Universidad Dr. José Matías Delgado
Facultad de Posgrados y Educación Continua

Seminario de especialización profesional

Ensayo científico

ALTERNATIVA DE SEGURIDAD PARA TRANSACCIONES EN EL COMERCIO ELECTRÓNICO POR MEDIO DE TELEFONÍA

Presentado por:
Luis Alberto Molina Quintanilla

Para optar al título de:
Maestro en Negocios Internacionales

Asesor:
Mtro. Rolando Franco

Antiguo Cuscatlán, 01 de septiembre de 2011

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El comercio electrónico ha venido formando parte de las economías de varios países en los últimos años, tanto es así que en la declaración sobre el comercio electrónico mundial adoptada por la Segunda Conferencia Ministerial (Ginebra), celebrada el 20 de mayo de 1998, se instaba al Consejo General de de la OMC a establecer un programa de trabajo amplio para examinar todas las cuestiones relacionadas con el comercio electrónico mundial que afectan al comercio.

Los países que se han dado cuenta de la importancia del comercio electrónico son los que están sacando mejor provecho, rompiendo barreras físicas que antes existían para el comercio, tanto en la comunicación como en la transferencia de pagos. Esto último es válido no solo para países, sino también para individuos; hoy en día existen sitios de comercio electrónico que no necesariamente pertenecen a grandes negocios, tal y como se verá más adelante en este documento.

En la actualidad cada vez hay más negocios en internet relacionados con empresas que quizás tenían poco o ninguna presencia en el comercio tradicional. Existe una tendencia a que personas visionarias vean oportunidades de negocios, y con un mínimo esfuerzo poderlas formar en internet, capaces de proporcionar un servicio.

En el mundo de internet, la seguridad y el comercio electrónico son dos grandes hitos de la era digital difíciles de lidiar; la brecha entre ambos fue tan pequeña que comenzaron a salir nuevos productos aun antes de que las tecnologías estén totalmente maduras. Nadie esperaba que internet, o más específicamente, la World Wide Web, crecieran tanto a un ritmo exponencial en los últimos años. Sus posibilidades para el comercio fueron rápidamente descubiertas por los más astutos, y en un tiempo récord pasó a transformarse en una mezcla de transacciones comerciales, financieras y de todo tipo. Había que vender rápidamente, no podía esperarse a estándares que velaran por la rigurosa implantación de todos los detalles. ¿Qué método resulta más cómodo e inmediato para pagar? La tarjeta de crédito. ¿Al usuario le preocupa la seguridad? Usemos un canal seguro para transmitir el número de la tarjeta. Fue así como en poco tiempo se impuso como norma tácitamente acordada el emplear SSL para cifrar el envío de datos personales, entre ellos el número de tarjeta, lo cual debería de tener, como mínimo, una, un sitio que realiza transacciones por internet.

Pero a pesar de existir esta medida de seguridad y otras que pueden ser aplicadas al comercio electrónico, actualmente son demasiadas las facilidades que tiene una persona para conseguir vulnerarlas, y como consecuencia también son demasiados los problemas e incertidumbres como para dejar las cosas como están. Día con día salen a luz diferentes formas de atacar un sitio y también constantemente están los expertos tratando de contrarrestar estas acciones.

En el presente documento se pretende demostrar que al ingresar datos privados por internet (como lo son números de tarjetas de crédito), estos pueden ser capturados y ser utilizados por personas malintencionadas a pesar de existir medidas de seguridad que tratan de impedirlo; pero, principalmente, se pretende proponer una

alternativa de seguridad adicional para disminuir el riesgo de que los datos sean capturados al momento de enviarlos en una transacción electrónica. En la propuesta se explica tanto el funcionamiento y los elementos que lo conforman como las tecnologías involucradas, tal como se detalla en el capítulo I; así como también se fundamenta la propuesta en principios de seguridad informática y cómo disminuir los riesgos para que ésta no sea vulnerada. También se procura colaborar con la comunidad de usuarios que constantemente buscan soluciones adicionales a la seguridad informática.

CAPÍTULO I

MARCO REFERENCIAL

1.1 El comercio electrónico y las tecnologías involucradas

En nuestra vida diaria han venido evolucionando muchas cosas, y la mayoría con tendencias tecnológicas; entre ellas podemos mencionar la rama de la medicina que junto con los avances tecnológicos ha podido prolongar la vida de muchas personas y encontrar curas y tratamientos a enfermedades que años atrás no las tenían. Así también podemos mencionar los avances en los medios de transporte y medios de comunicación, entre otros.

El intercambio de bienes y servicios no ha sido la excepción a la constante evolución; el comercio electrónico no es más que una nueva forma de realizar negocios, con la variante de que ahora se realizan utilizando las TIC disponibles. Actualmente ya no solo podemos hablar de bienes y servicios, sino también del intercambio de información, por lo que algunas personas la han llamado "la era del conocimiento", donde el saber es muy valorado, inclusive mucho más que algo tangible. Hoy en día la información está al alcance de todos, con la facilidad de acceder a internet en cualquier lugar, siendo ésta, parte importante para el rápido crecimiento y evolución de las TIC.

Para el comercio electrónico, las tecnologías son variadas, pero, como todo en la vida, existen unas que sobresalen, otras que son íconos en la industria, y otras que están de moda; entre las más utilizadas están los lenguajes en que un sitio web puede ser programado, los estándares de comunicación, etc. También existen TIC que no necesariamente son parte del comercio electrónico; pero que, conforme las necesidades que van surgiendo, estas se van integrando. Un ejemplo de esto es la telefonía, que poco a poco ha ido evolucionando, y hoy en día es utilizada mezclando tanto telefonía tradicional con digital. En algunos casos la telefonía digital puede utilizarse de manera automática para realizar procesos que humanos realizan de forma aburrida y monótona, tal es el caso de recordatorios para fechas de eventos, cuando usuarios desean conocer sus saldos en bancos, o bien para una empresa como recepcionista digital en un PBX redirigiendo las llamadas a diferentes departamentos de la misma, dependiendo de la extensión digitada (IVR). Google utiliza el servicio de telefonía para verificar[1] si realmente es un humano el que está solicitando crear una cuenta de correo, y no un robot generador de spam.

Pero el comercio electrónico esta basado en gran parte sobre internet y todo lo que esta tecnología implica.

[1] Google. "Incidencias comunes relacionadas con la verificación de la cuenta a través de un mensaje SMS o de una llamada de voz.". http://mail.google.com/support/bin/answer.py?answer=114129 [consultada el 25/03/2011/].

1.2 Páginas web y lenguajes de programación

Internet, en general, es un conjunto de mucha información, la cual consta en gran parte de texto e imágenes; pero que en los últimos años se han agregado contenidos multimedia, como por ejemplo video y audio.

Para poder mostrar todo este contenido fue necesario crear un estándar, y es así como surgió el lenguaje llamado HTML, que son las siglas de HyperText Markup Language (Lenguaje de Marcado de Hipertexto). Este es un lenguaje para crear páginas en internet, que posteriormente son las que vemos desde un navegador web, como por ejemplo, desde Internet Explorer en Windows y Safari en Mac, ambos navegadores web. HTML consta de una serie de marcas llamadas etiquetas, las cuales sirven para representar imágenes, textos, enlaces, videos, etc., todo ello escrito dentro de un archivo de texto. Se podría hacer la analogía de una página web con un documento realizado en un procesador de texto, como Microsoft Word, en el que se pueden insertar imágenes, tablas, textos de diferentes colores, tamaños, etc.

En general, el Lenguaje de Marcado de Hipertexto sirve para definir la apariencia del documento web a ser mostrado; pero éste solamente muestra contenido estático, es decir contenido que no cambia, a menos que se modifique el archivo de texto HTML.

Posteriormente surge la necesidad de poder mostrar contenido dinámico, es decir contenido que cambie de acuerdo a situaciones específicas, como por ejemplo contenido que cambie de acuerdo al usuario que esta viendo la información, como lo podrían ser los estados de cuenta de un banco. Otro ejemplo podría ser el correo electrónico, porque es contenido que no siempre es el mismo: son correos diferentes los que el usuario necesita visualizar, pero todo mostrado siempre en formato HTML.

Es por esto que surgen diferentes lenguajes de programación, los cuales pre-procesan la información contenida con bases de datos o tareas que se le ha programado que haga, generando como resultado un documento HTML, que es el que finalmente el usuario ve con los resultados. Entre estos lenguajes de programación para páginas web se pueden mencionar ASP de Microsoft, Java de Sun Microsystems (actualmente adquirida por una empresa mundialmente conocida por su potente gestor de base de datos llamada Oracle), y PHP entre otros. Este último muy popular por ser uno de los lenguajes considerados como software libre, es decir que los programadores pueden crear programas con este lenguaje, y dichos programas pueden ser usados, copiados, estudiados, modificados y redistribuidos libremente. Estas características de PHP dieron la pauta para que se volviera muy de moda entre los usuarios de software libre y software como código abierto, así como en sitios donde alquilan espacios para alojar sitios web dando soporte para alojar también documentos PHP.

En la categoría de comercio electrónico PHP también ha tenido mucho involucramiento, tal es el caso de software diseñado especialmente para el llamado software del “carrito de compras”, o “shopping cart” donde de forma fácil puede

montarse un sitio completo para vender productos y/o servicios, como por ejemplo el software llamado osCommerce, PrestaShop y Magento, entre otros[2].

Existe también la posibilidad de poder descargar desde internet trozos de software (llamadas librerías) que otras personas han desarrollado para que sean reutilizados por programadores en sus proyectos, reduciendo así el tiempo de programación de dichos proyectos y reutilizando programas que otras personas ya han creado. Un ejemplo de estas librerías pueden ser las que permiten a programas realizados con PHP se conecten hacia Paypal, Authorize.net o 2Checkout(2CO), los cuales son sitios que procesan peticiones de pago, es decir tener la posibilidad de conectarse a estos sitios de terceros para que realicen las tareas de cobro y procesamiento del pago.

1.3 IED y TEF

El intercambio electrónico de datos (o IED por sus siglas) consiste en el intercambio de datos estructurados entre dos computadoras, que generalmente son computadoras de dos diferentes empresas a las que podríamos llamar socios comerciales; dicho intercambio se realiza utilizando un formato estándar para que ambos lados puedan entenderse y comunicarse entre sí. A menudo los datos que se intercambian son datos de transacciones comerciales, aunque esto no impide que puedan intercambiarse otro tipo de información de utilidad para ambas empresas, como por ejemplo inventarios de productos, precios, etc.

Al IED se le considera una de las primeras formas del comercio electrónico, y esta tecnología vino a disminuir costos, como por ejemplo en los procesos administrativos y utilización de papel, así como también vino a disminuir errores en los datos y documentos.

Como ya se mencionó, los datos son transferidos de forma estándar y estructurada, y para ello existen varios formatos, entre los que se encuentra el ANSI X12, utilizado en Estados Unidos; y EDIFACT, éste último, uno de los más utilizados en todo el mundo.

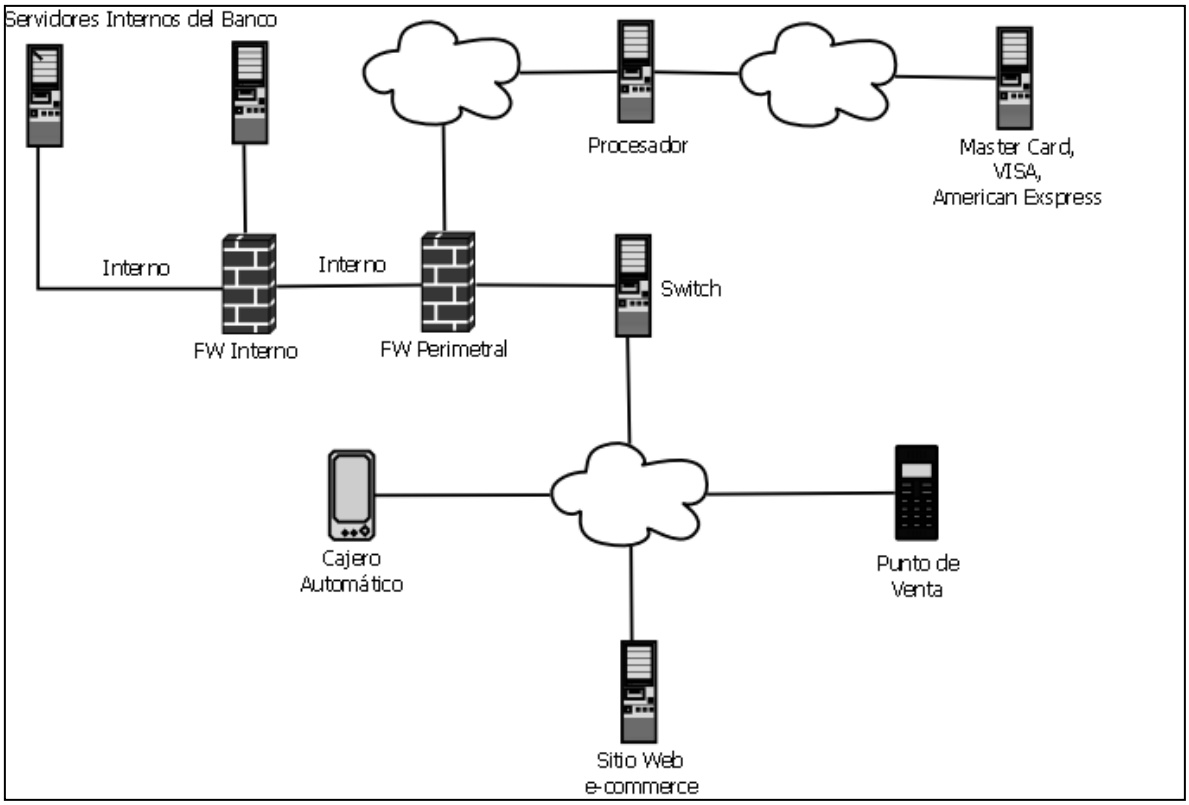
Dentro del IED se encuentra la transferencia electrónica de fondos (o TEF, por sus siglas), la cual consiste en transferir cualquier tipo de fondos por medios electrónicos de manera inmediata. A partir de este concepto es que comienzan a surgir diferentes tipos de IED, entre los que se encuentran las tarjetas de plástico (de crédito o de débito), que por medio de cajeros automáticos obtienen una serie de servicios bancarios, y posteriormente los puntos de venta (conocidos como POS por sus siglas en inglés, de “Point of Sale”), que potenciaron de gran manera los comercios. Tanto los cajeros automáticos como los puntos de venta es importante mencionarlos en este documento, ya que ambos utilizan la red de datos para transferir información,

[2] Open Source Ecommerce Software. http://ecommerce.about.com/od/directoryofsoftware/a/Open-Source-Ecommerce-Software.htm [consultada el 15/03/2011].

igual como lo hace un sitio web de comercio electrónico para realizar las transacciones comerciales.

En una transacción de comercio electrónico se encuentran involucradas varias partes, cada una realizando una acción específica, tal como se muestra en el figura 1.

Figura 1: Actores involucrados en una transacción en línea



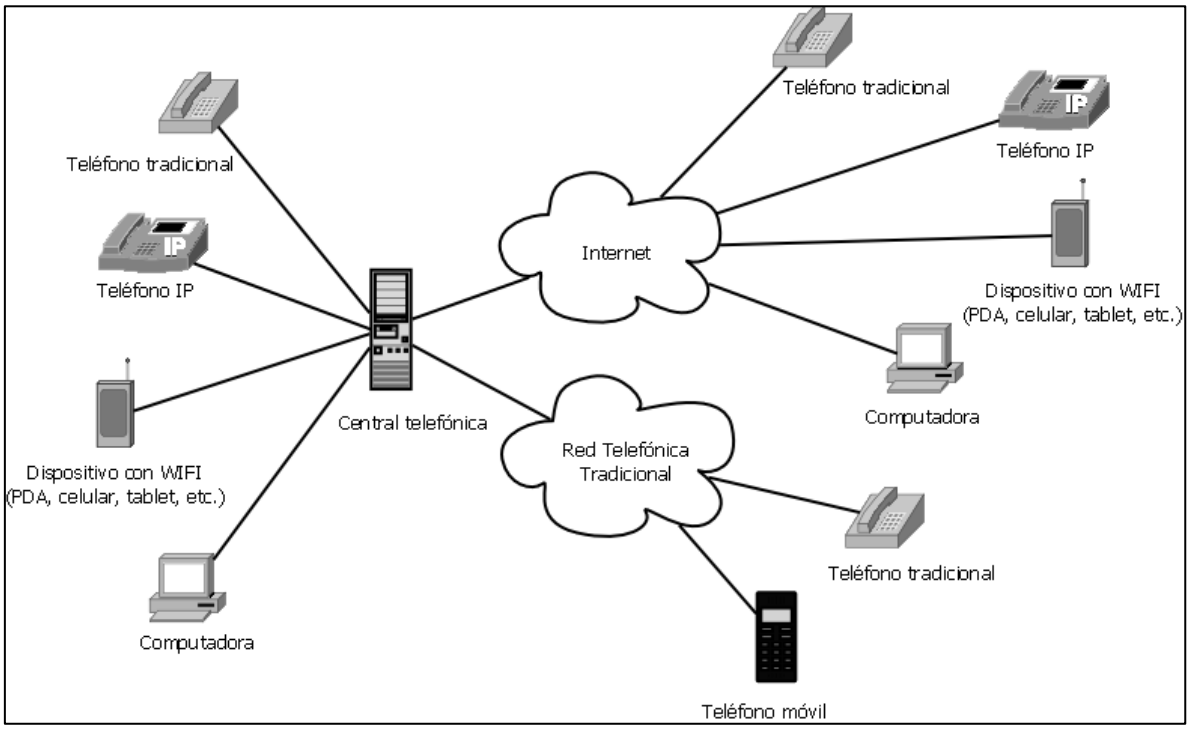
Fuente: Creación propia.

1.4 Voz sobre IP

Voz sobre IP, o también llamado VoIP, consiste en que la voz viaje a través de internet. Esto significa que se envía la señal de voz en forma digital, en lugar de enviarla en forma analógica, como se hace en la telefonía convencional. Lo de "IP" es porque utiliza el protocolo llamado IP, el cual hace posible el envío y la recepción de datos a través de una red.

La tecnología de voz sobre IP permite mezclarla a la red de telefonía análoga (tradicional). Tal como se muestra en figura 2, tanto dispositivos de telefonía digital como de telefonía análoga pueden interconectarse entre sí, y a la vez conectarse también a dispositivos remotos por medio de internet o por medio de la red telefónica tradicional, prácticamente a cualquier parte del mundo.

Figura 2: Funcionamiento de voz sobre IP



Fuente: Creación propia

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas que no necesariamente estén conectadas a internet, como por ejemplo en la red de una empresa, oficina o inclusive dentro de una red en doméstica.

Actualmente la voz sobre IP es utilizada para algunos servicios en internet. Un ejemplo que se ha vuelto muy popular en lo últimos años es el servicio que brinda la empresa luxemburguesa llamada Skype, la cual ofrece un software con el que pueden realizarse llamadas y videoconferencias de forma gratuita entre dos o más personas que tengan el software instalado; pero Skype también permite realizar llamadas telefónicas hacia números convencionales en cualquier parte del mundo

por un costo mínimo. Otro ejemplo de voz sobre IP es utilizado en el sector de la banca, donde el cliente puede consultar sus estados de cuenta, realizar transacciones, pagos, etc. Todo esto desde un teléfono.

Dentro de la tecnología de voz sobre IP se encuentra un software que por sus características puede considerarse como un ícono dentro de este rubro; dicho software es Asterisk, creado por el estadounidense Mark Spencer, quien posteriormente fundó la compañía Digium, empresa que vende servicios y productos relacionados a la voz sobre IP.

Asterisk consiste en un programa libre y de código abierto cuyas funcionalidades son las de una central telefónica (PBX), y cuenta con características que anteriormente sólo estaban disponibles para costosos sistemas propietarios, como por ejemplo buzones de voz, llamadas en espera, entre otras.

Asterisk proporciona un núcleo central de conmutación, con cuatro APIs para la carga modular de aplicaciones de telefonía, las interfaces de hardware, control de formato de archivo y codecs. Permite la conmutación transparente entre todas las interfaces soportadas, permitiendo que se unan a una mezcla diversa de sistemas de telefonía en una única red de conmutación.

Asterisk está desarrollado principalmente en GNU/Linux para x/86 y funciona en GNU/Linux para PPC, junto con OpenBSD, FreeBSD y Mac OS X. En general, es compatible con cualquier sistema basado en estándares UNIX.

Asterisk no requiere hardware adicional para Voz sobre IP. Para la interconexión con equipos de telefonía digital y análoga, Asterisk es compatible con varios dispositivos de hardware, más notablemente con todo hardware fabricado por Digium, el creador de Asterisk. Para mayor información respecto al hardware soportado oficialmente por Asterisk, puede consultarse el sitio oficial de Asterisk[3]. También puede visitar una lista (no oficial) de hardware conocido que funciona con Asterisk en el sitio de voip-info.org[4].

Asterisk soporta una amplia gama de protocolos para el manejo y transmisión de voz sobre interfaces de telefonía tradicional, incluyendo H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), y Skinny Client Control Protocol (SCCP). Asi también Asterisk varios códecs de audio, entre los que se encuentran G.729, GSM, ILBC/Speech, G.722/G.723 y G711a/G.711u.

Utilizando el protocolo de voz sobre IP llamado Inter-Asterisk eXchange (IAX), Asterisk combina el tráfico de voz y datos sin problemas entre redes diferentes. El uso de la voz en paquetes permite a Asterisk enviar datos como información URL e imágenes en línea con el tráfico de voz, permitiendo una integración avanzada de información.

[3] Hardware soportado por Asterisk. http://www.asterisk.org/support/hardware [consultada el 03/09/2001].
[4] Página de referencia de hardware que se sabe que funciona con Asterisk. http://www.voip-info.org/wiki/view/Asterisk+hardware [consultada el 03/09/2001].

Una característica que hay que mencionar, para efectos del presente trabajo, es la de poder implementar dentro de Asterisk un IVR, o Respuesta de Voz Interactiva, por sus siglas en ingles, que consiste en un sistema telefónico capaz de recibir una llamada e interactuar con el usuario a través de grabaciones de voz, entregando y/o capturando información por medio del teléfono, permitiendo de esa forma el acceso a servicios de información u otras operaciones.

Es importante mencionar que dentro de un IVR están involucradas otras tecnologías, como por ejemplo el DTMF o sistema de marcación por tonos, que consiste en el marcado de números por medio de tonos de frecuencias determinadas. También existen las tecnologías de TTS y ASR; la primera, utilizada para transformar texto a audio; y la segunda, para reconocer las palabras del usuario, transformándolas en órdenes que entenderá el sistema.

1.5 Seguridad en informática y el comercio electrónico

El concepto de seguridad dentro de informática está fundamentado en tres elementos básicos: confidencialidad, integridad y disponibilidad. En unos textos suele agregarse la autenticidad como parte de los tres anteriores, pero en general, lo que tienen en común es que si en alguno de ellos se encuentra una debilidad este puede ser vulnerado, y por lo tanto comprometer la seguridad del sistema o la red.

Así también, en seguridad informática se menciona que debe haber un balance entre seguridad, funcionalidad y facilidad de uso; por ejemplo, si la seguridad aumenta, la funcionalidad y la facilidad de uso decrementan. El entorno utópico que debería existir es que los tres elementos estuvieran en un nivel alto, pero por lo que hemos visto esto no es posible. Y muchas veces las medidas de seguridad que se implementan dificultan al usuario utilizar la tecnología y también su nivel de funcionalidad.

Tomando como principio de que **en informática no todo es totalmente seguro** y **que siempre existe la probabilidad de que se encuentren vulnerabilidades en los sistemas**, el objetivo de la seguridad informática es minimizar los riesgos y dificultarle el trabajo a los usuarios mal intencionados llamados “hackers”; y es por esto que entre más medidas de seguridad se tengan, es mucho mejor, y sobre todo en aplicaciones o entornos en los que la información involucrada sea de mucha importancia, como lo es el comercio electrónico, en el que transacciones y dinero se encuentran en juego.

Para el comercio electrónico existen medidas que minimizan los riesgos para que la seguridad no sea vulnerada; y entre los más utilizados se encuentran el protocolo de comunicación SSL. Este protocolo proporciona un canal de comunicación cifrado entre dos equipos: en este caso, la máquina del cliente y la del vendedor. Cuando un cliente solicita realizar una conexión segura a un sitio, comienza un intercambio de mensajes para negociar la seguridad, y en esta negociación se intercambian unas claves, las cuales son necesarias para cifrar la información; así como también en esta fase de negociación se intercambian certificados digitales.

SSL (Secure Sockets Layer) es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del navegador web “Netscape Navigator”. Hoy constituye la solución de seguridad implantada en la mayoría de los servidores web que ofrecen servicios de comercio electrónico y transacciones similares o sitios que requieran un nivel de seguridad entre dos puntos. Para pagar, el usuario debe rellenar un formulario con sus datos personales (tanto para el caso del envío de los bienes comprados, como para comprobar la veracidad de la información de pago) y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. Baste con que se utilice como mínimo un canal seguro para transmitir la información de pago, y el comerciante ya se ocupará manualmente de gestionar con su banco las compras. El canal seguro lo proporciona SSL. Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura. SSL deja de lado demasiados aspectos para considerarse la solución definitiva.

La razón de intercambiar certificados digitales es que, por ejemplo, si nosotros ciframos la información hacia y desde un sitio, ese sitio debería ser confiable; pero puede darse el caso de que ese sitio sea falso y entonces la medida de seguridad no nos sirve de nada, y es por eso que el certificado digital garantiza que el sitio no es falso, y que una tercera entidad certifica que ese sitio es quien dice ser. A esta tercera entidad se le llama Autoridades Certificadoras (AC), y se encarga de autenticar los sitios y de emitir certificados digitales para estos sitios.

El certificado digital no es más que un archivo electrónico que contiene datos de identificación personal del emisor de los mensajes, la clave pública y la firma del prestador de servicios de certificación.

Pero a pesar de existir medidas como estas, cada día los hackers buscan nuevas formas de explotar las vulnerabilidades en los sistemas de seguridad, y como se menciona en el capítulo siguiente, existen técnicas para poder realizarlo, y ahora con la facilidad de acceso a internet y a herramientas gratuitas; un usuario que no necesariamente sea experto en la materia puede ser una amenaza.

Si los datos que viajan entre un extremo de la comunicación al otro no se encuentran cifrados o asegurados de alguna manera, cabe la posibilidad de que puedan ser interceptados y leídos; pero si al contrario, estos se encuentran debidamente cifrados, estos pueden ser capturados pero no interpretados.

Al hablar de seguridad en el comercio electrónico también es importante mencionar otros protocolos que existen para asegurar las transacciones en dicho entorno, y uno de ellos es SET, cuyas siglas en inglés significan “Transacción Electrónica Segura”, y como su nombre lo indica, es un protocolo para asegurar las transacciones electrónicas. Este protocolo fue desarrollado en 1995 por VISA, Mastercard, IBM, Microsoft, Netscape y Verisign, donde la gran ventaja consiste en que todas las partes involucradas (cliente, comerciante y bancos) son aseguradas, protegiendo los datos que son transferidos entre ellos y utilizando técnicas criptográficas muy

seguras, obligando a todos los involucrados a utilizar esquemas rígidos de certificación autorizados por entidades independientes (autoridades certificadoras) a todos ellos; aparte de que tanto el comprador como el vendedor necesitan cada uno un software que implemente el protocolo de pagos SET, así como certificados digitales compatibles y apropiados para el mismo.

Pero a pesar que el protocolo SET está orientado a aplicaciones de comercio electrónico con un alto grado de seguridad, no goza de la popularidad frente a otros protocolos como SSL, debido a que parte de sus puntos fuertes sean al mismo tiempo puntos débiles, como lo es el hecho que del lado del cliente deba de tener certificados y software especiales para la transacción; esto hace que sea un proceso difícil y engorroso de utilizar para el comprador. SET es un ejemplo donde se puede observar uno de los principios ya mencionados sobre seguridad, en el que se dice que debe existir un equilibrio entre seguridad, funcionalidad, y facilidad; haciendo que este protocolo aumente la seguridad pero disminuya la funcionalidad y facilidad para el usuario.

SSL le ha tomado ventaja y popularidad a otros protocolos de seguridad, entre ellos SET, por su fácil uso e implementación, a pesar de que SSL no ofrece la seguridad ni las garantías de los otros; pero es funcional y agrega un nivel de seguridad adicional al momento de realizar transacciones.

CAPÍTULO II

DEFINICIÓN DEL PROBLEMA

2.1 Alcance

Debido a que la alternativa propuesta de seguridad se centra en la captura de datos al momento de pagar en una venta por internet, el presente documento se limita a detallar el funcionamiento de dicha propuesta solamente para la captura de datos de tarjeta de crédito y la comunicación entre el sitio web de comercio electrónico y el cliente; no se entrará en detalles del proceso de compra en línea ni en el procesamiento y validación de los datos de tarjeta de crédito; sin embargo, serán mencionados y se explicará la relación que estos tienen en el proceso completo.

2.2 Planteamiento del problema

Mucho se ha hablado de comercio electrónico en los últimos años, y muchos sitios han formado parte de esto como íconos, por ejemplo eBay[5], que es un sitio muy popular de subastas en internet, así como también el sitio de la compañía DELL[6], en la que los usuarios pueden ingresar para personalizar y comprar sus computadoras. Otro sitio que puede mencionarse, pero que en lugar de vender productos vende servicios es GoDaddy[7], la cual ofrece sus servicios de alojamiento para sitios web, así como la de reserva de dominios en internet, entre otros servicios. GoDaddy, al igual que muchos otros sitios del mismo rubro, ha proporcionado la facilidad de que una persona con conocimientos intermedios de informática pueda crear un sitio web sin mucho esfuerzo y a un precio asequible.

Tomando de nuevo el tema de venta de servicios por internet, hay sitios en los que les permiten utilizar software o servicios gratis por un tiempo limitado, o utilizarlo con ciertas características limitadas, lo cual permite crear una especie de “anzuelo” para los clientes, quienes al probar dicho software o servicio adquieren la versión completa por un precio definido. Un ejemplo de estos sitios es el de Prezi[8], un sitio donde se pueden crear presentaciones similares a PowerPoint de Microsoft, a diferencia de que en Prezi las presentaciones son “no lineales”, es decir que no van de diapositiva en diapositiva, permitiendo al usuario agregar efectos de zoom y enlazar las ideas diagramadas en la presentación. Prezi ofrece la creación de un servicio básico, el cual es gratis, pero si el usuario desea puede adquirir el servicio intermedio o uno más grande, los cuales incluyen características adicionales pero a un precio adicional.

Como se puede observar, existen diferentes modalidades en las que las empresas pueden vender sus productos o servicios, y no necesariamente la empresa debe de

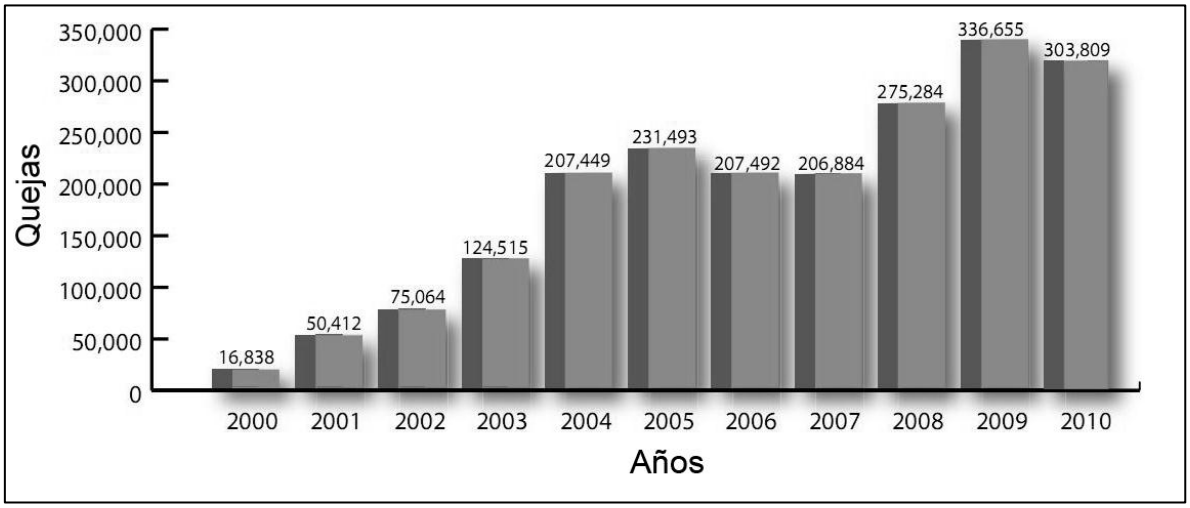
[5] Ebay. http://www.ebay.com [consultada el 27/03/2001].
[6] Dell http://www.dell.com [consultada el 27/03/2001].
[7] GoDaddy http://www.godaddy.com [consultada el 27/03/2001].
[8] Prezi. http://www.prezi.com [consultada el 03/04/2011].

contar con un espacio físico a donde ir a adquirirlos, como tradicionalmente se hace; todo es realizado a través de internet.

Tal como se comentaba, en internet existe la facilidad de que una persona pueda crear y alojar un sitio web a un precio mínimo si necesariamente ser un experto en la materia; eso es algo bueno desde el punto de vista de que se puede expandir fácilmente un comercio e incrementar sus canales de venta desde internet. Pero, como todo en la vida, esto también tiene sus puntos en contra, o de desventaja que hay que tomar en cuenta, como por ejemplo el hecho de que cualquier persona pueda poner un negocio en internet significa también que cualquier persona puede hacerse pasar por un negocio "lícito", que en realidad es falso, para realizar fraudes a sus clientes. Un ejemplo de estos fraudes podría ser el ofrecer productos, pero que una vez el cliente los ha pagado, estos productos nunca llegan al cliente; o también se puede mencionar el caso en el que un cliente aparentemente esta pagando por internet un producto de modo seguro, pero que realmente la empresa es falsa y utilizan los datos de la tarjeta de crédito del cliente para robarle dinero o realizar compras en otros sitios.

Según el IC3[9], en su reporte anual del año 2010[10], existe una tendencia al alza de las quejas recibidas, tal como se muestra en la figura 3.

Figura 3: Comparación anual de quejas recibidas en el sitio de la IC3[11]



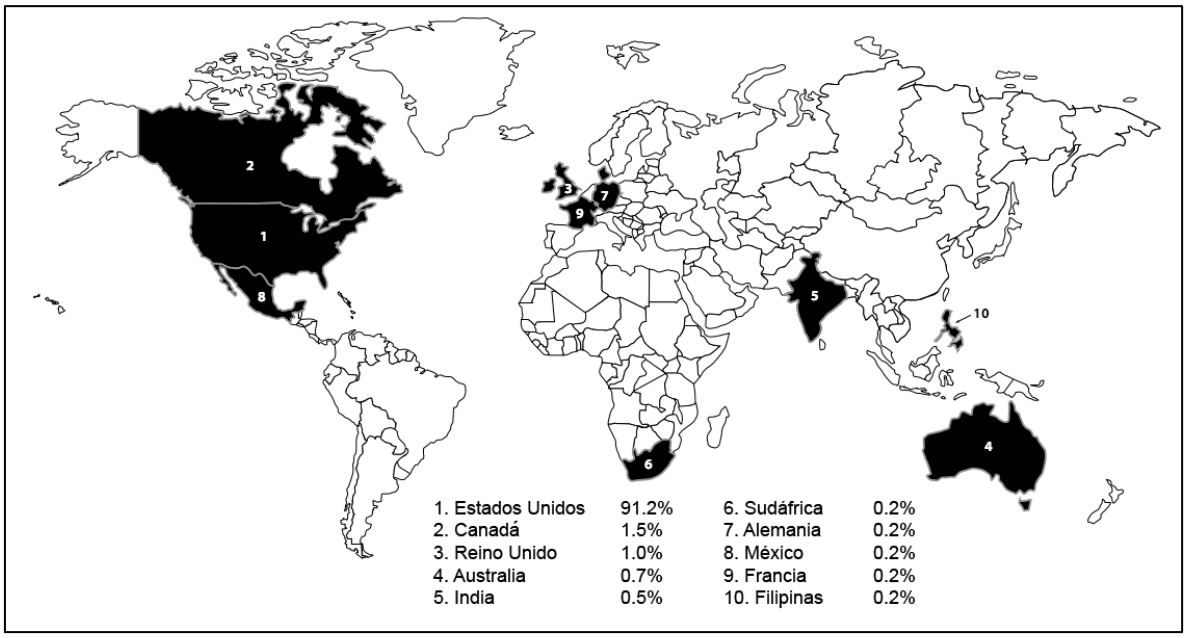
Fuente: Reporte para el año 2010 del Internet Crime Complaint Center (IC3)

Esto demuestra que así como internet se va extendiendo junto con las tecnologías asociadas a ella, así también se incrementan los riesgos de usarlas y de que otras personas hagan uso inadecuado de estas tecnologías para realizar fraudes.

[9] Internet Crime Complaint Center (IC3). http://www.ic3.gov [consultada el 03/04/2011].
[10] National White Collar Crime Center. 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [consultada el 03/04/2011].
[11] Para ver las definiciones de tipos de quejas recibidas, sus categorías y subcategorías, referirse al anexo 1 y anexo 2.

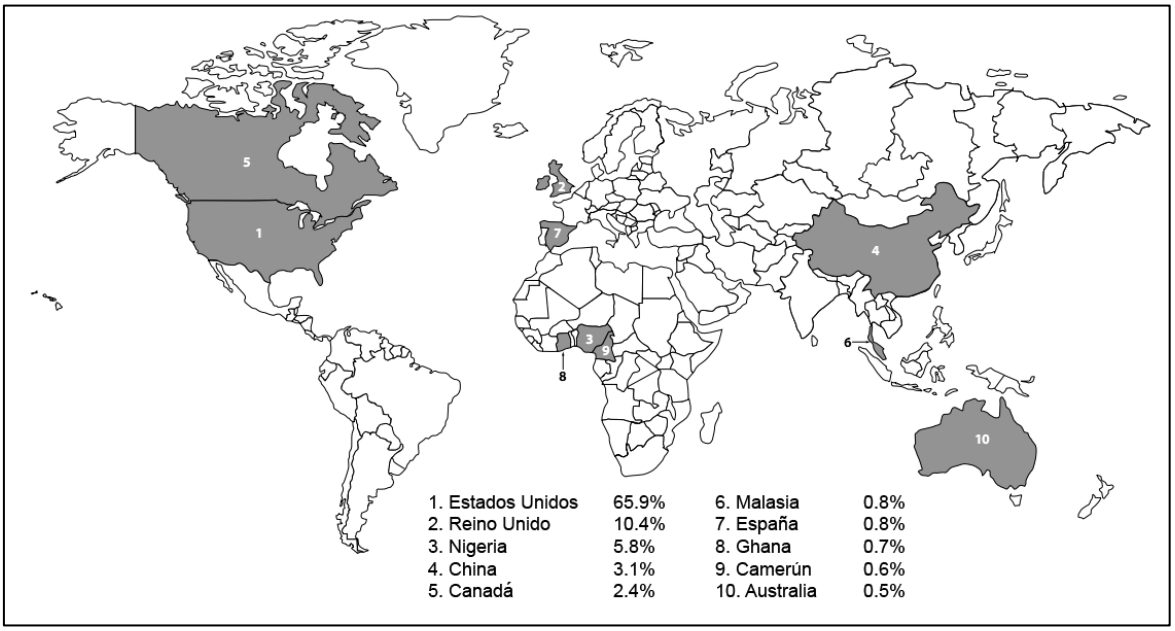
Observando, tanto la figura 4 como la figura 5 se puede distinguir que Estados Unidos ocupa el primer lugar en cuanto a quejas, así como también el origen de crímenes reportados, lo cual viéndolo desde el punto de vista de negocios internacionales, Estados Unidos es uno de los países que tienen bastante comercio con otros países, incluyendo El Salvador.

Figura 4: Top 10 de países: Quejas individuales (numeradas por rango)



Fuente: Reporte para el año 2010 del Internet Crime Complaint Center (IC3)

Figura 5: Top 10 de países: Perpetradores individuales (numeradas por rango)



Fuente: Reporte para el año 2010 del Internet Crime Complaint Center (IC3)

De las quejas registradas por la IC3, y para propósitos del presente documento, se tomarán de los 10 primeros tipos de crímenes reportados que se muestran en la tabla 1 los siguientes datos: el robo de identidad, con un 9.80%; delitos informáticos y fraudes de tarjetas de crédito, con 9.10% y 5.30%, respectivamente, sumando un total de 24.20%, el cual representa casi una cuarta parte del total de crímenes reportados.

Tabla 1: Top 10 por tipos de crímenes reportados

Tipo	**Porcentaje**
1. De no entrega de pago/mercadería	14.40%
2. FBI relacionadas con estafas	13.20%
3. El robo de identidad	9.80%
4. Delitos informáticos	9.10%
5. Fraudes varios	8.60%
6. Fraude de adelantos de pago	7.60%
7. Spam	6.90%
8. Subastas fraudulentas	5.90%
9. Fraudes de tarjetas de crédito	5.30%
10. Fraudes de pago en exceso	5.30%

Fuente: Reporte para el año 2010 del Internet Crime Complaint Center (IC3)

Los tres tipos de crímenes reportados que han sido seleccionados incluyen fraudes relacionados con la seguridad en el comercio electrónico. De acuerdo a la definición de esos tipos de crímenes, los datos de la víctima, en el robo de identidad, son utilizados por el atacante; es decir que el atacante de alguna forma captura u obtiene esa información de la víctima. Para poder capturar esos datos, generalmente los llamados “hackers” utilizan diversas técnicas, entre ellas se puede mencionar la técnica denominada “el hombre en el medio” (conocida también como “man in the middle”), la cual consiste en que el atacante se posiciona entre la computadora de la víctima y el sitio de comercio electrónico (u otro destino), y de esa forma puede capturar todo el tráfico que se origina desde un lado al otro y viceversa. También existe otro tipo de ataque muy popular para capturar datos en transacciones, ya sea de comercio electrónico, banca, etc. Dicho ataque es conocido como “Phishing”, el cual consiste en que el atacante suplanta un sitio válido enviando un mensaje a la víctima, solicitándole con engaños, datos privados, generalmente usuarios y contraseñas. En ocasiones los “phishers”, como se le conocen a estos atacantes, envían correos electrónicos con formularios y logos similares a las reales, a quienes están suplantando, o también solicitando ingresar a direcciones web similares a las

reales; pero que en este caso son falsas y suelen redirigir a la víctima a sitios completamente parecidos a los reales, engañando de esta forma a la víctima y dándole "confianza" visual para digitar sus datos privados.

Existe también otro tipo de ataque llamado "Pharming", similar al phishing, pero con la variante de que el atacante explota vulnerabilidades del servicio de DNS (Sistema de Nombres de Dominio) redirigiendo al usuario a un sitio falso, haciéndole creer que el sitio es verdadero.

En cuanto a delitos informáticos se refiere, la definición nos menciona malware, es decir software de origen malicioso, como los virus (principalmente virus de tipo caballos de Troya), spyware, etc. Siendo tipos de programas, que en algunos casos (dependiendo del tipo) no son destructivos, que no eliminan información, sino que la capturan y luego es enviada a los creadores de dichos programas. Un ejemplo puede ser en el que la victima descarga un software desde un sitio en internet, pero no se percata que ese software le instala otro software malicioso el cual le captura toda la información que éste digita; posteriormente el atacante recolecta toda esta información capturada y puede tener acceso a todas las cuentas en las que la víctima ha ingresado, así como también enterarse de todo lo que la víctima ha digitado, incluyendo usuarios, contraseñas, números de tarjetas de crédito, etc.

Finalmente, cuanto se habla de fraudes de tarjetas de crédito, en algunos casos se realizan cuando la víctima compra por internet, y dicha información de tarjetas de crédito es capturada y luego utilizada por el atacante para realizar otras compras, las cuales son cargadas a la tarjeta de crédito de la víctima.

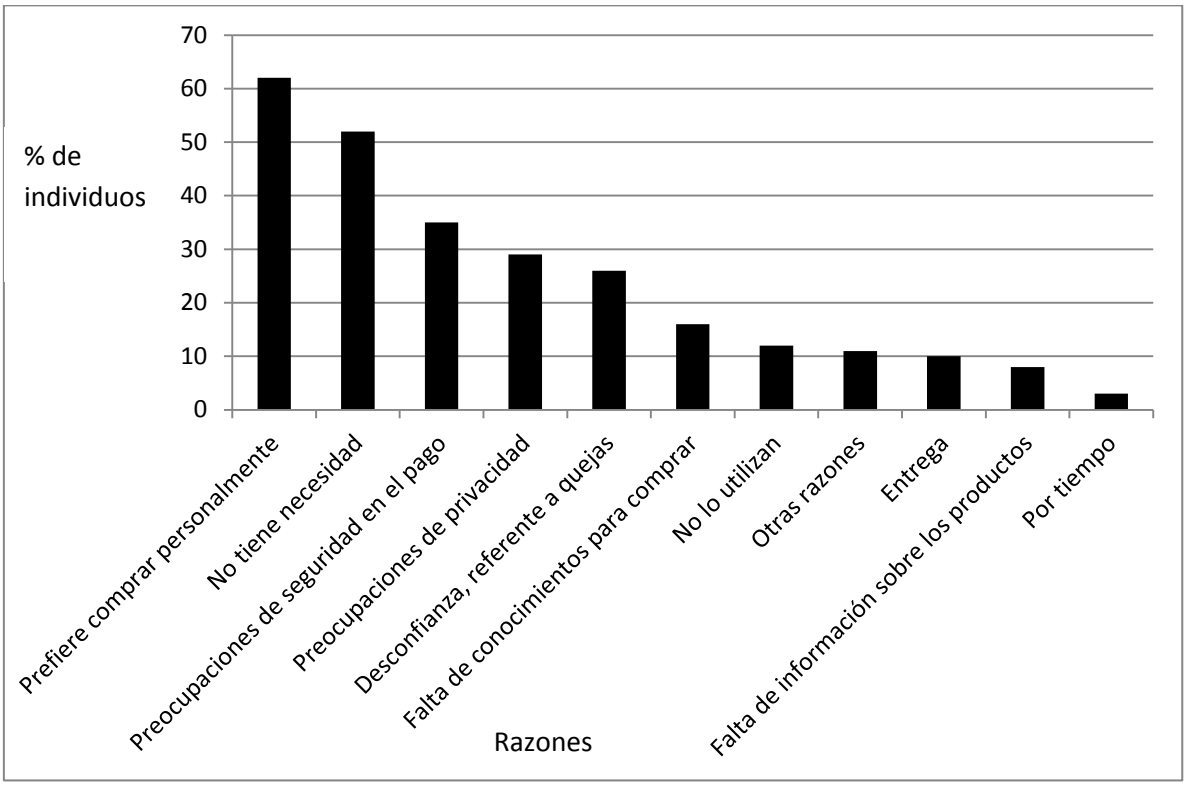
Estos tipos de crímenes pueden ser evitados en gran medida, y para ello existen medidas para contrarrestar los potenciales ataques; entre ellos podemos mencionar el uso de antivirus en las computadoras, verificar que los sitios visitados son realmente los sitios que dicen ser, así como verificar qué sitios en los que se realicen transacciones importantes, o donde se digiten datos privados (como por ejemplo contraseñas) utilicen certificados de seguridad validados por entidades certificadoras reconocidas a nivel mundial, entre otras. Pero por muchas medidas de seguridad que se tengan para evitar los crímenes, estos no pueden evitarse en su totalidad, y tal como se menciona en la teoría de seguridad informática, no todo es totalmente seguro.

A pesar de que existan medidas de seguridad, hay personas que no compran desde internet por diferentes razones. La figura 6, sacada de un artículo[12] presentado por la Eurostat[13], muestra el porcentaje de individuos que respondieron a las razones por las que prefieren no utilizar internet en la compra de productos o servicios, y entre ellas se puede observar la preocupación por la seguridad en el pago, así como también la preocupación por la privacidad y la desconfianza.

[12] Comisión Europea. (2011). "Sociedad de la Información 2011). http://epp.eurostat.ec.europa.eu/statistics_explained/images/6/60/Information_society_2011.xls [consultada el 13/04/2011]

[13] Oficina de Estadística de la Unión Europea. http://epp.eurostat.ec.europa.eu [consultada el 19/04/2011]

Figura 6: Razones por las que no se utiliza la internet en la compra de productos o servicios



Fuente: Artículo estadístico de información sobre las sociedades de la Unión Europea presentado por la Eurostat con datos del 2010.

2.3 Objetivos

Objetivo general

- Proponer una alternativa de seguridad en el comercio electrónico, utilizando telefonía IP.

Objetivos específicos

- Plantear un modelo de seguridad para la transferencia de datos entre el sitio web de comercio electrónico y el cliente.
- Mostrar el uso de telefonía IP como tecnología complementaria en el comercio electrónico.

CAPITULO III

INVESTIGACIÓN Y DIAGNÓSTICO

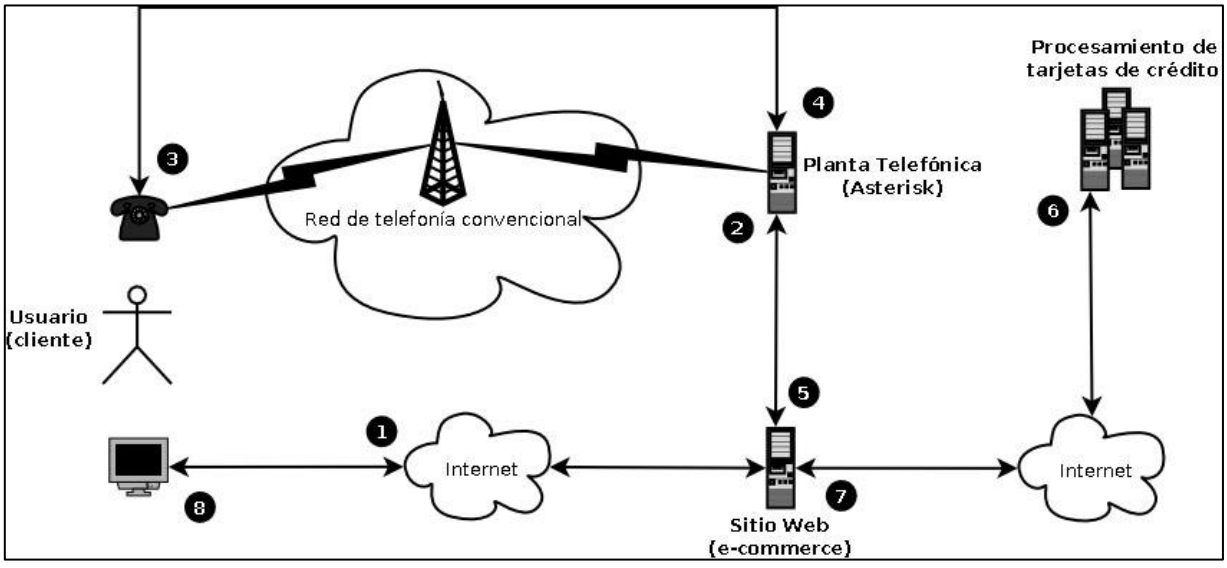
Debido al problema planteado en el capítulo anterior, donde se muestra que algunas personas temen comprar por internet debido a la desconfianza e inseguridad que sienten al realizar dicha transacción, ya que sus datos personales o de tarjetas de crédito pueden ser capturados por terceros; y que a pesar que existen medidas de seguridad siempre hay personas que buscan la manera de vulnerar la seguridad, el presente documento propone la implementación de una alternativa de seguridad en el intercambio de información en el comercio electrónico, específicamente al momento de intercambiar datos importantes y privados.

Antes de explicar el funcionamiento, es importante mencionar que el intención de proponer esta alternativa no es el dar una solución definitiva al problema de seguridad en el comercio electrónico, sino, como su nombre lo dice, una “alternativa” a implementar para aumentar el nivel de seguridad en las transacciones del comercio electrónico, la cual junto a las otras medidas de seguridad ayudarán a incrementar el nivel de seguridad.

3.1 Desarrollo

Todo comienza cuando un usuario, al cual se le llamará cliente, ingresa a un sitio web para realizar una compra en línea, y posteriormente hay una secuencia de pasos que se detallan a continuación y que se muestran en el figura 7:

Figura 7: Funcionamiento de la solución



Fuente: Creación propia

1. Una vez el cliente ha decidido los productos o servicios a comprar y los ha agregado al carrito de compras, pasa al siguiente paso que sería el "checkout", en donde generalmente se muestra un detalle de lo que ha comprado, subtotales y un total general a pagar. En esa misma sección se le solicita al usuario datos personales, como por ejemplo sus nombre, apellidos, dirección de residencia, teléfonos, país, etc. Así como también el método de pago que desea utilizar, y en caso de ser por medio de tarjeta de crédito/débito en un sitio web normal, se le solicitará que digite los datos de la tarjeta a utilizar; pero en este caso, aparte de ingresar los datos tradicionalmente, existirá una opción en la que el cliente solicite que le sea marcado a un número telefónico. Por lo tanto, deberá ingresar un número de teléfono válido al cual poder ser contactado en esos momentos.
2. Posteriormente, el servidor web envía el número de teléfono registrado por el cliente a la planta telefónica, el cual se encargará de llamar al cliente y solicitar los datos de la tarjeta de crédito/débito. En la planta telefónica reside un software encargado de realizar la llamada telefónica de forma automática. Tanto el sitio web como la planta telefónica no necesariamente tienen que estar separados; pueden estar ubicados en un mismo servidor, pero por razones de rendimiento y por separación de roles que realizan cada uno, pueden separarse.
3. El paso siguiente es cuando la planta telefónica realiza la llamada al teléfono del cliente, solicitándole los siguientes datos:
    a. El número de la tarjeta, ya sea de crédito o de débito. Generalmente este número es de 12 dígitos.
    b. La fecha de expiración de la tarjeta, estos corresponden al número de mes (Ej.: "01" para enero, "02" para febrero, etc.) y los dos últimos dígitos del año (Ej.: "14" para el año 2014).
    c. El código de seguridad de la tarjeta, también llamado CVV (card verification value) o CVC (card verification code), entre otros. Este código, por lo general está ubicado en la parte posterior de la tarjeta, y dependiendo de quién es el emisor de la tarjeta, (Ej.: VISA, Mastercard, etc.), así variará el número de dígitos, o inclusive también puede variar la ubicación y encontrarlo ubicado en la parte del frente de la tarjeta.

    El cliente no siempre va a conocer los datos que se le están solicitando, y en ocasiones tampoco sabrá dónde están ubicados. Es por eso que al momento de solicitar la llamada telefónica (en el primer paso) le aparecerá una ventana informativa explicándole los datos que le serán solicitados, la ubicación de estos y la forma en que serán digitados en el teléfono; de esa manera el usuario tendrá una guía.
4. En este punto, el cliente ingresa los datos solicitados, discando en el teléfono por medio del teclado numérico. Al finalizar, al cliente se le dictará un código, al cual se le ha llamado "Código Dictado por Teléfono" (CDT). Este código deberá ser digitado en la página del sitio web donde se esta realizando la compra. Los propósitos de este código son dos: el primero, como forma de que la planta telefónica manifiesta que los datos han sido recibidos; y el segundo es el de agregar un nivel adicional de seguridad al verificar que los datos intercambiados son exclusivamente entre el cliente y la empresa del

comercio electrónico. Estos datos, al momento de ser digitados son enviados inmediatamente a la planta telefónica.

5. Una vez recibidos los datos de la tarjeta de crédito, la planta telefónica envía los datos al sitio web.
6. De aquí en adelante el proceso de verificación de los datos de la tarjeta son similares al realizado normalmente en cualquier proceso de compra en línea tradicional. El sitio web envía los datos a un switch, el cual se encarga, en este caso, de ser el intermediario entre el banco y el procesador. Este esquema puede variar; por ejemplo, en lugar de un switch, podría existir una pasarela de pagos directamente proporcionada por el banco, o también podría utilizarse un sistema como Paypal[14], que procesa pagos de comercio electrónico, por lo que cobra una comisión. En general, el sitio web tiene que enviar los datos de la tarjeta de crédito a alguien que verifique aspectos como la validez de la tarjeta, suficiencia de saldo y descargo del monto en el saldo del cliente. Esto frecuentemente no es realizado por el mismo sitio web, sino por un tercero. Los datos viajan a través de internet hacia los servidores pertinentes para ser procesados.
7. En caso de realizarse correctamente la transacción, se pasa un código al sitio web, indicándole que todo esta bien; pero si existe algún problema o inconveniente en la transacción (Ej.: número de tarjeta incorrecta, fondos insuficientes, etc.), entonces se pasa un código al sitio web indicándole el tipo de error ocurrido.
8. Finalmente, el cliente es informado de que la transacción ha sido realizada satisfactoriamente o si ha ocurrido un error, y de ser este último, se puede realizar el proceso nuevamente desde el primer paso.

Cabe mencionar que el flujo mostrado anteriormente es uno de varias configuraciones que puede tener, por ejemplo, el servidor web y la planta telefónica, que pueden residir en un mismo servidor; así como también la parte encargada de validar la tarjeta de crédito/debito puede variar, ya sea que pertenezcan a una institución bancaria, y al momento de validar la tarjeta se debe conectar con ellos, o bien puede ser una pasarela de pago como Authorize.net o FistData.

La decisión a tomar dependerá de algunos factores: uno de ellos es si el servicio de validación es compatible con la plataforma que se ha escogido para realizar el sitio web del vendedor y si esa forma de compatibilidad incluye bibliotecas de código disponibles para que la programación pueda realizarse entre el sitio de validación y el sitio web del vendedor.

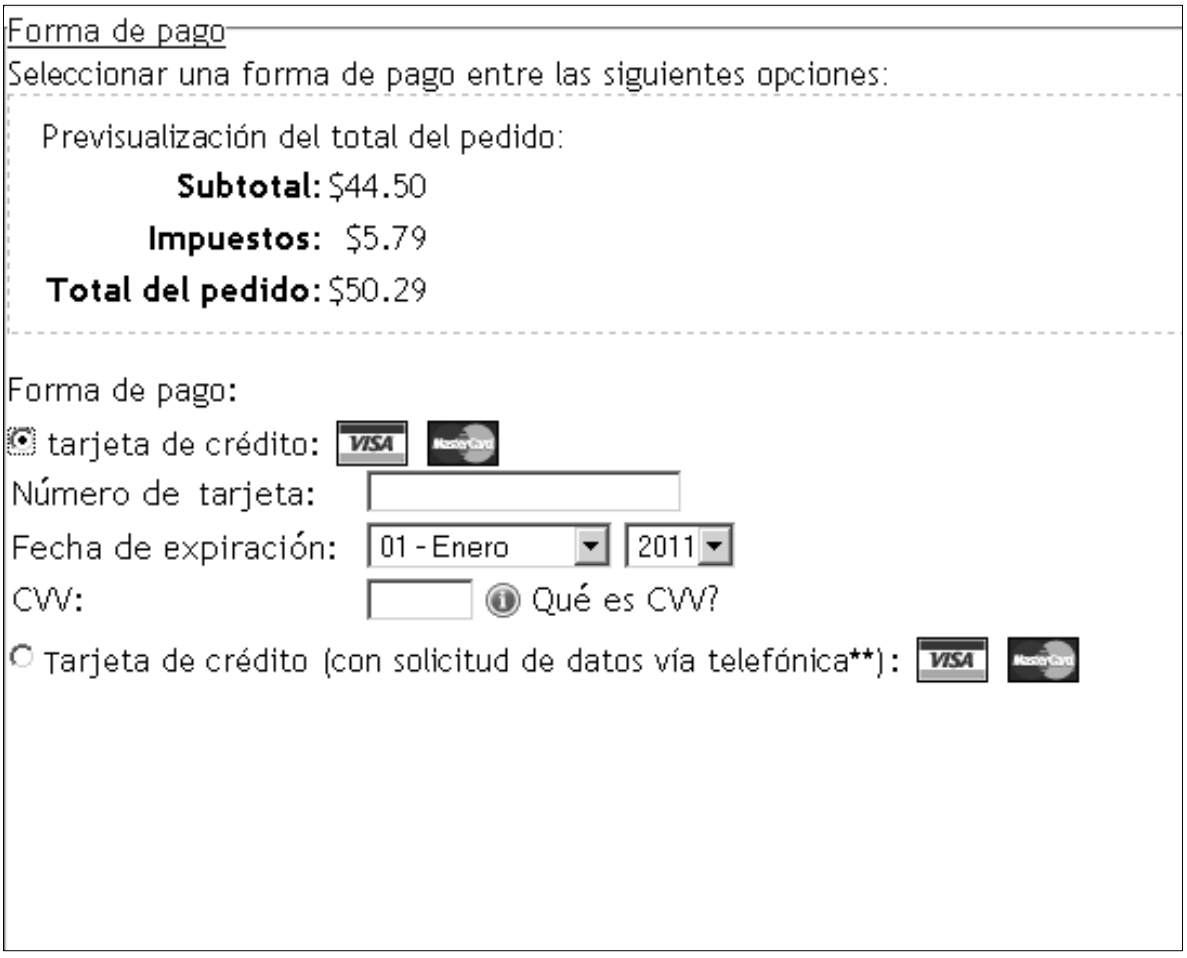
Otro aspecto que influye en seleccionar el tipo de validador de las tarjetas es el precio. En este punto el precio incluye tanto el servicio, que generalmente es una cuota fija ya sea anual o mensualmente; así como también en algunos casos se incluye el costo por transacción realizada, y en otros casos se agrega también un porcentaje de acuerdo a la transacción efectuada. El aspecto económico de la propuesta se ve más a detalle en el capítulo siguiente.

[14] Paypal. http://www.paypal.com [consultada el 22/04/2011].

Continuando con el funcionamiento, es necesario tocar algunos puntos técnicos importantes de la propuesta: uno de ellos es detallar la forma cómo se comunica el servidor web (que aloja el sitio de comercio electrónico) con la planta telefónica y viceversa.

En principio, al momento en que el usuario se encuentra en la pantalla de checkout, le aparecerán dos opciones de formas de pago con tarjeta: la primera es la forma cómo se hace en cualquier sitio web por medio de un formulario, y la segunda por medio de una llamada telefónica; si el usuario selecciona ingresar los datos de la tarjeta de crédito por medio del formulario tradicional, tal como se muestra en la figura 8, se le solicitará ingresar el número de tarjeta, el mes y el año de expiración, así como el código verificador CVV.

Figura 8: Ingreso tradicional de datos de tarjeta de crédito

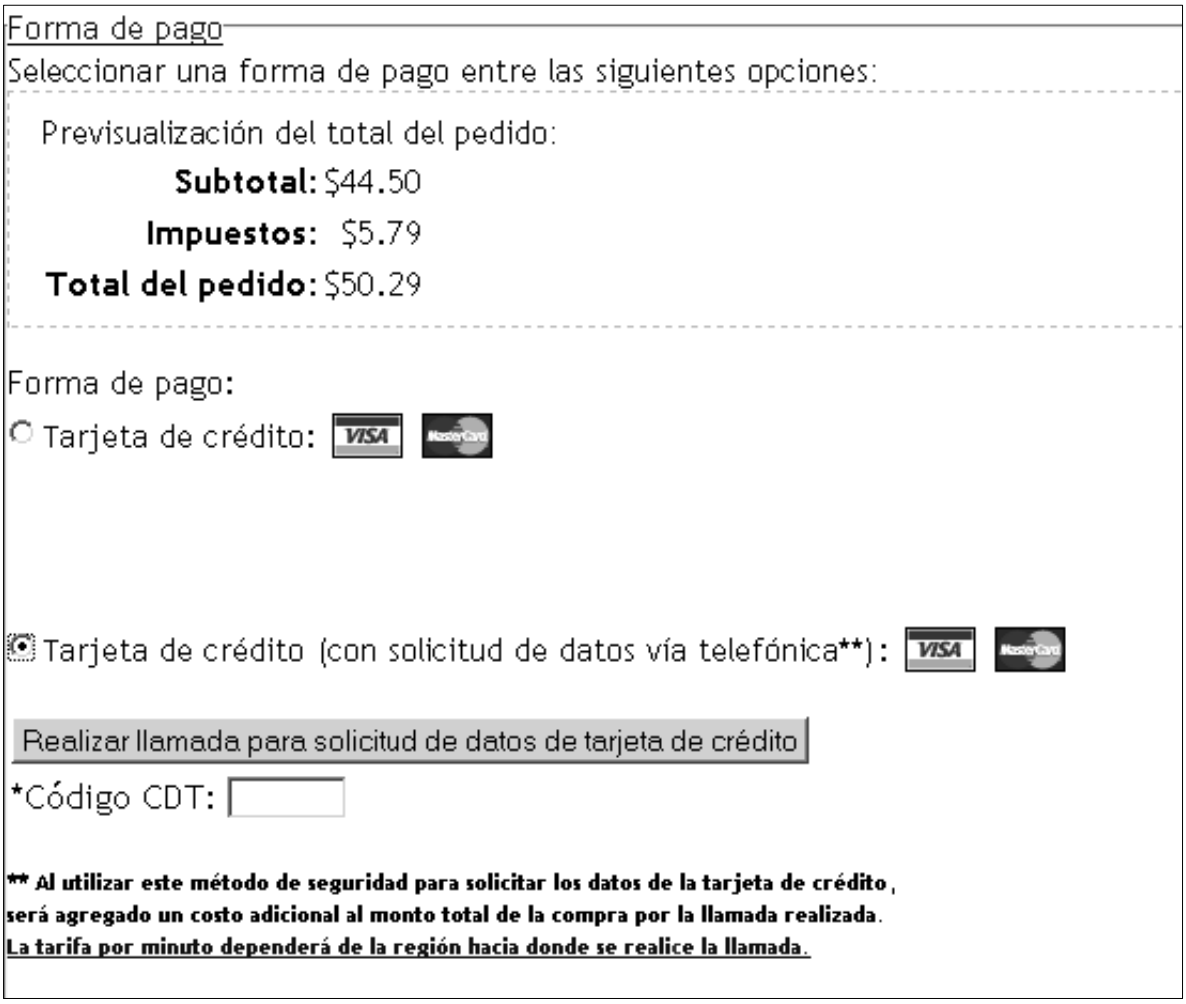


Fuente: Creación propia.

Pero si el usuario selecciona la opción propuesta en el presente documento, la cual consiste en solicitarle los datos de tarjeta de crédito por medio de una llamada telefónica que le realizará el sistema, tal como se muestra en la figura 9, se mostrará

un botón, el cual al presionarlo se realizará una llamada al usuario solicitándole los mismo datos mencionados en la opción anterior.

Figura 9: Ingreso de datos de tarjeta de crédito solicitados por medio de telefonía



Fuente: Creación propia.

Junto con el botón para solicitar la llamada, aparecerá un campo llamado “Código CDT”, el cual se le dictará al usuario al finalizar la llamada.

También aparecerá un mensaje advirtiendo al usuario que dicha opción tendrá un costo adicional que será cargado al monto total de la compra.

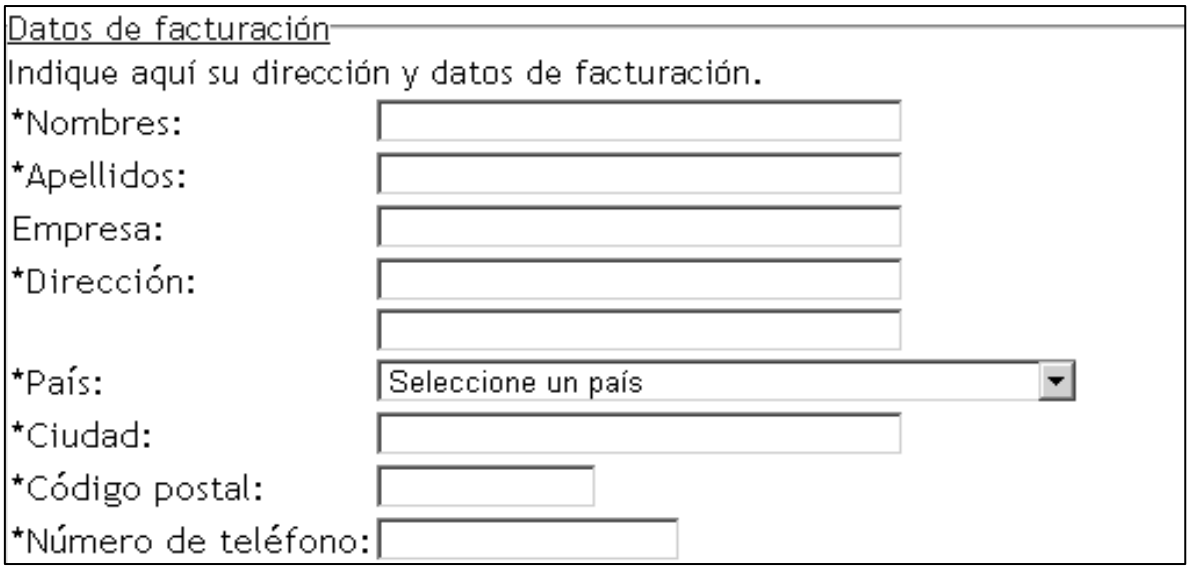
En el preciso instante en que el usuario presiona el botón para solicitar la llamada el servidor web envía una serie de datos a la planta telefónica; pero antes de detallar los datos enviados es necesario recordar quién hace el papel de planta telefónica, y ese es el software llamado Asterisk, que es extremadamente flexible, tanto es así que puede convertirse de una simple computadora a una planta telefónica multiusos capaz de interconectarse con otros sistemas, e inclusive poder programarle

pequeños programas para realizar tareas específicas. Con esta breve explicación de lo que puede hacerse con Asterisk, se entenderá mejor su funcionamiento.

Continuando con la explicación, entre los datos enviados del sitio web a la planta telefónica Asterisk se encuentran: primero, un canal (channel) que le sirve a la planta telefónica para saber por cual de los n canales disponibles se puede realizar la llamada. En Asterisk las llamadas pueden salir por diferentes canales, siendo estos canales IP que se conectan a redes IP, como por ejemplo internet, o bien por canales conectados a líneas telefónicas tradicionales análogas. Asterisk puede configurarse inclusive para que tenga más de un canal por donde realizar las llamadas, siendo cada uno de ellos de diferentes proveedores de telefonía, y aprovechar esta ventaja para que, dependiendo del número a donde se realizará la llamada, así seleccionar el canal que represente el menor costo para la empresa; por ejemplo, si el número es de una compañía X, entonces seleccionar el canal de salida donde el costo por minuto de llamada sea de menor valor para números de esa compañía.

Otro dato que es enviado a la planta telefónica es el número de intentos para poder contactar al cliente. Puede darse el caso de que el usuario no conteste la llamada, ya sea porque el número ingresado es incorrecto o por cualquier otro motivo. En esos casos, si se piensa en negocio, la empresa podría decidir cobrar por el intento de llamada realizada, pero que no fue contestada por parte del usuario; o bien podría cobrarse por intento de llamada adicional (aparte del costo por minuto de duración), es decir que si por ejemplo al realizar dos intentos de llamadas, y estos no son satisfactorios, entonces a partir del tercer intento se agregará un costo adicional. Junto con este dato van también de la mano los dos siguientes: el número de segundos que la planta telefónica esperará a que el usuario conteste antes de dar por finalizado un intento, y el número de segundos que transcurrirá para que la planta telefónica espere entre un intento y otro para volver a realizar la llamada. Y por último, un dato que no puede faltar es el número de teléfono hacia donde se realizará la llamada. En este último dato, se le antepone todo lo necesario para realizar llamadas fuera del país; y dependiendo del país que el usuario ha seleccionado en el formulario de los datos de facturación, como se muestra en la figura 10, así se antepone el código de país correspondiente.

Figura 10: Formulario de datos personales al momento de checkout

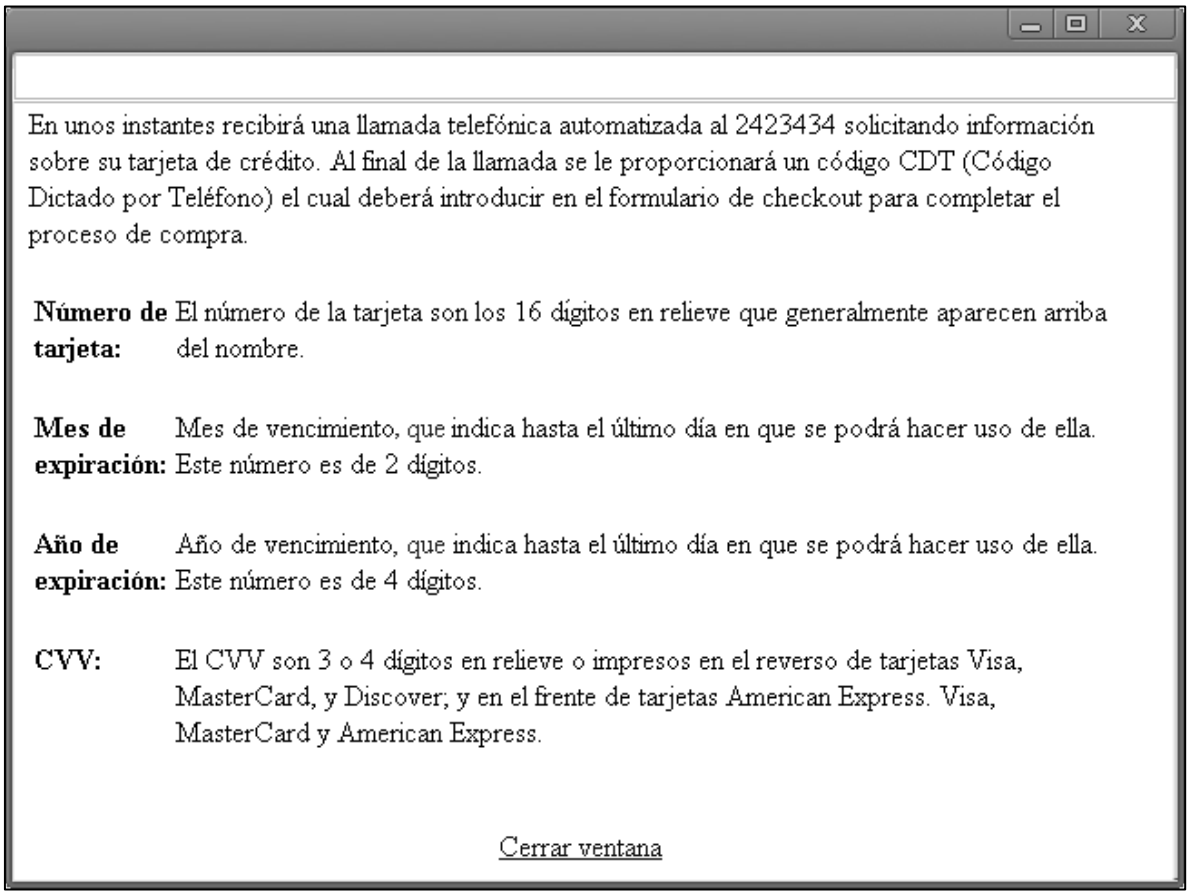


Fuente: Creación propia.

Todos estos datos son puestos en un archivo dentro de una carpeta especial en Asterisk, generalmente llamada “outgoing”, la cual al identificar la existencia de archivos dentro de ella estos son leídos e inmediatamente se realiza una llamada según los datos de cada archivo.

Cuando el usuario recibe la llamada, la planta telefónica comienza a reproducir un mensaje pregrabado, donde se da un breve saludo y se le explica al usuario los datos que debe ingresar y la manera de digitarlos, comenzando primero por el número de tarjeta de crédito, luego con la fecha de expiración (mes y año) y finalmente el CVV. Cada dato está programado para ser capturado de acuerdo al número de dígitos que estos tienen, y así evitar errores, por ejemplo, para el número de tarjeta de crédito el sistema espera que el usuario digite 16 dígitos, para el mes de expiración espera que digite 2 dígitos, y así sucesivamente. En caso el usuario no tenga conocimiento de lo que tiene que digitar, aparecerá una ventana donde se le explica que es cada dato y como digitarlos desde celular, tal como se muestra en la figura 11.

Figura 11: Ventana informativa al momento de realizar la llamada



Fuente: Creación propia.

Al terminar de digitar todos los datos solicitados, la planta telefónica le dictará el código CDT, cuyo significado es “Código Dictado por Teléfono”, que servirá para que el usuario lo digite en el formulario de checkout (ver figura 9), confirmando así que los datos han sido ingresados completamente, y permitiendo pasar al siguiente paso de la transacción, donde los datos son procesados y verificados por las partes correspondientes a dichas tareas. Se puede observar que el procesamiento y la verificación de la tarjeta de crédito no dependen del tipo de pago que ha seleccionado el usuario, ya que siempre los datos son pasados al sitio web y éste los delega para procesarlos y verificarlos.

CAPÍTULO IV

PROPUESTA

La idea de agregar seguridad al comercio electrónico utilizando telefonía se basa en el hecho de que, como se menciona en el capítulo II, si una persona ingresa datos en una página de internet, estos datos pueden ser capturados, ya sea por un hacker utilizando cualquiera de las técnicas para capturar información, o por un malware (Ej.: virus de tipo caballo de Troya), que en ambos casos los datos son capturados y finalmente van a caer en manos de otras personas. Por lo tanto, al ingresar los datos y que estos viajen por un medio telefónico, los métodos de intercepción de datos por delincuentes, mencionados anteriormente, quedan sin razón de ser, porque para que tengan efecto, estos datos deben ser digitados en la computadora, específicamente en el sitio web de la transacción. Para interceptar los datos por medios telefónicos el atacante debería interceptar la llamada entre ambos puntos (el cliente que está comprando y el sitio web del vendedor que realiza la llamada), cosa que no es imposible, pero que le dificulta de gran manera al atacante el realizarlo en comparación a las técnicas tradicionales ya mencionadas.

La conceptualización de la idea anterior se fundamenta en uno de los principios de seguridad, que también es mencionado en el capítulo II, donde se dice que la seguridad informática está basada en mantener la confidencialidad, integridad y disponibilidad de los datos. En este caso, enfocando el trabajo en dos de los tres aspectos, y procurando que los datos enviados por medio telefónico mantengan tanto su integridad, para que no sean alterados, como su confidencialidad, para que no sean vistos o interceptados por terceros.

En todo proyecto es importante siempre la parte económica, y para éste no es la excepción. En una configuración como la propuesta, se pueden tomar precios actuales del mercado y estimar un presupuesto, tal como se muestra en la tabla 2. Ahí puede observarse la inversión inicial en hardware, software y mano de obra para la implementación de todo el sistema.

Tabla 2: Presupuesto para la implementación

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	TOTAL
INVERSION			
Servidor PowerEdge 2970: Six Core @2.2Ghz,32Gb,3x1Tb	1	$5,179.00	$5,179.00
Tarjeta digital Digium 1TE122BF T1/E1/J1/PRI PCI, con cancelación de eco.	1	$803.00	$803.00
Instalación	40 (horas-	$80.00	$3,200.00

	hombre)		
Software	0	$0.00	$0.00
		Subtotal	$9,182.00
		IVA	$1193.66
		TOTAL	**$10,375.66**
GASTOS FIJOS			
Mantenimiento	5 (horas-hombre mensuales)	$60.00	$300.00
Cuota por enlace E1	1 cuota mensualmente	$165.00	$165.00
		Sub-Total	$465.00
		IVA	$60.45
		TOTAL	**$525.45**

Fuente: Con base en cotizaciones de proveedores. Los precios podrían variar según los costos de los proveedores y la infraestructura cotizada.

Cabe mencionar que el presupuesto de la implementación mostrado en la tabla 2 es únicamente para la implementación de la planta telefónica y su puesta en marcha; no incluye la implementación del sitio web de comercio electrónico ni el servicio entre el sitio web y el procesamiento de las tarjetas, ya que la alternativa propuesta en este documento se enfoca en agregar una medida adicional a la captura de los datos de tarjeta de crédito y no en la implementación de todo el sitio de comercio electrónico. Se asume que al momento de la implementación ya se cuenta con un sitio web donde se venden productos y/o servicios, el cual se integrará a la alternativa propuesta de seguridad.

Con respecto a la inversión inicial, el servidor es la computadora en la que se instalará el sistema que servirá como planta telefónica. Se propone un servidor con capacidad suficiente como para poder soportar transacciones web y servir al mismo tiempo de planta telefónica.

La tarjeta digital es necesaria para poder conectar la salida del enlace a internet (para este caso, un enlace E1), el cual servirá para realizar las llamadas telefónicas por medio de telefonía sobre IP. Para estas tarjetas existen varios modelos, dependiendo de cuantos puertos esta tenga, tanto para telefonía digital como para telefonía análoga, así variará el precio. Aquí se ha puesto un modelo que tiene un puerto para conectarse a un enlace E1.

La mano de obra está estimada en 40 horas-hombre para la implementación; y el Software tiene un valor de cero, ya que se propone la utilización de software de código abierto y software libre, como Asterisk, para la planta telefónica y Linux como sistema operativo.

En cuanto a los gastos fijos, estos son los que se estarán pagando mensualmente; ahí se menciona el mantenimiento, el cual se estima en cinco horas-hombre mensuales para que el sistema esté funcionando correctamente y pueda dársele mantenimiento tanto preventivo, para evitar problemas, como también mantenimientos correctivos en caso de que sea necesario.

Una parte principal para que todo funcione bien es el enlace por el cual las llamadas telefónicas son realizadas. Aquí se propone un enlace E1 que generalmente es utilizado con este propósito de plantas telefónicas, el cual brinda una capacidad 2Mbps y 30 enlaces simultáneos de voz. Este enlace es el que une al servidor con la telefonía y pone a disposición el recibir como realizar llamadas, que en este caso son las llamadas salientes las que más se utilizarán para contactar al usuario y solicitarle los datos.

También es importante agregar a tal presupuesto una parte variable (gasto variable), que dependerá de las transacciones que se realicen. Para ello se muestran en la tabla 3 las tarifas de consumo telefónico a nivel internacional por minuto, según el destino a donde se realice la llamada telefónica.

Tabla 3: Tarifas de consumo telefónico internacional por minuto según destino

DESTINOS	TARIFAS POR MINUTO
Nacional	$0.039
Estados Unidos y Canadá	$0.090
Hawaii, Alaska, Puerto Rico	$0.090
México	$0.120
Belice	$0.180
Panamá	$0.120
Guatemala, Costa Rica, Honduras	$0.100
Nicaragua fijo	$0.100
Nicaragua móvil: Bell south, Enitel, Satelital, Secom móvil	$0.340
Suramérica	$0.290
Europa	$0.350

África, Asia, Oceanía	$0.500
Caribe	$0.290

Fuente: Con base en cotizaciones de proveedores. Los precios podrían variar según los costos de los proveedores y la infraestructura cotizada.

Se propone que el costo por minuto de llamada realizada al momento de solicitarle los datos de tarjeta al usuario será cobrado dentro del monto de la compra; pero se menciona en el capítulo anterior, y se le mostrará la opción al usuario para que pueda decidir si desea que la solicitud sea por medio de un formulario tradicional o a través de una llamada telefónica.

Si se hacen cálculos, el negocio invertirá $6,759.66 en activo fijo (servidor y tarjeta para enlace E1). Ese monto al depreciarlo contablemente durante cinco años tendría un valor que se irá amortizando mensualmente, de $112.66, el cual sumado a los $525.45 de los costos fijos se tendría un punto de equilibrio de $638.11, cuyo monto tendría que ser por lo menos el mínimo a venderse mensualmente adicional para no obtener pérdidas. Este monto debería ser adicional a lo que el negocio sin la alternativa de seguridad vendería normalmente, ya que el negocio cuenta con un punto de equilibrio propio en cual se basan los precios de los productos o servicios vendidos.

Con respecto a los costos variables, que para este caso se ha contemplado el costo por minuto de llamada, se propone cargárselo al usuario en el monto de la compra total, para que el negocio no absorba dichos costos.

4.1 Análisis costo-beneficio

Pero… ¿qué beneficios trae esta propuesta al negocio?, ¿ayudará al negocio a obtener más ganancias o no? Para responder la primera pregunta puede hacerse la analogía con empresas que, a pesar de que cuentan tanto con vigilantes como con cámaras de seguridad, también adquieren un servicio de seguridad adicional en caso de que suceda algo dentro del negocio (como por ejemplo un asalto): un equipo de policías llega al lugar inmediatamente, fuertemente armados; pero a pesar de estas medidas de seguridad, la empresa también decide instalar detectores de metal en la entrada del negocio para evitar el ingreso de armas. Este ejemplo se puede comparar con una empresa en internet, donde invierten en seguridad para que, tanto el cliente como la empresa, se sientan seguras. Hoy en día hay personas que pagan por seguridad adicional, y más aún cuando se encuentra dinero de por medio, como en las transacciones por internet. De acuerdo a esto, el beneficio es seguridad adicional.

En cuanto a la segunda pregunta, toda inversión se realiza con el propósito de obtener más ganancias, y por lo tanto la propuesta de seguridad adicional está pensada también con ese propósito. Con la propuesta de seguridad se propone que el negocio sea más rentable a medida que más clientes compren en ese sitio, debido

a que el negocio se diferenciará de otros menos seguros. No significa que el negocio venda más, sino que por causa de estar el sitio más seguro genere más confianza en los clientes, y por lo tanto sean más los clientes que compran en ese sitio.

Dado que las inversiones en seguridad informática se justifican en función del riesgo de lo que se está queriendo proteger o asegurar, se puede observar la matriz de la tabla 4 donde se visualizan diferentes tipos de inversión en seguridad informática.

Tabla 4: Matriz de tipos de inversión en seguridad informática.

RIESGO/VISIBILIDAD	**Alto**	*Proyecto Estratégico*	*Proyecto de Actualización*
	Bajo	*Proyecto de Negocio*	*Proyecto Cotidiano*
		Alto	**Bajo**
	IMPACTO/GANANCIA		

Fuente: Remenyi, A.H. Money y M. Sherwood-Smith. (2000). The effective measurement and management of IT costs and benefits. Butterworth-Heinemann.

El cuadrante que interesa tomar en cuenta para el presente documento es el de "Proyecto de Negocio", donde **proyectos de este tipo tienen un alto impacto frente a la competencia y mucho valor agregado para el cliente**.

El negocio debe de tener claro lo que está dispuesto a ceder y aceptar frente al tema de seguridad, asi como lo que esperará del mismo, **cuyo factor clave desde el punto de vista del cliente y la organización son la confianza y valor agregado.**

En un enfoque más amplio de la seguridad informática, un análisis costo-beneficio para una inversión de ese tipo debe enfocarse en la inseguridad informática, es decir, cuantificar en términos de dinero el costo que tendría un accidente de seguridad informática, si llegase a suceder, frente a la inversión realizada para mitigar dicho accidente.

En la décima segunda edición del reporte anual presentado en el 2011 por CyberSource acerca de tendencias de fraudes en pagos en línea[15] realizada a un grupo de comerciantes en Estados Unidos durante un período del año 2010, se muestra que para ese año tenían un promedio de 0.9% de pérdidas sobre los ingresos debido a fraudes en línea. Esto nos da la información para poder estimar de forma cuantificable un análisis de costo-beneficio para el modelo propuesto. Por ejemplo, si un negocio tiene ingresos mensuales por ventas en línea de $100,000 su estimación de pérdidas por fraudes en línea sería de $900; por lo que el análisis de costo-beneficio sería de la siguiente manera:

[15] CyberSource. 2011 Online Fraud Report.
http://forms.cybersource.com/forms/FraudReport2011NACYBSwww2011. [consultada el 02/09/2011].

$$\text{Costos / Beneficios} = 638.11/900 = 0.70$$

$$\frac{638.11}{900} = 0.70$$

Lo anterior demuestra que, en este caso si se tiene factibilidad económica, ya que los beneficios son mayores que los costos. Si la razón obtenida hubiera sido mayor de 1.0, entonces la propuesta no hubiera sido factible económicamente.

El análisis costo-beneficio para el modelo propuesto en el presente documento puede resumirse de la siguiente manera:

$$\frac{638.11}{(Ingresos\ por\ ventas\ en\ línea\ mensuales) \times 0.009}$$

Donde *638.11* representan el total de los costos mensuales de la inversión, *"Ingresos por ventas en línea"* representan los ingresos obtenidos por ventas en línea, y *0.009* representa la estimación del porcentaje que esos ingresos obtengan pérdida por fraudes en línea.

Para finalizar, no esta de más mencionar que la tecnología de telefonía por medio de voz sobre ip puede ser utilizada de muchas maneras, aunque en nuestro país aún no se ha explotado lo suficiente. El hecho de que en Asterisk puedan programarse tareas especificas y la gran flexibilidad que este software tiene, puede ser de gran beneficio para un negocio, por mencionar una de sus utilidades: el automatizar encuestas. Imagine que necesita realizar una serie de encuestas a un número determinado de personas; esto puede realizarse dejando programado Asterisk para que realice las llamadas automáticas, y utilizando el mismo procedimiento de cuando el usuario digita los datos de tarjeta en el comercio electrónico, así también una persona podría digitar sus preferencias o datos que se necesite investigar.

Aplicaciones para el comercio electrónico también podrían mencionarse. Imagine el escenario donde usted recibe una llamada telefónica informándole que el producto que usted compró por internet ya fue despachado, e inclusive puede recibir una llamada notificándole que el producto ya está en aduanas, listo para ser retirado e indicándole el monto a pagar por conceptos de impuestos.

Como se muestra, muchas aplicaciones puede tener esta tecnología; y como dice una frase muy conocida: "El límite es la imaginación".

Para ver una demostración de la alternativa de seguridad para comercio electrónico propuesta en este documento, puede dirigirse a la URL siguiente: http://luispolainas.blogspot.com/2011/07/captura-de-datos-de-tarjeta-de-credito.html

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- A medida que una empresa tenga más barreras de seguridad al momento de realizar una transacción en el comercio electrónico, ésta será menos propensa a fraudes informáticos.
- La tecnología actual de voz sobre IP tiene la capacidad y la flexibilidad como para que las empresas puedan sacar el máximo provecho a su favor.
- Actualmente no existe total confianza por parte de los usuarios en realizar transacciones en comercio electrónico.

Recomendaciones

- Las empresas que realizan comercio electrónico deben implementar el mayor número de medidas de seguridad posible. La alternativa de seguridad propuesta en el presente documento ayudará con este propósito, disminuyendo el riesgo a fraudes.
- Utilizar la tecnología disponible de voz sobre ip para aplicarla en necesidades específicas que las empresas puedan tener, con el objetivo de diferenciarse de otras empresas del mismo rubro.
- A las empresas que realizan comercio electrónico, invertir más en seguridad para brindar confianza a sus clientes y a la vez concientizar a los usuarios en su importancia.

BIBLIOGRAFÍA

Darie, C. y E. Balanescu. (2008).*Beginning PHP and MySQL E-Commerce: From Novice to Professional.* Apress.

Del Peso, E. (2001). *Peritajes informáticos*. Díaz de Santos, S. A.

Departamento de Tratamiento de la Información y Codificación del Instituto de Física Aplicada del Consejo Superior de Investigaciones Científicas de España. http://www.iec.csic.es [consultada el 23/05/2011].

EC-COUNCIL. (2009). *Ethical hacking and countermeasures.* Cengage Learning.

Fernández, E. (2004). *Conocimientos y aplicaciones tecnológicas para la dirección comercial.* ESIC Editorial.

Gomillion, D. y D. Dempster. (2007). *Construyendo Sistemas Telefónicos Con Asterisk.* Packt Publishing.

Khare, R. (2006). *Network security and ethical hacking.* Luniver Press.

Meggelen, J. V. et al. (2007). *Asterisk: the future of telephony.* O'Reilly.

National White Collar Crime Center. (2011). 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [consultada el 03/04/2011].

Obaidat, M. S. y N. A. Boudriga. (2007). *Security of e-systems and computer networks.* Cambridge.

Oppliger, R. (2009). *SSL and TLS: theory and practice.* Artech House.

Oram, A. y J. Viega. (2009). *Beautiful security.* O'Reilly.

Qin, Z. (2009). *Introduction to E-commerce.* Springer.

Radu, C. (2003). Implementing *electronic card payment systems.* Artech House.

Rivas, G. y A. Ricotta. (2005). *Seguridad en el comercio electrónico.* Escuela Universitaria de Estudios Empresariales Vigo.

Sanz, J. R. et al. (2008). *Gestión del cobro de las operaciones de venta internacional.* Editorial Club Universitario.

Schneider, G.P. (2003). *Comercio electrónico*. Thomson.

United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport. http://live.unece.org/trade/untdid/welcome.htm [consultada el 04/04/2011].

Remenyi, A.H. Money y M. Sherwood-Smith. (2000). The effective measurement and management of IT costs and benefits. Butterworth-Heinemann.

GLOSARIO

Alojamiento web: Servicio ofrecido donde pueden almacenarse archivos para poder ser vistos desde internet.

Asterisk: Es una PBX de código abierto con capacidades de VoIP.

Base de datos: Conjunto de información que se puede almacenar en más de un archivo o en más de un tipo de registro.

Caballo de Troya: Comúnmente conocido como “Troyano”, es un programa que parece realizar una función cuando en realidad hace algo más.

Certificado digital: Es un adjunto electrónico para un archivo, el cual verifica la identidad de su fuente.

Checkout: Donde los compradores verifican lo que han pedido y pagan por su compra, generalmente con tarjeta de crédito.

Clave pública y privada: Se basan en la utilización de una pareja de claves por parte de cada usuario. La clave privada debe ser custodiada por su propietario y nunca debe darse a conocer a ningún usuario. La clave pública, por el contrario, debe ser facilitada a todos los usuarios con los que queremos establecer una comunicación.

Comercio Electrónico (e-commerce): Intercambio de bienes y servicios por medios electrónicos.

Dominio: Nombre asignado a una dirección IP con el cual se identifica un sitio web en internet.

Enlace E1: Formato de transmisión digital, generalmente con 30 líneas de teléfono y 2 canales de señalización, de 64k cada una.

Etiquetas: Elementos de la sintaxis de HTML para crear páginas web.

HTML: Protocolo de transferencia de hipertexto, encargado de intercambiar información por la web.

Internet: Es una red de redes, es decir, un conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma.

IP: Significa “protocolo de internet” y proporciona a los dispositivos direcciones únicas.

Lenguajes de programación: Conjunto de símbolos, palabras claves y reglas gramaticales para construir sentencias (instrucciones, ordenes) sintáctica y semánticamente correctas.

Malware: Tipo de software malicioso que realizan diversas tareas no autorizadas una vez que entran a la computadora.

PBX: En ingles “Private Branch Exchange”, donde terminan todos los circuitos eléctricos de unión con los abonados, verificándose en ella su selección e interconexión, así como otras funciones, por ejemplo: información del abonado de si puede efectuar una llamada, indicar la ocupación total de los enlaces, etc.

PHP: (Procesador de hipertexto). Lenguaje de programación interpretado, orientado a la web.

Pharming: Engaño que redirige a los usuarios a sitios web falsos.

Phishing: Es un fraude que llega a su buzón de correo electrónico pareciendo correspondencia oficial de una compañía importante, y está diseñado para engañarlo a fin de divulgar información confidencial como su número de tarjeta de crédito, número de seguro social o número de cuenta bancaria.

Protocolo de comunicación: Un protocolo es un conjunto consensuado de normas que determinan cómo debe funcionar algo. Estas normas hacen posible que distintos ordenadores repartidos por todo el mundo puedan intercambiar datos.

Spam: Correo no solicitado. Últimamente el spam no solo aplica a correo electrónico sino a cualquier tipo de mensaje no solicitado.

SET: Significa “Transacción Electrónica Segura” y es un protocolo inventado exclusivamente para realizar comercio electrónico con tarjetas de crédito.

Servicio de DNS: Encargado de convertir direcciones IP a nombres de dominio.

Servidor: Es un conjunto de ordenadores encargados de prestar algún tipo de servicio al resto de los usuarios (por ejemplo, correo electrónico, transferencia de archivos, conversación, etc.).

Software: Es un conjunto de programas que gestionan y controlan el hardware. Se encuentran almacenados en dispositivos de almacenamiento, como por ejemplo discos duros.

SSL: Son las siglas de “Secure Socket Layer” y se encarga de crear una conexión entre el cliente y un servidor.

TIC: Tecnologías de la información y la comunicación.

VoIP: Es el protocolo de voz por internet, y transmite conversaciones de voz sobre la misma.

ANEXO 1

DEFINICIONES DE TIPOS DE QUEJAS[16]

De no entrega de pago / mercancías (no subasta): El comprador no recibió los elementos comprados, o el vendedor no recibió el pago de los artículos vendidos.

FBI relacionados con estafas: Estafas en la que un criminal se hace pasar por el FBI para defraudar a las víctimas.

El robo de identidad: El uso no autorizado de información de identificación personal de la víctima para cometer fraude u otros delitos.

Delitos Informáticos: Delitos que se dirigen a redes de computadoras o dispositivos directamente, ó 2) delitos facilitados por redes informáticas o dispositivos.

Fraudes varios: Variedad de estafas significativas para defraudar al público, tales como estafas para trabajar desde casa, sorteos y concursos fraudulentos, asi como otros esquemas fraudulentos.

Fraudes de adelantos de pago: Criminales que convencen a la víctima de pagar una cuota para recibir algo de valor a cambio, pero en realidad no dan nada de valor a la víctima.

Spam: Correos masivo no solicitados producidos en serie.

Subastas fraudulentas: Las transacciones fraudulentas que ocurren en el contexto de un sitio de subastas en línea.

Fraude de tarjetas de crédito: Cargos fraudulentos y/o no autorizados de mercancías y servicios a una víctima por medio de tarjetas de crédito.

Fraude de pago en exceso: Un incidente en el que la víctima recibe instrucciones de depositar dinero en una cuenta de banco, y los fondos en exceso o un porcentaje del dinero depositado será enviado de nuevo a la víctima.

[16] Internet Crime Complaint Center (IC3). “Reporte para el año 2010”. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [consultada el 04/04/2011]

ANEXO 2

CATEGORÍAS Y SUBCATEGORÍAS DE LAS QUEJAS[17]

Fraude de adelantos de pago	Fraude de inversiones
Subastas fraudulentas	Fraude de inversiones
Fraude en las subastas - Quejas del Consumidor	Esquemas de pirámide
Fraude en las subastas - Falsas	Fraudes varios
Fraude en las subastas - Falsificación de pago	Fraudes varios
Fraude en las subastas - Devoluciones fraudulentas	Fraude al Consumidor no de subastas - Otros
Fraude en las subastas - Fondos insuficientes	De no entrega de pago / de mercancías (no subasta)
Fraude en las subastas - Cuenta no existente	Fraude de pago en exceso
Fraude en las subastas - No entrega	Frude de Pago (cheques sin fondos, cuenta no existente, los fondos son insuficientes o inexistentes)
Fraude en las subastas - No Pago	Fraude por falta de pago (otros)
Fraude en las subastas - Otros	No subasta - No Pago
Fraude en las subastas - Fraude de pago – Otros	No subasta - El pago robado
Fraude en las subastas - Robos	No subasta - Cuenta no existente
Fraude en las subastas - Pago robados	No subasta - Fondos insuficientes
Las compras de subastas no autorizadas	Las compras no autorizadas (sin tarjeta de crédito)
Chantaje o extorsión	Pornografía / material obsceno
Chantaje	Pornografía Infantil

[17] Internet Crime Complaint Center (IC3). "Reporte para el año 2010". http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf [consultada el 04/04/2011]

Extorsión / correos	Obscenidad
Fraudes por caridad	Poner a disposición material sexualmente explícito para menores de edad
Quejas del Consumidor (no subasta)	Solicitud sexual / Comunicaciones obscenas con menores de edad
Falsificación	Transmitir material obsceno a menores de edad
Suplantación de identidad	Abuso sexual
No subasta - Falsificación de pago	Acoso sexual
No subasta - Devolucines fraudulentas	Delitos sexuales – Otros
No subasta - Entrega de productos falsos	Atraer / Viajar
Fraude por Tarjeta de Crédito	Prostitución (NIBRS: delitos de prostitución)
Destrucción / Daños / Vandalismo de la Propiedad (incluyendo delitos informáticos)	Fraude de relación
Adware	Fraude de alquiler
Abuso de equipo (otros o desconocidos)	Fraude de alquiler - No su propia casa
Virus de computadora	Fraude de alquiler – Otros
Spyware	Fraude de alquiler - Pago en exceso
Robo de servicios computacionales (este delito casi siempre consiste en piratería informática)	Spam
Hacking	Delitos de robo de propiedad
Hacking de la cuenta	La piratería musical
Drogas / Delitos de Estupefacientes	La piratería de software
Tráfico de drogas	No subasta - Venta de Bienes Robados
El tráfico de drogas con receta	Infracción en línea de derechos de autor
Fraude de empleos	Amenazas Terroristas (5 subcategorías)
Las estafas relacionadas con el FBI	Amenaza Terrorista
Delitos por juegos	Terrorismo (otros)

De juego en línea	Financiación del terrorismo
Juegos de Azar	Terroristas de Información
Robo de identidad	Reclutamiento de terroristas
El robo de identidad - el tráfico de información de identificación	
Robo de identidad	
Negocios ilegales	
Otros negocios ilegales	
El tráfico de mercancías ilegales (venta de cosas que han sido robados o falsificadas)	
Intimidación (amenazas no relacionadas con el terrorismo y el ciber-acoso)	
Otras conductas amenazantes	
Amenaza	
Cyber-Stalking/Abuso en foros	