medios y sistemas que impliquen las transacciones electrónicas de los usuarios, además de promocionar y crear nuevas formas y medios de comercio electrónico, con el objetivo de mejorar la calidad de vida de las personas.

Según la OMC (Organización Mundial del Comercio), el comercio electrónico lo define como “*La producción, publicidad, venta y distribución de productos a través de redes de telecomunicaciones*”. Contar hoy día con el acceso al internet ha permitido que se desarrolle este nuevo tipo de comercio, lo que a su vez ha

proporcionado a la sociedad el acceso a nuevos productos y mercados de manera global.

1.1 UNOS AÑOS ATRÁS

En el mundo antiguo,surgió el comercio cuando el hombre observó que ciertos individuos ó regiones poseían alguno tipo de riqueza que de alguna manera le eran muy útiles a otros individuos ó regiones que no tenían la posibilidad de adquirir tal riqueza, el surgimiento de ésta necesidad generó que el hombre buscara una forma de intercambiar esas riquezas entre los individuos, esto condujo a que en la edad antigua los mercaderes crearan extensas caravanas con animales y medios de transporte de la época los cuales movilizaban distintos tipos de recursos entre oriente y el viejo mundo, posteriormente, los Fenicios desarrollaron el transporte marítimo de productos por el mediterráneo, años después, con la llegada de la Revolución Industrial,surgió lo que se denominó el *comercio*y a partir de ese punto, el comercio creció de manera global y complementaria con el crecimiento tecnológico, científico e industrial desde aquellaépoca. Una vez surgió el comercio, esto le permitió al mundo estar mas interconectado y con acceso a nuevas y mejores cosas, ayudando en la evolución de la humanidad. Junto con la internet nació el comercio electrónico, el cual encontró una nueva vía de expansión, nuevas formas de intercambio comercial, nuevas culturas, comunidades, etc.

El verdadero uso del comercio electrónico comienza a mediados del año 2000 y en la actualidad este tipo de comercio maneja gran cantidad de las transacciones electrónicas realizadas a nivel mundial. Esto se debe en gran medida a la globalización de las comunidades y a la necesidad de las grandes compañías e individuos en reducir el tiempo, documentaciones, costos, etc, en distintos procesos comerciales. En la actualidad, se encuentran en la internet una gran cantidad de tiendas virtuales que basan sus sistemas de comercialización, ventas

y pagos en el comercio electrónico exclusivamente y que compiten con otras tiendas en línea, esto evidencia un nuevo tipo de negocio en crecimiento que es usado diariamente y su uso viene creciendo exponencialmente. Con la internet, el comercio electrónico conquistó una nueva vía para su uso y crecimiento en medios masivos y de fácil acceso.

En general, podríamos indicar que el comercio electrónico incluye cualquier tipo de transacción ó intercambio comercial que usa cualquier medio de transmisión de datos como el internet. El comercio electrónico incluye la compra y la venta, además, la búsqueda de información de productos y servicios, publicidad de ellos, reservaciones, etc. Se podría decir que la mayor utilidad que provee elinternet al comercio electrónico es la oportunidad de hacer publicidad, darse y dar a conocer productos y servicios, mostrarse comercialmente de forma mundial y encontrar nuevos mercados. Ésta gran posibilidad esta limitada en los otros tipos de medios de comunicación. De acuerdo a los distintos medios de comunicación usados por el comercio electrónico, éste lo podríamos dividir en dos tipos de comercio electrónico, los cuales son:

1.2 COMERCIO ELECTRÓNICO DIRECTO

En este tipo de comercio electrónico, todo el proceso de compra y venta del producto ó servicio físico ó virtual se realiza usando los medios electrónicos.

1.3 COMERCIO ELECTRÓNICO INDIRECTO

Aquí, todo el proceso de compra y venta del producto ó servicio, físico ó virtual no se realiza completamente usando los medios electrónicos sino que adicionalmente emplean otros tipo de medios físicos para confirmar ó completar las transacciones comerciales.

El talón de Aquiles en la total aceptación y que nos evita hablar ó tener un comercio electrónico directo puro ó absoluto es la desconfianza en las formas de efectuar los pagos de las compras, la cual es experimentada por los compradores y vendedores de los productos ó servicios ofrecidos, ésta desconfianza, se ha convertido en un muro sicológico y de ingeniería por derribar y que ayudará a una mayor aceptación y crecimiento del comercio electrónico. A la desconfianza experimentada por las partes, se le podría sumar otro obstáculo con menor medida de problemática, éste es el desconocimiento de las partes involucradas en una operación de comercio electrónico sobre los diferentes medios de pagos electrónicos y las diferentes medidas de seguridad desarrolladas y que diariamente se trabaja en mejorarlas, teniendo estas dos deficiencias, aun no podríamos referirnos a un comercio electrónico directo absoluto en el que todo el proceso de compra y venta se realice de manera virtual y con el uso de los medios electrónicos.

Para que el comercio electrónico se efectué, éste se compone de tres elementos básicos, los cuales son el *comprador ó consumidor*, quien es la persona que adelanta las consultas y adquisición de cierto producto ó servicio, el *comerciante ó vendedor*, es el individuo ó empresa que ofrece y vende un determinado servicio ó producto y por último estan los *intermediarios ó entes financieros*, los cuales tienen la responsabilidad de verificar, efectuar y concretar el pago de la venta y compra de un producto ó servicio, realizando la transacción electrónica entre el *comprador y el vendedor*. En los intermediarios podríamos incluir también, la logística, publicidad, transporte de productos, etc. Las transacciones efectuadas por los *intermediarios*, tomando como un ejemplo cierta entidad financiera, pueden ser realizadas de diferentes formas, desde el banco del comprador ó del vendedor, transacciones entre los bancos, entre entidades propietarias de tarjetas de crédito y/ó debito, entre otros, ellos siempre tienen el trabajo de realizar las transacciones electrónicas. Es importante resaltar que existen otros tipos de agentes que intervienen eventualmente en las transacciones electrónicas, estos otros agentes

generalmente trabajan sobre la seguridad y logística en las transacciones electrónicas, estos otros agentes podrían ser compañías ó agentes certificadores, empresas de transporte, de correo físico, entre otros.

1.4 ETAPAS DE UNA TRANSACCIÓN ELECTRÓNICA

El proceso de completar una transacción electrónica, se completa básicamente en cuatro etapas y que se asemejan a la manera en que se realizan otros tipos de transacciones comerciales, *consulta, pedido/pago y entrega*.

1.4.1 Etapa 1. El *comprador*, realiza la *consulta*, obtiene la información y datos del producto ó servicio de su necesidad.

1.4.2 Etapa 2. Los entes financieros, toman la información del *comprador* y *producto*, posteriormente le solicitan la respectiva autorización del pago del producto ó servicio.

1.4.3 Etapa 3. Una vez completada y verificada la autorización, se efectúa el pago del producto ó servicio al vendedor.

1.4.4 Etapa 4. En esta fase se completa la transacción electrónica, el *vendedor* realiza la entrega del producto ó servicio mediante algún sistema físico de entrega ó mediante el uso de la red al *comprador*.

De acuerdo a lo anterior, es importante indicar que todas las partes que constituyen un a transacción electrónica deben estar conectados entre si, ya sea unidos mediante una red interna, internet ó físicamente. Por ser comercio electrónico, idealmente deberían estar todos interconectados mediante alguna red de telecomunicaciones. Los medios de pago acordados entre *vendedor y*

comprador, ayudaran a definir las partes que participarían en la transacción electrónica.

El comercio electrónico con el transcurso del tiempo se verá forzado a trabajar en varios retos de cara al futuro, diferentes a la seguridad de la información el cual es primordial, esos retos se pueden resumir en cuatro temáticas:

- La personalización en las transacciones electrónicas, actualmente se pueden encontrar muchos y variados software que le permiten a los distintos sitios web de comerciantes y compañías crear espacios comerciales en la web únicos, los cuales se pueden enfocar en los gustos y preferencias especificas de los clientes y consumidores, un ejemplo palpable de ello se puede evidenciar en el sitio de comercio electrónicowww.amazon.com, en donde ellos lograron diseñar su propio CRM (Customer Relationship Management, por sus siglas en ingles), con el cual logran identificar las preferencias de los consumidores.
- El diseño de un sitio web interactivo, amigable y de fácil uso y entendimiento para los clientes y consumidores.
- Crear aplicaciones de fácil acceso para proporcionar los servicios a los consumidores.
- Cumplimiento en la consolidación de una compra-venta, mejorar la satisfacción del cliente y entrega de los servicios y/ó productos, lo cual se puede lograr concentrando esfuerzos en las cadenas de suministros, logística e inversión monetaria.

2. MEDIOS DE PAGO

En el comercio electrónico, existen distintas maneras de efectuar los pagos, éstos representan una forma de transacción electrónica entre *vendedor y comprador*.Es importante mencionar que los medios de pago constituyen un componente importante en la seguridad del comercio electrónico, debido a que dependiendo del medio de pago a utilizar, éste tendrá asociados mayores ó menores riesgos a la seguridad.Con estas formas de pago electrónico se logran concretar la mayoría de las transacciones electrónicas comerciales, las cuales se enuncian a continuación, aunque algunas de ellas no se encuentran muy difundidas en Colombia:

2.1 DINERO ELECTRÓNICO

Es sabido que por dinero tenemos el concepto que es aquel instrumento de pago comúnmente aceptado por los individuos y la sociedad. Con esto en mente, el dinero ó moneda es considerado de tal manera solo si cumple su objetivo comercial de ser un método de intercambio, de sistema contable y de elemento representativo de un valor. Una manera generalizada para denominar el *dinero electrónico*, podría ser estableciendo que es todo aquellaforma de dinero que se crea y usa solo de manera electrónica y a través de la internet ó alguna red de telecomunicaciones. Se podría indicar también, que el *dinero electrónico* es un tipo de representación de la denominación del valor en el mundo real del dinero, pero visto y aplicado desde los medios y canales electrónicos. Por ello, también es conocido como e-money ó dinero virtual. Con él, en la mayoría de los casos se completa alguna compra-venta ó transacción electrónica. Muchas compañías ó entidades bancarias y comerciales, usan el dinero electrónico como elemento de valor en las transferencias electrónicas de fondos, depósitos dirigidos, entre otros. Se pueden encontrar dos tipos de dinero electrónico, el *dinero electrónico de hardware* y el *dinero electrónico de software*. Para el primero podríamos citar el

ejemplo de las conocidas *tarjetas prepago*, con este tipo de tarjetas, los individuos efectúan los pagos en dispositivos terminales que usan las redes de telecomunicaciones, éstas tarjetas, además, tienen la capacidad de almacenar una cantidad limitada de manera electrónica ó virtual un valor que representa una cantidad monetaria en el mundo físico comercial,en un ordenador ó algún tipo de cuentaelectrónica y que se encuentra a disposición para el consumo del portador. Este tipo de dinero ó forma de pago no obliga al uso ó intervención de una entidad bancaria. Estos tipos de elementos, poseen bandas magnéticas, chips electrónicos, entre otros tipos de dispositivos que contienen la información relacionada.

Por otro lado, está el *dinero electrónico de software*, éste emplea dispositivos electrónicos de pago que basan su funcionamiento sobre el uso de un software instalado en los dispositivos electrónicos finales de pago, se requiere que tanto el consumidor como el vendedor manejen y posean el software de la aplicación.Para el uso de este tipo de dinero, es necesario el uso de modem, redes electrónicas de alguna entidad bancaria ó la internet, es necesaria la comunicación con alguna entidad bancaria para realizar los pagos de la compra-venta de un producto ó servicio. El dinero electrónico tiene los atributos de ser seguro, versátil, no tiene fronteras, puedes ser anónimo y reutilizable.

2.2 SISTEMAS DE CRÉDITO Y DEBITO

Los sistemas electrónicos de crédito y debito son una forma detransacciónelectrónica, ella funciona en internet con solo con poseer una cuenta de correo electrónico y una cuenta bancaria. De esta manera, se pueden efectuar pagos ó recibir dinero por medio del uso del internet. Este sistema anula el requerimiento de proporcionar la dirección y el número de sus tarjetas de crédito ó debito cada vez que el consumidor efectué un pago electrónico. Estos sistemas permiten almacenar de manera segura la información correspondiente sobre el

consumidor y sus cuentas bancarias. La información requerida es proporcionada al sistema de cobro electrónico de la compañía ó del vendedor. Este medio de pago electrónico, permite a la empresa ó vendedor proporcionar una cuenta bancaria al comprador, en la cual se puede efectuar la transferencia de dinero y completar el pedido.

2.3 TARJETAS DE CRÉDITO Y DEBITO

Este sistema de pago electrónico es el mismo que utilizan los individuos al emplear sus tarjetas de crédito ó debito de su entidad bancaria para efectuar los pagos de la compra-ventas de un producto ó servicio usando las redes de telecomunicaciones. Las grandes compañías usan actualmente el protocolo SET (Secure Electronic Transaction) para proporcionar un nivel de seguridad a este tipo de transacciones.

2.4 SISTEMAS DE MICRO PAGO

Los sistemas de micro pagogeneralmente son una forma de realizar los pagos de una transacción electrónica de poco valor, como la compra de música, ciertos tipos de libros, informes periódicos PDF, entre otros. Los usuarios de esta modalidad realizan una recarga ó compra de dinero anticipada de cierta cantidad definida por el mismo usuario y se carga a un bono prepago, cuenta, entre otro elemento. Una vez los usuarios gastan el dinero en la cuenta, ésta puede ser recargada. Con esta modalidad no es necesario el uso de tarjetas de crédito, realizar transferencias bancarias en las compras, tener suscripciones, entre otros. Solo se debe contar con un correo electrónico ó un teléfono móvil. Los micro pagosfuncionancomo una cuenta prepago, virtual y gratuita.

Estos sistemas de pago electrónico constituyen una parte fundamental en la conclusión de las transacciones electrónicas, debido a que por medio de estos

sistemas, se logra la transferencia de dinero entre el consumidor y el vendedor por la compra-venta.

3. CLASIFICACION DEL COMERCIO ELECTRONICO

Según las partes que participan en el comercio electrónico, se realizó la siguiente clasificación del mismo, aunque el crecimiento de ellos ha sido en distinta proporción.

3.1 COMERCIO ENTRE EMPRESAS (B2B)

Business to Business son sus siglas en ingles. Esta clase indica la relación comercial entre empresas ó entre vendedores. Es el tipo de comercio que más se ha beneficiado con los avances en las tecnologías de las comunicaciones, esto es debido aque con la aparición del comercio electrónico las compañías han logrado bajar sus presupuestos y gastos en procesos internos y entre las partes, además, han logrado ampliar sus mercados. Con esta modalidad, las compañías pueden realizar negociaciones entre ellas, solicitar productos ó servicios, intercambiar información, crear concesiones, entre otros. En muchos casos, el acceso a sus portales web se encuentra restringido con nombres de usuarios y contraseñas para poder completar las transacciones electrónicas.

3.2 COMERCIO ENTRE EMPRESAS-CONSUMIDORES (B2C)

Business to Costumer son sus siglas en ingles. Este tipo de comercio muestra la relación comercial entre las empresas ó vendedores y sus clientes ó consumidores, es una relación bidireccional. Este modelo de comercio electrónico, se basa en concretar una transacción comercial mediante el uso de la internet, el usuario visita la pagina web de un determinado vendedor ó compañía y efectúa una compra-venta.También se puede dar la situación en la que un individuo establece las reglas de venta de cierto producto ó servicio a una empresa. Específicamente, los actores en este modelo son un *vendedor ó empresa* y un *individuo ó consumidor*. Generalmente, este modelo de negocio ofrece mejores

precios en los productos ó servicios a sus consumidores, adicionalmente, la empresa ó vendedor tiene la posibilidad de reducción de costos en infraestructura de su negocio y la posibilidad de acceder a un mercado global.

3.3 COMERCIO ENTRE CONSUMIDORES (C2C)

Costumer to Costumer son sus siglas en ingles. Indica la relación comercial entre individuos consumidores que no son empresas. Aquí, los individuos consumidores poseen un portal web en donde completan transacciones electrónicas con otros individuos consumidores. Se emplea mucho la modalidad del intercambio de productos. Se ha observado que este tipo de modelo comercial ha sido objeto de desconfianza y restricciones por parte de algunos gobiernos y grandes empresas trasnacionales debido a la legalidad de sus productos, patentes, derechos de autor, entre otros.

3.4 COMERCIO ENTRE CONSUMIDORES-GOBIERNO (C2G)

Costumer to Government son sus siglas en ingles. Muestra la relación comercial entre un consumidor y una entidad pública o del gobierno. En este modelo de negocio, las entidades administrativas ó gobiernos diseñan y emplean sitios web para el uso de los ciudadanos ó empresas, en donde ofrecen facilidades para el uso de ciertos servicios. Estos sitios web, generalmente tienen el propósito de recaudar ó recibir el pago de impuestos y servicios públicos, para realizar publicaciones gubernamentales y legales, cronogramas de actividades, ayuda al ciudadano, entre otros servicios. Muchos gobiernos han empleado este tipo de modelo comercial con el objetivo de facilitar a sus ciudadanos la solicitud de documentos de identificación, pasaportes, entre otros. En ocasiones, las dependencias de algunos gobiernos empelan sus propios sitios web.

3.5 COMERCIO ENTRE EMPRESA-GOBIERNO (B2G)

Business to Government son sus siglas en ingles. Indica la relación comercial existente en una compañía ó vendedor y una entidad pública ó del gobierno. Este modelo de negocio opera de manera similar al tipo C2G, la diferencia está establecida en que las partes no son los individuos consumidores ó ciudadanos, sino, las empresas. Los sitios web propuestos por los gobiernos permiten a las compañías el pago de impuestos, procesos jurídicos, procesos de licitaciones, entre otros servicios.

3.6 COMERCIO ENTRE EMPRESA-EMPLEADO (B2E)

Business to Employee son sus silgas en ingles. Muestra la relación comercial existente entre una empresa y sus empleados. Es un nuevo término que ha venido surgiendo con el crecimiento del comercio electrónico. Este tipo de transacción electrónica se ha venido enfocando en el trámite de formularios por parte de los empleados, sobre las hojas de vida de sus empleados y la base de datos de las compañías, también se utiliza para el diligenciamiento de los formularios para la gestión de vacaciones de los empleadosen las compañías, entre otros.

Con el crecimiento exponencial en el desarrollo de nuevas tecnologías informáticas y de comunicaciones en los últimos años y los venideros, ayudarán a que el comercio electrónico se establezca como la forma más usada de transacciones comerciales. Con tal crecimiento tecnológico, las compañías que más se han beneficiado con el comercio electrónico están ubicadas en los Estados Unidos, este beneficio se dio gracias a que en ese país hacia los años 90 se estableció públicamente el protocolo *www* (worldwide web), por ello, se podría decir que en esa nación es donde se da el mayor uso de este medio y la que mas popularizado tiene el uso de este tipo de comercio.

4. MODALIDADES DE SELECCIÓN Y COMPRA EN LINEA

Como consecuencia delcrecimiento y avance tecnológico, el comercio electrónico ha tenido una evolución en el diseño de aplicaciones para lamodalidad de selección y compra en línea de productos ó servicios en las paginas web de los vendedores, ésta evolución se ha dado de tres formas con la implementación de los *formularios HTML*, el *carrito de compras* y los *almacenes virtuales*.

4.1 FORMULARIOS HTML

Ésta modalidad de selección de productos ó servicios dentro de la pagina web del vendedor, emplea un formulario virtual, el cual, incluye la mayoría de la veces el producto ó servicio, su descripción, la descripción del vendedor y del comprador, luego, esta información se envíavía correo electrónico al vendedor. La limitante que posee, se debe a que si se tienen muchos productos se tendrían igual numero de formularios, lo cual hace impráctico, demorado, consta de mucha información reunida en una sola pagina y esto lo hacedifícil de presentarlos.

4.2 CARRITO DE COMPRAS

Es muy usada en estos tiempos. Con el uso de esta manera de selección virtual de productos ó servicios, el comprador podría solamente indicar su preferencia sobre uno ó varios productos dentro de un océano de posibilidades ofrecidos en la pagina del vendedor, además, en muchos casos cada uno de ellos posee una pagina virtual con la descripción especifica de cada uno de ellos, los productos ó servicios de su interés. Esta forma de selección, adicionalmente emplea un sistema que permite calcular precios totales, parciales, intereses, tasas de cambio, impuestos, etc.

4.3 ALMACENES VIRTUALES

Con esta modalidad de selección, compra y venta en línea, se incluyen funciones de administración y atención personalizada por parte del vendedor. El vendedor puede manipular constantemente la información de sus productos ó servicios, realizando actualizaciones de sus mercancías, precios, versiones, modelos, categorías, etc., también, podría ocultar, adicionar ó eliminar productos por periodos de tiempo, podría también diseñar concursos ó establecer promociones, de igual manera, ayudan también a los vendedores en el control de inventarios y presupuestos, permitiendo a su pagina ser mas interactiva y amigable para los consumidores.

En nuestros días se ha podido observar que Estados Unidos es el país quien es la punta de lanza en el desarrollo de nuevas tecnologías de las telecomunicaciones a nivel mundial, además, siendo la internet un sistema de comunicaciones abierto también ha permitido que otros países usen el comercio electrónico como un medio para alcanzar mayores desarrollos en todos sus aspectos, lo cual, ha llevado a que se cree un nuevo tipo de frontera virtual entre los países desarrollados, los que se encuentran en vía de desarrollo y entre aquellos que aun no han entrado de lleno en la era digital de las telecomunicaciones. El comercio electrónico ha permitido a los consumidores tener mayor rapidez, comodidad, facilidad y en ciertos casos mejores precios de productos ó servicios, de igual manera, ha permitido que crezca nuevas empresas y las ya existentes están adoptando estas nuevas tendencias del comercio que permiten alcanzar nuevos mercados, incrementar sus ventas y descubrir nuevas formas de dar a conocer sus productos ó servicios, por otra parte, las compañías quienes comienzan a incursionar en este medio han visto que apuntar hacia esa nueva tendencia tecnológica reduce costos, se podrían buscar alianzas estratégicas con patrocinadores, compañías de publicidad y socios en el área de las telecomunicaciones que ayudarán a que sus negocios sean mas competitivos y

con mayores oportunidades. Debido a que la internet se ha convertido en el medio de comunicación preferido por la sociedad para transmitir y compartir información, que permite mejores formas de comunicación entre las personas y el medio por el cual se tiene mayor acceso a una gran diversidad de productos y servicios. Por lo tanto, es importante comprender este nuevo tipo de tecnología, el *comercio electrónico*. Con el crecimiento del comercio electrónico, se ha observadoque éste ha sido un motor de cambio en las estrategias de mercadeo, de competencia e incluso ha podido llegar a cambiar la estructura comercial de empresas.

El comercio electrónico tiene dos características importantes denominadas EDI (*Electronic data interchange*) y EFT (*Electronic fund transaction*). El *EDI*, permite el intercambio de datos por medios electrónicos y su aplicación se podría entender tomando como una ejemplo un tienda que maneje su inventario de manera electrónicamente sistematizada y según su información cierto producto "*X*" no debería estar por debajo de una cantidad "*Y*" de referencia en su inventario de bodega, en caso que se encuentre por debajo del nivel de referencia"*Y*", el sistema enviaría por medios electrónicos una orden de servicio a su proveedor del producto "*X*" , para que este realice un envió de dicho producto y se mantengan los inventarios de las bodegas con reservas suficientes. Complementario a esto, se encuentra el *EFT*, el cual permite la certificación ó consolidación de la transacción electrónica; para esta acción tomando como ejemplo la situación en que un cliente realiza el pago en la entidad financiera de un vendedor a quien le ha realizado la compra de cierto producto ó servicio, seguido a esta acción, interviene el *EFT*, el cual realizará la verificación de los datos del cliente y números de cuenta, si no encuentra inconvenientes las compra-venta finalizará, de lo contrario emitirá algún tipo de mensaje por medios electrónicos de la invalidez de la transacción electrónica.

5. MEDIOS PARA IMPLEMENTAR Y USAR EL COMERCIO ELECTRONICO

El comercio electrónico se apoya en un amplio rango de aplicaciones de la tecnología, pero las más importantes son en las que el comercio electrónico trabaja y se desarrolla, éstas son el internet *WWW*, las redes y el correo electrónico.

5.1 REDES

Desde que surgieron las redes de telecomunicaciones, éstas se convirtieron enuna estructura básica y fundamental para el flujo y crecimiento del comercio electrónico. Actualmente existen dos clases de redes de telecomunicación en las que el comercio electrónico tiene mas influencia, ellas son las redes privadas *EDI* y las redes *VAN* (*Value-added networks*). Estas ultimas son las mas usadas en nuestros días, debido a que ellas proporcionan al comercio electrónico valores agregados como mayor seguridad, confiabilidad, tiene la posibilidad de ser supervisadas y vigiladas mas de cerca y con mas detenimiento, adicionalmente, tienen la posibilidad de realizar un seguimiento del rastro de la información, pero, tiene el inconveniente de ser costosas, la razón de ello, es que este tipo de redes requieren un tipo de mantenimiento exclusivo, requieren líneas privadas de alta velocidad y su numero de usuarios puede ser limitado. Como resultado de esto, la opción mas viable en las telecomunicaciones es el uso de internet. El internet es el medio que resulta mas fácil, económico y accesible para todas las partes que intervienen en las transacciones electrónicas (consumidor, vendedor y proveedor) y que les permite de mejor manera desenvolverse y darse a conocer globalmente. Así, lo único que necesitarían las partes para involucrarse en el comercio electronico seria una computadora, un servidor y acceso a internet, aunque se debe tener en cuenta que la internet tampoco es un medio seguro para latransmisión de información.

5.2 CORREO ELECTRÓNICO

El correo electrónico en el comercio electrónico permite un trato más personalizado y exclusivo entre consumidores, vendedores y proveedores. Éste comportamiento se da gracias a que el correo electrónico es una forma de comunicación mas rápida y directa entre las partes. Este canal de comunicación ayuda a compradores y vendedores a concretar transacciones, realizar acuerdos, solicitar información específica sobre los productos ó servicios, etc. Las compañías y vendedores usan el correo electrónico para publicitar sus productos ó servicios a sectores específicos de sus mercados y/ó para anunciar ofertas, promociones, descuentos, etc. a sus clientes exclusivos.

5.3 WWW

Representan las siglas en ingles de *The World Wide Web*. La web es el medio de comunicación más grande y más importante en el que el comercio electrónico fluye. Hoy en día, la gran mayoría de los productos y servicios existentes se pueden encontrar en las web, incluso aquellasque desconocíamos. En la actualidad, podemos encontrar compañías y vendedores que usan la web para publicitar y vender sus productos al por menor, también, se encuentran muchas compañías y vendedores que recién incursionan en el comercio electrónico en la web y que también son visionarios del crecimiento del comercio electrónico y el aumento de la seguridad que requieren las transacciones electrónicas. Con la disponibilidad de la web, las compañías y vendedores pueden hacer compra, venta y entrega de productos y servicios que en la gran mayoría de los casos también son virtuales ó digitales, por ejemplo, música, fotos, software, libros, etc.

Con lo mencionado, el comercio electrónicoha modificado y mejorado las relaciones entre las partes que actúan en él, vendedores, consumidores y proveedores. Las grandes compañías usan el comercio electrónico como una

manera de integrar todas sus herramientas tecnológicas y la consecución de otras más con el objetivo de proporcionarle mayor valor a la compañía, mayor crecimiento y más credibilidad por parte de sus consumidores y proveedores.

6. ATRIBUTOS Y PERJUICIOS DEL COMERCIO ELECTRONICO

Podríamos indicar ciertos puntos sobre los cuales el comercio electrónico ha permitido un crecimiento y/ó mejoramiento de los procesos, estos son:

a. Ha permitido mayor facilidad, comunicación y eficiencia en las relaciones comerciales entre las partes involucradas en las transacciones electrónicas (vendedor, consumidor, proveedores).
b. Ha permitido una mayor cobertura de los mercados y el surgimiento de nuevas formas de negocio y comercio.
c. Con el comercio electrónico, el flujo de información es más eficaz, rápido y enfocado, permitiendo también a las compañías mantener un control y supervisión en el flujo interno y externo de su información, así como el control de sus procesos (administrativos, recurso humano, económico, etc.).
d. El comercio electrónico, ha permitido el desarrollo de tecnologías de la información, las comunicaciones y la seguridad de la misma, tanto en el flujo como en las transmisiones de información de todo tipo.
e. Incursionar en el mercado global.
f. Mejores relaciones entre las partes involucradas.
g. Reducción de costos publicitarios y comerciales.
h. Estrategias de mercadeo focalizadas en clientes específicos y acceso exclusivo a nuevos y potenciales consumidores.
i. Facilidad, rapidez y comodidad para realizar las transacciones.
j. Acceso a gran cantidad y variedad de productos y servicios.
k. Posibilidad de una mejor y más detallada consulta de los productos y servicios solicitados.
l. Posibilidad de control de precios y presupuestos.

Según la *CMT* (*Lacomisión del mercado de las telecomunicaciones*), en España el crecimiento en ventas del comercio electrónico en el 2011 tuvo una crecimiento

del 27,5 %, lo que representa una cifra alrededor de los 9.201 millones de euros en transacciones electrónicas. Con el crecimiento de comercio electrónico también deberían crecer y mejorar algunos puntos importantes que han traído ciertos perjuicios al comercio electrónico y sobre los cuales el comercio electrónico existe y se rige. Estos puntos los podríamos enunciar así:

a. En primer lugar se tiene el concepto de normatividad legal, en ello se debe mejorar y crear nuevas legislaciones que permitan tener un marco legal bien estipulado ya que en ello se ha tenido poco avance, con tales legislaciones se definirían aspectos de seguridad, acceso a la información y sobre todo la privacidad, avanzando en el desarrollo de esto,también se tendrán avances en temas de legislación que incluyen métodos de buenas practicas de uso del sistema, de procedimientos de seguridad en las transacciones electrónicas, de autentificaciones, de derechos de autor, en el desarrollo de esquemas ó procedimientos del mercadeo adecuado, entre otros.
b. Por otra parte tenemos que mirar el crecimiento y el mejoramiento en el aspecto tecnológico, enfocado en el desarrollo y mejoramiento en la normatividad técnica y de ingeniería para la transmisión de la información y de los canales ó medios para su flujo y sus posibles limitaciones.
c. Si no se cuenta con los elementos básicos (computadores, redes, acceso a internet, etc.), el acceso e implementación tendrá dificultades.
d. Desconfianza en la autenticidad de las transacciones electrónicas.
e. Proceso de aceptación por parte de los individuos en la incursión de nuevas tecnologías en el comercio.
f. Procesos de reclamaciones, garantías, cambios, entre otros, de productos ó servicios.
g. Seguridad.

6.1 PROBLEMÁTICAS ASOCIADAS AL USO DEL COMERCIO ELECTRÓNICO

Como todo método de negociación y comercial, el comercio electrónico experimenta tres tipos de problemáticas muy importantes en el momento de efectuar algún tipo de transacción electrónica, estasproblemáticas son la privacidad, las legislaciones de los gobiernos y entidades internacionales y la constante evolución tecnológica.

6.1.1 Privacidad. Actualmente no se puede negar la existencia de cierto temor y desconfianza por parte de los consumidores al efectuar cualquier tipo de transacción electrónica y aun más si hablamos de usar el *internet* como canal para efectuar pagos ó transacciones electrónicas. Se puede observar que la mayoría de las compras que se concretan a través de la web, necesariamente usan los números de las tarjetas de crédito de los consumidores, pero realizar este procedimiento no es seguro si se desconocen las vías adecuadas para realizarlo de una forma mucho mas segura y reduciendo los riesgos que la información caiga en manos inadecuadas. Es importante tener en cuenta, que al realizar cualquier transacción electrónica, el comprador en la mayoría de las situaciones no tiene certeza de la identidad y confiabilidad del vendedor, la misma situación se presenta del vendedor hacia el comprador.

6.1.2 Legislación. Se ha observado, que los gobiernos de los distintos países y los entes internacionales reguladores no han avanzado mucho en temas legislativos, en la creación y divulgación de leyes que normalicen, juzguen y guíen el uso del comercio electrónico. Aun para muchos usuarios, no son completamente claros los métodos de seguridad tales como las firmas electrónicas, certificados electrónicos, validez de contratos electrónicos, derechos de autor, validación ó copia de marcas, patentes, entre otros.

6.1.3 Evolución industrial y tecnológica. Podemos observar que la tecnología y la industria cambian y mejoran constantemente, lo cual también induce cambios en las tecnologías de las telecomunicaciones y por consiguiente en el comercio electrónico. Por tal motivo, las compañías, consumidores y proveedores deben adaptarse rápidamente a estos avances, y estos cambios se ven reflejados en la voluntad y capacidad de transformar sus mercados, sus socios comerciales, necesidades, aplicaciones, redes, entre otros. La capacidad y voluntad de evolución en una compañía podría ser directamente proporcional a su capacidad tecnológica y del interés de crecer y evolucionar en el comercio electrónico.

Como se ha señalado, el surgimiento y desarrollo del comercio electrónico, ha dado la oportunidad a usuarios (vendedores), organizaciones y distintos rubros comerciales de negociar y competir con sus productos y/ó servicios de manera global, el comercio electrónico a su vez también ha permitido el incremento de ventas y publicidad a menores costos y esfuerzos de inversión monetaria. Sin embargo, paralelamente se incrementan las amenazas y riesgos que deben ser tratadas de la mejor manera. Los beneficios del comercio electrónico se deben mirar desde dos perspectivas, una de ellas es mirar los beneficios que percibe el consumidor y por otro lado los beneficios que el vendedor percibe. Para los consumidores, los beneficios que generalmente se encuentran son mejores precios, promociones, mayores y mejores ofertas de productos y servicios, mayor comodidad y en algunos casos se podría dar una mejor atención del vendedor con el seguimiento personalizado de la compra-venta. Ahora, los vendedores y organizaciones comerciales, pueden ver sus beneficios en la reducción de costos operativos y de administración, mayores y diversos focos de mercado, menores costos de comercialización, también pueden tener la posibilidad de acceder mas rápido y de manera mas directa a los clientes, es decir, mercadeo 1 a 1, adicionalmente, los vendedores tiene la posibilidad de emplear la red de internet como un nuevo canal publicitario y comercial con acceso a ella mas fácil y a costos reducidos. Complementario a los beneficios anteriores, el hecho que una

organización comercial incursione en el comercio electrónico y figure en la red mundial, es sinónimo de una buena imagen, competitividad y solidez.

De igual manera que se hizo con los beneficios, también es necesario mirar los riesgos desde el punto de vista de los consumidores y desde el punto de vista de los vendedores. Los principales riesgos están asociados a la seguridad en la transmisión de la información y en las transacciones electrónicas; en muchos casos, se encuentran sitios web que no cuentan con un sistema de seguridad de la información que permita tener en reserva y confidencialidad la información relevante proporcionada por los usuarios, por su parte las organizaciones comerciales y vendedores deben proporcionar un sistema de seguridad de la información que permita tener la información de los usuarios protegida de manipulación, robo, adulteración de identidades, entre otros. Cuando una compañía ó vendedor incorpora la red de internet como uno de sus canales comerciales, implícitamente asocia al desempeño de su organización una serie de riegos propios de la red tales como virus, spam, hackers y otras amenazas a la seguridad que más adelante se tocarán.

7. ACTIVIDADES Y MEDIOSDE INFLUENCIA DEL COMERCIO ELECTRONICO

La *OCDE* (*Organización para la cooperación y el desarrollo económico*), formuló una clasificación de las actividades comerciales dentro del comercio electrónico de acuerdo a las ofertas, mercados y acciones propias de cada una de estas categorías, ellas son:

7.1 COMPRA Y VENTA DE PRODUCTOS

Esta categoría incluye la comercialización y/ó negociación de un bien usando cualquier tipo de transacción electrónica.

7.2 VENTA Y PRESTACIÓN DE SERVICIOS

En este punto se incluye cualquier tipo de servicio que se aplique digitalmente (servicios de soporte de escritorio, asistencia técnica por medios electrónicos, consultas, entre otros,) el cual es vendido ó solicitado por algún consumidor. Estos tipos de servicios están diseñados con un enfoque puramente digital, para ser usados ó aplicados vía internet, redes u otro tipo de medio electrónico.

7.3 COMERCIALIZACIÓN DE SOFTWARE

Esto incluye la compra-venta, comercialización, descargas y actualizaciones de programas y/ó aplicaciones desde la internet ó algún otro medio electrónico.

7.4 SUMINISTRO DE INFORMACIÓN

Esta categoría involucra la venta, comercialización ó intercambio de información, contenidos especializados, catálogos, noticias, entre otros, por medio de transacciones electrónicas.

7.5 PUBLICIDAD

La internet es el medio por el cual se puede dar a conocer productos y/ó servicios de manera masiva y también de manera sectorizada con menos costos, mas rápido y mejor enfocado a mercados específicos de interés.

7.6 ENTRETENIMIENTO

Esta categoría incluye la comercialización y compra-venta de cualquier producto y/ó servicio de entrenamientos, ocio, juegos y novedades.

7.7 COMERCIO GLOBALIZADO

Aquí se incluye aquellos tipos de modalidad comercial ó intercambio de información que involucra e incluye la prestación de servicios de manera digital alrededor del mundo, las 24 horas del día y todos los días del año. En esta categoría están incluidos los servicios meteorológicos, comercio de divisas y acciones, servicios especializados, entre otros.

Para un vendedor ó empresa, es muy importante figurar en la internet. Esta presencia se define por el grado de influencia en los medios que quiere plasmar en el mercado, en sus consumidores ó proveedores, de tal manera, la forma de figurar en internet es mediante la creación de un portal web, sitio web, pagina web, entre otros, de su compañía, servicios ó productos, por lo tanto, podríamos definir cuatro tipos de formas de cumplir este objetivo según la complejidad de ese grado de influencia que se desea reflejar en sus consumidores, mercado ó proveedores:

7.8 SITIO WEB INSTITUCIONAL

El objetivo primordial de este tipo de aplicación es poder exhibir la compañía ó vendedor en el internet. Para ello, es necesario el diseño de una pagina web en donde la compañía ó vendedor expone a sus visitantes las actividades a las cuales se dedica, su funcionamiento, constitución, entre otra información institucional. Con esto se promueve la publicidad y divulgación de la compañía en el mercado. Se ha observado que algunos optan por incluir un catalogo virtual de los productos ó servicios ofrecidos, en donde incluyen cierta información y características de ellos.

7.9 SITIO INTERNO CORPORATIVO

Con esta aplicación, se pretende optimizar y apoyar los procedimientos internos de las compañías ó vendedores, adicionalmente, optimiza la comunicación entre las diferentes partes que podrían constituir una compañía. En otras palabras, se podría denominar una *intranet*. Así, la compañía se apoya en la red de internet para compartir, transmitir, publicar ó intercambiar información pero solo dentro de las fronteras virtuales de la empresa representadas en su intranet.

7.10 SITIO E-COMMERCE

Con el diseño y aplicación de esta modalidad ya se busca la venta y compra de los productos ó servicios que la compañía ofrece a sus consumidores por medio del internet utilizando un sitio web. Aquí, el vendedor tiene la posibilidad de implementar un sistema de pago electrónico que sea eficiente, automático, de fácil manejo y ante todo, seguro.

7.11 SITIO INTERACTIVO

Esta modalidad apunta a optimizar la comunicación e interacción entre las partes que completan una compra-venta electrónicamente. Esto se logra creando un sitio que permita reunir, fusionar y complementar las distintas actividades virtuales y las actividades físicas del mundo real que efectúan todas las partes que constituyen en su totalidad una transacción electrónica, así, lograr aunar todos los procedimientos tanto internos y externos de la compañía, socios, consumidores, proveedores, logística, entre otros.

Se ha observado que el comercio electrónico tiene tres puntos de vista desde los cuales se le da un enfoque particular a esta modalidad de comercio, estos puntos son el ámbito comercial ó de negocio, la perspectiva de las comunicaciones y el punto de vista de la prestación servicios. Desde el punto de vista comercial, el comercio electrónico podría verse como la inclusión de nuevas tecnologías en los procesos de gestión, logística, automatización de procesos empresariales, entre otros que permiten un mejor proceso de comercialización de los productos ó servicios. Por otro lado, enfocando el comercio electrónico desde la perspectiva de las comunicaciones, se podría indicar que el comercio electrónico es una forma de intercambio de datos e información, productos, servicios ó pagos, el cual utiliza cualquier método de comunicación ótransacción electrónica como teléfonos, computadores, entre otros. Ahora, viendo el comercio electrónico desde el punto de vista de la prestación de servicios, podríamos formular que el comercio electrónico es una herramienta que permite gestionar acercando y estrechando las relaciones entre las partes involucradas en cualquier tipo de transacción electrónica.

8. PARTICULARIDADES DEL COMERCIO ELECTRONICO

De acuerdo al tratamiento y desarrollo del comercio electrónico, se ha podido determinar que el comercio electrónico posee ciertas particularidades que hacen posible que el comercio electrónico se destaque y sea mas prolijo para todas las partes que se involucran en esta actividad, estas particularidades están involucradas en todas las etapas de cualquier transacción electrónica, desde las consultas, pedidos, pagos y entrega, ellas se han podido enunciar de la siguiente manera:

8.1 PERSONALIZACIÓN

Con esto, el comercio electrónico tiene la posibilidad de tener mediante las tiendas virtuales, información detallada tanto de productos ó servicios, clientes, proveedores y las transacciones previas que se hayan realizado entre ellos. Se podría llevar una trazabilidad, tener y consultar bases de datos y entregar información adicional sobre los productos ó servicios ofrecidos. Hay un mayor y mejor flujo de información entre las partes involucradas.

8.2 DENSIDAD Y CALIDAD DE INFORMACIÓN

Esto involucra la cantidad, utilidad y confiabilidad de la información que se suministra acerca de los productos ó servicios en el mercado. En el comercio electronico se puede encontrar una gran cantidad de información de este tipo y diariamente crece, lo mas importante es determinar que información es la mas útil y relevante.

8.3 INTERACTIVIDAD

Esto indica la mayor y mejor fluidez de comunicación entre las partes que se involucran en las transacciones electrónicas. El comercio electrónico permite una comunicación bidireccional (consumidor-vendedor, vendedor-proveedor) mas detallada.

8.4 MULTIMEDIA

Con la ayuda de las nuevas tecnologías y la internet, es posible hacer mas llamativo para el consumidor los productos ó servicios ofertados, promociones, descuentos, entre otros. La multimedia permite agregar movimiento, color, fotografía, videos, texto, imágenes, etc. Que podría mostrar mas detalladamente, de mejor manera y mas atractivo para el consumidor.

8.5 ESTÁNDARES

Debido a que elinternet es un medio globalizado, esto ha permitido establecer normatividades ó procedimientos a nivel mundial para la participación en el comercio electrónico. Lo que permite a las partes que están involucradas en tal actividad hablar un mismo idioma y una misma manera de efectuar las transacciones electrónicas, haciendo este tipo de actividad más fácil de efectuar, con mayor y mejor acceso a consumidores y mercados. Para inmiscuirse en el comercio electrónico se cumplen ciertos pasos que son los mismos que se aplican en todos los sitios web de comercio electrónico a nivel global.

8.6 GLOBALIZACIÓN

Esto indica que el mercado existente para las compañías y vendedores que están en el comercio electrónico son todos aquellos consumidores a nivel mundial que

tienen acceso a internet ó cualquier otro medio de telecomunicaciones. Con el comercio electrónico las fronteras comerciales internacionales, nacionales e incluso en ocasiones regionales se rompen. Se pretende llegar a todos los rincones en donde las nuevas tecnologías de la información nos lleven.

8.7 UBICUIDAD

Esta particularidad indica la disponibilidad total del comercio electrónico para el *consumidor y vendedor*, es decir, que el comercio electrónico no duerme, lo podemos realizar desde cualquier punto con acceso al internet, a cualquier hora y cualquier día. Diferente al comercio convencional en donde debemos hacer presencia física para realizar cualquier compra y venta de un producto ó servicio.

9. SEGURIDAD EN EL COMERCIO ELECTRONICO

Hoy en día, se observa que los usuarios consumidores tienen un bajo nivel de confianza para usar la internet como canal para usar un determinado medio de pago electrónico en las transacciones electrónicas. Con frecuencia, los pagos electrónicos los efectúan los consumidores utilizando el número de su tarjeta de crédito y contraseñas, realizar este procedimiento no siempre es seguro en la internet sin tener los conocimientos y herramientas adecuadas y seguras para efectuar este proceso. Con esto mente, se podría pensar también que los consumidores que emplean sus tarjetas de crédito para realizar los pagos electrónicos, no tiene la certeza de la autenticidad y legalidad de la identidad del vendedor, homologo a esto, el vendedor también se ubica en tal situación. Los usuarios que emplean sus tarjetas de crédito para realizar los pagos electrónicos no pueden tener plena certeza que su número de tarjeta de crédito y contraseñas sean capturados y empleados de manera inadecuada ó maliciosa, semejante a esto, el vendedor no tiene plena certeza de que tal tarjeta de crédito cuente con los fondos suficientes ó sea legal para concretar la compra-venta.

Como se mencionó anteriormente, una de las desventajas y quizá la más importante del comercio electrónico es la *seguridad* en las transacciones electrónicas y las redes. Se podría indicar, que la seguridad en las transaccioneselectrónicas tiene el mismo nivel hasta cierto punto que las compras realizadas en el mundo real y físicamente, esto depende en gran parte también del nivel de seguridad que nosotros mismos como usuarios, consumidores ó vendedores implementemos. Sin embargo, ésta desconfianza expresada por las partes involucradas en una transacción electrónica y la comunidad en general, se ha producido en gran medida por la falta de información ó información incorrecta sobre la implementación y uso de las transacciones electrónicas en el comercio electrónico, además, muchas personas creen hoy en día que la internet es un medio inseguro. Por talesrazones, los usuarios, consumidores y/ó vendedores

generalmente tienen desconfianza a tres puntos principales dentro del proceso de la conclusión de una compra virtual ó cualquier otro tipo de transacción electrónica, los cuales son:

a. Tener una reacción negativa ó de desconfianza al tener que proporcionar sus datos personales ó comerciales y que estos puedan ser usados de manera fraudulenta.
b. Mostrardesconfianza al momento de elegir los medios de pagos debido a que sus tarjetas de crédito ó información comercial sufra algún tipo de ataque y caiga en manos inadecuadas.
c. Experimentar desconfianza por las tiendas ó vendedores virtuales que son poco conocidas ó de las cuales no se tienen muchas referencias, ya que estas podrían comportarse como fachadas para actividades ilícitas, podrían no existir, entre otros obstáculos.

Se podría señalar también, que la seguridad en las transacciones electrónicas generalmente sufre ataques de virus, troyanos, hacker, gusanos, entre otros tipos de ataques. Estos tipos de amenazas realizan ataques a los equipos, bases de datos, inventarios, software, hardware, entre otros sistemas informáticos. Estos ataques, en muchos casos son realizados a redes, software, entre otros sistemas que manejan gran cantidad de información y a su vez muy importante, ésta actividad podría llevar a los usuarios a tener serios líos con su información tales como:

a. Suplantaciones de identidad (Phising).
b. Pérdidas económicas y financieras como resultado de transacciones de fondos ó información no autorizada por los usuarios de una cuenta a otra. Robos y estafas electrónicas.
c. Perdida de información confidencial ò de gran valor como patentes, derechos de autor, procedimientos específicos, entre otros.

d. Perdida en posible apertura de nuevos ó ampliación de negocios, ya que por medio de un ataque informático se podría llegar a deshabilitar, desaparecer, cambiar el estado ó disponibilidad de un sitio web de una compañía ó vendedor. Lo cual traería graves consecuencias comerciales a los afectados.
e. Acceso y uso de los recursos de un sitio web de manera inadecuada ó ilegal, haciendo uso de información privilegiada de manera fraudulenta.
f. Uso de publicidad engañosa, falsa ó negativa que se podría plasmar dentro del sitio web de un vendedor ó empresa que llevaría a que los usuarios pierdan su respeto y confianza en un sitio web.

Estos riesgos informáticos y los que se puedan asociar de similar manera, pueden llegar a disminuirse si las compañías y vendedores implementan serias, sanas y efectivas formas y prácticas de combatir los ataques informáticos en sus tecnologías aplicadas de las telecomunicaciones. Es importante recordar, que no todos los riesgos y ataques informáticos a los consumidores y vendedores pueden ser combatidos y reducidos por los métodos tradicionales de seguridad y prevención informática.

La seguridad en el comercio electrónico enfoca su trabajohacia cuatro directricesbásicas, las cuales ayudan a proporcionar un mayor nivel de seguridad en las transacciones electrónicas y el comercio electrónico en general, estas directrices son la *integridad*, la *confidencialidad*, la *autenticidad* y el *no repudio dela información*.

a. La *integridad* de la información hace referencia a la verificación de los datos transmitidos y almacenados, para que éstos no sobrelleven ningún tipo de alteración que pueda llevar a que ellos sean falsos, estén incompletos ó implícitamente contengan algún otro tipo de amenazas como virus, troyanos, entre otros. El propósito es evitar que la información sea manipulada, modificada ó intervenida.

b. La *confidencialidad* de la información, refiere a las vías establecidas para determinar quien y quien no tiene la facultad para ver ó tomar los datos transmitidos. El propósito de ésta directriz es conducir a que las transacción electrónicas sean privadas y de carácter secreto, de tal manera que ningún agente externo salvo las parte involucradas en las transacciones puede acceder y descifrar la información contenida.
c. La *autenticidad*, apunta a que se de una verificación e identificación de las partes involucradas en cierta transacción electrónica. Invita a determinar la coincidencia en la identidad de los individuos.
d. El *no repudio de la información* apunta a establecer que cierto usuario quede identificado como el propietario, actor ó emisor de la información transmitida ó la transacción electrónica efectuada sin que él tenga la posibilidad de negar tal condición ó su transacción electrónica.

Es claro mencionar que sin unas políticas ó estrategias de seguridad en las redes de telecomunicaciones, el comercio electrónico no será explotado ni aprovechado en todas sus dimensiones y aun más importante, la confianza transmitida por los consumidores tendría la tendencia a ser nula. La seguridad en el comercio electrónico debe ser entendido como una arquitectura de seguridad, de tal manera que ella se enfoque en las amenazas internas y externas a la seguridad de la información, además, el hecho de entender la seguridad como una arquitectura, crea la necesidad que ésta sea escalable con el transcurso del tiempo y con el aumento en la necesidades de seguridad en las ya crecientes redes de telecomunicaciones. La seguridad en las redes de telecomunicaciones y el comercio electrónico también trabaja en la protección de los activos de las compañías y vendedores, como regla general, las organizaciones comerciales y vendedores deben entender que la seguridad de la información se interpreta como un costo asociado al bienestar y crecimiento de las compañías y no como un agente generador de utilidades y dinero.

9.1 MEDIDAS BÁSICAS PARA MEJORAR LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Con el aumentodel uso del comercio electrónico y las transaccioneselectrónicas en la red global de internet y el aumento, mejoramiento y surgimiento de nuevas tecnologías, desarrollo de software y hardware, implícitamente y en paralelo crecen los riesgos a la seguridad en los medios de telecomunicaciones asociados a las transacciones electrónicas. Por tal motivo, el comercio electrónico y la internet buscando reducir los riesgos mencionados, se han enfocado en tener en cuenta cuatro puntos fundamentales para el desarrollo de medidas básicas que permitan comprender y reducir los riesgos de amenazas y ataques informáticos, esto puntos son:

a. El aumento en el número de usuarios consumidores que pretenden realizar transacciones electrónicas en las redes de telecomunicaciones de manera segura para adquirir un producto ó servicio aumenta considerablemente a diario.
b. Los vendedores, consumidores y empresas buscan métodos y aplicaciones prácticas, de fácil manejo y amigables para el usuario, que permitan la ejecución de las transacciones electrónicas, además, los buscan seguros y a bajos costos.
c. Los bancos y entidadesfinancieras, buscan que las compañías desarrolladoras de software, provean a estas entidades de aplicaciones y software con altos estándares de calidad y seguridad, además, que los proporcionen a precios competitivos.
d. Los bancos, entidades financieras, los vendedores, compañías físicas y virtuales, consumidores, compañías administradoras de medios de pagos (tarjetas de crédito, debito, micro pagos, etc), entre otros, pretenden y deben definir su tipo y manera de establecer su modalidad de comercio electrónico sin llegar a afectar su estructura y procedimientos comerciales.

De acuerdo a los puntos anteriores, para llegar a establecer una solución optima, que ayude a definir el modelo de comercio electrónico que mas se ajuste a las necesidades y características de las partes involucradas y a las transacciones electrónicas; las compañías, vendedores, consumidores y proveedores desempeñan un papel fundamental en definir y establecer lineamientos y especificaciones que lleven al desarrollo de las soluciones, éstos lineamientos deberían ofrecer:

a. Confidencialidad en las telecomunicaciones y transacciones electrónicas.
b. Autenticar los actores en las transacciones electrónicas.
c. Proporcionar integridad en el manejo de la información.
d. Proveer disponibilidad de los recursos y servicios ofrecidos.

9.2 PRINCIPALES AMENAZAS YMECANISMOS DE INTRUSIÓN EN CONTRA DE LA SEGURIDADEN EL COMERCIO ELECTRÓNICO

Con el uso de la internet y el comercio electrónico, implícitamente se acarrean una serie de amenazas, que los vendedores y consumidores deben atender para no poner en riesgo toda la información útil y significativa cuando se este usando el comercio electrónico ó cualquier otra transacción electrónica.

Se podría entender por amenaza, cualquier situación, condición ò acción en un entorno de red de telecomunicaciones, que permita a un intruso ò atacante violar la seguridad, confidencialidad, integridad y disponibilidad de los servicios, recursos, información, etc., de tal red con propósitos inadecuados ò ilegales. La amenazas a la seguridad en un entorno de red de telecomunicaciones y a las transacciones electrónicas, se puede dividir en dos tipos, las *amenazas externas* y *amenazas internas*.

9.2.1 Amenazas externas. En ésta primera, el intruso se encuentra fuera del entorno de cierta red de telecomunicaciones ó fuera de la compañía, es una persona ó software externo a la organización que no pertenece y no tiene acceso a los servicios, recursos , productos y/ó información clasificada. Estas amenazas son las que reciben mas atención, la razón para esto, es el temor a los atacantes externos y desconocidos, quienes podrían hacer uso del internet publica para acceder a la información de manera fraudulenta y con propósitos oscuros.

9.2.2 Amenazas internas. Las *amenazas internas*, son las mas complicadas de detectar, controlar y neutralizar, la razón de ello, es que los ataques y el intruso se encuentra dentro de la organización y el entorno red de telecomunicaciones, también posee acceso a información, usuarios, contraseñas, entre otro tipo de información relevante y confidencial.

Generalmente, las amenazas en la seguridad en las transacciones electrónicas, están dirigidas al hurto de dinero por parte de los atacantes, con el objetivo de no ser descubiertos, se han desarrollado una serie de tipos de ataques a los usuarios y a las transacciones electrónicas; estas se podrían enunciar de la siguiente manera:

9.2.3 Carding y Skimming. Este tipo de amenaza es común por nuestros días. Se comporta como un doble proceso, en ellos, el atacante actúa usando tarjetas de manera ilícita y fraudulenta (*carding*) y posteriormente efectúa la copia y robo de información impresa en la banda magnética adjunta a las tarjetas (*skimming*). Con este modelo de proceder, el atacante podría obtener información personal de los usuarios, números de cuentas bancarias, numero de tarjetas entre otra información confidencial de los usuarios.

9.2.4 Pharming. Con este método de amenaza, el atacante podría instalar en la computadora del usuario (sistema operativo de computadores y servidores) algún

tipo de software, aplicación ò plugin, que tomará información y la enviará al atacante, lo cual sucede de manera transparente al usuario, también podría efectuar acciones como denegar servicios, entre otros. En la mayoría de los casos, se ha observado que este tipo de software malicioso reside de manera indefinida en las computadoras hasta que sea detectado y eliminado. Las aplicaciones más usadas en la actualidad son los denominados *Troyanos*, con el uso de este tipo de amenaza, se podría abrir paso a la ejecución de otro tipo de amenaza como el *Man in themiddle*, un Troyano, permitiría a un atacante ubicarse entre una dirección IP y el nombre del servidor al que responde. Los Troyanos y otros tipos de software malicioso pueden crear *backdoors* y accesos no autorizados a los equipos de los usuarios sin su aprobación previa. Este modelo de amenaza deja vulnerable los equipos de usuarios finales, lo que lleva al robo de su información y tener control de manera remota sobre el equipo victima.

9.2.5 Clickhacking. Este tipo de ataque, actúa en la mayoría de los casos sobre los navegadores, entre otros servicios y productos web. Su proceder se basa en capturar ó manejar remotamente el click sobre los tabs, pestañas, botones, etc. en los browser ò servicios web de los usuarios. Con este tipo de amenaza, el atacante ejerce control sobre el equipo final, conduciendo de manera forzosa y engañosa al usuario a *clickear* sobre cierto vinculo ò link en el browser ò unapágina web, lo cual, conduciría al usuario final a otros sitios web con virus y otras amenaza asociadas sin que el usuario lo perciba.

9.2.6 Malware. El objetivo de este tipo de amenaza, es el robo de información de acceso a diferentes sitios de uso frecuente e importante por parte de cierto usuario. Con este tipo de amenaza los códigos maliciosos se enfocan en el robo de datos en aquellos sistemas infectados.

9.2.7 Spyware. Este tipo de amenazas están definidas como una serie de códigos malintencionados, diseñados con el propósito de capturar información útil, valiosa

y confidencial de los usuarios. Generalmente usa un tipo de gusano ó troyano para que el atacante pueda acceder y controlar remotamente cierto tipo de red de computadores. En muchos casos, los atacantes usan el *keylogger*, el cual se podría definir como un tipo de aplicación que permite al atacante determinar que teclas han sido pulsadas en el teclado de la victima.

9.2.8 Phishing. Este tipo de amenaza también permite a los atacantes el robo de información útil y confidencial de los usuarios. Con este tipo de amenazas, el atacante adquiere información básica y relevante de los usuarios realizando la simulación de alguna identidad falsa de las victimas y usuarios, el atacante realiza una suplantación de identidad que permite acceder a lo servicios e información de los usuarios.

9.2.9 Scam. Este tipo de amenaza esta enfocada en los sitios web de empresas y vendedores. De esta manera, los atacantes usan sitios web como método para realizar los robos. En la mayoría de los casos, lo atacantes crean perfiles, sitios web, productos, servicios, entre otros, totalmente falsos ó inexistentes con el propósito de engañar a los usuarios implementando datos y reputación de otros vendedores ó empresas que también puede ser falsos ò de los cuales también se ha robado información.

Conociendo los tipos de amenazas contenidas en las redes de telecomunicaciones, es común escuchar de los consumidores y vendedores que usan el comercio electrónico preguntarse si las compañías, vendedores ò sitios web son seguros, si tal compañías ò vendedores son confiables y corresponden al tipo de servicio ó producto ofrecido ó si la información suministrada por las partes para completar las transacciones electrónicasexperimenta algún tipo de riesgo, también es común preguntarse si la figura detrás de cierto sitio web es realmente quien estipula ser ó se hace pasar por alguien más y como se dispone toda la información suministrada por las partes.

Además de los tipos de amenazas mencionadas anteriormente, es importanteconocer las partes que están involucradas dentro de los procesos de transacciones electrónicas fraudulentas, estas partes son:

a. El *usuario* ó *consumidor*, quien dispone de un servicio de redes de telecomunicaciones, una computadora ó dispositivo y un navegador que le permitirá buscar y ubicar el sitio web de su interés en donde encontrará el producto ò servicios requerido.
b. El *sitio web* del vendedor ó compañía.
c. Los *proveedores*, generalmente son agentes externos, los cuales actúan como complementos para realizar las transacciones de manera confiable y segura. (Estos pueden ser, los proveedores de servicios de internet, lo bancos ó entidades financieras que proporcionan los medios de pago, entre otros).
d. El *intruso* ó *atacante*de la red de telecomunicaciones, quien se responsabiliza de usufructuar a los consumidores, los sitios web y proveedores con el propósito de obtener beneficios de manera fraudulenta.

Con frecuencia, los intrusos antes de realizar los ataquesinformáticos a las redes de telecomunicaciones, aplicanciertos procedimientos y mecanismos para detectar los puntos débiles, comportamientos y movimientos de sus victimas en la red, de esta manera determinarían el tipo de ataque y la manera de actuar del intruso haciendo que nuestra información sea vulnerable. Estos mecanismospodrían enunciarse así:

9.2.10 Embaucar al consumidor. En este mecanismo, el intruso realiza un seguimiento al comportamiento de la victima. Generalmente actúan para obtener nombres de *usuarios de registro y contraseñas*, en sitios web de entidades financieras y bancos, redes sociales, sitios web de suscripciones, entre otros.

9.2.11 Seguimiento a dispositivos finales. Desafortunadamente, hoy aun existen una gran cantidad de usuarios y consumidores que desconocen las amenazas y vulnerabilidades de las redes de telecomunicaciones, debido a esto y otros factores como falta de conocimientos en el manejo de los dispositivos finales, los usuarios llegan a desactivar ó eliminar ciertas propiedades y funciones de seguridad de sus dispositivos finales, haciendo de ellos unos dispositivos vulnerables a los ataques informáticos por parte de un intruso, quien no desaprovecharía una situación como la mencionada para aplicar alguna de sus técnicas y conocimientos para determinar tal punto débil en los dispositivos finales y acceder a la información.

9.2.12 Espiar la red. El uso de este procedimiento, implica que el intruso tenga control sobre los datos que fluyen entre los dispositivos finales y los servidores, también tiene la posibilidad de interceptar paquetes de datos que fluyen entre servidores, esto lo logra con el uso de algún software criptográfico que permite descubrir la información que circula en la red.

9.2.13 Violación a la privacidad y a la seguridad. Durante el flujo de datos e información entre el origen y el destino, estos en la mayoría de los casos deben pasar por dispositivos ó aplicaciones que se encuentran en el camino y en ellos podría suceder la copia, modificación, captura, entre otros procesos que son trasparentes a los usuarios y que podrían poner en riesgo la información y datos puestos en la red. En muchos casos, la información se usa encriptada con algún método de los que actualmente existen y los cuales son difíciles de descifrar. En ciertos casos, la información se podría poner en riesgo al encontrar *plugins* (Java scripts, ActiveX, etc.) implícitos en los sitios web de empresas y vendedores para descargar y digitar información sobre ellos como parte del proceso de la transacción electrónica.

9.2.14 Robo y fraude en el internet. Este tipo de proceder se da cuando los intrusos intentan convencer ó engañar a los usuarios y consumidores a usar, acceder ó realizar cualquier tipo de transacción electrónica con sitios web que no cuentan con una buena reputación, no son conocidos ó simplemente son sitios web creados por los atacantes como fachadas de comercio electrónico legitimo, pero en el trasfondo es usado para actividades ilegales. Los consumidores son dirigidos a proporcionar información y realizar pagos por servicios ó productos inexistentes.

9.2.15 Intervención a la integridad de los datos. En muchos casos, las falencias en la integridad de los datos ocurre de manera accidental pero también existe la gran probabilidad que la modificación de los datos sea intencional, con el propósito de adquirir y usar información de manera inadecuada. La alteración en los datos desde el origen al destino podría ocasionar un gran impacto en las actividades comerciales de vendedores y compañías en el internet.

9.2.16 Denegación de servicios de internet. El propósito de este tipo de ataque, es tumbar servicios disponibles en el internet para los usuario y consumidores. Este tipo de proceso causa un gran impacto negativo en los vendedores y compañías. Los atacantes se valen de herramientas y conocimientos avanzados de informática para explotar las debilidades de los protocolos de comunicaciones en internet, los cuales, son los medios para realizar el uso y poner a disponibilidad de usuarios y consumidores muchos servicios para el uso de internet y las transacciones electrónicas.

9.3 MÉTODOS DE PROTECCIÓNEN CONTRA DELAS AMENAZAS EN LA RED

Teniendo en cuenta los mecanismo y tipos de amenazas en contra de la seguridad en el comercio electrónico y la manera en que los atacantes buscan las vulnerabilidades de las redes y sistemas de telecomunicaciones, es de suma

importancia y necesario diseñar e implementar barreras, protecciones, procedimientos, protocolos, entre otros tipos de artilugios y medios para reducir los riesgos de fraude y robo de información relevante de los usuarios. Para consumar y realizar este propósito, tanto los ingenieros como las partes involucradas en la creación, implementación y uso de estos artilugios podrían tener en cuenta ciertos requisitos elementales, tales como:

9.3.1 Implementar políticas y procedimientos de seguridad para el uso de los sistemas de telecomunicaciones. Esto aplica para las compañías y vendedores, quienes cuentan con personal que tiene acceso a los medios, servicios, recursos, dispositivos, etc., de las entidades a las que pertenecen. Esto se menciona, teniendo en cuenta que la razón de la mayoría de los casos de ataques y amenazas en la seguridad proviene del interior de las propias entidades.

9.3.2 Proporcionar seguridad perimetral en las redes detelecomunicaciones. Este punto hace referencia a laimportancia de implementar servicios de Firewall, antivirus, sistemas de autentificaciones, VPN, entre otros.

9.3.3 Proveer métodos y procedimientos de autorización. Esto indica valerse de mecanismos y protocolos que permitan autorizar ó denegar el uso de recursos, aplicaciones y datos propios de la red de telecomunicaciones, además, de gestionar la autorización de acceso e interacción de usuarios con la red.

9.3.4 Emplear sistemas de encriptación. Es importante implementar métodos de clave pública y privada que garanticen la integridad y autentificación de los datos, información y aplicaciones en redes y sistemas con altos niveles de riesgo y que requieran mejores controles y trazabilidad a los procesos que en ellas se ejecutan.

9.4 ELEMENTOS A PROTEGER DE LAS AMENAZAS Y ATAQUES EN COMERCIO ELECTRÓNICO

Para comenzar con la implementación de la seguridad en las transacciones electrónicas, es básico identificar que elementos son los más importantes por proteger de los riesgos informáticos y que aportarían en gran medida a evitar la captura de la información de los usuarios. Teniendo en mente esto, se podría establecer algunos componentes elementales del comercio electrónico que cumplen un rol significativo al momento de efectuar las transacciones electrónicas, que deben ser protegidos y evitar el fraude, esta protección debe ser constante y se debe ir adaptando a los cambios en la informática, ya que en caso de que alguno de ellos falle, la red de telecomunicaciones, su información, recursos, servicios, etc., estarían en riesgo y ese elemento particular se convertiría en una vulnerabilidad que los intrusos no dudarían en atacar. Podríamos enunciar estos elementos a proteger como el *sistema operativo de los servidores*, el *software delos servidores web*, el *transporte de los datos* y el *software browser de usuariosfinales*.

9.4.1 Seguridad del software de browser de usuarios finales. Este componente indica la seguridad que debe establecerse en el software que emplean los usuarios finales para ingresar a la red y navegar en ella (Mozilla, GoogleChrome, Internet Explorer, entre otros). En estos componentes, priman las vulnerabilidades propias de los navegadores y los componentes web activos. Los componentes web activos tales como ActiveX, Applets de Java, entre otros son muy comunes encontrarlos hoy día en las redes de telecomunicaciones, ellos permiten la ejecución, carga, descarga, navegación, entre otras funciones en distintos sitios web. Con los componentes y contenido web, existen ciertos riesgos que están implícitamente en ellos y en un segundo plano, sin que el usuario final se percate de ello, se ejecutan códigos maliciosos. Por otra parte, sucede que con los navegadores, a los usuarios finales no les queda otra alternativa que confiar en

que su navegador no sea vulnerable a los ataques en las redes de telecomunicaciones, la razón de esto, es que en general, no se cuenta con el código fuente de ellos que permita su verificación, análisis y búsqueda de vulnerabilidades que contenidas.

9.4.2 Seguridad en el transporte de datos. Este componente es el que más esfuerzos y recursos ha recibido con el propósito de garantizar *la seguridad de la información y reducir los riesgos de ataques*. Este punto es primordial en la seguridad en las redes de telecomunicaciones, ya que garantizando la seguridad en el transporte de los datos, se está garantizando la confidencialidad, la autenticidade integridad de la información. La necesidad de implementar este tipo de seguridad, surge de la inseguridad que lleva en si el uso de la red de internet, en ella, los datos podrían ser capturados, leídos, modificados, eliminados, etc., por un atacante durante el flujo de ellos en los diferentes medios y canales de transporte de la información. Para proporcionarle mayores niveles de seguridad al transporte de los datos, se han diseñado e implementado diferentes artilugios como las firmas digitales, criptografía, certificados de autenticidad, protocolos de comunicaciones seguras tales como el SSL (*Secure Socket Layer*), el cual, es el protocolo estándar usado hoy día para la transmisión de manera segura de los datos e información en la red de internet y el protocolo TLS (*Transport Layer Security*) estos últimos dos, son los protocolos en los cuales se enfoca esta monografía, también existe el protocoloSET (*Secure Electronic Transaction*).

9.4.3 Seguridad en los servidores web. Los servidores web están compuestos por tres elementos; *los programas yaplicaciones de interfaz* entre los software del servidor web y *lasbases de datos* contenidas, las bases de datos del los servidores web que incluyen la información de usuarios, además, contiene información sobre productos y servicios., el otro elemento es el *software del servidor*, quien es el responsable de contestar todas las solicitudes de conexión e información procedentes de los navegadores de los usuarios. Se ha observado,

que generalmente, los intrusos enfocan sus ataques al software del servidor y el software de las interfaces entre las bases de datos y el software del servidor. Es claro afirmar, que en un determinado servidor web, es directamente proporcional el número y nivel de vulnerabilidades a la cantidad y tipo de servicios que dicho servidor ofrece. Además de las fallas de seguridad contenidas en los servicios que pueda ofrece un servidor, se deben sumar las fallas de seguridad en los programas, ellas están contenidas en el código de programación de ciertas aplicaciones y programas, son muy comunes y conducen a la ejecución anormal e insegura de ellos, ésta condición es bien conocida y explotada por muchos atacantes, para ello, es importante contar con actualizaciones, controles y vigilancia en las versiones de software que se emplean, éstas actualizaciones modifican ò eliminan estos errores de programación. El software de los servidores web, posee un administrador ò root, quien realiza la instalación de ellos y posee todos los accesos y derechos sobre todo el sistema, por lo tanto, estos administradores tiene privilegios sobre la ejecución de dichos programas, entre esos privilegios podemos encontrar poder abrir los puertos 80 (*http*) y 443 (*SSL*) ò realizar modificaciones sobre los archivos de registro del sistema. Por tal motivo, es importante pensar en muchos casos y de acuerdo a los niveles de seguridad establecidos, crear restricciones a los privilegios de ejecuciones de aplicaciones ò programas y usos de puertos mediante la configuración del software del servidor. Es indispensable que los servidores web cuenten con mecanismos que permitan tener controles de acceso, lo cual reduce en gran medida las vulnerabilidades y riesgos de ataques, estos mecanismos de seguridad para el control de acceso se podrían ser *las restricciones por dirección IP ó por nombre de host, autenticaciones por contraseñas y autenticación por certificados digitales*.

Para el propósito de esta monografía, solo se hará mención a la *autenticación por certificados digitales*. La razón de esto, se basa en que al efectuar el control de acceso por medio de la implementación de certificados digitales, se esta implementado a su vez el protocolo de seguridad *SSL*. Este mecanismo se logra

implementar cuando los clientes poseen sus certificados digitales emitidos por cierta entidad certificadora. Estos certificados digitales, contienen la información de los clientes, como también, contienen las claves necesarias para efectuar la encriptación de la información. Esto es un procedimiento transparente a los usuarios y le imprime un mayor nivel de seguridad a las transacciones electrónicas.

9.4.4 Seguridad en el sistema operativo. Es claro que todas las aplicaciones diseñadas para el comercio electrónico están basadas en alguno de los sistemas operativos existentes. Por lo tanto, si estos sistemas operativos llevan consigo algún tipo de vulnerabilidad, es muy probable que la información contenida en determinado servidor esté a merced de los ataques informáticos. En muchos casos, las vulnerabilidades ó debilidades de un sistema operativo se pueden corregir ó modificar replanteando las opciones de configuración de ellos, también se podría realizar modificando las opciones de seguridad que por defecto están configuradas dentro de ellos. Las vulnerabilidades de los sistemas operativos podrían ser *las opciones de configuración por defecto, debilidades de software de red, ataques de negación de servicios y métodos de autenticaciones débiles*.

10. PROTOCOLOS DE SEGURIDAD

Un protocolo de seguridad es un sistema ó procedimiento que regenta y especifica las normas para ejecutar las transacciones electrónicas y que éstas puedan tolerar ataques y amenazas de carácter malicioso. Los protocolos de seguridad se crean teniendo en cuenta las debilidades y vulnerabilidades de los sistemas informáticos, las necesidades de seguridad y los riesgos a la seguridad a los cuales podría estar comprometido. Los protocolos de seguridad son los canales mediante los cuales se crean los medios seguros y confiables para realizar los distintos tipos de transacciones comerciales en el internet. Emplear estos protocolos, le brinda al usuario final la seguridad y confiablidad que buscan en las transacciones electrónicas que realiza en la internet. Estos tipos de protocolos también son denominados protocolos criptográficos ò protocolos de cifrado. Estos tipos de protocolos emplean procedimientos criptográficos ó de codificación relacionados con la seguridad de la información y datos, ayudando a reducir los riesgos a que esta información sea visible ó detectada por individuos ajenos ó indeseados por nosotros, principalmente dentro de la internet, en las aplicaciones del comercio electrónico y transacciones. Los protocolos de seguridad, se han convertido en un conjunto de procedimientos empleados para la protección de servidores y usuarios del internet contra ataques malicioso a su información.

Estos protocolos manejan un lenguaje de maquina que permite la comunicación y el entendimiento entre los distintos dispositivoselectrónicos y sus lenguajes de programación, reduciendo el riesgo que estos sufran de algún tipo de ataque malintencionado. Se usan generalmente para el transporte de información a nivel de capa de aplicación con un nivel de seguridad. La implementación de un protocolo de seguridad, emplea por lo menos el uso de contraseñas, autenticación, cifrado y transporte seguro de información. Los protocolos de seguridad se pueden clasificar de acuerdo a su utilidad ó finalidad y de acuerdo a los individuos que intervienen en el intercambio de información.

Cierta información es enviada en forma de un texto plano y claro, el protocolo de seguridad trabaja mimetizando dicha información por medio de un proceso de encriptación, lo cual producirá un texto encriptado; el proceso de recuperar nuevamente la información encriptada se denomina desencriptamiento.

Los protocolos de seguridad proporcionan tres elementos primordiales sobre los cuales trabaja la seguridad de la información y los cuales se deben garantizar para proporcionar seguridad en internet y las transacciones electrónicas, estos son; la *confidencialidad*, *integridad* y *autenticidad*.

10.1 AUTENTICIDAD

Proporciona la confiabilidad que la información enviada de un origen a un destino sea entregada y recibida por el emisor y receptor auténticos y verdaderos.

10.2 CONFIDENCIALIDAD

Permite que los datos e información enviados y recibidos sean confiables a través de sistemas de encriptacion, ya que si estos son interceptados ó sufren algún tipo de ataque, la información interceptada no será útil al atacante debido a que la información se encuentra encriptada.

10.3 INTEGRIDAD

Este punto provee la garantíade permitir que la información enviada debe ser recibida por el receptor sin ninguna alteración ó modificación sufrida durante su recorrido en el medio.

10.4 SISTEMAS DE AUTENTICACIÓN

Actualmente, se usan tres tipos de sistemas para la autenticación basados en el tipo de información y el tipo de tecnología que se emplean para asegurar la identidad e información de los usuarios. Estossistemas son:

10.4.1 Contraseña/Password. Éste sistema estipula, que cada usuario debe poseer una clave ó una contraseña que le permita acceder al sistema de información y debe ser conocida únicamente por dicho usuario, seguidamente, por medio de algoritmos matemáticos, el sistema verificara la contraseña y determinará el acceso ó no a la información. Éste es el método que es más usado, básico y conocido en nuestros días.

10.4.2 Smartcards. Este método implementa la adiciónde unelemento físico que los usuarios poseen, un hardware inteligente. Este sistema provee a los usuarios con un dispositivo ó chip electrónico que le permite almacenar y procesar su información de manera segura. Estos dispositivos electrónicos, poseen capacidad de almacenamiento y cifrado de información. En la actualidad, este tipo de chip electrónico es empleado en las tarjetas de crédito ó debito en las entidades bancarias ya que permite a los bancos y establecimientos comerciales, guardar la información de los usuarios en un chip como método adicional de seguridad a un nivel superior de la banda magnética que en nuestros días es muy vulnerable a los ataques. Posee la desventaja de la necesidad del uso de hardware adicional en los dispositivos terminales para realizar la lectura y verificación de la información contenida en los mencionados chips electrónicos. También utiliza el sistema de contraseñas para la verificación y acceso a la información.

10.4.3 Autenticación biométrica. Estos tipos de autenticación son los más desarrollados tecnológicamente y costosos, se emplean para proporcionar niveles de seguridad electrónica muy altos. Para el empleo y desarrollo de estos sistemas

se ha usado y desarrollado la inteligencia y aprendizaje artificial, el seguimiento y reconocimiento de ciertos patrones. Para implementar este tipo de sistema, es necesario captar e identificar patrones y características únicas físicas de los usuarios finales, en nuestros días, los patrones mas usados son las huellas digitales, reconocimiento del ojo humano y reconocimiento de la voz. El proceso de este sistema utiliza una serie de dispositivos electrónicos que permiten captar ó leer el patrón físico del individuo, seguidamente se identificara las características de tal patrón que permitirá ó no la validación ó acceso a la información comparándola con la información almacenada en una base de datos y de referencia para tales patrones y características.

10.5 PRINCIPALES FUNCIONES DE LOS PROTOCOLOS DE SEGURIDAD SOBRE LA SEGURIDAD DE LA INFORMACIÓN

La función primordial de los protocolos de seguridad es proveer la seguridad en las transacciones electrónicas en el internet, ésta seguridad se enfoca principalmente a tres elementos básicos que constituyen una transacción electrónica:

10.5.1 Asegurar los datos e información que fluyen en los medios electrónicos entre usuarios. Con esto, se pretende reducir los riesgos de interceptar, modificar y/ó destruir la información que fluye en los canales electrónicos. Por lo tanto, se trata de camuflar la información relevante en medios de información con supuesta baja importancia usando los mecanismos de encriptación, de modo que ella no pueda ser interpretada por un atacante sino únicamente por las partes interesadas en los datos.

10.5.2 Proteger los dispositivos de los usuarios finales. Con esto, se busca que la información ó aplicaciones descargadas por los usuarios finales no les causen algún tipo de daño aellosó a sus dispositivos electrónicos.

10.5.3 Asegurar las bases de datos, servidores y la información en ellos contenida. Los dispositivos servidores deben permitir el acceso y la modificación de su información sin alterar negativamente su funcionamiento. El acceso y la capacidad para esto, solo se proporciona a usuarios autorizados y capacitados, realizando esto con la protección de los protocolos de seguridad.

Para suplir estas necesidades de seguridad, integridad y confiabilidad en las transacciones electrónicas ha surgido y se han implementado una serie de herramientas informáticas, estas son el protocolo SSL y TLS. El protocolo SSL (Capa de conexión segura) y el protocolo TLS (Seguridad de la capa de transporte) son protocolos informáticos, los cuales, permiten realizar la tarea de encriptar la información que circula en la internet, suministran la seguridad fundamental en las comunicaciones electrónicas dentro de la internet. Estos protocolos proporcionan la confiabilidad, integridad y autenticación de la información suministrada dentro de las transacciones electrónicas, se encuentra definido principalmente dentro de la publicación estándar RFC2246, aunque, posee otras publicaciones como estándar de extensión de estos protocolos. Esta herramienta informática es comúnmente usada por tiendas en internet, bancos y cualquier otro tipo deorganismo que brindeunservicio ó producto que requiera el intercambio de información personal, confidencial ó que requieran contraseñas dentro del internet principalmente. Entidades tales como VISA, MasterCard, American Express y otras grandes entidades comerciales y financieras aprueban el SSL y el TLS como mecanismo de defensa de la informaciónen el comercio electrónico.

Estosprotocolos implementan la negociación de los algoritmos que permitirán las comunicaciones entre el usuario final y el proveedor del servicio ó producto en la internet, el intercambio de claves publicas y la reserva de las privadas, la autenticación de certificados digitales emitidos por una autoridad certificadora (AC) y el cifrado de los datos para suministrar la seguridad fundamental en las

transacciones electrónicas. Estos protocolos se ejecutan de manera transparente al usuario y al proveedor del servicio ó producto y entre la capa de aplicación y la capa de transporte del modelo TCP/IP, comúnmente, se ejecutan junto al protocolo de internet http, proporcionando seguridad contra ataques conocidos como *Man in the middle*.

El proceso de la comunicación segura entre el usuario y el proveedor del servicio ó producto, se da cuando el usuario por medio de un navegador web realiza una solicitud al sitio web seguro de su preferencia, en donde indica que desea establecer una comunicación, mostrando la información sobre el protocolo SSL/TLS que maneja, seguidamente, el sitio web seguro debería responder la solicitud positivamente de acuerdo a las información de los protocolos suministrada, al realizar esto, posteriormente, el sitio web seguro deberá dar a conocer su certificado digital seguro de navegación, al obtener el navegador la información de dicho certificado, éste realizara una verificación de la integridad del certificado digital, verifica la vigencia del certificado y comprueba que éste haya sido emitido por una autoridad certificadora conocida y confiable. Una vez finalizada esta etapa, la conexión segura con el sitio web se establece y la información que fluye estará protegida en gran medida. Se debe recordar y sugerir que se requiere tomar medidas de seguridad adicionales que el usuario debe tener presente al realizar las transacciones electrónicas, ya que el uso de sitios web seguros y la implementación de estos protocolos no garantiza la totalidad de la seguridad de la información en la red, es una manera de mitigar los riesgos de seguridad informática, cada día los intrusos y atacantes afinan sus habilidades y herramientas con el objetivo de burlar la integridad y confiabilidad de la información digital.

10.6 CRIPTOGRAFÍA

Se entiende por criptografía como “el arte ó ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos”.[1]

Los pricipales objetivos de la criptogafia son:

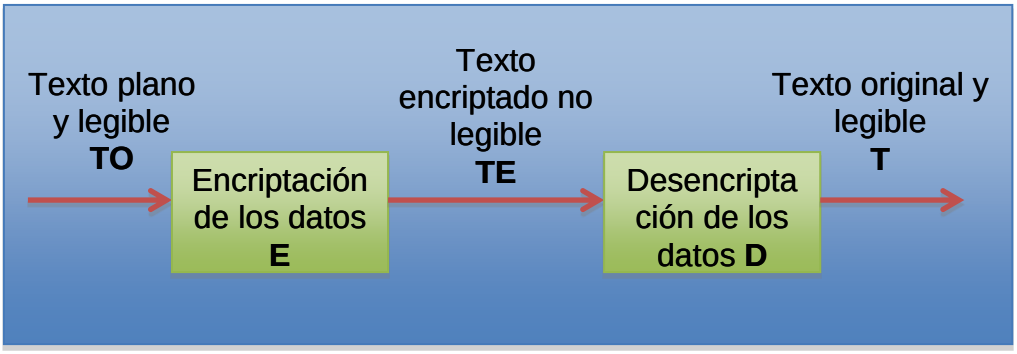
a. Garantizar la confidencialidad de la información en las transacciones electronicas.
b. Mantener la autenticidad y no repudio en las transacciones electronicas, es decir, permitir la confiramacion de las identidades de las partes involucradas en tal proceso.
c. Proporcionar la integridad de los datos y la información transmitida en las transacciones electronicas, es decir, impedir que tales datos sean alterados durante su transmisión.

La encriptación ó criptografía es un mecanismo de la seguridad de la información que apunta a garantizar la confidencialidad de los datos. Es una rama de las matemáticas que se preocupa por la seguridad en la información digital que fluye en las redes de telecomunicaciones. La encriptación trabaja en disminuir los riesgos que la información transmitida pueda ser leída y recuperada por un atacante de la información. Podemos establecer que la encriptación se comporta como una transformación de los datos y de la información en el transporte de los mismos.Ésta transformación se da de tal manera que solo las partes interesadas (emisor-receptor) en la información puedan leerla y entenderla únicamente por

[1]Basado en el material de estudio e informacion proporcionado por el Ingeniero Jorge Alberto Medina Villalobos CISSP en la asignatura Seguridad en Redes, Especializacion en Telecomunicaciones UIS 2012-2013.

medio de un sistema de claves ó llaves de desencriptacion. El modelo básico que muestra el proceso de encriptación se puede observar en la figura 1.

Figura 1. Modelo básico del proceso de encriptación.



Diseño propio.

Es importante mencionar que lo textos encriptados pueden llegar a ser de mayor dimensión que los textos planos legibles. Según la figura 1, **TO**representa el texto plano original y legible, **TE** hace referencia al texto encriptado y no legible. Por lo tanto, se puede decir que la encriptación de los datos se realiza en función del texto plano original y legible, entonces; **E** (**TO**) = **TE**, por lo tanto; **D** (**TE**) = **TO**, también se podría establecer que **D** [**E** (**TO**)] = **TO**.

Hoy día, los protocolos de seguridad en el comercio electrónico existentes son SSL, TLS, SET, 3D Secura, HTTPS, IPSec, PCT.

Con el tiempo, se ha observado que la criptografía se ha convertido en uno de los mecanismos más usados y seguros para mantener la privacidad y seguridad de la información que se transmite. Es decir, que el objetivo básico y primordial de los sistemas de encriptación es proporcionar la privacidad en las telecomunicaciones entre los usuarios finales, esto lo logra llegando a alterar los datos originales de tal modo que solo pueda ser leído e interpretado por las partes interesadas, así, si estos datos son interceptados, solo podría ser inteligibles para las partes

involucradas en la transmisión de los datos. Es importante aclarar que la criptografía solo nos protege de la interceptación de los datos transmitidos mientras estos se transmiten entre las partes en una transacción electrónica.

10.6.1 Criptografía de clave pública. La implementación de clave pública más utilizada es la basada en algoritmos presentados por Rivest-Shamir-Adelman (RSA).

La criptografía de clave pública consiste en una pareja de dos claves: la *clave pública* y la *clave privada*.La *clave pública* se utiliza para publicar la información cifrada, la cual solo podrá ser descifrada con la respectiva clave privada. No hay problema por el tamaño que posee cada llave pública, aunque en la actualidad se utilizan tamaños como 1024 y 2048 bits, tamaños mayores a los cifradores simétricos. La implementación de los algoritmos de llave pública es más lenta que los algoritmos simétricos. Con la implementación de este tipo de algoritmos, las partes involucradas en una transacción electrónica, podrían intercambiar las claves públicas de cifrado de manera no segura mientras que se conserve la clave para desencriptar. El diseño de algoritmos de clave publica es un proceso bastante complejo, ya que ello se basa en teorías numéricas, lo que implica que el desarrollo de un algoritmo de éste tipo, requiere el surgimiento de un paradigma matemático con especiales características.

La encriptación de clave pública define lo siguiente:

a. Encriptación y desencriptación que permite la comunicación segura entre las partes. Antes de enviar un mensaje, el remitente encripta ó codifica la información. El receptor desencripta ó descifra la información luego de recibir el mensaje, el cual no ha podido ser entendido por algún intruso.
b. No repudio.

Como se ha mencionado anteriormente, el proceso de encriptación de clave pública es más dispendioso que la encriptación de clave simétrica, esto debido al número de cálculos que se tienen que realizar. Debido a este hecho, la codificación de clave pública no es muy utilizada en transacciones de grandes cantidades de datos.

Se debe tener en cuenta lo siguiente al momento de utilizar criptografía de clave pública:

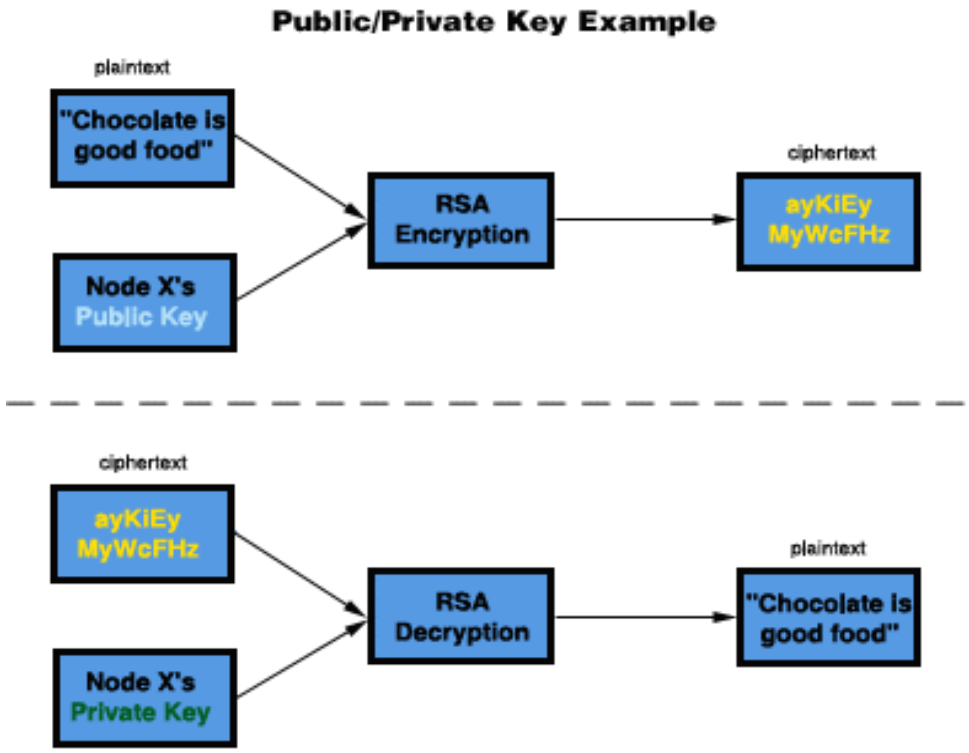
a. Puede ser usada en un entorno de acceso público, como Internet
b. La seguridad de este tipo de criptografía depende en gran medida de no perder la clave privada

Las claves públicas, como su nombre lo indica están disponibles para todo el público, indicando esto que cualquier usuario podría hacerse de ella, emplearla para encriptar un mensaje y enviarlo. Las principales características de los criptosistemas de clave pública las podríamos definir de la siguiente manera:

a. Elimina el riesgo y el requerimiento del intercambio de las claves usadas.
b. Si los datos transmitidos son cifrados con una clave pública, entonces ésta misma clave pública es inservible para lograr descifrar tal mensaje.
c. Generalmente, las claves privadas no se originan de las claves públicas.

En la figura 2 se muestra el proceso de cifrado y descifrado utilizando el método de llave Pública.

Figura 2. Par de Clave Pública.



Tomado de IBM, Software Information Center. Disponible en: http://publib.boulder.ibm.com/infocenter/tpfhelp/current/index.jsp?topic=%2Fcom.ibm.ztpf-ztpfdf.doc_put.cur%2Fgtps5%2Fs5rcd.html

10.6.2 Criptografía Simétrica. En este tipo de criptografía, la llave utilizada para cifrar y descifrar los mensajes transmitidos es la misma tanto en el emisor como en el receptor de los mismos. Este tipo de algoritmo criptográfico es más rápido y más sencillo de implementar que el algoritmo de llave publica. Algunas de las ventajas que se pueden distinguir en transacciones que utilicen este método criptográfico son:

a. La creación de una clave segura para cifrar contenido en una transacción es relativamente barata.
b. El tamaño de las claves es mucho menor que las claves de Criptografía Pública.

Dentro de este ámbito, el mayor inconveniente que se presenta es el intercambio de la clave secreta entre las partes, dado que se pone en riesgo la privacidad de la misma, conllevando a que se requiera de una clave adicional que necesitarán las partes para poder leer la llave simétrica, creando una gran dependencia entre la llave y su respectiva clave. Si esta clave es accidentalmente difundida, existe el riesgo de que un usuario no autorizado que encuentre la llave simétrica atente contra la confidencialidad y autenticidad de los mensajes transmitidos. Es importante que el intercambio de claves entre las partes en una transacción electrónica se deba efectuar de manera segura. La capacidad de los algoritmos simétricos para proteger los datos en una transmisión en una red de telecomunicaciones podrían depender de factores tales como:

a. Confidencialidad de la clave.
b. Imposibilidad para descifrar la clave.
c. Dificultad para violentar el algoritmo de cifrado.
d. Inexistencia de *backdoors* y vulnerabilidades de seguridad que conlleven a desencriptar la información sin la respectiva clave.
e. La probabilidad de descifrar los datos conociendo fracciones de él.

La criptografía posee algunas limitaciones y en muchos casos, éste sistema no funciona de la mejor manera ó no se comporta como la solución mas adecuada para ciertas situaciones entre las que se encuentran:

a. Aquella información que este depositada en un servidor y que no se encuentre encriptada, la criptografía no tiene la capacidad de proteger, esto quiere decir que, si dicho servidor se encuentra configurado para enviar la información encriptada, la criptografía si protege los datos en la transmisión de ellos, pero no protege aquellos datos originales que en el servidor se encuentran almacenados sin encriptar, ya que un atacante podría violentar la seguridad en el acceso al servidor y obtener toda esa información almacenada sin encriptar.

b. La capacidad para evitar el robo de las claves de cifrado no es un alcance de la criptografía. La criptografía permite el uso de claves para descifrar la información, pero es responsabilidad de los usuarios mantener segura y confidencial tales claves, en su almacenamiento y la manera de intercambiarlas, ya que si ellas caen en manos de un atacante la información estaría en grave riesgo.
c. La criptografía no actúa sobre aquellos ataques de negación de servicios. Esto indica, que éste sistema no es la solución más recomendada cuando se tienen ataques a las redes de telecomunicaciones en donde el objetivo primordial no sea el acceso al contenido de la información ó datos.
d. Sobre los registros y rastros del envió e intercambio de información, la criptografía no tiene un papel fundamental ni protagónico. Para efectuar el análisis y seguimiento a estos registros y envíos, existeun procedimiento llamado *análisis de trafico*, con el cual, se logra determinar el intercambio de información entre un usuario A de origen y un usuario B de destino. La criptografía solo oculta tales datos en la transmisión de los mismos.
e. La criptografía no cuenta con la capacidad de reaccionar en contra de algoritmos criptográficos con defectos ó que hayan sido manipulados. La probabilidad de que un algoritmo criptográfico sea alterado con el propósito de hacerlo inútil ó malicioso no se puede descartar y los riesgos serian muy altos, sin embargo, estos riesgos de alteraciones se lograrían reducir si se diseñan e implementan buenas y mejores políticas de seguridad en las redes, además, las vías para obtener tales algoritmos criptográficos deberían ser canales confiables y seguros.
f. La criptografía no llega a proteger contra ataques de usuarios internos de una red, delatores ó errores humanos. Se podría decir que las personas son el eslabón mas débil dentro de una red de telecomunicaciones, la razón de ello, es que las personas ó individuos podrían caer en la tentación ó quizá en el error involuntario de divulgar ó manipular la información que se encuentra cifrada , la seguridad proporcionada por la criptografía no tiene tal alcance.

Las tecnologías de algoritmos de cifrado simétrico (de llave privada) y asimétrico (de llave publica y privada) tiene sus propias ventajas y desventajas; para la tecnología de cifrado simétrico se puede establecer que la velocidad de cifrado y descifrado es mayor que el mecanismo de cifrado asimétrico, también tiene la ventaja de ser un mecanismo adecuado para el proceso de cifrado de grandes cantidades de datos; sin embargo, sus desventajas se ven reflejada en la dificultada para el manejo y manipulación de la clave privada, esto indica que la distribución y almacenamiento de ella se torna dificultoso. Por otra parte, el sistema de cifrado asimétrico (de llave publica y privada) brinda una solución al problema de la manipulación de las claves, pero cuenta con la desventaja que el algoritmo de cifrado es bastante complejo y las velocidades para los procesos de cifrado y descifrado de los datos es mucho mas lenta que elmecanismo de cifrado simétrico, el cifrado asimétrico es adecuado para el cifrado de pequeñas cantidades de datos. Aunque para aplicaciones practicas, los ingenieros con frecuencia emplean una combinación de los dos sistemas de cifrado.

10.7 PROTOCOLO SSL

En diversos entornos de intercambio de datos basados en Internet, por citar un ejemplo el comercio electrónico, se requiere de una infraestructura que provea por sobre todas las cosas confianza en los usuarios finales al momento de realizar transacciones electrónicas; uno de estos mecanismos es el protocolo Secure Sockets Layer (SSL).

SSL es un protocolo creado en 1994 por Netscape Corporation para brindar seguridad en las transacciones electrónicas sobre internet; el cual proporciona autenticación, integridad y confidencialidad a los distintos tipos de relación entre cliente y servidor que se realiza sobre redes de computadoras, muy comúnmente internet, mediante el uso de criptografía y haciendo uso de los certificados SSL, los cuales contienen información exclusiva y autenticada sobre cada propietario de

dicho certificado; esta información es validada y respaldada por entidades certificadoras. El protocolo SSL, además de ofrecer el cifrado de la información, también puede realizar operaciones tales como la autenticación de servidores, integridad de los datos y en algunas ocasiones podría proporcionar la identificación de los usuarios en conexiones TCP/IP.Para velar por la integridad de los datos que viajan por medio de la red en una conexión segura, SSL calcula un mensaje *Resumen* antes de transmitirlo y este valor debe permanecer idéntico en el momento en el cual arriba en el receptor. Si esta condición no se cumple, el mensaje se descarta debido a los cambios ocurridos durante la transmisión. SSL brinda autenticación a nivel de cliente y de servidor, además de brindar una conexión segura por medio de cifrado y descifrado de información, proporcionando un alto grado de confidencialidad.

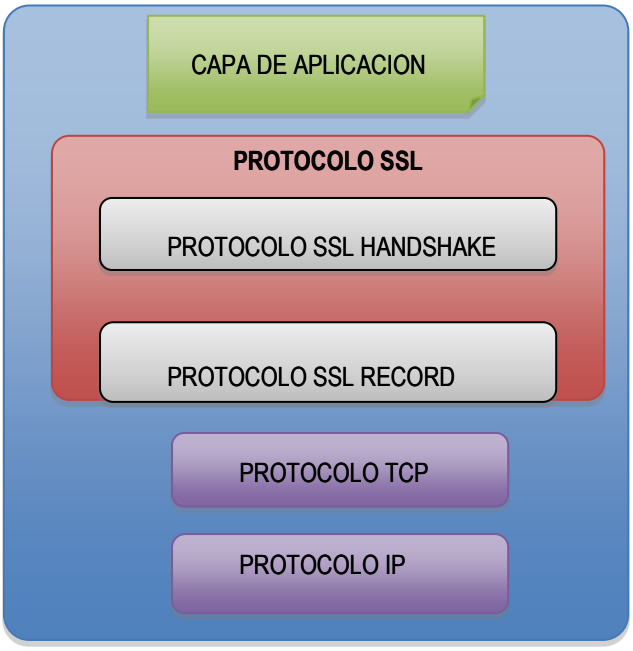
Éste protocolo, provee a las transacciones electrónicas canales seguros entre los servidores y navegadores para el transporte de los datos.SSL es el protocolo estándar a nivel mundial en la seguridad de la información, el cual libra una batalla tecnológica en contra de las amenazas informáticas que hoy en día encontramos en las redes mundiales de telecomunicaciones. Éste también aporta en la seguridad de la información proporcionando a los usuarios finales un mayor grado de certeza de que esta accediendo a sitios web validos y seguros en sus consultas. Este protocolo además de realizar protección a la información transmitida, también ofrece seguridad a servicios tales como TELNET, FTP, SMPT y otros. El objetivo primordial del SSL, es proporcionar el cifrado de los datos en la comunicaciones entre usuarios y servidores, implementando sistemas de claves ó llaves y algoritmos de encriptación. El protocolo SSL proporciona un método de autenticación tanto para el usuario como para el servidor, éste proceso se efectúa de manera independiente a las aplicaciones. En éste protocolo, el proceso de realizar la identificación y autenticación de las partes involucradas en una transacción electrónica, requiere de la implementación e intercambio de claves publicas y claves privadas, lo que disminuye los riesgos de adulteración y

falsificación de identidades, como también, proporciona un mayor nivel de integridad de la información. El protocolo SSL lo podemos definir en las RFC 2246, 2712, 2817, 2818, 3268, 3546 y 4279. Usa el puerto TCP 443 para establecer la transmision de datos, el cual está definido como el puerto estandar para las conexiones seguras en Internet.

El protocolo SSL se ubica entre la capa de Transporte y Aplicación, actuando básicamente sobre protocolos como TCP, HTTP, SMTP, NNTP (la figura 3 ilustra tal ubicación de ejecución) y actualmente está siendo utilizado sobre UDP. La versión 2 del protocolo presenta varios problemas de seguridad ya conocidos, sin embargo ésta proporciona elementos que son aprovechados por la siguiente versión del mismo:

a. Algoritmo de Clave Pública (RSA)
b. Rivest de Cifrado 2 (RC2), RC4
c. Estándar de Cifrado de Datos (DES)
d. Algoritmo de Resumen del Mensaje 5 (MD5)

Figura 3. Ubicación del protocolo SSL para suejecución entre la capa de aplicación y transporte.



Diseño propio.

La última versión del protocolo SSL (SSL v3.0) proporciona mejoras respecto a sus versiones predecesoras, tales como protección contra nuevos ataques, nuevos algoritmos de criptografía, y la capacidad de forzar a utilizar versiones más recientes de SSL, además de presentar interoperabilidad, es decir, independencia de código sobre el cual se opera.

Para que el protocolo SSL proporcione los niveles de seguridad en las transacciones electrónicas, se basa en dos tipos diferentes de algoritmos de cifrado de seguridad, los cuales son el *cifrado de clave pública ó asimétrica* y el *cifrado de clave privada ó simétrica*. Generalmente el protocolo SSL se vale de una serie de algoritmos de cifrado simétrico de datos para la transmisión de la información, comúnmente se emplean DES, Triple-DES, RC2, RC4 ó IDEA. En temas de seguridad de la información, el protocolo SSL es muy versátil, ya que él

posee una amplia posibilidad de algoritmos de cifrado que puede emplear en las transacciones electrónicas y el comercio electrónico.

El algoritmo de cifrado RSA, con frecuencia se emplea para efectuar la autenticación de las partes y los datos, éste algoritmo además de encriptar los datos transmitidos, cifra las claves mediante un algoritmo de cifrado de clave publica, por otro lado, el algoritmo MD5 con frecuencia se emplea como un algoritmo de resumen digital (hash). En el protocolo SSL, la clave para el inicio de sesión es la empleada para efectuar el cifrado de los datos que se transmiten entre los usuarios y el servidor seguro, para cada inicio de sesión ó transacción electrónica se genera una nueva clave, lo cual se convierte en un obstáculo para un atacante, debido a que si violenta una de ellas, ésta no será útil para descifrar próximas transacciones electrónicas.

Como se ha mencionado, el protocolo SSL proporciona una conexión segura entre cliente y servidor, la cual posee las siguientes características:

a. *Conexión Privada*. Acuerdo entre las partes para establecer una clave secreta usando algoritmos de criptografía simétrica, los cuales se mencionarán con detalle posteriormente.
b. *Clave Pública*. Para establecer la identidad de cada uno de los extremos.
c. *Conexión fiable*. El mensaje incluye un mensaje de comprobación, Message Authentication Code (MAC).
d. El protocolo SSL se ejecuta entre los protocolos de aplicación tales como HTPP, SMTP, etc. y sobre el protocolo de transporte TCP.
e. Generalmente, el protocolo SSL se emplea en compañía del protocolo HTTP para ejecutar el protocolo HTTPS.
f. El principal objetivo de la ejecución del protocolo HTTPS, es proporcionar un mayor nivel de seguridad en los sitios web (www) cuando se ejecutan aplicaciones que involucren transacciones electrónicas ó comercio electrónico.

Este proceso incluye el uso de claves y certificados digitales con el propósito de autenticar la identidad de las partes involucradas.

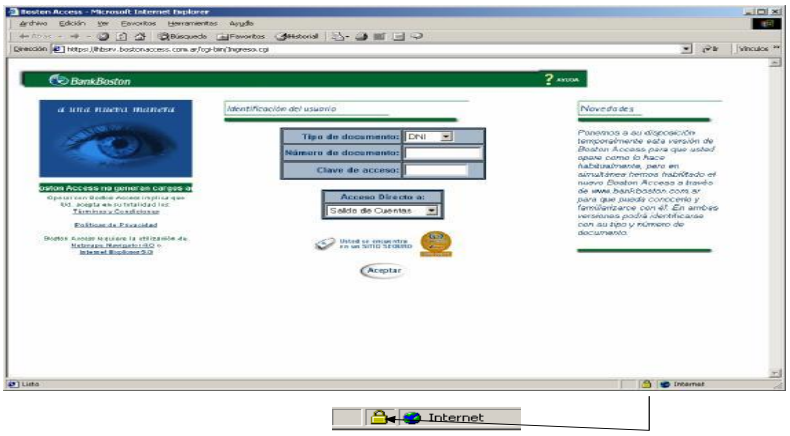
g. Existe en la red de internet la aplicación*OpenSSL*, la cual, es la más difundida en la red que emplea este sistema de seguridad de la información.
h. Emplea el cifrado de la información que se transmite.
i. Autenticación de las partes involucradas en las transacciones electrónicas (usuario y servidores). Permite la verificación de la identidad de los usuarios y servidores.
j. Proporciona integridad en los datos transmitidos. Imposibilita los intentos de adulteración ó modificaciones a los datos que son transmitidos.

En el comercio electrónico, el protocolo SSL actúa cifrando los números de las tarjetas de crédito e información privilegiada de los usuarios, específicamente; el protocolo SSL cifra los datos transmitidos entre los usuarios y el servidor, con un algoritmo de cifrado simétrico. En el comercio electrónico, el protocolo SSL no tiene la suficiencia para llegar a concretar definitivamente un transacción electrónica ó una compra en línea, esta incapacidad se ve reflejada en no poder efectuar la verificación de la validez de las tarjetas de crédito ó debito, en la inhabilidad para autorizar y procesar la operación de transacción electrónica directamente con las entidades financieras y bancos. En un intercambio de datos, el protocolo SSL asegura que los datos no serán alterados una vez estos son transmitidos desde el navegador en los dispositivos finales hasta el servidor, una vez fuera de estos limites, los datos podrían ser manipulados.

En el comercio electrónico, suponiendo que el servidor web emplee funciones criptográficas soportadas por el protocolo SSL y suponiendo también que los usuarios en las transacciones electrónicas emplean un navegador el cual reconoce el protocolo SSL, los clientes tendrán la certeza de estar obteniendo información y datos confiables de los vendedores con solo identificar el cambio de **http** a **https** en la dirección de URL en los navegadores web

(http://www.nombre.com por https://www.nombre.com), con esto, también se tiene la certeza que los datos enviados a los servidores web se realiza de manera confiable. Adicional a lo anterior, los clientes también puedenidentificar el acceso a un sitio web ó a cierta información segura, si en sus navegadores se muestra un icono con la figura de un candado cerrado, lo que indica que dicho sitio web es soportado y protegido por el protocolo SSL, la figura 4 ilustra lo mencionado.

Figura 4. Icono (candado) que indica que se accede a un sitio web soportado por el protocolo SSL.

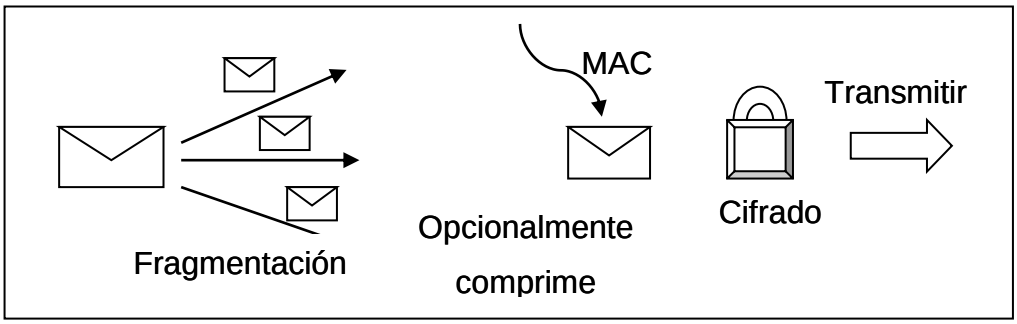


Basado en los resultados de la investigación y navegación sobre internet.

Cuando se va a establecer una comunicación ó transmisión de datos entre un usuario y un vendedor ó un servidor web, el protocolo SSL permite la apertura de varias sesiones SSL entre ellos, pero lo anterior, no es algo que comúnmente se realice, adicionalmente a ello, dentro de una sesión SSL se pueden establecer varias conexiones SSL y el estado activo ó no de éstas ultimas depende del protocolo *Handshake*.

El protocolo SSL, tiene la particularidad de poder asegurar otros servicios y protocolos aparte de HTTPS en la red de internet.

Figura 5. Proceso de transmisión de un mensaje usando el Protocolo SSLen una conexión Cliente-Servidor.



Diseño propio. Basada en RFC 6101.
http://datatracker.ietf.org/doc/rfc6101/?include_text=1

10.7.1 Como funciona el protocolo SSL. Básicamente, una vez se hayan completado y establecido la solicitud de comunicación entre un usuario final y un servidor, éstos deben acordar, determinar y establecer la manera en la que se comunicaran para luego iniciar la transmisión entre ellos de manera cifrada. Para acordar y determinar la forma de comunicación, el protocolo SSL inicialmente ejecuta un subprotocolo denominado SSL Handshake, el cual analizaremos mas adelante. SSL termina su ejecución una vez termine la transacción electrónica. Este proceso lo podríamos resumir en tres etapas, las cuales son:

a. **Solicitud SSL**. Ésta es la primera etapa y generalmente se da cuando un usuario final utiliza su navegador para tener acceso a un servidor seguro, el cual es identificado por estar precedido por https://. La comunicación entre las partes se realiza por medio de un puerto diferente al puerto por el cual normalmente el servicio se ejecuta (http). Luego de establecer la petición de comunicación entre las partes, entra en acción el subprotocolo SSL Handshake.
b. **Subprotocolo SSL Handshake**.Este subprotocolo tiene la misión de establecer pautas en la comunicación entre el usuario final y el servidor. Esto se ejecuta en cinco pasos:

- **Client Hello**.En este punto, el usuario se presenta y le solicita al servidor que haga lo mismo, es decir, que se autentique. En este momento, el usuario y el servidor determinan y acuerdan los algoritmos de cifrado que emplearán en la transmisión de los datos de manera segura.
- **Server Hello**.Aquí, el servidor efectúa su presentación. Replica al usuario final enviando su certificado digital (emitido por una autoridad certificadora) de manera encriptada, también envía la clave ó llave publica y el algoritmo de cifrado que se empleara.Es importante mencionar,que el algoritmo de encriptación que implementarán las partes será el mas robusto que ellos pueda soportar (usuario y servidor).
- **Aprobación del usuario**.En este paso, el usuario final recibe de manera cifrada el certificado digital del servidor, posteriormente y disponiendo de la clave publica enviada por el servidor, el usuario procede a desencriptar el certificado digital del servidor y así se constata que éste ha sido proporcionado por una autoridad certificadora confiable y es autentico. El certificado es inspeccionado para comprobar su autenticidad mediante la revisión de fechas, URL del servidor, nombres de entidades certificadoras, entre otras características. Seguidamente, el usuario final genera una nueva llave ó clave basada en la clave publica del servidor y en el algoritmo que soporta, la cual es enviada en forma de respuesta al servidor.
- **Verificación**.En este punto, tanto el usuario final como el servidor, tienen en su poder la nueva llave ó clave que fue generada por el usuario final en el paso anterior (Aprobación del usuario). Posteriormente y para verificar la integridad de los datos, las partes intercambian llaves ó claves buscando sus coincidencias, al concretarse éstas coincidencias, se podría decir que el Handshakellega a su fin, lo que da paso a que la transacción electrónica inicie.
- **Transmisión de datos**.A partir de esta etapa, todos los datos y la información son transportados de manera encriptada con el uso de las llaves que poseen tanto el cliente como el usuario final. Estas claves también serán empleadas

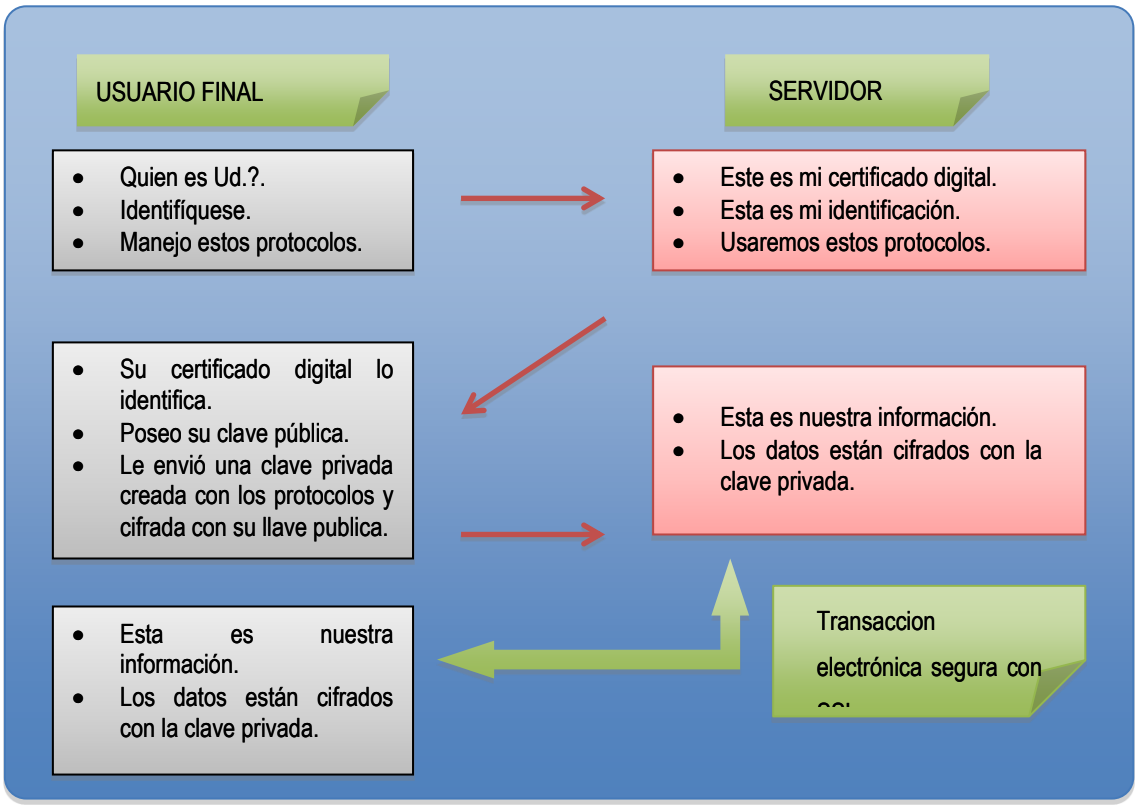
por el destinatario para llevar a cabo la desencriptacion de los datos y poder tener la información legible.

c. **Finalización del protocolo SSL**.Una vez entre el usuario final y el servidor se haya completado la transacción electrónica y también hayan finalizado las consultas por parte de los usuarios finales, ellos abandonarán el servidor. Así, se le indica que la sesión segura ha terminado y posteriormente el protocolo SSL terminara su intervención.

La figura 6, ilustra de manera básica el proceso de interacción entre el usuario final y el servidor cuando emplean el protocolo SSL en el momento de efectuar una transacción electrónica de manera segura. Adicional a esto, se podría evidenciar que la implementación del protocolo SSL se efectúa en sus etapas básicas:

- Acordar entre las partes el algoritmo de seguridad que emplearan en la transacción electrónica.
- Autenticación por medio de certificados digitales.
- Compartir las claves públicas y privadas.
- Cifrar los datos transmitidos.

Figura 6. Como funciona el protocolo SSL.



Diseño propio.

Anteriormente, se mencionó que el protocolo SSL se ejecuta de manera transparente tanto a los usuarios finales como a los protocolos que se ejecutan sobre TCP. Con ello, la IANA diseño una tabla 1 en donde estableció un número de puerto asignado directamente a cada uno de estos protocolos que se ejecutan sobre TCP. Estos mismos puertos son equivalentes para la ejecución de estos mismos protocolos pero basados en SSL/TLS.

Tabla 1. Puertos TCP asignadosa los protocolos de ejecución en sesión SSL sobreTCP.

PROTOCOLO	PUERTO TCP	IDENTIFICADOR
HTTP	443	HTTPS
SMTP	465	SMTPS
NTTP	563	NTTPS
LDAP	646	LDAPS
TELNET	992	TELNETS
IMAP	993	IMAPS
IRC	994	IRCS
POP3	995	POP3S
FTP – Datos	989	FTP-DATA
FTP - Control	990	FTP-CONTROL

Tomada dewww.iana.org/

El protocolo SSL proporciona comunicación segura de datos entre cliente y servidor dentro del ámbito de una transacción electrónica, basándose en un conjunto de características ó capacidades que permiten brindar, como se mencionó anteriormente, la *confiabilidad*, *integridad* y *autenticidad* en los datos. Estas características ó capacidades son:

10.7.2 Autenticación del Servidor SSL. Con esta característica, el cliente puede estar seguro de que la información enviada por medio de los canales electrónicos está siendo recibida por el *servidor* que en realidad se dice que es, para esto se utilizan técnicas criptográficas que permiten validar que la comunicación se está haciendo con las partes reales y no con terceros.

10.7.3 Autenticación del Cliente SSL. Para complementar la autenticación, el cliente SSL debe verificar por medio de técnicas criptográficas que es quien dice ser.

10.7.4 Encriptación de la Información. Para agregar dificultad a intrusos que buscan interceptar el tráfico de datos por la red, se han desarrollado técnicas de encriptación ó codificación que hacen mucho más difícil la interpretación de los mensajes en una transacción electrónica. Actualmente se distinguen varios algoritmos de codificación donde cabe recordar que en una comunicación entre cliente y servidor debe existir el mismo algoritmo de codificación en ambas partes de la transacción.

10.7.5 Compresión de la Información. En una transacción electrónica se permite, además de la encriptación, la compresión de la información que es transmitida entre cliente-servidor y viceversa, permitiendo esto que los mensajes tengan menor peso y sea más fluida la comunicación entre las partes.

10.7.6 Protección Contra Falsificación. Para salvaguardar la integridad de los datos en una comunicación cliente-servidor, se emplean elementos como Código de Autenticación del Mensaje (MAC – por sus siglas en inglés) y un resumen codificado del mensaje; si estos datos permanecen inalterados al momento de arribar al receptor, se supone que el mensaje no ha sido falsificado.

El protocolo SSL está compuesto por dos capas, Protocolo de Transporte, SSL Record Protocol y Protocolo de intercambio de claves, SSL Handshake Protocol, además de dos sub-protocolos adicionales, Protocolo de notificación de Alertas, Alert Protocol y Protocolo de Actualización de Cifradores, Change Cipher Spec Protocol[2].

10.7.7 SSL Record Protocol. Este protocolo se encarga de encapsular los datos transmitidos y recibidos, operando sobre la base de protocolos de transporte

[2] Para información más detallada, visite la siguiente página donde se describe el protocolo SSL en la RFC 6101. http://datatracker.ietf.org/doc/rfc6101/?include_text=1

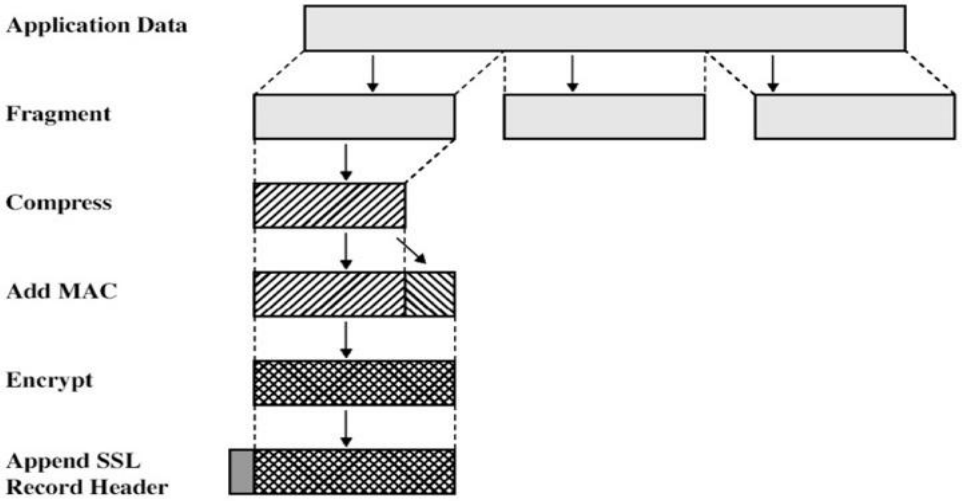
confiables, como TCP y proporcionando dos servicios a las conexiones SSL: confidencialidad e integridad de los mensajes.

El Record protocol, básicamente toma los datos transmitidos y los encripta por medio de los algoritmos de cifrado de llave simétrica como DES y RC4, a ellos les aplica una *MAC* (*Message Authentication Code* por sus siglas en ingles) con lo que verifica la integridad de los datos.

El Record protocol realiza diferentes operaciones a los mensajes transmitidos en una conexión cliente servidor, como se muestra en la figura 7. El protocolo toma los mensajes, si estos son mayores a 2^{14} bytes, los fragmenta, si es necesario los comprime, posteriormente les añade una MAC para luego aplicarle un cifrado, un dato determinístico que puede ser un número de secuencia del mensaje, un número secreto generado por la clave maestra de la transacción, para luego transmitirlo por medio de un protocolo de transporte confiable como TCP. Cuando llegan a su destino, se aplican los pasos inversos para poder ser dirigidos a una aplicación que los recibe en un nivel superior.

En el proceso anteriormente descrito, el mensaje fragmentado y comprimido, junto con la MAC son encriptados utilizando clave simétrica, ésta encriptación no sobrepasa los 1024 bytes y se añade al fragmento que será transmitido. Para finalizar el proceso de preparación para la transmisión se agrega una cabecera al fragmento. Este proceso se evidencia en la figura 7.

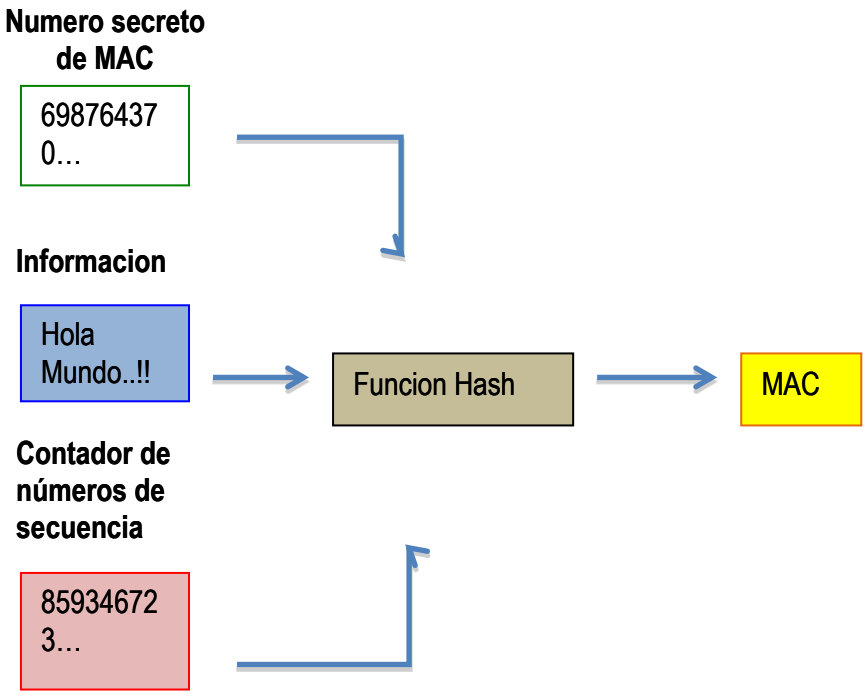
Figura 7. Proceso de preparación de los fragmentos de mensaje por medio de SSL Record.



Tomado de http://www.facweb.iitkgp.ernet.in/~sourav/SSL.pdf

Durante el proceso del SSL Record Protocol, una vez se haya efectuado la fragmentación de los datos mayores a 2^{14}, la compresión de los datos se efectúa al emplear un algoritmo que se ha determinado y acordado en el inicio de sesión ó se podría emplear el algoritmo *Null* en la situación en la que no se realice la compresión de los datos. Durante la fase de autenticación y verificación de la integridad de los datos, éste protocolo calcula un resumen de la información, el cual es sumado al numero secreto empleado por el usuario y el servidor y sumado también a un numero identificador de secuencia de la sesión, con estos tres elementos, se asigna una función *Hash*, la cual, proporcionará la MAC que será adicionada al mensaje (Ver figura 8). La autenticación del mensaje se comprueba empleando los números ó claves privadas que solo comparten el usuario y el servidor seguro, además de los números de secuencia de sesión, los cuales se transmiten de manera cifrada. La integridad se logra mediante las funciones *Hash* como se indica en la figura 8.

Figura 8. Integridad de la información en el SSL Record Protocol.



Diseño propio.

Por otra parte, la *confidencialidad* la logra gracias a la implementación de un algoritmo de cifrado simétrico y una clave privada que se obtiene del *Handshake*. El cifrado lo puede efectuar de dos maneras:

a. En *bloques*, el cifrado de la información se realiza en bloques que constan de 64 bits, si la longitud de la información no es múltiplo de 64 bits ó es menor a ello, se rellenará el espacio con bits y esto será enunciado en el formato del mensaje. Los algoritmos que generalmente se emplean son RC2 y DES.
b. En *streaming*, lo efectúa de manera que aplica un OR Exclusiva entre los bytes y un algoritmo RC4.

Otra misión que tiene el SSL Record Protocol, corresponde a realizar tareas de seguridad sobre los datos y mensajes provenientes de la capa de aplicación (http,

ftp, smtp, etc.), para ello hace uso de los parámetros establecidos y determinados con el protocolo *Handshake*.

10.7.8 SSL Handshake Protocol. El protocolo Handshake se encarga de tomar el Record protocol para establecer una conexión entre cliente-servidor y proveer todos los parámetros para establecer una conexión segura.

SSL utiliza una combinación de clave pública con clave simétrica. La encriptación de clave simétrica es más rápida que la encriptación de clave púbica, pero esta última provee técnicas de encriptación más efectivas.

Una sesión SSL siempre comienza con un intercambio de mensajes llamados SSL handshake. El protocolo de enlace SSL permite que el servidor se autentique para el cliente SSL usando técnicas de clave pública. Esto permite que tanto cliente como servidor cooperen en la creación de una llave simétrica para cifrar y descifrar mensajes. El Protocolo de enlace SSL también permite que el cliente se autentique con el servidor.

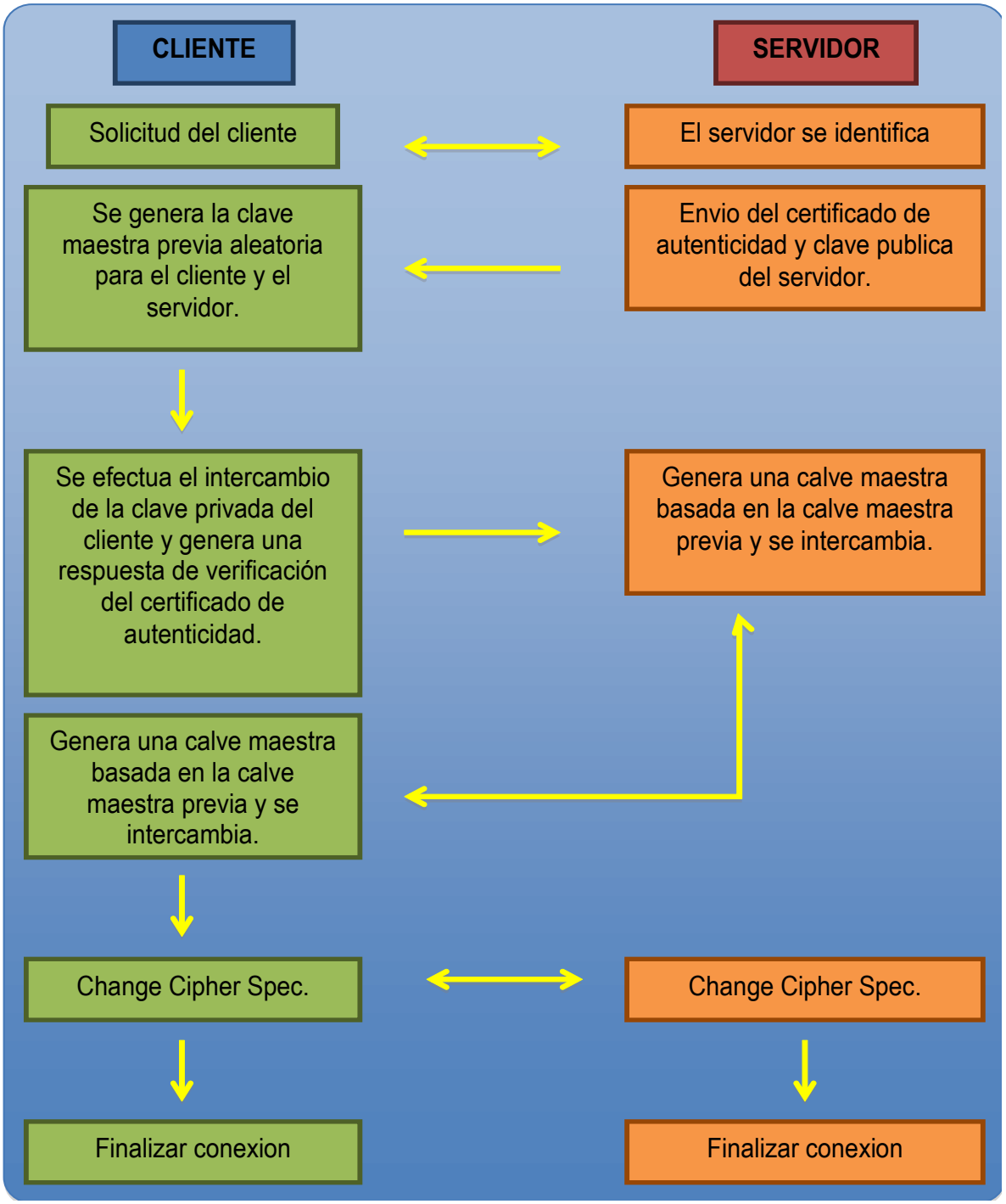
El protocolo Handshake de SSL, es responsable de establecer, mantener y finalizar las conexiones SSL. Con éste protocolo, se determinan y establecen parámetros para las sesiones y las conexiones asociadas a ellas. El protocolo Handshake de SSL maneja dos subprotocolos asociados, ellos son:

a. **Change cipher spec**., se emplea como un mensaje único para cambiar de estados activos a estados pendientes.
b. **Alertas**, ellas corresponde a mensajes de notificación de errores en las conexiones, ellos podrían llegar a forzar una terminación abrupta de una sesión.

En la figura 9 se puede observar de manera resumida el proceso del protocolo Handshake ó de enlace SSL.De acuerdo a la figura 9, en el recuadro en donde indica la Solicitud del cliente, hace referencia al primer mensaje que un cliente envía a un servidor seguro cuando establece contacto con él, además, enuncia los parámetros a utilizar durante la sesión, estos parámetros son:

- Hora y fecha.
- Números identificadores de sesión.
- Algoritmo de cifrado.
- Algoritmo de compresión.
- Versión del protocolo.
- Método de conexión.

Figura 9. Proceso del protocolo Handshake SSL.



Diseño propio. Basado en RFC 6101. The SSL Protocol versión 3.0. Disponible en http://datatracker.ietf.org/doc/rfc6101/?include_text=1

Durante el inicio del proceso del protocolo handshake de SSL, el servidor envía un mensaje de identificaciónal cliente, en el que incluye los algoritmos requeridos para establecer la conexión entre cliente y servidor, generalmente se emplean los algoritmos propuestos e incluidos en el mensaje de *solicitud del cliente*, sino, se generara un mensaje de error. Seguidamente, el servidor envía el *certificado deautenticidad* ó la *clave publica del servidor*, es decir, que en este punto el servidor envía su certificado X.509v3, sino cuenta con él, entonces enviará su llave publica sin certificación, en este momento el cliente decide si acepta ó no el uso de una clave sin certificado para continuar con la conexión. En algunos casos, los servidores web también podrían solicitar los certificados de autenticidad del cliente. Posteriormente, el cliente genera una *clave maestra previa aleatoria*, la cual equivale a un número randomico que se emplea para generar una clave maestra, ésta a su vez, se emplea para calcular y determinar todas las claves y números secretos usados en el protocolo SSL, se envía de manera encriptada junto con la clave publica del servidor. Una vez se concreta el intercambio de claves, se envía un mensaje de *Change Cipher Spec*., con el cual se indica el inicio de una sesión segura. Para finalizar la etapa de ejecución del protocolo *Handshake de SSL*, se envía un mensaje de *finalización de la conexión*, con este mensaje se logra comprobar que la negociación y calculo de parámetros y claves se efectuó y trabajan correctamente.

10.7.9 Sesión y estados de conexión. Una sesión SSL segura puede contener múltiples conexiones seguras y adicionalmente a esto, las partes pueden contener varias sesiones simultáneas[3].

El estado de sesión presenta los siguientes elementos que permiten una conexión segura entre las partes:

[3] Para mayor información visite la página de la referencia Oficial del protocolo SSL versión 3, RFC 6101. http://datatracker.ietf.org/doc/rfc6101/?include_text=1

10.7.9.1 Identificador de sesión. Es un conjunto de bytes arbitrarios que son escogidos por el servidor para identificar si una sesión está activa ó detenida.

10.7.9.2 Certificado de pares. En el caso de criptografía Pública, X.509v3 es el estándar UIT-T[4]. Este campo puede ser nulo.

10.7.9.3 Método de compresión. Antes de realizar el proceso de encriptación de los datos, se establece el algoritmo de compresión de la información.

10.7.9.4 Cipher Spec. En esta etapa se establece el algoritmo de compresión de los datos para que ellos sean posteriormente transmitidos.

10.7.9.5 Clave secreta maestra. Es una secuencia de 48 bytes que son compartidas entre el cliente y el servidor.

10.7.9.6 IS resumable. Es un indicador que permite conocer si se pueden establecer nuevas conexiones.

Los siguientes elementos forman parte del estado de conexión:

10.7.9.7 Numero randomico entre cliente y servidor. Corresponde a un número aleatorio que es intercambiado entre el cliente y el servidor cada vez que una sesión es establecida.

10.7.9.8 MAC para escritura en el servidor. Corresponde al dato cifrado utilizado en las operaciones MAC para realizar la escritura en el servidor.

---

[4] La descripción de este estándar se encuentra fuera del alcance de este documento. Definición Oficial disponible en el RFC 6187: X.509v3 Certificates for Secure Shell Authentication. http://datatracker.ietf.org/doc/rfc6187/

10.7.9.9 MAC para escritura en el cliente. Hace referencia al dato cifrado usado en las operaciones MAC para efectuar la escritura en el cliente.

10.7.9.10 Llave de escritura en el servidor. Clave que emplea el servidor para encriptar los mensajes y el cliente la emplea para descifrar la información.

10.7.9.11 Llave de escritura del cliente. Clave que es empleada por el cliente para encriptar los mensajes y ésta misma es empleada por el servidor para desencriptar la información.

10.7.9.12 Inicialización de vectores. Cuando un bloque *CBC* (*Cipher Block Chaining*) es cambiado a modo de uso, éste vector de inicialización es mantenido para cada llave. Este campo es inicializado en primera instancia por el subprotocolo *Handshake*. Posteriormente, el bloque final de texto cifrado es mantenido para un siguiente uso.

10.7.9.13 Números de secuencia. Cada parte involucrada en la transmisión reserva un conjunto de números de secuencia para transmitir ó recibir mensajes por cada conexión. Cuando se establece un cambio de cifrado en la conexión, los números de secuencia se resetean a cero. Los números de secuencia no pueden excederse de $2^{64} – 1$.

10.7.10 Capa de registro. La función de la capa de registro se centra en recibir los datos e información sin interpretar que provienen de capas superiores ubicadas en bloques no vacíos de un tamaño arbitrario. Dentro de esta capa se aplican una serie de técnicas tales como fragmentación, compresión y

descompresión de los datos del mensaje, registro de protección de carga y Cipher Spec.[5]

10.7.11 Protocolo de notificación de alertas. Dentro de la capa de registro se admiten varios tipos de contenidos, entre ellos se encuentra los mensajes de alerta. Los mensajes de alerta tienen la responsabilidad de indicar la gravedad del mensaje y un indicador de alerta. Cuando un nivel de alerta es fatal, las comunicacionesson inmediatamente finalizadas; para tal caso, otras conexiones pueden continuar pero el identificador de la sesión debe ser invalidado para evitar conexiones fallidas. De igual manera que los mensajes propios de la transmisión, los mensajes de alerta también se cifran y se comprimen. Dentro de esta etapa, se pueden visualizar dos categorías de alertas: *Alerta de cierre* y *Alerta de error*.

10.7.11.1 Alerta de cierre. Tanto el cliente como el servidor deben compartir información acerca del conocimiento de finalización de la conexión para así evitar un ataque por truncamiento. Cada parte debe inicializar el intercambio de mensajes de cierre.

El mensaje denominado *close notify* indica que el transmisor no enviará más mensajes en esta sesión. Cualquiera de las partes puede generar un mensaje de tipo *close notify* para dar por terminada una sesión y los mensajes que se transmitan después de la alerta de cierre serán ignorados.

10.7.11.2 Alerta de error. El manejo que se le da a los mensajes de error en el subprotocolo *SSL Handshake* es realmente simple: Cuando una parte detecta un error en la transmisión, envía un mensaje de notificación a la parte que realizo la emisión. Perder los identificadores de sesión, llaves y secretos de conexión

[5]La descripción de estas funciones esta fuera de los límites de este documento, para mayor información visite la página de la referencia Oficial del protocolo SSL versión 3, RFC 6101. http://datatracker.ietf.org/doc/rfc6101/?include_text=1

conlleva a efectuar una transmisión fallida. Alertas de error tales como *unexpected message*, *Handshake failure*, *no certificate*, *unsopported certificate* y *certificate unknown*, son algunos de los mensajes de notificación que se pueden visualizar.

10.7.12 Certificados digitales SSL. Un certificado digital SSL permite que un servidor valide su identidad, es decir, dice quien dice ser. De esta manera, se genera mayor confianza en los usuarios al momento de efectuar una transacción electrónica. Los certificados digitales SSL emplean como método para encriptar los datos el sistema de criptografía simétrica, la cual fue tratada anteriormente.

Además de ofrecer autenticidad, los certificados digitales SSL garantizan que los datos y la información transmitida no ha sido manipulada posterior a la creación y transmisión de los datos, ya que al mensaje original se le adicionan caracteres que permiten ser descifrados con la llave privada mencionada anteriormente, llevando a que el emisor del mensaje no pueda negar la creación de tal mensaje, es decir, permite el *no repudio*.

10.7.12.1 Contenido de un certificado digital SSL. Estos certificados poseen la siguiente información:

- Dominio para el cual se expidió.
- Propietario del certificado.
- Ubicación geográfica del propietario del certificado.
- Fecha y validez del certificado.

10.7.12.2 Tipos de certificados SSL. Según las necesidades que tenga un negocio virtual que son el resultado del área de desempeño de éste, los *certificados digitales SSL* se puede clasificar de la siguiente manera:

a. **Certificados de servidor**. El certificado de servidor proporciona a un sitio web la seguridad y por ende, la confiabilidad del negocio virtual para establecer una comunicación segura entre las partes que interactúan, involucrando así al protocolo SSL dentro del servidor web.
b. **Certificados para WAP**.Son certificados que aportan una transmisión segura a transacciones soportadas bajo plataformas móviles. Haciendo uso de la encriptación de los datos.
c. **Certificados personales**. Son certificados que se emplean principalmente en mensajes de correo electrónico; un usuario puede firmar los correos electrónicos para que solo sean vistos por el receptor al cual han sido dirigidos los mensajes.
d. **CAs Corporativas**.Esto es implementado en compañías que quieren disponer de certificados de diversos tipos para los usuarios, ya sean empleados, clientes, proveedores, entre otros. Estas tienen la posibilidad de crear cualquier tipo de certificado según sea la necesidad de cada usuario ó servidor.
e. **Certificados para firmar código**.Esto permite a los desarrolladores de software firmar sus productos para que éstos sean distribuidos de forma segura.

La manera para adquirir estos certificados digitales SSL, se efectúa por medio de una entidad certificadora reconocida, comúnmente podemos encontrar esto definido como un *Notario Electrónico*, las cuales certifican que el interlocutor emisor es quien pretende ser, garantizando así, un mayor nivel de seguridad en las transacciones electrónicas y favoreciendo a la autenticación y no repudio en la transmisión de la información.

Para adquirir un certificado digital SSL, primero se deben comprobar una serie de referencias que aseguran la identidad del emisor y receptor de la información. Una vez el certificado se otorga a la entidad ó usuario, él se construye con una llave pública del servidor que solicita el cifrado, posteriormente, el usuario ó la entidad

responde firmando con una llave privada que asegura que el solicitante es verdaderamente quien estipula ser.

Para identificar en primera instancia si un sitio web es seguro ó que por lo menos implementa una solución de seguridad basado en el protocolo SSL, basta con observar la barra de direcciones y debe aparecer la figura de un *candado* ó una *llave* de acuerdo al navegador web que el usuario emplee, como se menciono anteriormente. Sin embargo, no basta solo con lo anterior, sino que se debe realizar la respectiva comprobación del certificado digital SSL.

10.7.13 Problemas y debilidades con el protocolo SSL. En esta sección de la monografía, se mencionarán las debilidades, problemas y errores comunes de éste protocolo. También se mencionarán algunas formas de corrección.

10.7.13.1 Inconvenientes con otros protocolos de la capa de transporte. SSL se ejecuta entre la capa de transporte y la capa de aplicación, lo hace de manera trasparente y se ejecuta sobre la mayoría de los protocolos TCP (HTTP, SMTP, etc.). El protocolo SSL no esta diseñado para soportar otros protocolos de la capa de transporte que no estén basados en TCP y que no estén orientados a la conexión como UDP. Hoy en día la implementación UDP ha tomado más protagonismo, por lo tanto, se han diseñado soluciones con un creciente grado de eficiencia que ha permitido la implementación de SSL sobre UDP. Para efectuar esto, generalmente se inicia una sesión SSL normalmente sobre TCP, en donde se acuerdan los parámetros para la transmisión de datos, seguidamente y con el resultado de tal acuerdo se da paso al cifrado de los paquetes UDP. Los paquetes UDP son independientes uno de otro, indicando esto que a la falta de uno de estos paquetes, ésta falta no afectará la transmisión de la información, por lo tanto, los paquetes UDP se encriptan y desencriptan independientemente uno del otro, además, cada paquete empleará su propia clave de cifrado.

10.7.13.2 No repudio en las transacciones electrónicas. El protocolo SSL no implementa ésta característica, pero solventa el requerimiento de no repudio, implementando en la transmisión de datos dentro de unasesión SSL, la característica de cada una de las partes involucradas en la transacción electrónica es que se autentiquen por medio de los certificados digitales. Estos certificados son verificados una vez recibidos y en el caso en que alguno de ellos sea inválido ó tenga incongruencias, entonces la sesión SSL será anulada y no se efectuará la transmisión de los datos.

10.7.13.3 Déficit en su eficiencia. La seguridad en las transacciones electrónicas es un factor que es inversamente proporcional a la eficiencia de los protocolos de transmisión de datos. Al iniciar una sesión SSL y establecer una conexión requiere el consumo de muchos recursos. Buscando que el consumo de recurso se minimice, en muchos casos, la solución para este inconveniente es la utilización de hardaware adicional para efectuar trabajos de cifrado y balanceo de cargas. La figura 10 ilustra una posible solución para la eficiencia en un servidor que emplea sesiones SSL.

Figura10. Infraestructura de internet incluyendo balanceador,cifrador y acelerador SSL.

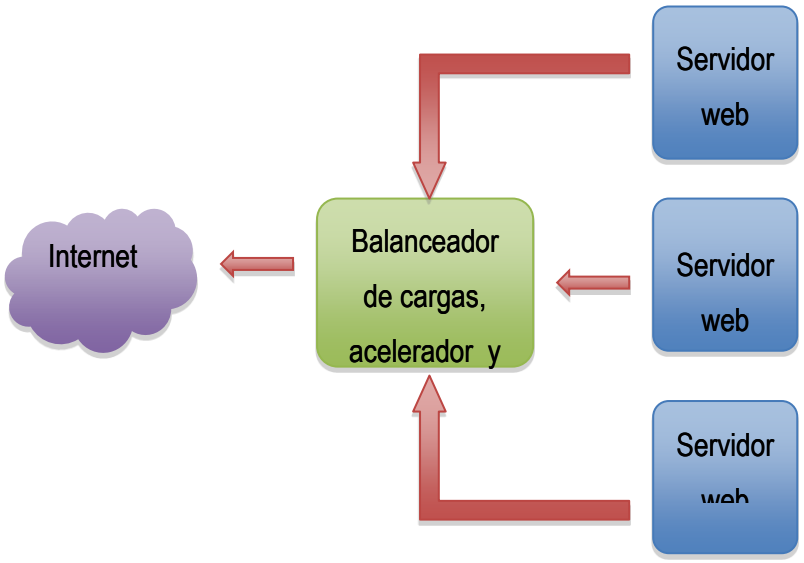


Imagen basada enhttp://jo.morales0002.eresmas.net/fencasa.html.

Con la infraestructura de la figura 10 se ilustra el hardware integrado adicional en el que se incluye el balanceador de cargas, el acelerador y el cifrador SSL.El hardware adicional, también tiene la característica de actuar con descifrador, lo que le da la posibilidad de realizar el enrutamiento de los datos hacia el servidor indicado. Esta implementación apoya la reducción de tiempos de respuesta reales, los cuales se acercan en gran medida a los tiempos de respuesta cuando se implementan servidores HTTP plano sin cifrar.

10.7.13.4 Fallas en la implementación de SSL. De acuerdo al historial de debilidades y vulnerabilidades del protocolo SSL[6] a lo largo del tiempo desde su diseño, se ha detectado que las fallas no se generan del diseño propio del protocolo sino más bien se ha observado que se generan a partir de fallas en la

[6]El historial de debilidades y vulnerabilidades del protocolo SSL se encuentra disponible en las listas de Security Focus y CERT.
http://online.securityfocus.com/advisories/ y http://www.cert.org/advisories/CA-1998-07.html

implementación de él ó en las aplicaciones que emplean éste protocolo. Es importante recordar que no podemos apoyarnos en la idea de tener una seguridad plena en la transmisión de nuestra información, ya que es muy riesgoso, debido a que ello nos conduciría a pensar que nuestra información se encuentra segura al implementar un protocolo que según toda la información disponible lo definen como seguro. Existen otros procedimientos complementarios que no son el caso de esta monografía, los cuales ayudan a mejorar los niveles de seguridad en la transmisión de datos y transacciones electrónicas.

10.7.13.5 Reserva de claves privadas en los servidores SSL. Una manera de elevar los niveles de seguridad digital es complementarla con la implementación de una buena seguridad física. Este complemento es necesario, ya que en la mayoría de los casos, no se puede permitir el acceso físico a tales servidores porque en ellos se almacena de manera física sus claves privadas. Una manera de mitigar los ataques de este tipo y evitar la perdida de las claves privadas es la implementación de un dispositivo externo que maneje un sistema UNIX, la razón para esto, es que con estos tipos de tecnologías si no se cuentan con los niveles de conocimiento y manejo de ellas, se dificulta considerablemente la recuperación y sabotaje de ellas. Las claves privadas que emplea un servidor SSL en el momento de efectuar las sesiones y conexiones para las transacciones electrónicas, no deben estar cifradas, lo cual, se transforma en una vulnerabilidad enorme y un atacante podría aprovecharla si logra contar con accesos y privilegios como usuario *root* del sistema. Hasta el momento, no se cuenta con alguna medida para mitigar este tipo de ataque, pero, los riesgos de este tipo de ataques se podrían manejar y mitigar si tales claves privadas se almacenan en los discos de los servidores SSL de manera encriptada y protegidas con el uso de complejos passwords que idealmente solo tendría conocimiento de ello el administrador del sistema.

El protocolo SSL no presenta muchas dificultades ni inconvenientes en su implementación, pero en general, podríamos decir que éste protocolo no provee una solución integral y totalmente segura a las transacciones electrónicas con respecto a la seguridad de los datos en un transmisión de ellos. Con el crecimiento del comercio electrónico y las transacciones electrónicas, paralelamente crecen las aplicaciones, usuarios, necesidades y amenazas en las redes de telecomunicaciones, lo que llevaría con el transcurso del tiempo, a que éste protocolo sea una herramienta insuficiente para la seguridad en las transacciones electrónicas del comercio electrónico.

Como complemento a las debilidades del protocolo SSL, podríamos decir, que tal protocolo en el comercio electrónico cuenta con la capacidad para proveer un canal seguro para la transmisión de números de tarjetas de crédito e información de clientes y vendedores, pero, en el momento de concretar una compra-venta de manera electrónica, no cuenta con la suficiencia para hacerlo, esto es porque el alcance del SSL no incluye la verificación de números de tarjetas de crédito e información de usuarios, la autorización de la transacción electrónica con el banco ó entidad financiera del cliente y los procesos complementarios con tales entidades. Sumado a esto, se ha visto que por medio del protocolo SSL se puede llegar a realizar ataques a la seguridad en servidores que han sido creados y configurados de una manera débil ó poco confiable, con el propósito de obtener información válida sobre tarjetas de crédito, débito, etc., esto lo podría logar un atacante diseñando un programa ó aplicación con la cual, probaría una serie de números de tarjetas de crédito de las cuales no se tiene certeza de su validez, efectuando compras en línea ficticias en ciertos servidores, así; los servidores tendrían dos opciones; en una de ellas emitiría un aviso indicando la invalidez de uno de esos números de tarjetas de crédito y en la segunda terminaría por aceptar uno de esos números de tarjetas de crédito, seguidamente, la aplicación diseñada abortaría el proceso de compra y registraría la información de validez de aquel numero de tarjeta de crédito aceptado por el servidor. De esta manera el atacante

podría hacerse de una gran cantidad de estos números de tarjetas de crédito validos. Adicional a esto, es importante contar e implementar siempre las ultimas versiones de los protocolos de seguridad en las redes de telecomunicaciones, para nuestro caso, es importante implementar la ultima versión del protocolo SSL, la razón de esto, es que las nuevas versiones de los protocolos siempre proporcionan un mayor y mejor nivel de seguridad que las versiones anteriores en las redes de telecomunicaciones, sino se cuenta con estas actualizaciones, un atacante con los conocimientos adecuados, podría efectuar un ataque de tal manera que el servidor y navegador web de su objetivo y que empleen el protocolo SSL como soporte a la seguridad, crean que es necesario la implementación de una versión anterior del protocolo de seguridad por razones de compatibilidades con el sistema, esto lo podría efectuar el atacante en el momento en que se ejecuta la sesión del *protocolo handshake*, de esta manera, el servidor de su objetivo podría entender que el navegador web del cliente solo soporta una versión anterior del protocolo SSL e implementara tal versión anterior para efectuar el cifrado de la información, entonces, el atacante sacará provecho de todas las vulnerabilidades y debilidades conocidas de tal versión anterior para realizar sus actos maliciosos. Interviniendo la sesión del *protocolo handshake*, un atacante podría manipular ó hacerse de los algoritmos de cifrado, con esto, un atacante podría conducir a que las partes involucradas en una transacción electrónica implementen un algoritmo de cifrado menos seguro ó con claves mas pequeñas con menos bits que permitirían una violación a la seguridad de la información mas fácilmente.

Teniendo en cuenta lo anterior, podríamos enunciar que el protocolo SSL no se convierte en una solución optima e integral para el comercio electrónico, específicamente al completar los pagos de manera electrónica, sin embargo, esto no implica que éste protocolo no se deba utilizar e implementar en otras dimensiones y etapas del comercio electrónico. El protocolo SSL proporciona canales seguros para las telecomunicaciones, las transacciones electrónicas y el

comercio electrónico, esto permite a los vendedores conceder a los clientes servicios tales como autenticaciones, trato personalizado, evitar que individuos externos husmeen las transacciones e información privada de los clientes, lo que conduciría a estrechar las relaciones comerciales y de confianza entre clientes y vendedores.

10.8 PROTOCOLO TLS

Transport Layer Security por sus siglas en ingles. Éste protocolo se definió por primera vez en Enero de 1999 con la RFC 2246[7]. En su versión 1.0 es el sucesor directo del protocolo SSL en su versión 3.0. Actualmente, la versión mas reciente de dicho protocolo es la versión 1.2, la cual se definió inicialmente en Agosto de 2008 en la RFC 5246 y posteriormente en Marzo de 2011 con la RFC 6176, en donde se hace explícito el no uso del protocolo SSL en su versión 2.0.

El protocolo TLS provee un nivel mas avanzado de seguridad sobre la internet entre el cliente y el servidor para evitar problemas de espionaje, manipulación ó falsificación de los mensajes transmitidos. El protocolo TLS siendo el sucesor del protocolo SSL, tienen en común el propósito de ser un protocolo para brindar seguridad en la transmisión de información entre un cliente y un servidor a través de canales de comunicación de datos como la internet. El protocolo TLS implementa como mecanismos de seguridad un sistema criptográfico de datos para evitar la manipulación, falsificación e interceptación de los mismos. Tal mecanismo criptográfico, esta basado en el uso de algoritmos matemáticos de cifrado tales como *AES* (*Advanced Encryption Standard*) y *RSA* (*Rivest-Shamir-Adleman*), adicionalmente emplea sistemas de claves publicas y privadas. Éste protocolo fue diseñado empleando una mezcla de sistemas criptográficos simétricos, asimétricos, firmas digitales, certificados digitales, entre otros, para

[7] The TLS Protocol Version 1.0. Dierks, T., Allen, C. January 1999. Disponible en http://tools.ietf.org/html/rfc2246. Accedido el 5 de Mayo de 2013

lograr establecer canales para la transmisión de información de manera segura para los usuarios.Entre las debilidades que presentaba el protocolo SSL en su versión 2.0, los diseñadores lograron visualizar una serie de deficiencias que obligo al mejoramiento de este protocolo, lo que derivo en su evolución y posteriormente el surgimiento del protocolo TLS, tales debilidades que podrian mencionarse de la siguiente manera.

a. Implementación de MD5 para la consecución de MAC débiles y más cortas.
b. Durante el proceso de autenticación y crifrado de los datos, no empleaba claves diferentes para cada uno de tales procesos.
c. Se transformó en un protocolo vulnerable a los ataques de truncamiento, falsificación, suplantación, etc., debido a que implementaba el protocolo TCP.

Visualizando lo anterior, el protocolo TLS en su primera versión (TLS 1.0), trabajo en remediar tales debilidades, implementado las siguientes mejoras:

a. Se dispuso la posibilidad de generar claves más largas y robustas.
b. Implementó una nueva técnica de funciones MAC en combinación con funciones *Hash* para mejorar la integridad y confidencialidad de los datos, lo que denomino funciones*HMAC*.
c. Se vale del uso del algoritmo DH, del algoritmo de cifrado Triple-DES y manejo de intercambio de claves.

Con lo anterior, se podría visualizar que entre el protocolo SSL y TLS existen diferencias que no son tan marcadas, pero ellas llevan al punto a que estos dos protocolos no puedan ser operados conjuntamente.

10.8.1 Principales diferencias entre el protocolo TSL y SSL

- Durante el funcionamiento del protocolo Handshake para establecer las conexiones cliente-servidorcuando se implementa el protocolo SSL, se emplean los mensajes *Certificate request* y *Certificate verify*, los cuales funcionan como medios de alerta de respuesta a las solicitudes de posesión de certificados de autenticidad entre los clientes y servidores, es decir, ellos son la respuesta a la solicitud de si poseen ó no tales certificados. Contrario a esto, en el protocolo TLS se establece que si el cliente no posee un certificado de autenticidad, éste no esta obligado a responder tal solicitud por parte del servidor.
- El protocolo TLS emplea un sistema más complejo, seguro y diferente al implementado por el protocolo SSL para la elaboración de las contraseñas de sesión y el cálculo de las MAC.
- TLS a diferencia del protocolo SSL, implementa un sistema de mensajes y códigos de alerta.
- Por tener la filosofía de ser código abierto y de carácter publico, el protocolo TLS no maneja el algoritmo de cifrado simétrico *Fortezza* ó *DSA*, ya que estos protocolos poseen un propietario y se requiere la consecución de sus derechos para su utilización, por el contrario SSL si soporta tales algoritmos de cifrado.
- Con el objetivo de eludir los ataques que emplean la observación y análisis de la longitud de los datos en una transmisión, el protocolo TLS emplea un mecanismo diferente para el relleno de los bloques.

Para el año 2006, se dio una actualización del protocolo TLS[8], lo cual trajo consigo unos cambios y mejoras en la protección contra ataques al sistema de cifrado en los bloques CBC.

[8]RFC 4346 de 2006.

10.8.2 Sistemas y algoritmos criptográficos para TLS. De manera similar al protocolo SSL, el protocolo TLS implementa una serie de algoritmos criptográficos buscando la seguridad en la transmisión de la información. Entre estos algoritmos criptográficos encontramos lo siguientes:

a. **Cifrado de clave simétrica**.[9]El protocolo TLS emplea este tipo de cifrado de manera similar que el protocolo SSL. Con éste algoritmo, los datos se cifran y descifran empleando la misma clave secreta. La clave y los datos transmitidos se cifran mediante este algoritmo y posteriormente se transmiten por medio de un canal de manera más segura, de esta manera, solo quien posee la clave tiene la capacidad para descifrar el mensaje transmitido. Con el fin de evitar que dichas claves secretas sean descubiertas por un intruso cuando se efectúa el intercambio de claves, el intercambio se realiza mediante el protocolo de intercambio de claves ó de encriptación *Diffie-Hellman* proporcionado por OpenSSL, garantizando así la reserva de las claves privadas. El cifrado de clave simétrica emplea varios tipos de cifrado los cuales son 3DES, AES, RC4, RC5, Blowfish, entre otros. Para garantizar la seguridad en la consecución de las claves privada es recomendable tener en mente la longitud de la clave, ya que la longitud de ella es directamente proporcional al nivel de seguridad ofrecido, generalmente se emplean claves de mínimo 80 bits. Actualmente, el protocolo TLS emplea como mecanismo de cifrado el estándar AES, debido a que es el sistema de cifrado mas seguro, empleando éstas claves secretas con longitudes de 128, 192 y hasta 256 bits, adicionalmente, AES tiene la característica de trabajar a nivel de bytes, posee operaciones matemáticas exclusivas tales como suma y multiplicación bit a bit, etc.

[9]Refierase a la sección 10.6.2. Criptografía Simétrica de éste documento, para evidenciar su funcionamiento y características.

b. **Cifrado de clave asimétrica ó pública**.[10] Este protocolo actúa de manera similar tanto con el protocolo TLS como con el protocolo SSL. Este algoritmo funciona utilizando un par de claves (privada y pública) por cada una de las partes involucradas en la transmisión de datos (emisor y receptor). Si los datos se cifran empelando la clave publica, entonces se descifran exclusivamente empleando la clave privada. El cifrado de clave pública emplea generalmente el algoritmo de cifrado RSA, el cual, es un algoritmo de cifrado muy seguro pero muy lento, ya que emplea claves con longitudes de 1024 bits ó mayores, lo que lo hace bastante lento debido a que emplea una gran cantidad de información para procesar. El protocolo TLS al emplear el sistema criptográfico de clave publica y el algoritmo de cifrado RSA tiene la posibilidad de firmar digitalmente la información transmitida, cualquiera de las claves empleadas puede ser usada para cifra ó descifrar los datos y el proceso para la generación y distribución de las claves es mas complejo.

c. **Código de autenticación de mensaje MAC**. El protocolo TLS emplea este sistema con el propósito de garantizar a los usuarios que la información transmitida no ha sido alterada, manipulada ó haya sufrido daños durante la transmisión de los mismos. Éste método se basa en la generación de un resumen de la información transmitida sumándole una clave generada para enviar la información, con ello se verifica que los datos no hayan sufrido cambio alguno en su contenido durante la transmisión. Este mecanismo tiene la ventaja que si no se conocen tanto los datos enviados como la clave generada no es posible leer e interpretar el mensaje de resumen, ello muestra que sino se cuenta con la clave no es posible generar una MAC. En la actualidad existen tres tipos de funciones MAC; CBC-MAC, HMAC y UMAC. El protocolo TLS emplea el tipo de función MAC HMAC; este tipo de función emplea una función Hash para generar un a función MAC ó HMAC, generalmente se emplea la opción de HMAC-SHA-256.

---

[10]Refiérase a la sección 10.6.1. Criptografía de clave publica de éste documento, para evidenciar su funcionamiento y características.

d. **Cifrado por bloques**. Este sistema criptográfico trabaja tomando cantidades fijas de datos (bloques) para efectuar el cifrado y descifrado de los mensajes transmitidos. Este método es bastante prolijo para efectuar el cifrado de la información empleando el protocolo TLS debido a la gran cantidad de datos que son empleados en la transferencia de información, así, ellos pueden ser operados por partes (bloques). Con el protocolo TLS, el sistema criptográfico por bloques puede emplear cuatro tipos de algoritmos de cifrado, los cuales son el *Modo ECB*, *Modo CBC*, *Modo CFB* y *Modo OFB*.

- **Modo ECB**.[11] Electronic Code Book por sus siglas en ingles. Este algoritmo se basa en la división en bloques de los datos transmitidos y de manera individual se efectúa el cifrado de cada uno de ellos. En el cifrado de los bloques no interesa el orden de operación de ellos, también tiene la ventaja de no ser susceptible a errores. Sin embargo, éste algoritmo tiene el inconveniente que si se encuentran mensajes iguales, los textos cifrados también serán repetidos, lo cual, se convertiría en cadenas de secuencias que podrian ser analizadas y descifradas por individuos ó software de ataque a la información.
- **Modo CBC**. Cipher Book Chaining por sus siglas en ingles. Este algoritmo de cifrado opera de manera máscompleja al anterior. Aquí, a cada uno de los bloques de datos sin cifrar se les suma el bloque de datos cifrado que lo precede, esta suma se efectúa bit a bit con XOR. Con este algoritmo de cifrado, cuando los datos son ingresados y divididos en bloques de longitud fija, al primer bloque de datos se le adiciona una cadena de bits aleatorios de igual longitud a la longitud de los datos del bloque que se denomina *vector de inicialización*. El modo de cifrado CBC permite que si se tienen bloques de datos iguales, el cifrado resultante de ellos será distinto, la razón de ello, es la adición del *vector de inicialización*. Con este algoritmo de cifrado, es muy importante que el receptor tenga conocimiento previo del contenido de los

[11]S. Horman. “SSL and TLS an Overview of a Secure Communications protocol,” Presentado en Security Mini-conf at Linux.Conf.AU Canberra, ACT, Australia, 2005, Abril, pp. 2-5, 10-17.

datos del *vector de inicialización* para efectuar las labores de descifrado de la información, por ello, es necesario que las partes involucradas en la transmisión de la información realicen el intercambio de tal vector de manera secreta y segura, generalmente, éste intercambio se efectúa enviando los bits del *vector de inicialización* como parte del encabezado del texto cifrado resultante del cifrado de los bloques de datos.

- **Modo CFB**.Sus siglas en ingles Cipher Feedback Mode. Este algoritmo de cifrado tiene la particularidad que emplea un *vector auxiliar*, al cual se le aplica directamente el cifrado con este algoritmo y no propiamente al mensaje plano original. De los datos cifrados resultantes de cifrar el *vector auxiliar*, se toma una cantidad *X* de bits (cifrados) y se suman a otra cantidad X de bits de los datos del mensaje original, el resultado corresponde a un nuevo mensaje de datos de *X* bits de datos cifrados. Los bits cifrados se emplea también para generar el siguiente *vector auxiliar* para el siguiente bloque de datos a cifrar. La cantidad n de los bits generados puede tener una longitud menor o igual a la longitud de datos del bloque de datos siguiente.
- **Modo OFB**.Output Feedback Mode son sus siglas en ingles. Éste modo de cifrado se ejecuta de manera similar a como lo efectúa el modo CFB. Para el modo OFB, la generación de un nuevo *vector auxiliar* se efectúa a través de los bits cifrados resultantes de aplicar el algoritmo de cifrado OFB y no de los bits cifrados resultantes de la suma del mensaje original más los bits cifrados resultantes del uso del algoritmo. Éste modo de cifrado tiene la posibilidad que al producirse errores en el cifrado de los bits y al efectuar el descifrado de los datos, el error solo afectara a dicho bit.

e. **Funciones Hash**.Esta función es denominada también como *función resumen*. Esta función produce un mensaje resultante con igual longitud ó generalmente con longitudes entre 128 ó 160 bits después de aplicar ciertas operaciones aritméticas, lógicas y computacionales a un mensaje de entrada. El mensaje de resultado es equivalente a un resumen único de un mensaje original con

ciertas variaciones que hacen del mensaje original un texto ilegible. La *función hash* genera cambios importantes y notorios en la informaciónoriginal con el propósito de hacer de ella información no legible e incomprendida para un intruso. Además, proporciona la posibilidad de evitar que la información original sea capturada y descifrada por cierto individuo malhechora partir de un resumen de ella. Con esta función, los usuarios tiene un nivel mas de seguridad en la transmisión de la información que se ve reflejado en la integridad de los datos, es decir, que cuando los datos son transmitidos entre cliente y servidor a través de una red de telecomunicaciones, los usuarios tendrán la certeza que la información no ha sido modificada en su contenido, por lo tanto, la *función hash* ofrece seguridad en la *integridad*de la información. Para verificar que cierta información no ha sido modificada en su contenido, al mensaje original de entrada se le aplica una *función hash* que dará como resultado un resumen de ella, ilegible y entre 128 ó 160 bits de longitud ó de igual longitud al mensaje original que se adjunta a la información enviada, el receptor, al obtener la información, aplicará nuevamente la *función hash* para comprobar que el resumen de resultado del mensaje corresponde idénticamente al resumen de la información generado antes de ser enviado, es decir, la integridad del mensaje se verifica con la concordancia entre los dos mensajes de resumen resultantes de aplicar la *función hash* antes de transmitir y después de recibir la información. Si tal coincidencia entre los mensajes de resumen no se da, indica esto que la información fue manipulada previamente. Actualmente, las *funciones hash* mas divulgadas y mas implementadas son las denominadas MD5 (Message Diggest #5), la cual produce resúmenes de 128 bits y están también las denominadas SHA1 y SHA2 (Standard Hash Algorithm), las cuales generan resúmenes de 160 bits. Las *funciones hash* tienen las siguientes características:

- Son funciones de compresión. Lo que indica que si se tiene mensajes de *n* longitud de datos, el resumen hash tiene una longitud fija. Generalmente, tal resumen es de menor longitud de bits que el mensaje original.
- Son funciones unidireccionales. Lo que refiere a que si se cuenta con un resumen *hash*, computacionalmente debe ser imposible descifrar el mensaje original a partir de tal resumen.
- Facilidad de cálculo. El calculo del mensaje resumen hash debe ser fácil de determinar contando con un mensaje original.
- Difusión. Esto hace referencia a que el resumen hash del mensaje original debe ser una función compleja que represente a todos y cada uno de los bits que constituyen el mensaje original.

Se podría decir que las *funciones hash* operan similarmente a como operan las funciones que cumplen las tareas de cifrado ó encriptación de la información, la diferencia que reside entre ellas es que al realizar el intercambio de información entre cliente y servidor, la información transmitida puede contener grandes cantidades de datos, lo que hace la operación de cifrado de datos lenta y con gran consumo de recursos, por lo tanto, con las *funciones hash*, las operaciones de cifrado se realizan solo sobre un resumen del mensaje original generado a partir de la *función hash* y no sobre todo el contenido de la información. Lo que hace las operaciones de cifrado mas rápidas y con menos consumo de recursos.Efectuar el cálculo del resumen de un mensaje original tiene el propósito de variar el tamaño de tal mensaje según su volumen original y al aplicar la *función hash*, tal volumen se traducirá en una cantidad fija de 160 bits generalmente. Este proceso se logra cuando el mensaje original se divide en varias partes, cada una de ellas compuestas por 160 bits, al completar tal división, se toman elementos de cada una de las partes divididas y se combinan entre ellos para formar el mensaje *resumen* ó *hash* con igual longitud de 160 bits. Finalmente, a este *resumen hash* de longitud fija se le aplica un

determinado algoritmo de cifrado implementando la clave privada del agente emisor de la información.

10.8.3 Objetivos del protocolo TLS

- **Autenticación de cliente y servidor**.La forma en que el protocolo TLS efectúa tal propósito es a través de la implementación del sistema criptográfico de claves (claves publicas y privadas), temática mencionada en la sección 10.6 Criptografía. Con ello se logra la autenticación tanto del cliente como del servidor, adicional a esto, se usan los certificados digitales obtenidos a través de alguna entidad certificadora reconocida.
- **Proporcionar integridad de la información**.El protocolo TLS vela para que los datos transmitidos en una red entre las partes interesadas, tengan la certeza que los datos no han sido manipulados ni modificados durante su emisión.
- **Privacidad de la información**.Esto refiere a la capacidad del protocolo TLS para evitar que los datos transmitidos en una red sean accedidos ó intervenidos por un intruso mientras ellos llegan a su destino.

El protocolo TLS similarmente al protocolo SSL se divide en dos subprotocolos; el *protocolo de registro* y el *protocolo Handshake TLS* (apretón de manos), dando esto seguridad en la conexión presentantadade dos maneras importantes:

a. **Conexión privada**.La comunicación entre las partes utiliza criptografía simétrica para codificar los datos transmitidos. Con cada conexión es necesaria una llave que es negociada en secreto por las partes involucradas en las transacciones.
b. **Conexión segura**.Esto se logra con mensajes de comprobación de integridad que se incluyen en los mensajes utilizando una MAC con llave.

El protocolo TLS provee conexión segura la cual presenta tres propiedades:

a. La identificación de cada una de las partes involucradas en una transacción puede hacerse usando criptografía de llave publica ó llave asimétrica, la cual es opcional en la comunicación, pero cada parte requiere de esto.
b. La negociación de una llave simétrica se efectúa de manera secreta y segura, es decir, que no estará disponible para intrusos ó para atacantes en el medio de una comunicación entre cliente y servidor.
c. Las partes involucradas en una transmisión de información están al tanto de los posibles atacantes ó intrusos, tanto así, que ningún atacante puede modificar la comunicación sin ser detectado por alguna de las partes.

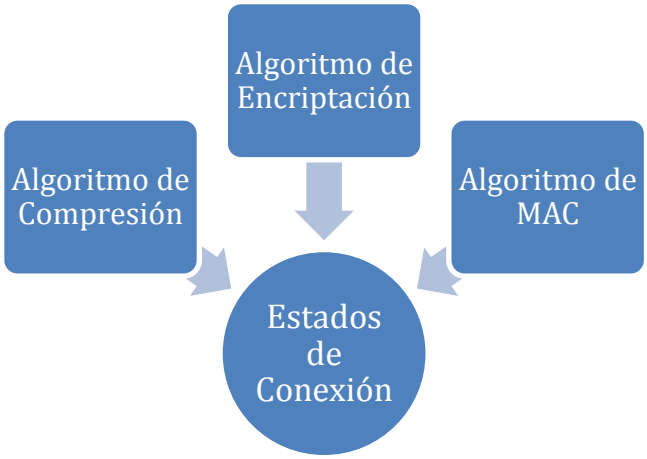
El protocolo TLS es independiente de los protocolos superiores que serán utilizados en una comunicación entre cliente y servidor. Al momento de establecer una transacción segura utilizando TLS no se especificanprotocolos ni seguridad en TLS; esta labor depende del diseñador de la seguridad en la transacción electrónica.

10.8.4 Protocolo de Registro TLS. En concordancia con su predecesor (Protocolo SSL Versión 3.0), el protocolo de registro TLS toma los mensajes a transmitir y les aplica las acciones de fragmentación, compresión, aplicación de MAC, encriptación y transmisión del mensaje resultante; al llegar al destino, se aplican las operaciones inversas para ser enviadas a protocolos de niveles superiores.

El protocolo de registro TLS posee *Estados de Conexión y Capa de Registro*, adicionalmente, se compone de cuatro subprotocolos los cuales son: *Protocolo de Enlace, Protocolo de Alerta, Protocolo de Especificación de Cambio de Cifrado (Change Cipher Spec.)y el Protocolo de Datos de Aplicación*.

10.8.4.1 Estado de conexión. Un estado de conexión TLS es el entorno ó modo de funcionamiento del Protocolo de Registro TLS, un estado de conexión define tres aspectos: *un algoritmo de compresión, un algoritmo de encriptación y un algoritmo de MAC*, como se indica en la figura 11.

Figura 11. Estado de Conexión. Basado en The Transport Layer Security (TLS) Protocol Version 1.2 T. Dierks, E. Rescoria.



Disponible en www.ietf.org/rfc/rfc5246.txt

Los parámetros de seguridad del protocolo TLS en estados de conexión de lectura y escritura son establecidos por los siguientes valores:

- **Fin de Conexión**.Si ésta entidad es considerada el cliente ó el servidor en la conexión.
- **Algoritmo PRF**. Éste es un algoritmo utilizado para generar claves desde una *master secret*.
- **Algoritmo de Cifrado Masivo**. Algoritmo usado para medir el tamaño de una llave para un cifrado masivo.
- **Algoritmo MAC**. Incluye el tamaño del valor retornado por un algoritmo usado en autenticación de mensajes.

- **Algoritmo de Compresión**. Aquí se incluyen todos los parámetros necesarios para la compresión de mensajes a transmitir.
- **Llave Maestra**. Clave secreta de 48 bytes utilizada por las partes implicadas en las transacciones electrónicas.
- **Valor Aleatorio del Cliente**. Un valor de 32 bytes dado por el cliente.
- **Valor Aleatorio del Servidor**. Un valor de 32 bytes dado por el servidor.
- **Estado de Compresión**. Estado actual del algoritmo de compresión.
- **Estado de Cifrado**. Presenta el estado actual del algoritmo de encriptación.
- **Llave MAC**. Es la llave MAC de la conexión actual, la cual se genera al inicio de la comunicación.
- **Numero de Secuencia**. Cada conexión presenta un número de secuencia que distingue entre los estados de lectura y escritura. El valor del número de secuencia en una comunicación electrónica debe ser cero cuando el estado de conexión se vuelve activo.

10.8.4.2 Capa de registro. La capa de registro recibe datos en bloques no vacíos de tamaños aleatorios, provenientes de capas superiores los cuales no son interpretados.

La fragmentación se aplica a bloques de información en registros de texto plano TLS y los transporta en secciones de longitud de 2^{14} bytes ó menor. Por otro lado, todos los registros deben ser comprimidos usando el algoritmo de compresión definido en el estado de sesión actual; ésta compresión se debe realizar sin perdidas de información y su longitud máxima debe ser de 1024 bytes.

10.8.4.3 Protocolo de Enlace TLS. El protocolo TLS posee tres subprotocolos que son usados para permitir que cada una de las partes establezca los parámetros de seguridad provenientes de la capa de registro, para autenticarse ellos mismos, para negociar parámetros de seguridad en determinada instancia y para reportar condiciones de error de cada parte. Entre estos se encuentran el

Protocolo de cambio de especificaciones de cifrado, para indicar transiciones en las estrategias de cifrado y *Protocolo de Alerta*, responsable de mostrar los diferentes mensajes correspondientes a diversos estados de la conexión.

Una sesión, de la cual es responsable el protocolo de enlace consiste en lo siguiente:

- **Identificador de Sesión**.Corresponde a una secuencia aleatoria de bytes escogida por el servidor para identificar un estado de sesión activa.
- **Certificado de Pares**.Este puede tomar un valor nulo; generalmente se emplea X509V3 para certificados de pares TLS.
- **Método de Compresión**.Es el algoritmo usado por las partes antes de la encriptación.
- **Especificación de Cifrado**. Aquí se especifica una función pseudorandomica para la obtención de llaves que se usaran en el cifrado de mensajes transmitidos en una transacción electrónica.
- **Secreto Maestro**. Secreto de 48 bytes compartido entre las dos partes que hacen parte de la transmisión.
- **Es Reanudable**. Es una marca que indica si la sesión puede ser usada para iniciar nuevas conexiones.

Los parámetros expuestos anteriormente, son usados para crear medidas de seguridad utilizadas por la capa de registro que protegerán los datos de la capa de aplicación en eventuales conexiones.

Siguiendo la línea de su predecesor (el protocolo SSL), el *Protocolo de Enlace* TLS precisa los siguientes pasos para establecer una conexión:

1. Enviar y recibir el mensaje de “Hello” los cuales preparan una eventual conexión.

2. Intercambio de los determinados parámetros criptográficos para conseguir el mensaje secreto maestro.
3. Intercambio de información de certificados y criptografía que permite a cada una de las partes, cliente y servidor, autenticarse entre si.
4. Generación de un secreto maestro partiendo de la compartición previa de un secreto pre-maestro.
5. Proveer seguridad a la capa de registro.
6. Permitir la verificación tanto del cliente como del servidor de sus contrapartes para constatar que tengan los mismos parámetros de seguridad.

Las capas superiores no deben ser exclusivamente dependientesde si TLS negocia con el canal mas fuerte y seguro entre las partes. Si bien el protocolo TLS minimiza el riesgo de ataque como el de hombre en el medio, siempre hay una forma de poder violar una transacción. Es por esto que los niveles de capas superiores deben se consientes de transmitir sobre un canal de sea altamente seguro dependiendo de sus propias necesidades.

Todos estos objetivos se consiguen en el *Protocolo de Enlace* con los mensajes "*Client Hello*" y "*Server Hello*"; cada parte transmite estos mensajes respectivamente, si no existe una respuesta desde su contraparte, de inmediato se debe producir un error que generará una conexión fallida.
Con respecto al intercambio de claves, hoy en día se emplean cuatro mensajes: *El Certificado del Servidor, Llave de Servidor Intercambiada, El Certificado del Cliente y Llave de ClienteIntercambiada*. Actualmente, el secreto debe ser los suficientemente grande, del orden de 46 bytes ó superior.

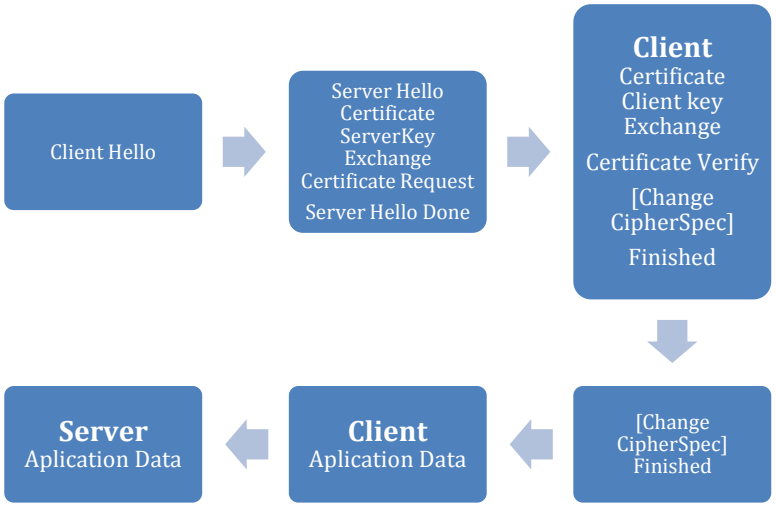
Posteriormente al intercambio de mensajes de saludo (Hello), el servidor envía un mensaje con su certificado de autenticidad que, dependiendo de si se envió el mensaje *Certificate Request* será ó no contestado por el cliente. Posteriormente, se envía el mensaje *Client Key Exchange* y el contenido de éste depende del

algoritmo de encriptación que se negocio entre *Client Hello*[12] y *Server Hello*[12]. Luego de esto, se comparte un mensaje *Change Cipher Spec* y el cliente copia la información de *Cipher Spec* en la corriente *Cipher Spec*. Adicionalmente, el cliente envía el mensaje de "*Terminado*"teniendo en cuenta los nuevos algoritmos, claves y secretos. El servidor hace su parte enviando un mensaje de *Change CipherSpec* y envía el mensaje de "*Finalizado*" con los nuevos parámetros de cifrado. En este punto, la sesión de enlace culmina y ambas partes ya pueden intercambiar información en las capas superiores de modelo OSI.

Este proceso mantiene la misma estructura de establecimiento de conexión que el protocolo SSL en su versión 3.0, la cual se puede evidenciar en la figura 12, donde se realiza una descripción grafica de éste procedimiento.

[12]La descripción detallada de los mensajes Hello no se aborda en esta monografía ya que escapa de los límites de la misma. Para mayor información visite la página oficial de la descripción del protocolo: The Transport Layer Security (TLS) Protocol Version 1.2. T. Dierks & E. Rescorla. Agosto de 2008.

Figura 12. Proceso de establecimiento de conexión entre cliente y servidor.



Elaboración propia. Basada en RFC 6101 – The SSL Protocol Version 3.0.
Disponible en www.datatracker.ietf.org/doc/rfc6101/?include_text=1

10.8.5 Calculo del Secreto Maestro. Para realizar el calculo del *Secreto Maestro* en una transacción cliente-servidor, se pueden utilizar diversos métodos pero el mismo algoritmo para convertir una eventual *Pre-Master-Secret*en la *Master-Secret*, donde la primera debería ser eliminada en cuanto se crea el *secreto maestro*.

Se debe tener en cuenta que el *secreto maestro* siempre tendrá una longitud de 46 bytes, mientras que la longitud del *secreto pre-maestro* variara dependiendo del método de intercambio de clave utilizado. Ejemplos de cifrado de clave pública son RSA y Diffie-Hellman.

10.8.5.1 RSA. Es un sistema tanto de encriptación como de autenticación de clave publica desarrollado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. Este

sistemas produce cifrado y autenticaciónusando claves publicas de las partes y la propia clave privada. Cuando un servidor intenta realizar autenticación e intercambio de claves, el *secreto pre-maestro* de 46 bytes es generado por el cliente bajo la utilización de la clave pública del servidor y posteriormente enviado al servidor. Luego de esto, las partes utilizan este *secreto pre-maestro* para generar el *secreto maestro*.

10.8.5.2 Diffie-Hellman. Es un protocolo de establecimiento de claves entre pares desarrollado por Whitfield Diffie y Martin Hellman. Este protocolo genera claves entre dos partes sin necesidad de que éstas hayan tenido contacto previo, usando un canal inseguro y de forma anónima. El proceso de creación del *secreto maestro* es el siguiente:

1. Las dos partes contienen un mismo *secreto pre-maestro*.
2. Con su clave privada, cada parte hace uso del *secreto pre-maestro* para generar la clave que será compartida entre ambos.
3. Luego de compartir la clave, desencriptan su clave privada y generan el *secreto maestro*, el cual será utilizado para encriptar los mensajes.

Para el caso del cifrado simétrico[13], algunos mecanismos utilizados son RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES ó AES (Advanced Encryption Standard).

10.8.5.3 RC2. Es un cifrado de bloque diseñado por Ron Rivest en 1987. RC2 es un cifrado de bloques de 64 bits con una llave de tamaño variable. RC2 (Rivest Cipher 2), es un cifrado débil que actualmente se torna fácil romperlo por un ataque de fuerza bruta.

[13] En el numeral 10.6.2. apartado Criptografia Simetrica se hace una breve descripción de éste.

10.8.5.4 RC4. Este es el sistema de cifrado de flujo mas utilizado por SSL/TLS. No obstante, en ocasiones ha sido considerado inseguro por algunos modos de uso, que ha llevado a considerarlo no recomendado para el uso de sistemas actuales. RC4 es un sistema de flujo de cifrado con tamaño de llave variable con operaciones byte-orientadas basado en permutaciones randomicas las cuales pueden arrojar posibilidades mayores que 10100. Debido a que proporciona un alto nivel de seguridad, es muy usado en las transacciones comerciales electrónicas.

10.8.5.5 IDEA. International Data Encryption Algorithm por sus siglas en ingles. Es un algoritmo internacional para el cifrado de datos, es un algoritmo de clave secreta creado en 1991 por James Massey y Xuejia Lai bajo el nombre de PES (*Proposed Encryption Standard*)en su primera versión. De acuerdo a una serie de modificaciones para mejorar sus robustezcambió de nombre a lo que se conoce como IDEA.

Este algoritmo utiliza una clave de 128 bits de longitud que lo hace inmune a los ataques de fuerza bruta; con esta clave, IDEA encripta bloques de texto plano de 64 bits en bloques de texto cifrado de igual longitud.

Tanto IDEA como DES ya no se recomiendan para usarse en las ultimas versiones del protocolo TLS y de hecho se ha eliminado de TLS V1.2; esto debido a que su uso en TLS no es generalizado además de dificultades en su interoperabilidad.

10.8.5.6 DES. Data Encryption Standard por sus siglas en ingles. Es un estándar para el cifrado de información. Emplea un cifrado de bloques que fue aprobado originalmente en 1976. DES emplea un bloque de 64 bits, de los cuales dispone solo de 56 bits de ellos para su protección, los restantes no son usados por este algoritmo.

En lo posible se debe evitar utilizar este algoritmo por las bibliotecas TLS debido a problemas de seguridad, si él es implementado, se debe asegurar que su uso no se haga de forma predeterminada.

10.8.5.7 Triple DES. Éste mantiene el mismo algoritmo utilizado por DES, la diferencia radica en quesolo se aumenta la longitud de la llave utilizada para evitar ataques del tipo "*Man in the middle*", el cual consiste en atacar ambos participantes en una transacción por medio de fuerza bruta y comparar los valores de salida de cada uno; si coinciden, probablemente se tendrá la clave correcta.

Aumentando la clave al triple, se logra una longitud de ella de 192 bits, de los cuales, son necesarios realmente 112 bits de ellos. Debido a su lentitud, DES actualmente se encuentra en desuso, siendo reemplazado por el algoritmo AES; sin embargo, DES sigue siendo utilizado por tarjetas de crédito y otros medios de pagos electrónicos.

10.8.5.8 AES. Advanced Encryption Standard son sus siglas en ingles. Es uno de los algoritmos de criptografía mas comúnmente usados en la actualidad por sistemas de criptografía simétrica. Estandarizado en el año 2002, AES es un algoritmo de red de permutación, bastante rápido tanto en software como en hardware, presenta facilidades de implementación y requiere poco consumo de memoria.

AES implementa el sistema de cifrado por bloques y cada bloque tiene una longitud de 128 bits y llaves de 128, 192 ó 256 bits. Actualmente no se conocen ataques eficientes a este algoritmo, los únicos conocidos son los llamadas ataques de canal auxiliar.

10.8.6 Aplicaciones e implementaciones del protocolo SSL/TLS. Actualmente, el protocolo SSL/TLS presenta un considerable numero de aplicaciones que,

inicialmente se basaban en la navegación Web (Protocolo HTTP), pero que ahora se encuentra difundido en otros protocolos como SMTP, POP, IMAP, FTP, NNTP, entre otros.

El funcionamiento de estos protocolos se realiza de la misma manera, solo cambia el uso de puertos TCP propios. Para el caso de HTTPS (HTTP seguro basado en SSL/TLS), el cual se usa para la navegación web segura, el puerto utilizado es el 443; y NNTPS (NNTP seguro basado en SSL), para el acceso seguro a News, el puerto utilizado es el 563. Generalmente, el uso del protocolo SSL/TLS se hace usando el protocolo de transporte fiable TCP; pero se han implementado soluciones que hacen uso de protocolos como UDP (User Datagram Protocol), DCCP (Datagram Congestion Control Protocol) y DTLS (Datagram Trasnport Layer Security), entre otros.

Aplicaciones basadas en el protocolo SIP (Session Initation Protocol) como VoIP hace uso del protocolo SSL/TLS para brindar seguridad e su implementación.

Una de las aplicaciones mas imporrtatnes del protocolo SSL/TLS es el comercio electrónico, el cual hace uso del protoclo HTTPS para hacer las paginas web de vendedores y compañías seguras en una transacción comercial por medio de criptografía de llave publica, haciendo uso de diversos medios de pago, entre los cuales se destaca la tajeta de crédito; entidades como Mastercard, Visa y American Express avalan el uso de este protocolo por considerarlo seguro.

10.8.6.1 Stunnel. Eventualmente, se hace necesaria la creación de canales seguros en una transacción comercial, estos canales comúnmente reciben el nombre de tuneles TLS/SSL. Existen aplicaciones que permiten la creación de éstos, tal como la herramienta *Stunnel*, la cual es una aplicación de código libre

multiplataforma creado por Michal Trojnara[14], que hace uso de criptografía de clave publica asi como certificados X.509 y demonios como POP2, POP3 e IMAP, para crear tuneles en una comunicación entre dos partes que no tienen implemenado el protcolo SSL/TLS de forma nativa.

10.8.6.2 Open VPN. El protocolo SSL/TLS se puede utilizar para envolver una red completa y crear una red privada virtual, tal es el caso de *OpenVPN*; el cual es una solución basada en código libre, que provee seguridad en redes que hagan uso de canales públicos usando encriptación y autenticacion *OpenSSL*; esta herramienta representa una mejora en cuanto a la facilidad de implementación frente IPSec, que es mas antigua y compleja de implementar. Ésta solución presenta algunos inconvenientes como la falta de compatibilidad con IPSec, además de la poca implementacion de ella.

10.8.6.3 FTPS. El protocolo de transferencia de archivos *FTP* permite transferir archivos de un computador a otro. Su uso se remonta al año 1971 y se ha podido mantener desde entonces debido a la implementación de la seguridad en su uso, seguridad brindada por el protocolo SSL/TLS que transforma este protocolo en *FTPS* ó *FTP* Seguro ó *FTP* basado en SSL/TLS. En una transferencia de archivos que utilice *FTPS* se realiza un intercambio de claves al momento de establecer una conexión. Existe *FTPSimplícito* que consiste en el uso del protoclo SSL/TLS en ambas partes de la transferecnia; para el caso contrario, el protocolo *FTPS* recibe el nombre de *FTPSexplicito*.

10.8.6.4 Open SSL. Es un conjunto de herramientas desarrolladas de manera libre por colaboradores alrededor del mundo que provee un servicio de librerías encaminadas a las aplicaciones comerciales haciendo uso del protocolo SSL/TLS.

[14]Para mayor información sobre esta herramienta, visitar Stunnel: Home. Disponible en: https://www.stunnel.org/index.html

OpenSSL se basa en una biblioteca *SSLeay* que se puede obtener y utilizar de manera libre para propósitos que pueden ser ó no comerciales[15].

10.8.6.5 GNUTLS. Es una biblioteca de librerías para implementar el protocolo *SSL/TLS* de manera libre en aplicaciones que requieran medidas de seguridad. Se basa en el lenguaje C para la creación de APIs para analizar y escribir certificados X.509; en buscar deficiencias e interoperabilidad. Éste conjunto de librerías se puede utilizar en programas que no son libres[16].

En la actualidad el protocolo *SSL/TLS* es la solución más difundida ó preferida por los desarrolladores y diseñadores de aplicativos que involucren transacciones entre cliente y servidor. Desde una visión general, el protocolo *SSL/TLS* presenta un nivel se seguridad basante robusto, sin embargo, actualmente se ha puesto en conocimeinto publico algunas de sus vulnerabilidades que conllevan a buscar nuevas alternativas para la protección de información clasificada.

10.8.7 Vulnerabilidades del protoclo SSL/TLS. Actualmente, se están haciendo visibles problemas graves de seguridad que muestran vulnerbilidades en el protocolo SSL/TLS, logrando éstas extraer claves seguras y mostrar el contenido cifrado que viaja por medio de canales electrónicos como la internet.

Algunas de las vulnerabilidades son subsanadas en la versión más actual del protocolo TLS (versión 1.2). Sin embargo, aactualmente se han encontrado algunas vulnerabilidades en la utilización del protocolo SSL/TLS en OpenSSL en todas sus versiones, incluyendo 1.0.1c, 1.0.0j y 0.9.8x, permitiendo la revelación

[15] Todos los recursos libres de OpenSSL se pueden obtener desde la página oficial, disponible en: http://www.openssl.org/contrib/
[16]Para mayor información visite: The GNUTLS Transport Layer Security Library. http://www.gnutls.org/

de información asi como denegación del servicio [17] . Para mitigar esta vulnerabilidad, se recomienda a los usuarios afectados actualizar sus versiones de OpenSSL a 1.0.1d, 1.0.0k ó 0.9.8y.

Algunos métodos de criptografía como RC4 son los mas recomendados a utilizar para lograr disminuir sustancialmente las vulnerabilidades en los protocolos de seguridad; estas vulnerabilidades son, en gran parte producto de ataques de tipo "*Man In The Middle* (*MITM*)" que consiste en la interceptación y posterior manipulación de los mensajes entre dos participantes en una transacción electrónica sin que ninguna de ellas se percate de tal violación.

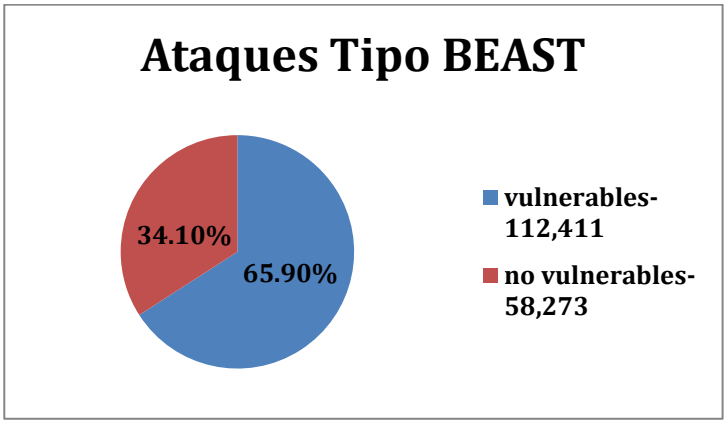
El método de cifrado CBC (*Cipher Block Chaining*), ha sido blanco de multiples ataques que permiten mostrar algunas falencias cuando el protocolo SSL/TLS usa este método de cifrado. Ataques del tipo MITM como BEAST, CRIME y Lucky Thirteen Attack, son algunos de los más mencionados.

10.8.7.1 BEAST. *Browser Exploit Against SSL/TLS* Tool son sus siglas en ingles. Esta es una vulnerabilidad del navegador en SSL/TLS, es un ataque descubierto en 2004 que no es propiamente del tipo MITM, debido a que la interceptación de los mensajes se puede hace desde un host de destino ó adyacente. Se requiere conocer el trafico SSL del usuario y "engañar" al navegador por medio de la inserción de código para que envie un mensaje de texto sin formato al servidor con el cual está realizando la comunicación; ya con estos dos elementos se procede a implementar herramientas de criptoanálisis y esperar a conseguir una cookie de sesion.

[17] Estas vulnerabilidades fueron investigadas por Nadhem AlFardan y Kenny Paterson, de la Universidad Royal Holloway, Londrés. Para mayor detalle se puede disponer de un informe detallado en la siguiente dirección: http://www.isg.rhul.ac.uk/tls/TLStiming.pdf

Para contrarrestar este tipo de amenzas, se recomienda que la sesion no este mucho tiempo activa, además, tomar la precaucion de cerrar correctamente la sesion cuando se haya terminado de realizar la comunicación con el servidor, ya que este tipo de ataque involucra tiempo y apropiación de cookies de sesion. De igual manera, el uso del protocolo TLS versión 1.1 acabaria con este tipo de amenaza, pues no es vulnerable a tal ataque. A inicios de Junio de 2013, había un gran numero de paginas web que presentan vulnerabilidad a este tipo de ataque, aproximadamente el 77% de las paginas que implementaron HTTPS. La figura 13 ilustra este fenómeno.

Figura 13. Relacion entre paginas web HTTPS con vulnerabilidad al ataque BEAST.



Elaboracion propia. Basada en la publicación mostrada en la pagina web https://www.trustworthyinternet.org/ssl-pulse/

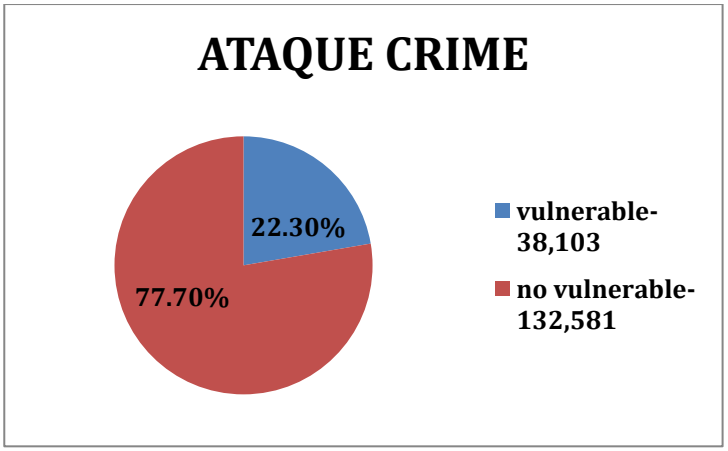
10.8.7.2 CRIME. Este tipo de ataque es un sucesor de BEAST y su modo de acción es similar, dado que se necesita engañar al navegador del usuario por medio de JavaScript para enviar texto sin formato al servidor web y por medio de un Sniffer que tenga acceso a la sesion cifrada entre cliente y servidor, esperar a obtener las cookies de sesion respectivas. Para el ataque BEAST se recomendó la actualización a versiones mas recientes del protocolo TLS, como la versión 1.1 y

1.2; además, de la migración al método de cifrado RC4, el cual no es vulnerable a este tipo de ataque.

CRIME es un ataque que no depende de un cifrado en particular (de hecho, algo que facilita el ataque CRIME es el uso del cifrado RC4) y es independiente del tipo de versión del protocolo TLS. En publicaciones recientes (Junio de 2013) mostradas por SSL Pulse se evidencia la vulnerabilidad de sitios web con soporte TLS frente al ataque CRIME. La figura 14 ilustra tal situación.

Algunas medidas pertinentes para contrarrestar este ataque, además de las expuestas en el ataque BEAST, es la deshabilitacion de la compresión SSL/TLS y la actualización periódica del software involucrado en la sesion cliente-servidor.

Figura 14.



Elaboracion Propia. Basada en la pubicacion mostrada en la pagina web https://www.trustworthyinternet.org/ssl-pulse/

10.8.7.3 Lucky Thirteen Attack. Este tipo de ataque utiliza un método llamado *Padding Oracle*, el cual, es el encargado de dar integridad a los datos y realizar el cifrado de los mismos. Utilizando una debilidad conocida en el modo de cifrado de bloque, CBC; se captura trafico cifrado que viaja por medio de internet, se

reemplazan los últimos bloques en mensajes transmitidos y se mide cuanto tiempo tarda el servidor en contestar; debido a que el tiempo que tardan en procesarse los mensajes que presentan un relleno (Padding) correcto es menor, se puede hacer un muestreo con grandes cantidades de mensajes TLS modificados y en base a esos se puede ocasionalmente encontrar el mensaje cifrado.

De igual manera que los ataques vistos anteriormente, para lograr contrarrestar el impacto de éste ataque, se recomienda utilizar el cifrado RC4 de igual manera que la versión 1.2 del protoclo TLS. Algunas implementaciónes como OpenSSL, GunSSL, NSS, PolarSSL, entre otros, han insertado parches de seguridad para contrarrestar este tipo de ataque.

11. ESTADO DEL COMERCIO ELECTRONICO EN COLOMBIA Y LATINOAMERICA

Hoy en dia ya tenemos y desde hace algún tiempo el surgimientodel paradigma de la sociedad de la información y las telecomunicaciones, el surgimiento de éste se dio debido al origen y desarrollo de las nuevas tecnologías de la información y las telecomunicaciones. Estas nuevas tecnologías nos permiten tener un mayor y mejor flujo de información y adicionalmente, los procesos de comunicación e intercambio de informacion han tenido un crecimiento significativo. El desarrollo y las mejoras en las nuevas tecnologías digitales han permitido que el flujo e intercambio de informacion logren llegar a más personas, a una sociedad más grande, con ansias de consumo, curiosidad ycomunicación.

Con estos nuevos desarrollos digitales, la sociedad ha enfrentado numerosos y diversos cambios sociales, culturales, económico y políticos, por lo tanto, nos vemos obligados a efectuar una medición a escala mundial, regional y nacional del estado actual del progreso de las nuevas tecnologías y de la comunida internauta en el contexto del acceso, impacto, uso y en el caso de esta monografía el consumo con las nuevas tecnologías de las telecomuicaciones enfocado al comercio electrónico específicamente el mas conocido y de mayor uso por la sociedad, el comercio electrónico tipo B2C (*Businness to Consumer*). Con el desarrollo de estas mediciones y estadisctas se permitirá tener una idea y comparación del estado actual y evolución del acceso y uso de las TIC a través del tiempo, específicamente dentro de los últimos 5 años, tanto entre los países de la región y Colombia. Con esta monografía se pretende además identificar los países y regiones nacionales de mayor y menor consumo en términos del comercio electrónico B2C mediante el uso de las TIC y tener un idea cuantitativa y cualitativa de las diferencias que existen en la región (Latinoamerica y Colombia) en cuanto a la penetración del comercio electronico, asi podremos obtener

información sobre las condiciones de consumo en la internet de la población Colombiana.

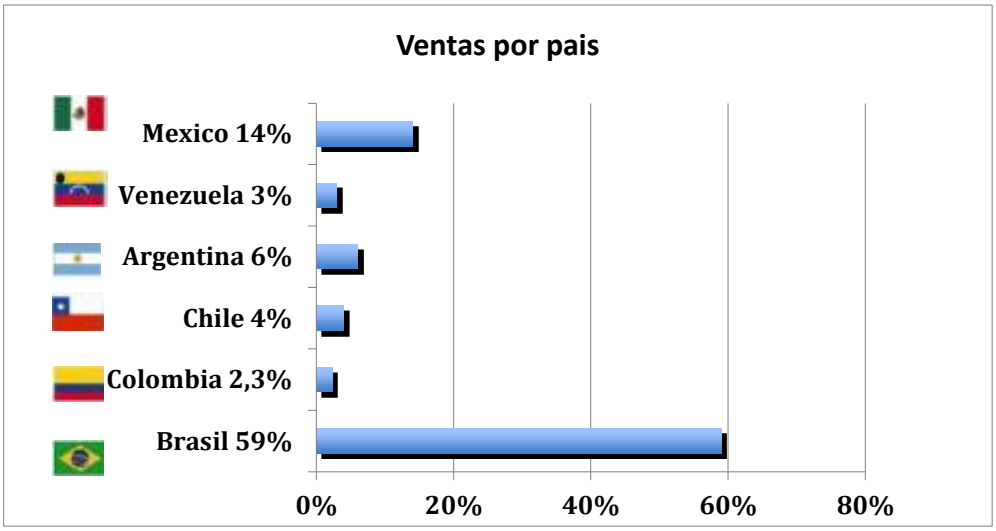
En la actualidad, se ha visto que la tendencia de los países latinoamericanos y especialmente Colombia en el consumo y transacciones electrónicas, tiene una inclinación hacia el consumo y compraventa de servicios y no de bienes y productos, la razón de esto, se debe al gran auge de ventas minoristas en línea y el numero de dominios registrados en la internet. Según estudios, Colombia es un país líder en esta tendencia, ya que en el contexto de dominios registrados, nuesto país se ubica en la region en el segundo lugar después de Argentina en poseer la mayor cantidad de dominios registrados con un total de 48 dominios por cada mil habitantes, después de producirse la liberación de los dominios en internet en el año 2010.

De acuerdo a estudios adelantados, en el mundo el comercio electrónico abarca el 2% del PIB, en Latinoamerica representa el 0,5% y unos años atrás en Colombia representaba menos del 0,2%. La principal razón de esto es que los Colombianos tiene desconfianza y miedo para efectuar compras por internet, es decir a la inseguridad sobre su información y datos. Sin embargo, a pesar de la baja dinámica del comercio electrónico en nuestro país, existen muchos colombianos que realizan compras por internet pero preferiblemente en tiendas del exterior como Amazon.com. Otra razón muy poderosa para la baja dinámicadel comercio electrónico y la compraventa de productos en linea es la muy baja taza de bancarización, lo que conlleva a que aquella población que no cuenta con espacios bancarios no tenga la posibilidad de efectuar compras por internet. Sumado a lo anterior, se ha detectado la falta de oferta de calidad en internet en nuestro país. Pero a pesar de todo, desde hace algunos años en Colombia se vienen efectuado compraventas en internet exitosas en sitios como Mercadolibre.com, pero en comparación con países como Brasil, Argentina, Chile y Mexico, nuestro país presenta un atraso considerable (ver figura 15). Con el

animo de mejorar esta situación, crear y fortalecer la confiaza del consumidor digital en nuestro país surgio una entidad gubernamental que se denomino la Camara Colombiana de Comercio Electronico (CCCE), además del surgimiento de compañías de alta calidad que han ayudado al aumento del dinamismo del comercio electronico, entre las que se pueden enunciar son Avianca, Falabella, LAN, Ktronix, Sony y la firma nacional ÉXITO. Éstas y otras compañías junto con la CCCE efectúan grandes esfuerzos con el objetivo de generar mayores compraventas de productos en línea y disminuir el letargo de Colombia en comparación con los países de la región con respecto al comercio electrónico del tipo B2C, un ejemplo de estos estos esfuerzos se ve reflejado en el lanzamiento por primera vez en nuestro país del "Cyberlunes" el pasado mes de Noviembre del 2012. Durante este evento digital, se reportaron cifras muy llamativas de las compañías que participaron, las cuales reportaron un aumento en el flujo de compraventas a través de sus sitios web cerca al 500%[18]. Adicionalmente, el gobierno nacional de Colombia adelanta programas encabezados por el Ministerio de las TIC que buscan ampliar la cobertura e infraestructura de las conexiones a internet. Sumado a esto, el sector bancario y financiero se esfuerzan por diseñar y poner al servicio nuevas estrategias de bancarización en busca de que el sistema de trajetas de credito y debito sean mas accequibles a las personas llevando a que estos nuevos usuarios se interesen por el comercio electrónico, tal es el caso de convenios entre bancos y empresas para efectuar los pagos de las nominas de sus empleados de manera electrónica con el uso de tarjetas debito.

[18]Cifras reportadas por la CCCE y estudios de la región efectuados por VISA.

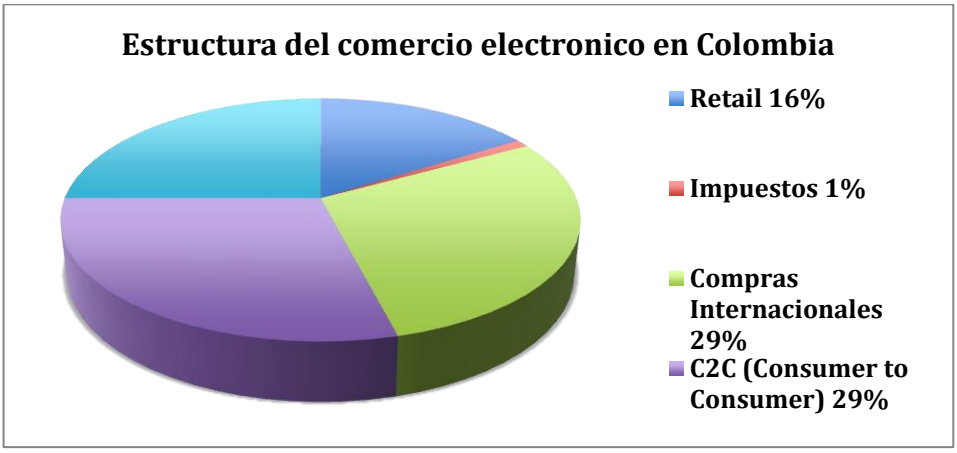
Figura 15. Participacion en ventas por pais.



Elaboracion propia. Basado en estudios del comercio electronico de Visa disponible en www.larepublica.co/otros_/e-commerce.pdf

Para el año 2011 según los estudios efectuados[18], en Colombia, un internauta usuariodel comercio electrónico tuvo un gasto promedio de US$45 y para el panorama de Latinoamerica un internauta gasta en promedio en el comercio electrónico US$50. Mostrando entre otras cosas que los internautas colombianos prefieren en orden descendente las compras internacionales en línea, el comercio electrónico tipo C2C, viajes, retail y el pago de impuestos, lo que se ilustra en la figura 16.

Figura 16. Estructura del comercio electronico en Colombia.



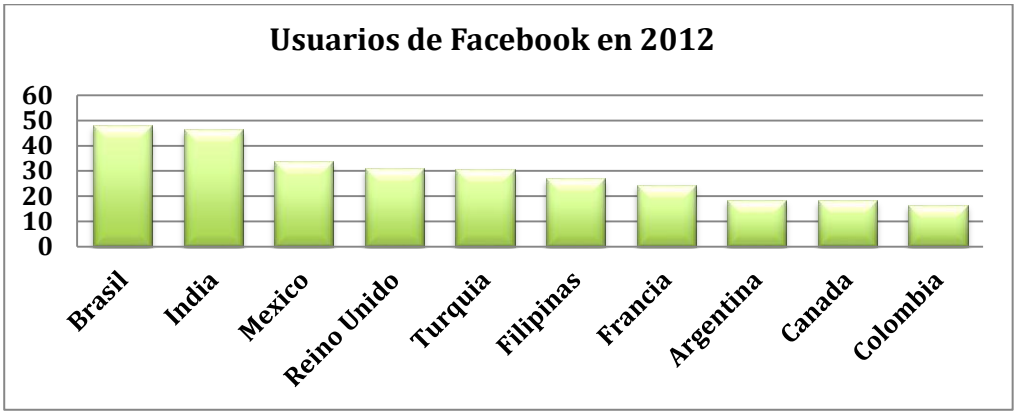
Elaboracion propia. Basado en estudios del comercio electronico de Visa disponible en www.larepublica.co/otros_/e-commerce.pdf

De acuerdo a estudios adelantados por *America Economia*, realizó una medición que denomino indice de e-Readiness, con el cual efectua una medicion del avance y aceptacion del comercio electronico en cada uno de los paises de la region latinoamericana. Con éste estudio, se busco obtener una calificacion de cada pais mediante la evaluacion del flujo de mercado, los indices de bancarizacion, la adopcion de nuevas tecnologias, la infraestructura tecnologia y la fortaleza de la oferta, los cuales son caracteristicas esenciales para el desarrollo del comercio electronico. Segun el estudio, Colombia obtuvo en sus calificaciones 0.77, 0.23, 0.27, 0.68, 0.11 respectivamente para cada unos de los puntos, para un total de 0.48. Comparando con otros paises se puede observar una gran diferencia ya que paises como Estados Unidos tuvo 2.48, Brasil 1.24, España 1.20, Chile 0.80, Uruguay 0.71, Argentina 0.69, Mexico 0.69, Venezuela 0.51 y Peru 0.42. Otro dato resultante de tal estudio mostró que el 98% de los colombianos navega diarimente en internet pero de tal poblacion se observó que tan solo el 4% efectua compraventas ó se sumerge en el comercio electronico con un gasto promedio de US$45.

Viendo la gran y creciente participacion de la poblacion latinoamericana en la navegacion en internet y el intensivo uso de las redes sociales por tal poblacion, especificamente en Facebook, ha surgido una nueva modalidad de comercio en linea que la denominan *social commerce*, con esta modalidad se prentende aprovechar el gran impacto y uso de las redes sociales con el proposito de incentivar y abrir nuevos canales para efectuar transacciones electronicas enfocadas al comercio electronico, con ello, tambien se logra llegar a sectores socieconomicos medio-bajos de la poblacion, quienes tambien son un amplio mercado en el cual se tiene poca incursion. Se sabe que hoy en dia las redes sociales centran su atencion en Facebook, la cual ocupa el 30% del tiempo en linea ocupado por lo internautas en 2011[19]. Sin embargo, aun no se tiene certeza de saber si tal plataforma es un canal apto para desarrollar el comercio electronico ya que aun no se cuentan con herramientas para medir ó replicar plenamente la experiencia de las empresas y marcas ofertantes en sus sitios oficiales, apesar de ello, ya existen muchas compañias que ha inscursionado en la plataforma y otras que se preparan para ello aprovechando la ubicuidad y masificacion de las redes sociales, prueba de ello son las aerolineas especificamente LAN.Cabe resaltar que en el mundo existen cerca de 850 millones de usuarios de *Facebook*, lo cual la ubica como la red social con mayor cantidad de usuarios, en Colombia se registraron cerca de 16,5 millones de usuarios de la red social, lo que permite ubicar a Colombia en el lugar 14 de los paises en el mundo con mas usuarios de *Facebook*[19]. Ver figura 17.

[19]Fuente: www.socialbakers.com

Figura 17. Usuarios de Facebook a nivel mundial en 2012.



Elaboracion propia. Fuente: www.socialbakers.com

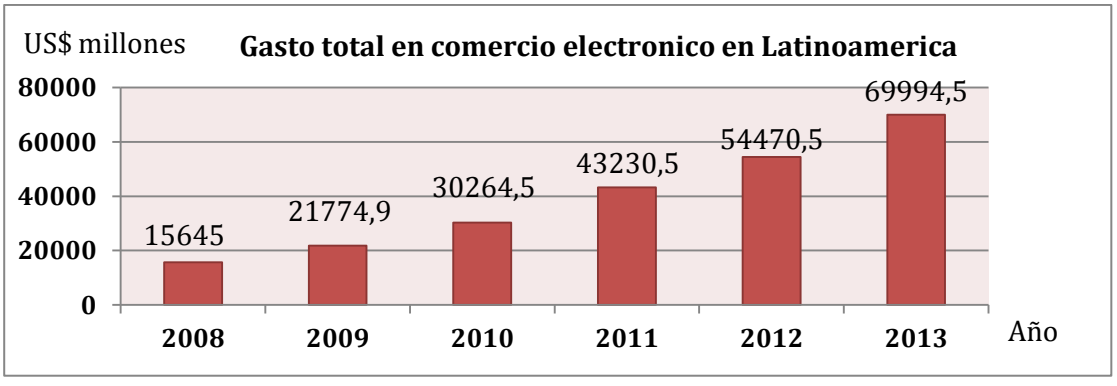
Si se analizan estas cifras podriamos indicar que Colombia se ubica en una posicion privilegiada con respecto a la penetracion de dicha red social por encima de muchos paises a nivel mundial y de la region, lo cual indica que Colombia poseería mas oportunidades para masificar el comercio electronico mediante el uso de las redes sociales.

En el 2011 con respecto al 2009, se contó con un aumento del 7% mas de consumidores on line en la region quienes reclaman mayor oferta del comercio electronico, lo que podria indicar que existe una mayor demanda debido a la tendencia de la disminución de uno de los obstaculos mas grandes del comercio electronico, el cual es la *inseguridad* en las transacciones electronicas.[20] En Mexico, en 2011 cerca del 63% de los mexicanos expresó tener mayor confianza al efectuar transacciones electronicas on line, lo que difiera y muestra un avance en la confianza de los consumidores con respecto al 2009 cuando los numeros indicaron que solo el 55% mostraba su confianza a las transacciones on line[21].

[20]De acuerdo a la encuesta de la Camara Argentina de Comercio Electronico en 2011.
[21]Basado en información suminstrada por CyberSource Latinoamerica, compañía adquirida por VISA para la gestión de seguridad y antifraude en transacciones electrónicas de más de 370 mil empresas.

Segun informacion del e-Instituto, el 70% de brasileros, argentinos y chilenos de su presupuesto anual gastan menos del 10% en consumos online, esto podría llegar a aumentar con el auge de los smarthphones y el surgimiento de las *billeteras digitales*, las cuales, se convertirían en una solución para el consumo de los usuarios del comercio electronico ofreciendo una manera mas segura y practica de efectuar transacciones electronicas comerciales por medio de smarthphones, tablet y PCs, con la implementación de ellas no se requerirá que lo usuarios constantemente introduzcan su información durante las transacciones. Como vemos, con el surgimiento y la adopcion de nuevas aplicaciones, tecnologia movil, las redes sociales, entre otros, está cambiando la manera de comunicarnos y las conductas de los consumidores en linea. En la figura 18 se puede observar el crecimiento anual (especificamente a partir del año 2008) en el gasto de los consumidores on line cada año, lo que refleja un aumento considerable en la confianza, habitos de consumo y el progreso del comercio electronico en la region, podemos observar el gasto en US$ millones en comercio electronico en la region Latinoamerica.

Figura 18. Gasto total en comercio electronico en Latinoamerica.



Elaboracion propia. Basado en America Economia Intelligence.

11.1 B2C EN COLOMBIA Y LATINOAMERICA

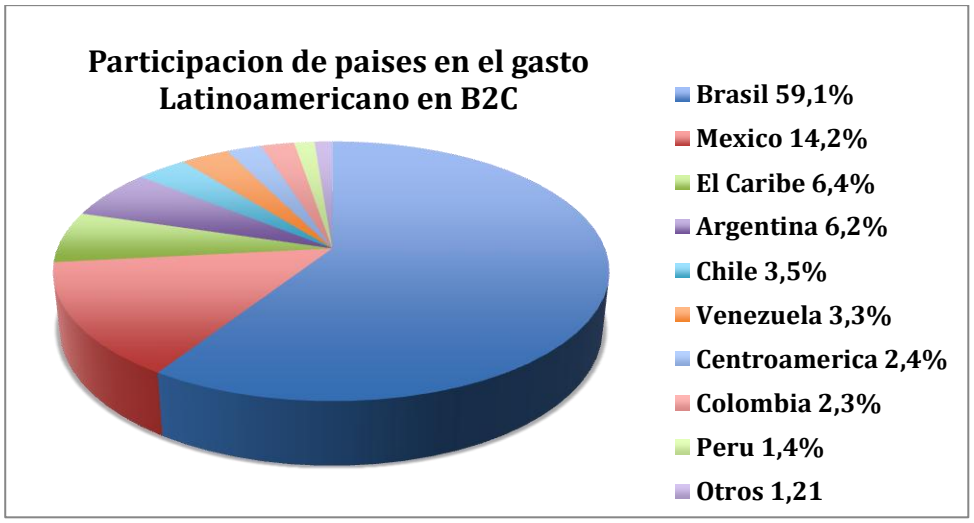
Para el año 2009 se tuvo que los ingresos totales del comercio electronico tipo B2C estuvieron alrededor de los US$ 22 mil millones, en 2011 se tuvo un incremento cercano a los US$ 43 mil millones lo que refleja un aumento del comercio electronico de casi el doble en solo dos años, un crecimiento del 98,5%. Esto podria indicar que las transacciones electronicas y el comercio electronico se duplican cada dos años, mostrando un acelerado crecimiento en el sector, eso se ve reflejado en paises como Brasil, ya que se registró como el primer pais en latinoamerica en donde el comercio electronico tipo B2C alcanzo el 1% como proporcion del PIB. Ademas de los esfuerzos del gobierno brasilero por fortalecer su economia bajo el marco del sector del comercio electronico proponiendo el mejoramiento de la bancarizacion, la infraestructura y cobertura de las nuevas tecnologias de las telecomunicaciones, ha incentivado el comercio electronico reduciendo tasas de interes e impuestos, efectuó cambios legislativos de cara al consumo de su poblacion, un ejemplo de ello es que en Brasil, la ley permite el reembolso sin costo adicional para los consumidores de los productos comprados de manera online, ello provocó una mayor confianza y seguridad en los consumidores, ademas, el mejoramiento en los procesos de logistica de las compañias con sus portales web. En latinoamerica, de cada 100 sitios web visitados por los consmuidores el 70% se encuentran en Brasil, el 87% de 78 millones de consumidores on line en Brasil visita los sitios web de retail.[22]

En la figuras 19 y tabla 2 podemos observar como se encuentra la participación por cada país de la región en su gasto enfocado al comercio electronico tipo B2C y la cantidad en millones de US$ que corresponde al gasto durante el año 2011, Colombia tiene una participación bastante resagada en comparación con la participación de otros países que nos superan como Venezuela, Mexico y

[22]Según datos de comScore, una de las principales compañías de estadísticas que efectúan la medición de la participación en internet de los consumidores en el comercio electrónico.

Argentina. En cuanto a Brasil, es el país que lleva la delantera con un 59.1% de participación. Podemos obsevar que Colombia muestra un crecimiento cercano al doble del gasto y participación en solo dos años en la región.

Figura 19. Participacion de paises en el gasto Latinoamericano en B2C.



Elaboracion propia. Basado en America Economia Intellingence.

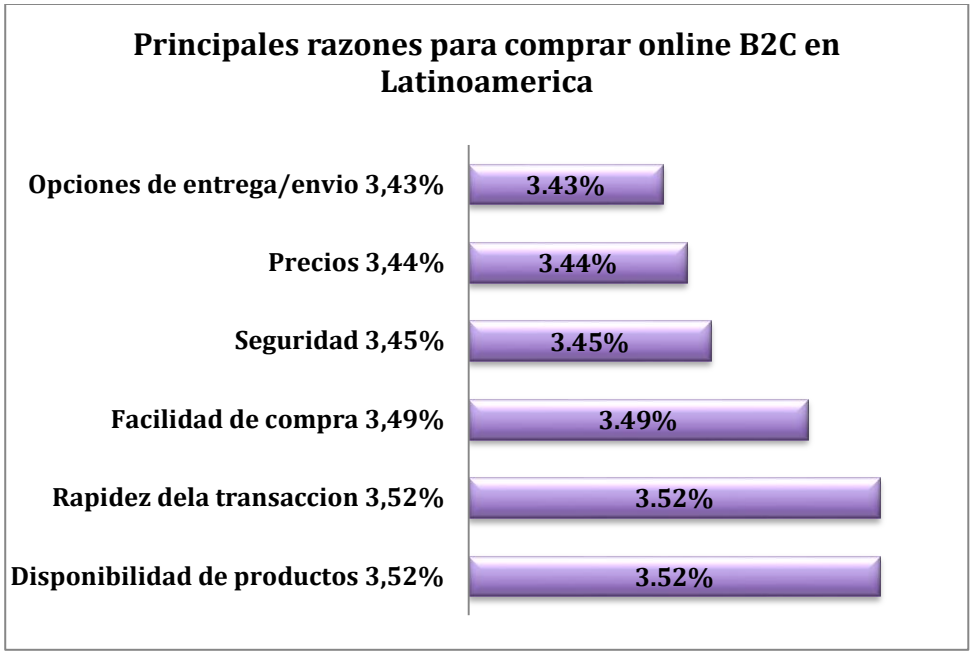
Tabla 2. Gasto en US$ millones de países Latinoamericanos en B2C.

Año → / Pais ↓	2008	2009	2010	2011
Brasil	3572,6	5230,4	7851,4	9500
Mexico	1010	1624,9	2330,5	4137,1
El Caribe	1244,7	1455,9	1895,5	2752
Argentina	732,8	875	1797,6	2695,3
Chile	919,5	1027,9	1141,6	1489,9
Venezuela	787,8	906,1	1117,8	1418,4
Centroamerica	563,9	637,2	729,6	1051
Colombia	301,9	435	606,8	998
Peru	250,9	276	426,9	611
Otros	260,9	306,5	366,9	525

Elaboracion propia. Basado en America Economia Intellingence

Podemos decir que en Colombia y Latinoamerica, los motivos por los cuales un internauta se ve mas atraído a realizar sus compras B2C a través de la web es por la mayor disponibilidad de productos, rapidez y facilidad en las transacciones comerciales y es de sorprender que la percepción de seguridad en las transacciones en la región ha aumentado ya que se observa que se ha ubicado este ítem por encima de puntos muy relevantes como los precios, descuentos y opciones de pago.Ver Figura 20.

Figura 20. Principales razones para comprar online B2C en Latinoamerica.



Elaboracion propia. Basada en America Economia Intellingence.

Los internautas colombianos poco a poco estan adoptando la tendencia de emplear la internet como un "*carrito del mercado*", ya que segun los estudios analizados, Colombia muestra cifras de crecimiento indicando que las compras tipo B2C en linea ya no son una excepcion ni un mito. Para el periodo de 2012, se estimó que el 35% de los compradoresgasto entre US$500 y US$1000 en compras en linea, lo que aun muestra un letargo con respecto a otros paises de la

region como Argentina, Chile, Venezuela, Peru, Mexico y Brasil en donde se promedió que el 61% de sus consumidores B2C on line gastaron mas de US$1000.[23]

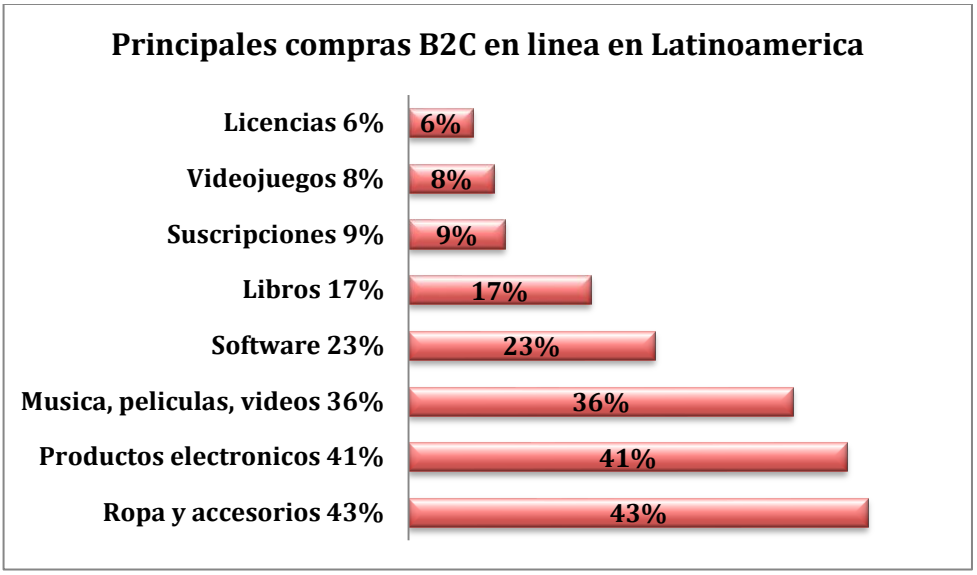
De acuerdo a los consumos y flujo de internautas en el sector de comercio electronico tipo B2C, el sitio web en ventas lider en la region es MercadoLibre.com. Alli, el 55% de los consumidores efectuaron transacciones electronicas en linea y el 81% solamente lo visito, a él le siguen Amazon.com con un 22% de consumidores y visitantes un 53%[22]. Enfocandonos a nivel nacional Colombia, el comercio electronico tipo B2C tuvo un mayor influencia en los sitos web de compañias como EXITO y Avianca, mostrando cifras que indican un 69% de internautas son visitantes mientras que el 31% ha efectuado transacciones electronicas comerciales, promoviendo a éstos como los portales web preferidos por los colombianos para efectuar compras en internet, a ellos le siguen las nuevas cadenas comerciales que incursionan en el pais como Falabella con 48% de visitantes y 15% de compradores, mientras que en la compra de tiquetes aereos y viajes, la compañia Avianca reportó que ha sido visitado por el 91% de los usuarios y el 49% ha realizado algun tipo de transacccion comercial electronica con ellos, a ella le siguen LAN con 53% de visitantes y 32% compradores.

El consumo del comercio electronico tipo B2C en Colombia y Latinoamerica muestra que ocho de cada diez compradores en linea en latinoamerica buscan, investigan y compran productos en linea cada semana en ese orden de prioridades. De esa proporcion de consumidores se ha logrado detectar que los productos mas demandados en linea son la ropa y accesorios, productos electronicos y ocio. Tambien se estableció la preferencia de los consumidores en usar las tarjetas de credito con un 74%, transferencias electronicas con un 41% y

[23]Informacion proporcionada por el Observatorio y Centro de Estudios de la Economia Digital del Instituto Latinoamericano de Comercio Electronico, que tiene como objetivo promover la informacion economica y metricas del comercio electronico y sus efectos en Latinoamerica.

las tarjetas debito con 41% para efectuar los pagos de manera electronica[24], lo que muestra que el temor de los consumidores colombianos con respecto a la seguridad de los datos y la informacion se encuentra en declibe, ya que los medios de pago mas usados son las tarjetas de credito, como resultado de los esfuerzos de las grandes compañias en generar la confianza en sus consumidores desarrollando e implementando estrategias para salvarguardar la seguridad de sus consumidores y fortalecer la bancarizaacion. Ver figura 21.

Figura 21. Principales compras B2C en linea en Latinoamerica.



Elaboracion propia. Basado en datos del Observatorio y Centro de Estudios de la Economia Digital del Instituto Latinoamericano de Comercio Electronico.

Siguiendo el crecimiento del comercio electronico en la region podemos obtener cifras que nos indican el gran y rapido auge que viene adoptando el comercio electronico en latinoamerica, por ejemplo; en Argentina, durante el 2012 el pais facturo cerca de US$3.3 mil millones con el comercio electronico y en 2011 obtuvo

[24]Informacion proporcionada por el Observatorio y Centro de Estudios de la Economia Digital del Instituto Latinoamericano de Comercio Electronico, que tiene como objetivo promover la informacion economica y metricas del comercio electronico y sus efectos en Latinoamerica.

un gasto en el sector de alrededor de US$ 2.6 mil millones, lo que muestra un incremento del comercio electronico cercano al 32% en el pais gaucho. En una encuesta adelantada a 540 argentinos seguidores del comercio electronico, el 57% dijo usar sus tarjetas de credito para efectuar los pagos de manera electronica. Argentina esta reportado como el pais con mayor nivel de penetracion en cuanto a los compradores efectivos en la red, lo que indica que el 43.9% de los internautas argentinos realizaron alguna transaccion electronica en 2012, comparado con los internautas brasileros con un porcentaje de 34%, mexicanos con un 19.6% y el 31,7% de todos los internautas en latinoamerica[25]. Por otra parte, durante el año 2011 Brasil reportó ventas totales por medio del comercio electronico cifras cercanas a los US$9200 millones y en 2012 reportó una cantidad cercana a los US$11000 millones en comercio electronico, lo que evidencia un crecimiento del 20% en el sector, esto con el empuje dado por el "*Viernes negro*" que llego a Brasil el 23 de Noviembre del 2012, en donde los brasileros reportaron gastos de mas de US$110 millones en compras en linea y durante la epoca navideña el comercio electronico aumento un 18% totalizando cifras cercanas a los US$1,5 mil millones en ventas por medio del comercio electronico. Los articulos mas solicitados en las compras en linea en Brasil son los celulares, accesorios para autos, computadoras, productos electronicos y ropa[26].

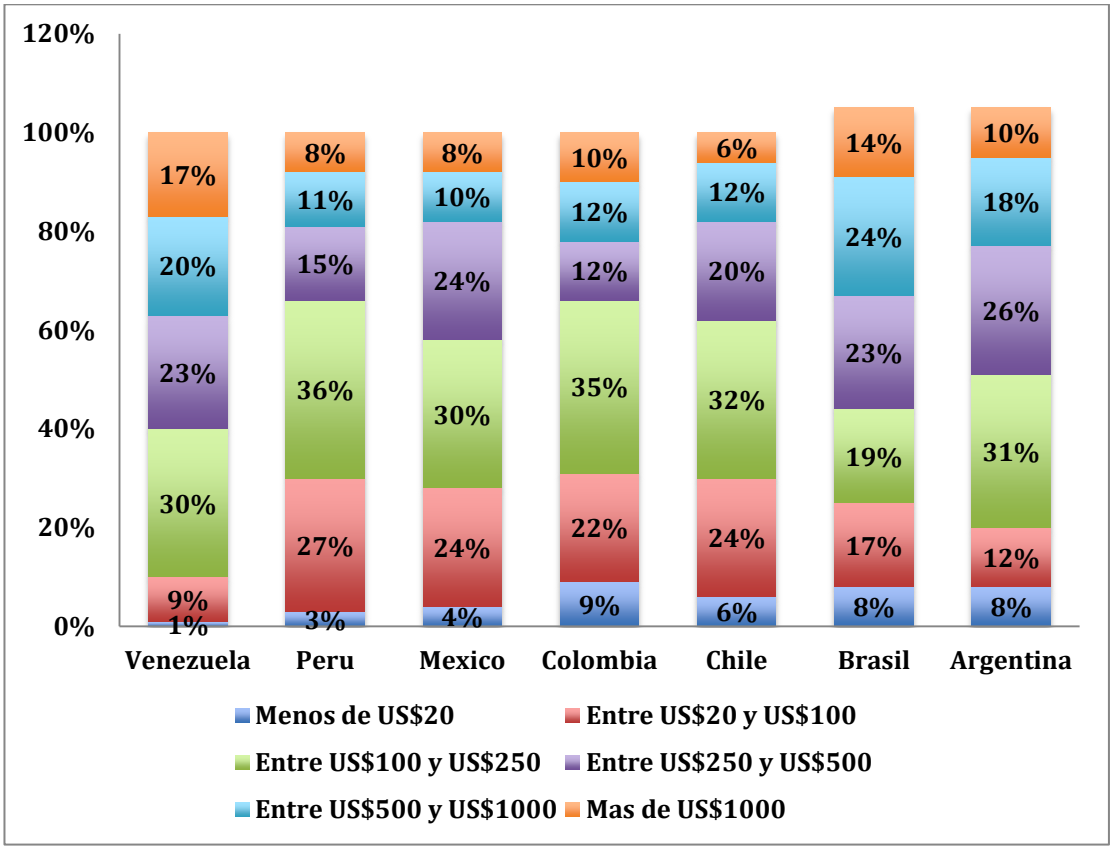
Mientras tanto, al norte de latinoamerica, Mexico reporto para el año 2011 ventas cercanas a los US$4200 millones por medio del comercio electronico y para el año 2012 reporto ventas alrededor de los US$6200 millones en el sector, cifras que indican un crecimeinto del 46% del comercio electronico en 2012 en Mexico. Los productos mas solicitados en las compras en linea por los mexicanos son los pasajes de avion ú omnibus con el 64%, hoteles con el 37%, musica y peliculas con el 37%, entradas a espectaculos con el 34%, libros con el 27%, ropa con el 23%, software con el 23% y celulares con el 18%. En promedio para el 2012, un

[25]Fuente: Camara Argentina de Comercio Electronico y e-Marketer.
[26]Fuente: e-bit, Mercadolibre.com y la Camara Brasilera de Comercio Electronico.

mexicano gasto en comercio electronico US$854, se estima que para finales de 2013 los internautas del comercio electronico en Mexico lideraran junto a Brasil la cantidad gastada por persona en el comercio electronico. El comercio electronico tipo B2C se espera que para finales de 2013 en Mexico se reporten ventas en linea cerca a los US$8 mil millones y para el 2016 se estiman cifras de US$12,9 mil millones en ventas, ademas se cree que para el 2016, Mexico contará con el 12.1% de los internautas usuarios del comercio electronico de latinoamerica, sin embargo, para ese mismo año se espera que Brasil siga en punta contando con cerca del 34,7% de los internautas usuarios del comercio electronico de latinoamerica.[27] En la figura 22 podemos observar para el 2012 las cifras que nos indican el porcentaje de los diferentes montos de gastos en promedio en US$ dolares en algunos de los paises latinoamericanos usando el comercio electronico tipo B2C, segun ella, en promedio un latinoamericano gasto en comercio electronico tipo B2C cerca de US$500 en los ultimos 3 meses del año y los paises quienes mas gastaron en comercio electronico tipo B2C fueron Brasil y Venezuela.

[27]Fuente: e-Marketer y la Asociacion Mexicana de Internet (AMIPCI).

Figura 22. Gastos en compras en linea en Latinoamerica.



Elaboracion propia. Basada en datos de e-commerce en Latinoamerica 2012, comScore Inc.

Mirando a otro de los grandes en el comercio electronico al sur de la region, Chile reporto para el año 2011 ventas mediante el comercio electronico cercanas a los US$1489 mil millones y para el 2012 reporto para el mismo sector ventas cercanas a los US$ 1,7 mil millones, cifras que muestran un incremento del comercio electronico en ese pais del 14%. Chile muestra que uno de los rubros en donde mas se efectuan las transascciones electronicas es el pago de impuestos con un 38%, le siguen los viajes con 29% y el 17% corresponde al retail. En este pais, el 65% de los internautas hacen uso efectivo del comercio electronico, lo cual es una cifra bastante alta en compraracion con otros paises de la region.[28] El

[28]Fuente: VISA y Camara de comercio de Santiago.

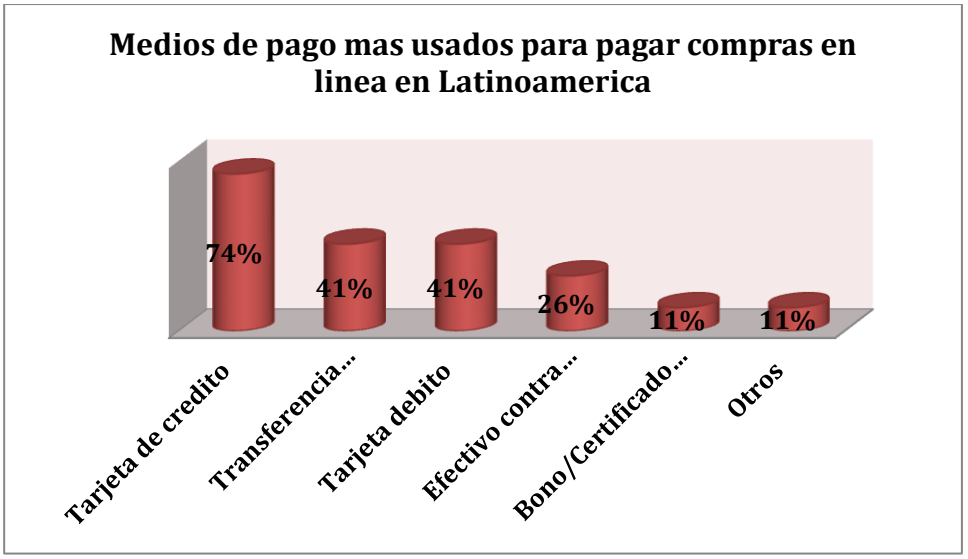
crecimiento en el comercio electronico tipo B2C en latinoamerica ha sido favorecido gracias a al incremento de computadores personales, moviles y de escritorio, al crecimiento del uso de la banda ancha, el aumento de los consumidores en internet, la creciente percepcion de seguridad en las transacciones electronicas, el aumento de compañias que incursionan en la internet con sus portales web. Con el surgimeinto de nuevos medios de pago electronicos como *PayPal*, surgen a su vez beneficios para los usuarios entre los cuales esta la facilidad de adquirir una cuenta, ofrece la posibilidad de efectuar pagos electronicos con tarjetas de credito y los datos de los usuarios como numeros de cuenta no son puestos a disposicion de los vendedores, esto ha sido visto por los comerciantes con una solucion poco costosa y sencilla de implementar. Por otra parte, organismos que ofrecen y manejan las tarjetas de pago electronico (tarjetas de credito, debito, prepago, etc) como VISA ó MasterCard han desarrollado sistemas para evitar los fraudes electronicos de tipo CNP (*Card No Present*), es decir, aquellos pagos electronicos que se realizan sin la presencia fisica de ellas de manera fraudulenta. Los propositos primordiales de estos nuevos sistemas es proporcionar un mayor grado de seguridad en las transacciones electronicas.

Un ejemplo de estos nuevo avances es el sistema 3-D Secura, en él, la entidad asocia la tarjeta de pago electronico a un sistema de autenticacion, el cual puede ser una contraseña seleccionada por el usuario ó dispositivo electronico cuyo codigo cambia cada cierto tiempo, tambien conocido como *Dongle*. Con ellos, al momento de efectuar alguna transacción electronica ó compra en linea en el sitio web de su preferencia y que se encuentre adscrito a tal sistema de seguridad, se le solicitara al usuario el numero de su trajeta de pago, las fecha de vencimiento de ella y el CVV (*Card Verification Value* ó *Criptograma Visual*), una vez completadas las verificaciones de tales datos, el consumidor sera enviado al sitio web de su entidad bancaria en donde deberá introducir los datos elegidos como su información de autenticación, de esta manera se puede salvaguardar la identidad

del usuario propietario de la tarjeta de pago electronico. Protegiendo contra el uso no autorizado y fraudulento de las tarjetas de pagos electronicos en las compras en linea y proporcionar mayor seguridad se estimula el comercio electronico.

En cuanto a los medios de pago empleados por los internautas usuarios del comercio electronico tipo B2C, en Latinoamerica la tarjeta de credito es el medio mas usado por la poblacion para efectuar los pagos de compras en linea a traves de los sitios web, a ella le siguen las transferencias electronicas y tarjetas debito, lo que da muestra que la bancarizacion y tenencia de un medio de pago como la tarjeta de credito es uno de los elementos que ayuda al crecimiento y fortalecimeinto del comercio electronico en la region. Ver figura 23.

Figura 23. Medios de pago más usado para pagar compras en linea en Latinoamerica.



Elaboracion propia. Fuente: Reporte de e-commerce en Latinoamerica 2012. ComScore Inc.

Este notorio uso de las tarjetas de credito, se debe principalmente a los esfuerzos adelantados por las entidades bancarias y financieras por tener mayor penetracion bancaria en la poblacion e intensificar el uso masivo de las TICs en los medios de

pago de las compañias y vendedores de retail. Adicionalmente, se busca la modernizacion de los medios de pago lo que implicitamente conlleva el mejoramiento en la seguridad en las transacciones electronicas al momento de efectuar las compras en linea. Actualmente, los medios de pago se enfrentan a nuevos retos y cambios relevantes que son producto del cambio en las preferencias de los consumidores en linea, la competencia, las innovaciones en la tecnologia, las nuevas regulaciones y la seguridad de la información. En la figura 23 vemos unas cifras que indican la preferencia de los usuarios por las tarjetas de credito como medio de pago electronico, sin embargo, se estan implementando y desarrollando actualmente nuevos productos de prepago los cuales tambien tienen un alto potencial para ser usados, un ejemplo de ello es que en Brasil ellos se usan para pagar salarios publicos ó subsidios a su poblacion, estos nuevos sistemas ofrecerían a los consumidores mayor seguridad, otros sevicios e incluso aplicaciones de fidelidad.

En cuanto a las nuevas regulaciones, éstas empujan el crecimiento y fortalecimiento del comercio electronico ya que por medio de ellas se busca la proteccion del consumidor en el marco de la seguridad de la informacion al momento de realizar las transacciones electronicas comerciales durante las compras en linea, por tal razon, desde el 1 de Enero de 2011 en latinoamerica toda entidad que este involucrada en el procesamiento y transmision de tarjetas (credito, debito prepago, etc) tiene por obligacion que cumplir con el estadr PCI DSS (*Payment Card Industry Data Security Standard*) ó Estandar para la Seguridad de los Datos en la Industria de Tarjetas de Pago, el cual, estipula que tales entidades deben contar obligatoriamente con los requerimientos minimos y necesarios para encriptar las comunicaciones, bases de datos y otros sistemas que empleen cualquier tipo de tarjeta de pago para las transacciones electronicas[29].

[29]De acuerdo al Informe Tecnocom sobre las Tendencias en Medios de Pago 2011.

Por otra parte, los avances en la TICs permiten al sector bancario desarrollar nuevos canales para hacer mas facil las transacciones electronicas y mayor seguridad en ellas para los consumidores, un ejemplo de ello es el surgimeinto desde hace algunos años de la banca por internet y la banca movil, las cuales permiten realizar transacciones electronicas de manera segura, rapida y comoda. En latinoamerica, el uso de la banca por internet como canal para efectuar transacciones electronicas tiene una tendecia al crecimiento, ya que el numero de transacciones electronicas y las cantidades que ellas representan aumentan cada vez mas, esto es un indicador del crecimiento de la confianza de los consumidores en cuanto a la seguridad de la informacion. Ver tabla 3.

Tabla 3. Banca por internet en Latinoamerica en 2010.

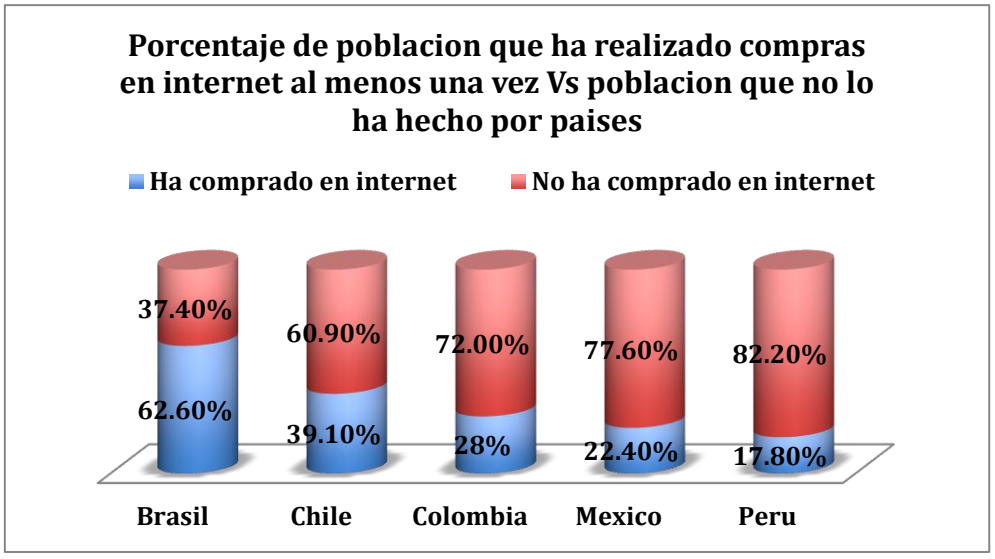
Pais	Cantidad de operaciones (milllones)	Valor (miles de millones US$)
Brasil	10571	6271
Chile	2145	N.D
Colombia	133	695
Mexico	521	2688
Peru	6	5,74

Elaboracion propia. Fuente: Informe Tecnocom sobre las Tendencias en Medios de Pago 2011.

Colombia y Chile se encuentran en una buena situación con respecto a la diversidad de medios de pago y el uso moderado de ellos, sin embargo, existe un gran segmento entre sus poblaciones que no cuenta con acceso a los medios de pago electrónicos. En Chile Colombia y Mexico existe la tendencia en la posesión de tarjetas de pagos electrónicos mas marcada en los estratos altos y medios de la población. En Colombia, la tarjeta de debito es el medio de pago electrónico más usado (40,3%).

Las compras por internet de cualquier producto y/ó servicio por la poblacion internauta consumidora en el comercio electronico es una realidad en la region, sin embrago aun existen grandes diferencias entre los paises. En Brasil las compras tiene gran protagonismo, alli el 62% de los internautas han afirmado haber concretado una compra en linea por internet al menos una vez, lo que muestra un alto nivel en el uso de los medios de pago electronicos, Colombia posee un 30% entre sus internautas[29]. Ver figura 24. Estas cifras indican que la bancarizacion de la poblacion tiene una relacion directamente proporcional a las compras por internet, es decir, a más poblacion bancarizada, mayor sera el flujo del comercio electronico. Es importante mencionar que el uso de los medios de pago electronicos no es la unica variable que define el estado del comercio electronico en la region, existen otras variables que los paises de la region emplean propiamente y muestran la diversidad de niveles de comercio electronico en cada uno de ellos. Esto quiere decir que la situacion particular de cada pais en cuanto al flujo y crecimiento del comercio electronico es distinto, dependiendo de las diferentes evoluciones que ellos presenten con el tiempo.

Figura 24. Porcentaje de poblacion que ha realizado compras por internet al menos una vez vs poblacion que no lo ha hecho por paises.



11.2 CLAVES PARA EL DESARROLLO DEL COMERCIO ELECTRÓNICO EN COLOMBIA

Uno de los obstaculos para el desarrollo del comercio electronico en la region sumado a la baja a tasa de bancarizacion en los colombianos y latinoamerica es que la mayoria de las compañias quienes tienen portales web, no los tienen optimizados para los dispositivos moviles, los cuales se han convertido en uno de los medios mas usado por los internautas para la navegacion e implicitamente para efectuar transacciones electronicas en internet debido a su ubicuidad y prolijidad. Segun datos de *ComScore*, nueve de cada diez internautas en la region han usado su smarthphone para efectuar compras en linea. En Colombia, los internautas expresaron adicionalmente presentar dificultades tecnicas (principalmente con los agentes prestadores de servicios de internet) a la hora de hacer las compras por internet lo que les impedia concretar el proceso y desmejorar la confianza del consumidor.

Siguiendo la información suministrada por la Camara Colombiana de Comercio Electronico, en Colombia el país vendió en 2011 a través de portales web en internet cerca de US$1000 millones en bienes y servicios y para el 2012 esa cifra estuvo cerca de duplicarse, lo que muestra que el comercio electrónico es un mercado que innegablemente es creciente. Ello también es un llamado a los comerciantes y emprendedores de las TICs a tener en mente y considerar que si no cuentan con la presencia de sus negocios en la web, estarían perdiendo clientes y millones cada segundo.

El comercio electrónico y las transacciones comerciales en línea necesariamente están relacionados a la capacidad de la infraestructura tecnologica, acceso, cobertura y conectividad de las TICs. Sabemos que Colombia actualmente es un

país que posee un 42% de penetración del internet en su poblacion[30] lo que es relativamente bajo en comparación con otros países de la región si se espera obtener resultados satisfactorios en cuanto al creciente desarrollo del comercio electrónico. Adicionalmente a la conectividad de la población, es necesario seguir realizando y mejorando los esfuerzos para proponer y poner en marcha nuevas y mejores estrategias que busquen la bancarización de la población, proporcionar mayores niveles de seguridad en las transacciones electrónicas, diseñar y establecer nuevas soluciones y modelos de pago en línea para aquellas personas que no cuentan con las posibilidades de adquirir algún tipo de tarjeta bancaria. Se requieren de tales esfuerzos ya que el éxito del comercio electrónico se encuentra ligado a la demanda, la infraestructura tecnologica, la penetracion y variedad de sistemas de pago electrónicos y la velocidad en la adopción de las nuevas tecnologías por parte de los consumidores internautas. Por lo tanto, los puntos sobre los cuales se deben enfocar las entidades bancarias, el gobierno y las compañías con portales web para el fortalecimiento y crecimiento del comercio electrónico las podríamos enunciar asi:

- **Espacios para crecer**. Se requieren muchos mas compradores para que exista mayor numero de compras mediante la optimización de portales web y plataformas para efectuar las compras en línea y pagos de ellas, además, de la incrusion de las compañías con sus negocios sobre la internet.
- **E-commerce móvil**. Optimizacion y fortalecimiento de los dispositivos móviles y sus plataformas para disminuir las deficiencias técnicas reportadas por los usuarios al momento de efectura compras en línea.
- **E-commmerce social**. Viendo la gran actividad de la población colombian dentro de las redes sociales, es importante que se realice el mejoramiento y se incluyan las posiblidades de efectuar comercio electrónico y pagos de las

[30]Según estudio de America Economia Intellingence.

compras en línea mediante la plataforma de las redes sociales siendo éstas un medio con gran potencial para el desarrollo del comercio electrónico.

- **Bancarizacion**. Las entidades bancarias y financieras no deben claudicar sino por el contrario mutar ó generar estrategias que permitan a la poblacion colombiana tener una mayor participación en la bancarización, reduciendo impuestos, intereses, mejorar estrategias de ahorro, etc, que hagan más llamativo su sector a la población y al comercio electrónico.
- **Desarrollo de TICs**. El gobierno nacional viene diseñando e implementando planes como el *Plan Vive Digital* y *Gobierno en línea* que impulsan tanto el crecimiento de la infraestructura de las TICs como la cobertura que ellas ofecen en el territorio nacional. Con ellas, el gobierno nacional busca llegar a las regiones mas apartadas buscando que mas colombianos tengan un mayor nivel de participación en el desarrollo del país, que la nacion se encuentre a la vanguardia de las TICs e implícitamente el fortalecimeinto y desarrollo del comercio electrónico.

Teniendo en cuenta lo anterior, hoy en dia se podría afirmar que Colombia es un país pionero en realizar tales esfuerzos buscando el crecimiento del comercio electrónico y del país en general. Muestra de ello es que las compañías que incursionan en el medio del comercio electrónico tipo B2C en Colombia llegan a duplicar sus ganancias en menos de un año, ya que los esfuerzos en la implementación de estategias de conectividad y penetración de internet en el país se han transformado en un modelo para la región. Aunque Colombia se encuentra ampliamente superada por otros países de la región en el marco del comercio electrónico, conectividad y penetración de la internet, el gobierno nacional realiza esfuerzos tales como el Plan Vive Digital y Gobierno en Linea, los cuales, buscaron contar con cerca de 6 millones de conexiones a internet para el año 2012 y se estima que para el año 2014 se cuenten con 8,8 millones de conexiones a internet con la ayuda de inversión de compañías de comercio electrónico en el país, con ello, Colombia se posiciona como un país lider en la región[29]. Como se

ha visto, Colombia aun esta lejos de países de la región como Brasil en el contexto del comercio electrónico, sin embargo, con los esfuerzos del gobierno, las compañías y las entidades financieras la brecha con aquellos países aventajados en el comracio electrónico se disminuye, esto debido al auge en las ventas en línea de tiquetes aéreos, dispositivos electrónicos, tickets, cupones, entre otros productos, además de toda clase de servicios públicos y privados.

11.3 EL COMERCIO ELECTRÓNICO EN COLOMBIA Y SUS CIFRAS

En Colombia durante el año 2010, con el impulso tecnológico del sector bancario y financiero, el país tuvo operaciones cercanas a los $915 billones de pesos mediante el uso de los medios electrónicos tales como internet, datafonos, bancamovil, entre otros, los cuales con la ayuda de las ciencias en telecomunicaciones y a los tipos de comercio electrónico, tales cifras representarían el comercio electronico en Colombia y las transacciones electrónicas mas usadas fueron consultas de saldo, recarga de minutos de celulares, transferencias de fondos y pagos de servicios publicos y privados.[31]

Si comezamos viendo el uso que generalmente le dan los colombianos a la internet, podriamos observar que las actividades que involucran el comercio electronico y las transacciones electrónicas tiene poca participación, tales actividades incluyen las transacciones con el gobierno con un uso por parte de los internautas de 5,3%, compras de productos y/ó servicios con el 7,1%, banca electrónica con el 11,9%, entre otros. Si se observa la evolución de estas actividades en los últimos años en Colombia, se observa el avance significativo en las transacciones con el gobierno puesto que antes del 2011 habia una participación del 3,9% y para el 2011 se reportó el crecimiento al 5,3%, igual comprotamiento tuvo la compra de servicios y/ó productos pasando del 6,2% al

[31] Siguiendo información suminstrada por la Asociacion Bancaria de Colombia, Asobancaria y Redeban Multicolor.

7,1%, por el contrario, la banca electrónica mostro uns disminucion en su actividad pasando del 12,1% al 11,9%. Ver tabla 4.

Tabla 4. Principales actividades en internet de los colombianos.

ACTIVIDADES	2009	2010	2011
Entretenimiento	60,9%	67%	69,8%
Banca Electronica	12,1%	12,6%	11,9%
Compras y ordenes	5,2%	6,5%	7,1%
Comunicación	81,1%	81,7%	83,4%
Educacion	62,2%	62,7%	60,2%
Informativa	78,8%	80,3%	80,4%
Gobierno	3,9%	3,7%	5,3%

Elaboracion propia. Basado en datos del DANE y la CRC.

Para el año 2012 en Colombia se llegaron a tener ventas por medio de dispostivos y canales electrónicos cercanas a los US$2000 millones[32]. Lo que podría indicar que las compras y transacciones electrónicas por internet vienen tomando protagonismo en los Colombianos, ya sea por su ubicuidad, comodidad, seguridad, rapidez y la ventaja de encontrar todo en un mismo lugar, además de esto, el comercio electrónico tiene la gran ventaja de ser una plataforma abierta las 24 horas del dia y todos los días, sin embargo, aun se cuentan con desventajas como la falta de oferta, productos, medios de pago, entre otros.

De acuerdo a estudios de VISA:

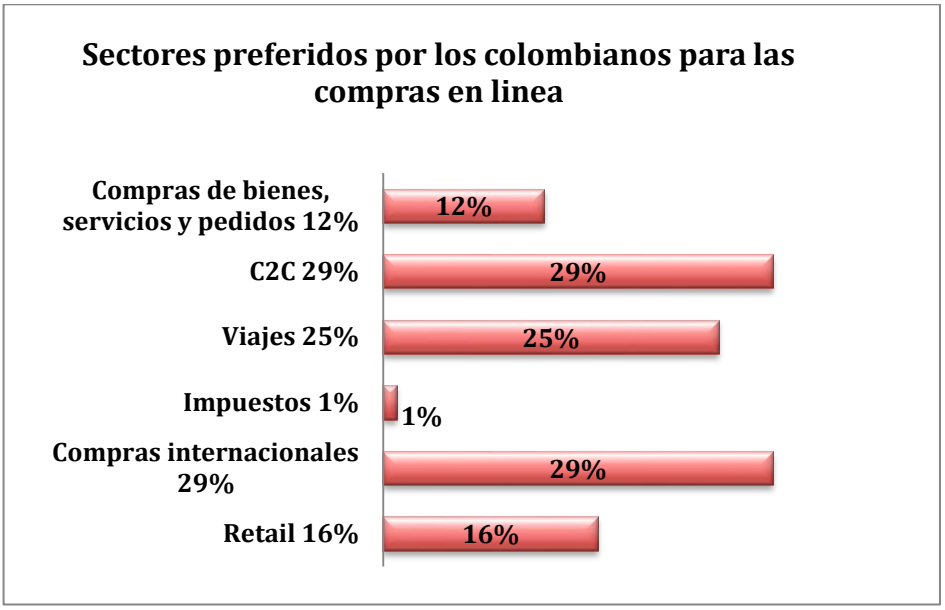
- 6 de cada 10 colombianos al momento de realizar una compra en línea consultan los productos y/ó servicio por la internet.

[32]De aceurdo a cifras de Cuponatic.com.co.

- Para el 2012, un colombiano trimestralmente gasto en promedio entre US$100 y US$200 en comercio electrónico.
- De las transacción comerciales electrónicas efectuadas durante el 2012, en Colombia el 25% de ellas se efectuo desde un dispositivo móvil.
- En 2012, US$300 millones se facturaron a través de cuponeras en línea en Colombia.
- Los productos que los colombianos compran mas en línea son viajes, tecnología, tratamientos de belleza y productos eróticos.
- Según los estudios, para el 2012 en Colombia se facturo gracias al comercio electrónico cerca de US$2000 millones.
- Los rubros más buscados para las compras en línea por los colombianos son retail, compras internacionales, impuestos, viajes y comercio C2C. Ver figura 25. El retail y las aerolíneas son los rubros con mayor potencial en el comercio electrónico en Colombia.

Sin embargo, Colombia tiene la particularidad y potencial frente a otros países en el área de pago de impuesto de la población por medio de los canales digitales e internet, la cual también es una forma de comercio y transacciones electrónicas.

Figura 25. Sectores preferidos por los colombianos para las compras en linea.



Elaboracion propia basados en estudios de VISA.

En Colombia, los tiquetes aéreos junto con los espectáculos, son los artículos que mas se compran por medio del comercio electrónico, portales como TuBoleta.com y Ticketexpress.com son los sitiso web mas usados por los colombianos para la compra de entradas a espectáculos, teatro, deportes, academia y conciertos[33].

Según los datos vistos, se ve que la oportunidades para efectuar compras en línea y realizar trasnsacciones electroncias en el internet vienen creciendo al punto que para muchos colombianos, la prcepcion de la inseguridad manifiesta en las transascciones comercial paso a un segundo plano. Se ha visto que en Colombia en promedio se tienen 120 mil mas consumidores de comercio electrónico cada año, lo que en cifras representan cerca de US$200 millones en compraventas[34]. Sin embrago, como se ha mencionado, el panorama no es el ideal, ya que Colombia aun cuenta con dificultades y escases de compañías que tengan

[33]Según datos de FENALCO.
[34]Según estudios en 2011 de la Revista Enter.

habilitados sus sitios web para efectuar transacciones comerciales electrónicas en la internet, sumado ello, aun contamos con poca penetración de la red de internet en muchos lugares del país, lo cual se convierte en un obstáculo para la masificación y mayor apertura del comercio electrónico, adicionalmente, existe el fenómeno recurrente en Colombia, el cual es la ausencia de sistemas y plataformas para efectuar los pagos de manera electrónica, por lo que aun podemos encontrar muchas tiendas nacionales quienes al habilitar sus servicios de compraventa en línea recurren a los procesoso de consignación bancaria, fax, entre otros, para efectuar los pagos de las compras efectuadas por sus clientes.

Como se manifestó anteriormente, los números han mostrado que anualmente se tiene un crecimiento aproximado de 120 mil consumidores de comercio electrónico en Colombia, cifra que representa aproximadamente el 0.29% de la población nacional, por otra parte en Estados Unidos las cifras muestran que hay aproximadamente 133 millones de personas quiene hacen uso recurrente del comercio elctronico, cifra que representa el 78% de su población[35]. En Colombia existe la particularidad que la población que lidera el consumo del comercio electrónico es la población mas joven, lo cual conlleva a dificultades para el crecimiento del comercio electrónico, ya que en Colombia las personas con un poder adquisitivo considerado están en edades que superan en promedio los 40 años, la cual corresponde a un sector de la población que no ha tenido la educación, destrezas y curiosidad por el uso de la internet como medio para efectuar las compras en línea.

Por otra parte, la seguridad de la información es muy importante, por lo tanto, es importante conocer y tener en cuenta ciertas cifras que no son publicadas. En Colombia diariamente en las calles se observan gran cantidades de robos, mientras que los robos y fraudes por internet en Colombia no supera el 1%, según

[35]Tales cifras son tomadas de estudios adelantados por eMarketer y Latin Trade.

informes de las entidades bancarias. Es importante resaltar que en Colombia la mayoría de los portales web de compañías que compran y venden en la internet poseen los firewalls y certificados digitales correspondientes con los cuales se garantiza a los consumidores un mayor nivel de seguridad en las transacciones eletronicas., incluso, hay entidades nacionales quienes expiden este tipo de certificados como la *Certicamara* de la CCCE.Aunque parece lo contrario, en Colombia cada dia es mas seguro realizar transacciones comerciales electrónicamente, sin embargo, aun existe el temor generalizado cuando los internautas se animan a realizar sus compras en internet por todo lo que se escucha y se sabe sobre los hackers, virus y fraudes en la internet, por ello, es importante que la comunidad internauta además adopte ciertas medidas de precaucion y conozca los métodos mas básicos de fraudes en la internet, con eso en mente, realizar transacciones electrónicas ó compras en internet se convertiría en algo sumamanete seguro y con muchas ventajas. Otro aspecto que ha impulsado el crecimiento del comercio electrónico en Colombia, es el inegable crecimiento y liderazgo de la nación en la región en cuanto a la cobertura y conexiones de banda ancha. En el país actualmente existen alrededor de 7 millones de usuarios con conexión a internet[36], sin embargo, aun nos aventaja países como Brasil, Chile y Argentina.

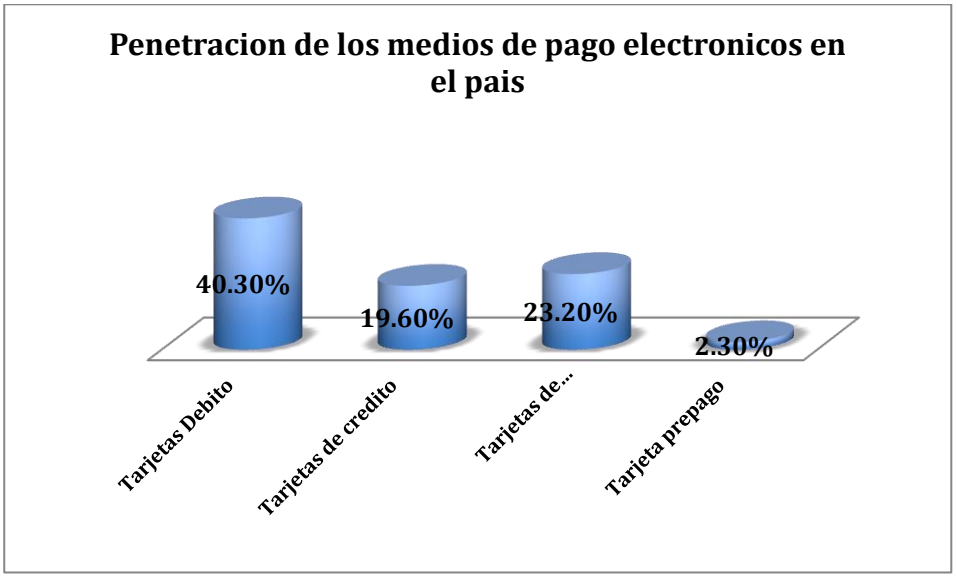
Actualemente, Colombia es uno de los países de latinoamerica que presenta el mayor y más rápido desarrollo y avance en el crecimiento del comercio electrónico. Se ha visto que en epocas navideñas las compraventas por internet llegan a crecer cerca de un 30% y 40% en Colombia[37]. Con ese alto potencial del país para el crecimiento y fortalecimiento del comercio electrónico, es importante que lso internautas y compañías del sector del comercio electrónico conozcan todos los factores que se relacionana a la calidad y seguridad de sus sitios web.

[36]Según cifras de la Comision de Regulacion de las Telecomunicaciones en Colombia (CRC).
[37]De acuerdo a la Camara Colombiana de Comercio Electronico, MinTIC y CRC en su reporte de Industria TIC, Agosto de 2012.

A pesar del letargo en comparación con otros países, Colombia actualmente se ubica en el puesto 5 entre los países de la región que presentan el mayor crecimiento en la cantidad de conexiones de banda ancha desde el año 2010, el país registra un aumento de 46% con respecto a países como Brasil, Argentina y Mexico quienes regsitrasn crecimientos del orden de 43%, 31% y 30% respectivamente, cifras que nos muestras que los esfuerzos del gobiernos como el plan *Vive Digital* para llevar cobertura y conectividad a la población que permitan el desarrollo y fortalecimiento del comercio electrónico han mostrado grandes avances[35]. Es bueno resaltar que en Colombia alrededor del 17% de las microempresas y pequeñas empresas se encuentran a la vanguardia en cuanto a la implementación de la internet como mecanismo para fortalecer sus negocios, ello también es muestra de los logros que viene surgiendo con el empuje del plan *Vive Digital* del gobierno nacional[35].

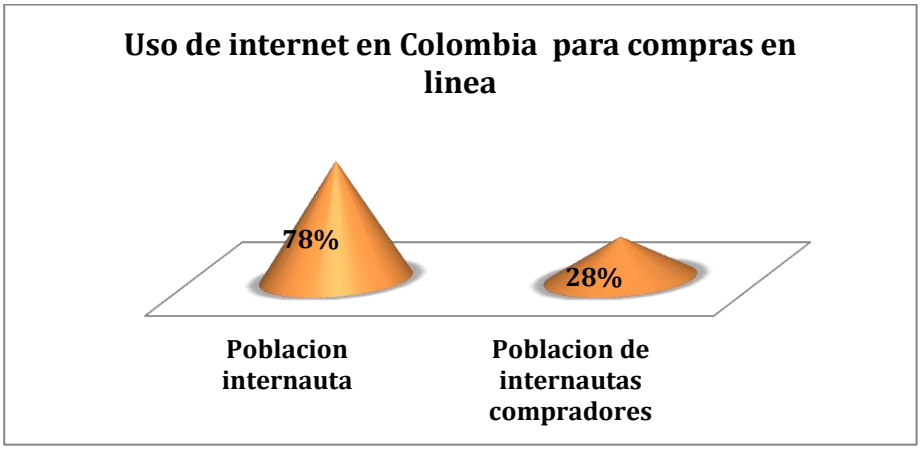
En cuanto a los medios de pago, encontramos una situación bastante desequilibrada en Colombia. Para el 2011 en el país se tenia el 57,6% de la población bancarizada, sin embrago, la penetración de los distinots medios de pagos electrconicos es desigual. La tarjeta debito es usada por el 40,3% de la población y es el medio de pago electroncio mas empleado en el país, mientras que las tarjetas de crédito son usadas solo por el 19,6% de la población que las posee. En Colombia la tarjeta debido generalemnte es usada para hacer compras en línea de artículos para el hogar, ropa y ocio, por otro lado, elmayor uso dado a las tarjetatas de crédito es para la compra de en línea de viajes, electrodomésticos y tecnología. Por otra parte, se viene incorporando en el país el uso de los portales web de las entidades bancarias para efectua actividades como consultas de saldos, sin embargo se espera que este comportameinto mejore. Las cifras nos han mostrados que el comeri electrónico en Colombia invlucra al 28% de los internautas. La tarjeta de crédito cubre un 40,4% de la poblacion y la debito cubre al 22,5%, lo que lso cnvierte en los mediso de pago electrónico mas empleados en el país. Ver Figura 26, 27.

Figura 26. Penetracion de los medios de pago electrónico en Colombia.



Elaboracion propia. Basado en datos del Informe Tecnocom sobre las Tendencias en Medios de Pago 2011.

Figura 27. Uso de internet en Colombia para compras en línea.



Elaboracion propia. Basado en datos del Informe Tecnocom sobre las Tendencias en Medios de Pago 2011.

CONCLUSIONES

Anteriormente el comercio electrónico en Colombia se presentaba como una utopia ó un tipo de comercio que representaba grandes riesgos de fraudes, robos y otro tipo de vulnerabilidades que llevarían siempre a la pérdida de dinero, productos, información, privacidad, entre otras cosas. Esto llevó a que en los colombianos surgiera y creciera el miedo a efectuar transacciones electronicas a través del internet. Sin embargo, en Colombia con el transcurso del tiempo, la evolucion de la tecnología mundialmente y el surgimeinto del interés por la seguridad de la información con la implementación de técnicas, sistemas y procedimientos enfoncados en la seguridad de la información, aquel temor viene trasnformandose en mito y ficción que van mucho mas alla de la realidad y los colombianos aumentan su dinámica en las compras por internet, prueba de ello son las crifras y números propocionados por entindades del gobierno y extranjeras.

Siguiendo las nuevas técnicas y procedimientos para el fortalecimiento del comercio electrónico a nivel nacional y regional enfocados en la seguridad de la informacion, lo esfuerzos que adelantan las entidades publicas y privadas en los países vienen y continuarán centrandose en el desarrollo y fortalecimeinto de la estructura tecnologica, cobertura en el acceso a la conectividad, bancarización y la generación de oferta con calidad. Si en Colombia se mantienen tales esfuerzos, podríamos llegar estar al mismo nivel que otros países de otras latitudes que no superan en el tema.

Con el surgimeinto y evolución de la internet y las redes de telecomunicaciones, junto con la creciente golbalizacion en todos los aspectos y la creciente dinámica en el uso de la internet, ello ha permitido el nacimineto de nuevos canales y formas de interaccion entre los internautas y sus intereses particulares, entre ellos fue el nacimiento del comercio electrónico, el cual se convirtió en una nueva

manera para efectuar transacciones electrónicas y obtener la participación y acercamiento incluso a sectores socioeconómicos quienes anteriormente no se encontraban la perspectiva de la sociedad.

El creceinte dinamismo en la actividad de los internautas en Latinoamerica, la globalización tecnologica y la dilusion de la sensación de inseguridad en las transacciones electrónicas a través de internet, son puntos detonantes para la bonanza y consolidación del comercio electrónico. Muestra de ello es el creciente porcentaje de participación de la población en la ejecucion de compras en línea dentro de los portales web de una gran varidedad de empresas dispoibles en la web.

La creceinte sensación de seguridad en las transascciones electrónicas a través de internet esta dada pricipalemente por los avances en el desarrollo de sistemas criptográficos y protoclos de seguridad para la web. La mayoría de las compañías que poseen portales web, los mantienen con códigos de seguridad, enlaces a entidades que brindan soporte y protección a los internautas y consumidores, números y datos de contactos directos con los que se pueden verificar las condiciones de seguridad y de la compra en línea, adicionalmente, cuentan con lo certificados de seguridad emitidos por entidades certificadoras autorizadas que proporciona mayor confianza y un mas alto nivel de seguridad en las transacción es electrónicas.

Entrelos principales atributos que ofrece realizar transacciones electrónicas y el comercio electrónico a través del internet, es poder economizar tiempo y dinero. Los internautas conusmidores pueden tener una mejor optimización de su tiempo ya que tiene la posibilidad de evitar trancones, de no someterse a horarios de atención de las tiendas, de no sportar largas filas y tumultos, tambien se cuenta con la opción de efectuar ese tipo de acciónes mientras los usuarios viajan, sumado a ello, tiene la ventaja que los usuario pueden hacer efectivo la entrega de

su compra de acuerdo a sus necediades y preferencias. Para economizar dinero, el comercio electrónico proporciona descuentos en productos, precios competitivos, ofertas atractivas a los consumidores y la posibilidad de hacer comparación de precios con infinidad de referencias. Por otra parte, el comercio elctronico ha ofrecido la posibilidad de ampliar los mercados permitiendo la interconexión entre usuarios de cualquier parte del mundo, es decir, aporta significativamente en la creceinte globalización de la sociedad.

En Colombia en los últimos años se ha visto un fuerte crecimiento en el comercio elcectronico con respecto a otros países de la región latinoamericana, esto es producto de la manera como la población viene adoptando la nueva tecnología TICs, las redes sociales y el crecimiento de las compras de bienes digitales, adicionalmente, lleva al cambio en el modo de comunicarnos y las conductas de consumo tanto en tiendas en línea com en las tiendas físicas.

Con esta monografía se observó que en Latinoamerica muchos comerciantes enfrentan muchas barreras para surgir y fortalecer sus negociso en la web, una de ellas es la poca confiaza de los internautas consumidores por la inseguridad que implicitamene acarrean las transacciones electrónicas, sin embargo, se evidenciaron conceptos y mecanismos como los protocolos SSL y TLS, los cuales se relacionana con el comercio electrónico al proporcionar mayores niveles de seguridad en la web.

El desarrollo de esa monografía permitio mostrar el uso de diversas tecnologías dispuestas para porporcionar seguridad en el comercio electrónico, para este caso los protocolos SSL/TLS, tabmien se mostraron algunas de las medidas de seguridad mas aplicadas. Se mostraron algunos conceptos que permiten a los usuarios internautas consumidores como identificar un sitio web seguro, adicionalmente se mostraron las variadas técnicas de certificación de sitios web, complementario a lo anterior, se mostraron las tecnias de cifrados y seguridad

mas comunes y mas robustas para conocer las maneras de evadir la insegruirdad y permitir a los comerciantes y consumidores tener mas confianza en el comercio electrónico.

En Latinoamerica aun existe las percepción de temor al momento de efectuar compras en línea ó alguna transasccion electrónica por todo lo que se ha divulgado sobre la interceptación de información confidencial de personas sobre la internet, las fallas de seguridad en algunas de las plataformas y paginas web disponibles en internet, virus y demás actuaciones fraudulentas, sin embargo, la realidad es otra ya que hoy en dia el comercio electrónico es cada vez mas seguro gracias a los adelantos en ciencias computacionales y matematicas, no obstante, es muy importante que los usuarios adopten medidas y procedimientos de precaucion personales ó corporativos para el uso de las redes de telecomunicaciones e internet.

La seguridad en las transacciones comerciales electrónicas se basa en un conjunto de políticas y tecnologías, además de consideraciones por parte de los usuarios que conlleven a hacer mucho más seguros los sistemas transaccionales.

Los protocolos más ampliamente difundidos para transacciones de comercio electrónico son SSL y TLS, avalados por entidades comerciales como VISA y MasterCard; estos protocolos se basan en compartir mensajes cifrados que se generan por medio de métodos criptográficos seleccionados por el diseñador del sitio web respectivo.

El nivel de seguridad presentado por los diferentes sitios web actuales, está ligado con el protocolo de seguridad utilizado así como su versión y método criptográfico implementado; según las estadísticas mostradas, los sitios web aún no actualizan a las versiones más recientes de los protocolos estudiados (TLS v1.2) dejando al descubierto problemas de vulnerabilidad frente a posibles ataques.

Con esta monografía ilustramos la importancia del conocimiento e implementación de los protocolos SSL/TLS en una gran cantidad de actividades que se realizan a través de las redes de telecomunicaciones, como es el comercio electrónico para que ellas se concreten de manera satisfactoria, garantizando la seguridad en ellas y generando confianza en los usuarios internautas.

En Latinoamerica entre los paiese y según las cifras vistas, los porcentajes de uso del comercio electrónico, penetración de las TICs, presencia de compañías con portales web, entre eotros factores son muy distintos, esto se debe en gran parte a la estructura de los mercados en cada no de ellos y como los canales digitales influyen sobre estos y su población, como la variedad de medios de pagos electrónicos,la percepción de seguridad en la internet, conectividad, etc, por lo tanto, aun no se podría definir un patrón único sobre el comportameinto sino que existen variedad de escenarios y actores que influyen sobre el crecimiento y fortalecimeinto del comercio electrónico.

Todas las medidas de proteccion que adopten los prestadores de servicios de telecomunicaciones, las compañías y usuarios de internet y el comercio electrónico en sus portales web deben proporcionar a los usuarios igualdad de acceso y seguridad, mientras que a los operadores de servicios, diseñadores web, administradores de redes, ingenieros, entre otros, incentivos para innovar e invertir en sistemas y procedimeintos de seguridad de la información, al diseñar una portal web o una red de telecomunicaciones ésta debe ser convergente y balanceada incluyendo los derechos individuales como la privacidad y la seguridad de la información deben estar gararantizados.

Los productos y medios de pago electronico que continuamente vienen surgiendo paralelamente al crecimiento del comercio electrónico, deber proporionar altos niveles de seguridad a los usuarios, deben ser fáciles de implementar, manejar un costo razonable y con tendencia a la masificación.

Cuando se van a seleccionar los medios de pago electrónico mas adecuados al negocio y para el usuario se deben tern en cuenta putnos tales como el esquema de seguridad requerido para prevenr los fraudes y robos, rapidez y facilidad del uso del medio de pago.

Los modelos de prevención de fraudes con la información de los internautas requieren altos protoclos de seguridad de comercio elctronico, como SSL y TLS, asi mismo, la integración de mecanismos de seguridad adicionales tales como *Verified by* VISA ó *Secure Code* de MasterCard. Adicionalmente, se deben generar y optimizar mecanimos de pre-validacion con los cuales a través de la inforamcion suminstrada durante las transacciones electrónicas se pude verificar el nivel de riesgo previo a las solicitudes de autorización y evitar los pagos de las compras en línea y las entregas de os productos y servicios.

Podemos decir que en la actualidad los medios de pagos electrónicos son seguros y los certificados de autenticidad emitidos por las autoridades certificadoras hacen que los portales web y otras entidades disminuyan los riesgos de intrusión y fraude de la información. Estos riesgos son generados por vulnerabilidades de sistemas y platafomras web de los comerciantes, mercado negro, robo de información en entidades financieras y bancos, entre otros. Por ello sin importar la procedencia de la informaiocn fraudulenta de los pagos, la responsabilidad en la seguridad de la información estará sobre el comerciante y la imagne de su negocia se vera afectada.

Citando algunas recomendaciones de seguridad para los usuarios al momento de efectuar las transacciones electrónicas ó compras en línea, ellos deben tener en cuenta puntos tales como aprender a reconocer los sitios web seguros de su preferencia mediante la verificación de los protocolos de seguridad implementados y los certificados de autenticidad, proporcionar datos de contacto efectivos con el propósito de efectuar verificaciones de datos y autorizaciones, conocer los

distintos modos de fraude electrónico y proteger la información de sus medios de pagos electrónicos.

Citando las principales recomendaciones de seguridad para los comerciantes y entidades quienes mantinen sus negocios en internet y manjena los sitemas de pagos electrónicos, ellos deberían tener en cuenta putnos tales como efectuar la contratación adecuada de los proveedores de servicios de internet quienes deben implementar y mantener estándares mundiales de seguridad en los pagos oomo la iplementacion de protoclos de seguridad como SSL y TLS, realizar esfuerzos para no generar vulnerabilidades en sus sistemas y plataformas mediante el almacenamietno de informaiocn sensible, los procesos de pagos electrónicos deben proporcionar confianza y mayor seguridad en los usuarios.

En Colombia todavía se pueden encontrar grandes limitaciónes en el contexto de la seguridad de la informcaionc en el comercion electrónico, ya que existen pocos proveedores ó entidades certificadoras en estándares internacionales de seguridad como SSL y TLS, lo que induce a que los comerciantes y entidades que participen en el comerci electronico invierntan, desarrollen e integren nuevas y mejores soluciones y mecanismos de seguridad en los medios de pagos electrónicos buscando la prevención de fraudes durante las compras en línea.

Las entidades financieras y los usuarios del comercio electrónico deben ir mas alla de las contraseñas básicas y las procedimeintos de bloqueos. Ellos deben enfocarse en la infromacion, donde y como están almacenados sus datos sensibles, como los pueden ver, transmitir y guardar. Esto debe ser integrado con los actuales procedimientos y mecanismos de prevención de perdidad de información, cifrado de los datos y autenticaciones como los protoclosos SSL, TLS y mecanismos de cifrado robustos, buscando proporcionar mayor seguridad y por ende mayor confianza en los consumidores.

Con esta monografia también se pretende dar a conocer algunas de la gran variedad de herramientas disponibles para efectuar compras en línea o alguna transacción electrónica de manera segura como los protocolos SSL, TLS y mecanismos de cifrado, tratando de mejorar e incrementar la confianza de los consumidores internautas con sus transacciones electrónicas. Se abordaron y revisaron las vulnerabilidades de los sitemas y redes de telecomunicaiones, asi como los mecanismos de cifrado de la información, se efectuo la mención sobre el funcionamiento, ventajas y dificultades de los protocolos para la seguridad de la infromacion (SSL y TLS) mas usados actualmente. Con esto se propuso mostrar que se peuden efectuar transascciones electrónicas y compras en línea de manera segura hoy en dia.

La implementación de los protocolos SSL y TLS en los portales web de los negocios en internet mediante el uso de los certificados digitales, las claves publicas y privadas y los correspondientes mecanismos de cifrado, proporcionana mayores niveles de seguridad y confianza en los consumidores internautas queines emplean las trasnmisiones y transacciones de datos electronicamente por medio de los servidores web.

Con la implemntacion de medidas de seguridad tales como los protocolso SSL/TLS se peude llegara a asegurar en gran medida al cliente la integridad y confiabilidad de su infromacion llevando a obtener una mayor confianza por parte del consuidor internauta, la cual es uno de los principales propósitos de las comapñias que incursionan en el comercio electrónico y quieren surgir y mantenerse en él. La idea de seguridad debe ser transmitidad a los usuarios consumidores, de lo contrario ellos se alejaran del medio, por eso, la seguridad es uno de los factores de los cuales depende el éxito ó fracaso del comercio electrónico.

Constanemente el comercio electroinico posee el reto de actualizarse con respecto a las amenazas y riesgos de la internet y las redes de telecomunicaciones, lucahr contra hackers y demás intrusos, quienes pretenden robar información de usuarios y comerciantes para actuar fraudulentamente, por ello, con la implementación de mecanismos de seguridad electrónica como los protocolos SSL/TLS proporcionana protección a los datos de comerciantes y usuarios del comercio electrónico, tal factor de seguridad puede llevar a que una comapñia sea exitosa ó no en el medio con su portal web.

Con esta monografía se evidencio que los protocolos SSL/TLS son la primera opción en sistemas y mecanismos de seguridad electrónica para el comercio electrónico, ya que existen otros mecanismos de seguridad que presenta mas restricciones en el marco de la implementación y uso de aplicaciones web, existen otros que no aportan ninguna novedad a la seguridad ó SSL/TLS lo realizan de mejor manera y finalmente encontramos aquellos que aportan mejores mecanismos y mayor seguridad pero se ven superados por los costos, mantenimeintos y facilidad en su implementación.

BIBLIOGRAFIA

- ¿Qué significa SSL? http://www.verisign.es/ssl/ssl-information-center/what-is-ssl/index.html
- A Simplified IDEA Algorithm. HOFFMAN, Nick. Department of Mathematics, Northern Kentucky University. Disponible en: http://www.nku.edu/~christensen/simplified%20IDEA%20algorithm.pdf
- BEAST y la seguridad de SSL/TLS: lo que significa para los usuarios y administradores Web. Publicado el 5 de octubre de 2011. Accedido el 10 de Junio de 2013. Disponible en: http://blog.trendmicro.es/beast-y-la-seguridad-de-tlsssl-lo-que-significa-para-usuarios-y-administradores-web/
- Camara Argentina de Comercio Electronico
- Camara Brasilera de Comercio Electronico
- Camara Colombiana de Comercio Electronico
- Camara de Santiago de Comercio Electronico
- DANE
- DES and IDEA Cipher Suites for Transport Layer Security (TLS). P. Eronen, Ed. Febrero de 2009. RFC 5469. Disponible en: http://tools.ietf.org/html/rfc5469
- Desarrollan herramienta de ataque contra SSL/TLS denominada CRIME. Publicado el 7 de Septiembre de 2012. Disponible en: http://www.computerworldmexico.mx/Articulos/25149.htm
- El protocolo SSL. Ariel Hernán Roel. Facultad de Ciencias Exactas – UNLP http://penta2.ufrgs.br/gereseg/unlp/tut1998/ssl.htm
- FENALCO
- Fundamentos de Seguridad en Redes: Aplicaciones y Estándares. William Stallings. Pearson Educación, 2003. http://books.google.com.co/books?id=cjsHVSwbHwoC&hl=es&source=gbs_navlinks_s

- Fundamentos y aplicaciones de seguridad en redes WLAN. Izaskun Pellejero, Fernando Andreu, Amaia Lesta. 2006. http://books.google.com.co/books?id=k3JuVG2D9lMC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- HOW TO. OpenVPN. Disponible en: http://openvpn.net/index.php/open-source/documentation/howto.html
- ISSN: 2070-1721 March 2011 S. Turner
- Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. ALAFARDAN,J. Nadhem; PATERSON, Kenneth G. Information Security Group. RoyalHolloway, University of London. 27th February 2013.
- Man-In-The_Middle Attack Against SSL 3.0 /TLS 1.0. SCHNEIER, Bruce. Publicado el 23 de Septiembre de 2011. Accedido el 11 de junio de 2013. Disponible en: http://www.schneier.com/blog/archives/2011/09/man-in-the-midd_4.html
- OpenVPN. MORENO LEON, Jesús. MOLINA COBALLES, Alberto. IES Gonzalo Nazareno. Disponible en: http://www.slideshare.net/jmorenol/openvpn-una-solucin-vpn-basada-en-ssltls
- Oracle parchea la vulnerabilidad explotada por BEAST. Publicado el 20 de Octubre de 2011. Accedido el 10 de junio de 2013. Disponible en: http://blog.segu-info.com.ar/2011/10/oracle-parchea-la-vulnerabilidad.html#axzz2WqrP2m4c
- ProhibitingSecureSocketsLayer(SSL)Version2.0RFC 6176 http://datatracker.ietf.org/doc/rfc6176/?include_text=1
- RSA Laboratories. 2012 EMC Corporation. What is RC4? Disponible en: http://www.rsa.com/rsalabs/node.asp?id=2250
- Secure Sockets Layer (SSL). http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzain%2Frzainhistory.htm

- SSL Pulse. Survey of the SSL implementation of the Most popular Web sites. Publicado el 5 de Junio de 2013. Accedido el 12 de Junio de 2013. Disponible en: https://www.trustworthyinternet.org/ssl-pulse/
- SSL TLS. CertSuperior.com Disponible en: http://www.certsuperior.com/SSLtls.aspx
- SSL, Secure Sockets Layer y Otros Protocolos Seguros para el Comercio Electrónico. José María Morales Vázquez. Master de Seguridad Informática, I Edición. Curso 2001/2002. Universidad Politécnica de Madrid. http://pics.unlugarenelmundo.es/hechoencasa/ssl%20secure%20sockets%20layer%20y%20otros%20protocolos%20seguros%20para%20el%20comercio%20electronico.pdf
- THE CRIME ATTACK. DOUNG, Thai. Disponible en: http://www.ekoparty.org//2012/thai-duong.php
- THE CRIME ATTACK. RIZZO, Juliano. Disponible en: http://www.ekoparty.org//2012/juliano-rizzo.php
- The GnuTLS Transport Layer Security Library. Disponible en: http://www.gnutls.org/
- The Secure Sockets Layer – Chapter 11 Dr. Sourav Mukhopadhyay's http://www.facweb.iitkgp.ernet.in/~sourav/SSL.pdf
- Video. Introducción al protocolo SSL. Alfonso Muñoz (UPM). Video. Ataques al protocolo SSL. Luciano Bello (Chalmers University) http://www.intypedia.com/?lang=es
- Welcome to the OpenSSL Project. OpenSSL: The Open Source toolkit for SSL/TLS. Disponible en: http://www.openssl.org/