UNVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

LICENCIATURA EN INFORMÁTICA ADMINISTRATIVA

“PROPUESTA PARA QUE LAS EMPRESAS DEDICADAS A E-COMMERCE USEN EL PROTOCOLO SECURE ELECTRONIC TRANSACTION “SET” PARA BRINDAR SEGURIDAD EN LAS TRANSACCIONES”

TESIS PRESENTADA POR:

YOSELIN MONSERRAT SANCHEZ CASAS

PARA OPTAR EL GRADO DE LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

ASESOR:

M EN A. JUAN CARLOS MONTES DE OCA LOPEZ

REVISORES:

LIA. ALEJANDRO DOMINGUEZ BOND

MTI. JORGE IGNACIO PÉREZ MORALES

"2014, 70 Aniversario de la Autonomía ICLA-UAEM"

TOLUCA ESTADO DE MEXICO, SEPTIEMBRE 2014

Índice de Abreviaturas

HW: Hardware;

SW: Software;

SI: Sistema de Información;

B2B: Business to Business;

B2C: Business to Consumer;

C2C: Consumer to Consumer

P2P: Person to Person;

B2A: Business to Administration;

C2A: Ciudadano y administración;

PKY: infraestructura de clave pública;

SET: Secure Electronic Transaction;

SSL: Secure Sockets Layer;

TDC: Tarjeta de Crédito;

TLS: Transport Layer Security Protocol.

Índice de Gráficos

Tabla de contenido

Introducción

La seguridad es un elemento primordial en los sistemas informáticos actuales. Preservar la información y la integridad de un sistema informático es muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer.

Y por tal motivo, es de gran importancia implementar protocolos de seguridad informática en empresas dedicadas a e-commerce para brindar Seguridad en las Transacciones, como en el presente trabajo de investigación, que se propone implementar el Protocolo Secure Electronic Transaction “SET”, que significa Transacción Electrónica Segura. Siendo este un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red, ofreciendo un grado de fiabilidad razonable, que es en lo que se basa todo tipo de seguridad informática, en el conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático.

El proyecto propone un protocolo fiable para erradicar problemas de inseguridad en las transacciones electrónicas. Y cabe mencionar que su desarrollo se llevó a cabo por medio de un análisis de diferentes autores que abordaron la misma temática, los cuales se mencionan en la bibliografía.

Capítulo 1: Marco Teórico

1. E-commerce

En la actualidad, el uso de e-commerce ha incrementado considerablemente, por medio de él podemos realizar transferencias electrónicas, comprar algún producto o simplemente navegar para realizar consultas, en donde en tiempos remotos, no existía esta posibilidad y todo era más complicado. Ante esta situación, podemos realizar fácilmente compras, ventas o intercambio de información a través de las redes de comunicación, como Internet; y nos brinda una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo.

El comercio electrónico en Internet irrumpió con gran fuerza a finales de los 90, prometiendo ser un elemento transformador de la sociedad en el siglo XXI. Aunque su evolución ha sido importante, no ha alcanzado las estimaciones iniciales (Martínez López, Mata Mata & Rodríguez Domínguez, 2009). Y comentan que uno de los principales problemas para este retraso ha sido la falta de herramientas que proporcionan confianza a los usuarios en el uso del modelo de comercio a través de redes de ordenadores.

Afortunadamente con el tiempo han ido surgiendo tecnologías y sistemas de pago electrónico que ofrecen garantías de seguridad e integridad para realizar estas transacciones de una forma fiable y de este modo, dar confianza a los usuarios. Por lo que los autores se enfocan en tres protocolos de pago más utilizados en el comercio electrónico, que brindan este tipo de seguridad buscada; ellos son:

SSL (Secure Sockets Layer), SET (Secure Electronic Transaction) y 3D Secure, con el propósito de disipar las posibles dudas en cuanto a la falta de seguridad en las transacciones electrónicas a través de Internet.

El e-commerce o comercio electrónico, como su nombre lo dice, es la compra-venta de cualquier producto o servicio; y es de gran importancia para cualquier empresa o tienda virtual.

En sentido amplio, lo podemos definir como cualquier forma de transacción o intercambio de información comercial; pero dependiendo del caso, puede tener diferentes acepciones, como por ejemplo: en las transacciones on-line, Domingo (2002) define al comercio electrónico como la aplicación de la tecnología de información avanzada para incrementar la eficacia de las relaciones empresariales entre socios comerciales. Y también menciona que la disponibilidad de una visión empresarial apoyada por la tecnología de información avanzada apoya para mejorar la eficiencia y la eficacia dentro del proceso comercial.

Por otra parte Pivaral Leal & Chajón Arriaza, 2000 definen a e-commerce como cualquier forma de transacción de negocios en la cual las partes interactúan electrónicamente.

Desde el punto de vista de las comunicaciones es el transporte de información, productos y/o servicios o pagos mediante canales de comunicación y redes de ordenadores. Desde la perspectiva de las empresas es una aplicación de la tecnología para la automatización de las transacciones entre organizaciones.

Según la Red Española de centros de negocio local (REDCNL, 2000) el comercio electrónico se puede definir como cualquier forma de transacción comercial en la que un suministrador provee de bienes o servicios a un cliente a cambio de un pago, donde ambas partes interactúan electrónicamente en lugar de hacerlo por intercambio o contacto físico directo (Conde, 2004). Acorde a los servicios es una herramienta que presenta la oportunidad de reducir costos, al igual que tiempo, aumentando así la calidad y la velocidad del servicio prestado. Y finalmente, desde la perspectiva del internauta es la posibilidad de comprar y vender productos y servicios en Internet sin tener que desplazarse.

Pero en términos generales, el e-commerce es una extensión del comercio y la tecnología, que en estos días constituye una forma moderna de hacer negocios que permite reducir costos, tiempos y espacios, y sustituye la interacción presencial entre vendedor y comprador por un flujo de información respecto del bien a vender, el cual también se produce en los dos sentidos, pues el comprador a su vez proporciona información al vendedor (Droguett Ibarra, Paine Cabrera & Riveros Contreras, 2010).

Así como cada autor tiene diferentes significados del e-commerce, se coincide en que es el intercambio de comprar o vender bienes, y es una forma dinámica de realizar cualquier tipo de transacciones vía Internet, en donde intervienen por ejemplo: compradores, vendedores, proveedores, el banco, los clientes, etc.

El comercio electrónico comprende una variedad de tecnologías, como son el intercambio electrónico de los datos, el mismo correo electrónico, las transferencias electrónicas, y los servicios de seguridad informática.

Uno de los objetivos de e-commerce es llevar ideas, servicios o productos a grandes mercados mediante el uso de la tecnología de Internet, ya que el suministrador y cliente interactúan a través de los servicios disponibles en la red, como la web o el correo electrónico.

Por otra parte, existen diversos tipos de productos que se comercializan a través de Internet, los cuales van desde libros hasta realizar pagos bancarios, por mencionar algún ejemplo, pero además de ellos, se comercializan productos como son:

A. Productos físicos: libros, electrodomésticos, juguetes;
B. Servicios: viajes, educación a distancia, etc.;
C. Productos bancarios: transacciones, cuentas, préstamos, depósitos;
D. Productos digitales, como son: noticias, música, software;
E. Otros.

1.1 Ventajas de E-commerce

Ya que e-commerce ahora es reconocido como una fuente principal de ingresos, algunas de las ventajas que brinda son:

A. Ofrece un mercado interactivo gracias a los diversos proveedores que existen, en donde los costos de ventas y distribución tienden a cero, es decir, se reduce de manera progresiva la necesidad de intermediarios;
B. Nos permite tener comunicaciones comerciales vía electrónica, facilitando así las relaciones comerciales;
C. Brinda soporte al cliente, estando disponible las 24 horas;
D. Reduce errores, tiempo y costos en el tratamiento de información;
E. Se facilita la creación de mercados y segmentos nuevos;
F. Permite aumentar la re-compra de productos y servicios (Negocios virtuales, 2013);

Además, otras ventajas que existen son:

G. Comodidad en las compras que realizamos;
H. Las entregas de las compras realizadas son inmediatas;
I. Flexibilidad en los medios de pagos;
J. Otras.

Todas estas ventajas son parte del término e-commerce, el cual engloba un aspecto muy importante, la eficiencia, la cual maximiza sus resultados.

1.2 Desventajas de E-commerce

Así como el comercio electrónico tiene ventajas, cuenta también con pequeñas desventajas, a continuación se mencionan:

A. Falta de seguridad al momento de realizar transacciones;
B. Las empresas dedicadas a e-commerce no brindaban integridad en sus servicios;
C. Pérdida de la privacidad, por lo que muchos usuarios demandan niveles más altos de seguridad, y los clientes en Internet necesitan asegurarse que sus transacciones sean privadas y de confianza;
D. Bajos y remotos niveles de servicio y complejas cuestiones legales.

1.3 Usos y beneficios del e-commerce

E-commerce lo utilizamos de manera habitual dentro de cualquier entorno en que nos desenvolvemos, o en diversas actividades que realizamos, por ejemplo, al efectuar alguna transacción electrónica, al realizar también compras de cualquier producto o servicio para uso cotidiano. En el caso de las empresas, se apoyan de los medios electrónicos para realizar diferentes procesos de compra-venta.

Otros usos que damos a e-commerce son:

A. Realizar transacciones bancarias;
B. Realizar compras y ventas de servicios y productos, por ejemplo la adquisición de algún boleto de avión, la compra de ropa, la reservación de hotel, etc.;
C. Pago de servicios domésticos;
D. Para realizar la consulta de estados bancarios;
E. Algunas empresas usan e-commerce para la creación de canales nuevos de ventas;
F. Acceso interactivo a catálogos de productos, listas de precios y folletos publicitarios;

G. Venta directa e interactiva de productos a los clientes;
H. Intercambio de documentos de las actividades empresariales entre socios comerciales, por ejemplo.

De todo ello, se obtienen diversos beneficios, como son:

A. La reducción del trabajo;
B. Transacciones comerciales más rápidas y precisas;
C. Acceso más fácil y rápido a la información;
D. Navegar para realizar consultas;
E. Comodidad de las compras mediante la Web;
F. Y la reducción de la necesidad de reescribir la información en los sistemas de información;

1.4 Tipos de comercio electrónico

De acuerdo con el criterio de los participantes que intervienen en las transacciones de e-commerce, se distinguen algunas categorías, entre las más importantes se encuentran las siguientes:

A. Empresas B2B, Business to Business;
B. Empresas y consumidor B2C, Business to Consumer;
C. Entre consumidores C2C o P2P, Consumer to Consumer o Person to Person;
D. Entre empresa y administración B2A, Business to Administration;
E. Ciudadano y administración C2A, Citizen to Administration.

Conde (2004) muestra estos cinco tipos de transacciones a través de Internet en el siguiente gráfico:

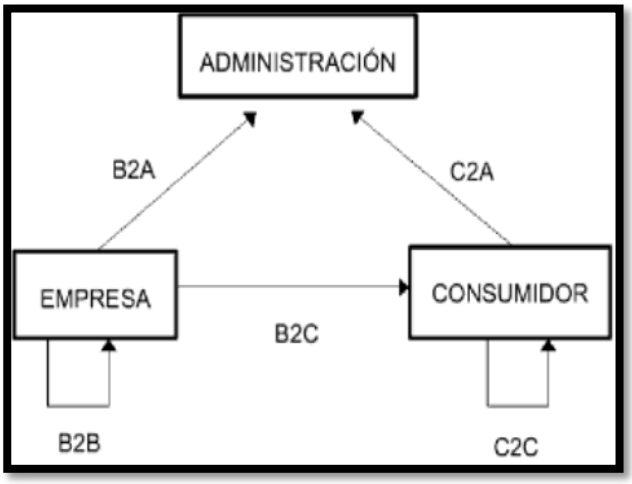

Gráfico 1: Categorías de Transacciones a través de Internet
(Conde, 2004)

De tal forma que el comercio electrónico B2B se refiere a la compra y venta de productos o servicios entre empresas; e-commerce B2C se refiere al proceso de venta electrónica entre la empresa o "tienda virtual" y el consumidor final. En cuanto a e-commerce C2C o P2P se refiere a la compra-venta de productos entre usuarios o consumidores finales. Y por último, e-commerce B2A y C2A engloba los servicios que ofrece las administraciones a empresas o particulares a través de Internet.

Por otra parte Droguett Ibarra et al. (2010) hace referencia a otros tipos de comercio electrónico:

A. Business to Goverment (B2G): comercio electrónico entre empresas y gobiernos. Aquí se optimizan los procesos de negociación y se aplican a sitios o portales especializados en relación con la administración pública.
B. Business to Employee (B2E): e-commerce entre empresas y empleados, se refiere a los procedimientos de RH a través de Internet. Normalmente se aplica por intranets.

C. Government to Government (G2G): e-commerce entre gobiernos, referido al comercio ya sea por prestación de servicios o por intercambio de bienes.

Y añade que dependiendo de la transacción que se lleva a cabo, el comercio electrónico se puede dividir en:

A. Comercio electrónico directo: es aquel en que el bien o servicio se paga y se entrega en línea.
B. Comercio electrónico indirecto: es aquel en el que el bien o servicio no se entrega en línea. Esto incluye el que pueda comprarse y pagarse en línea, pero entregarse directamente.

El comercio electrónico o e-commerce aporta muchos beneficios a las empresas y los clientes, en donde Droguett Ibarra et al. (2010) menciona la presencia global, en que los límites de e-commerce no están definidos por fronteras geográficas, sino por la cobertura de las redes de computadoras. Y otros como el aumento de la competitividad y la calidad del servicio, permitiendo a los proveedores estar más cerca de sus clientes.

E-commerce ofrece productos y servicios personalizados, en donde los proveedores pueden tener información detallada de las necesidades de cada cliente y así ajustar sus productos y servicios.

También e-commerce brinda beneficios como la reducción de tiempo, costos y precios, lo que constituye una de las mayores contribuciones del comercio electrónico. Por mencionar algún ejemplo, los costos son menores, ya que no se necesita realizar gastos de mantención, personal y suministros de una tienda real, todo es virtual. Existen nuevas oportunidades de negocio, nuevos productos y servicios, junto con la redefinición de mercados para productos y servicios existentes, el comercio electrónico también proporciona productos y servicios completamente nuevos.

Cual sea el tipo de comercio electrónico que se efectúe, la Procuraduría Federal del Consumidor. PROFECTO (2012), establece las siguientes medidas de precaución:

Al realizar operaciones comerciales en línea, es importante tener en cuenta los siguientes aspectos:

1. El proveedor debe informar claramente su identidad, denominación legal y datos de ubicación física (dirección, teléfono y fax), para que el ciber-consumidor pueda hacer alguna reclamación (en caso de que se presente algún problema);
2. El proveedor por internet está obligado a brindar una descripción veraz de las características de los productos (para que el consumidor pueda tomar una decisión de compra bien informada);
3. En el caso de los proveedores mexicanos en línea, los precios deben estar expresados en moneda nacional y, en caso de existir cargos adicionales por envío de los productos, se deben señalar claramente, junto con las condiciones y formas de pago;
4. El portal debe declarar sus políticas de privacidad. Esto es importante porque es probable que se requiera al ciber-consumidor que revele datos de carácter privado, como el número de la tarjeta de crédito;
5. También deben estipularse con claridad las políticas de devolución de mercancías, así como las garantías, las condiciones generales de la transacción, restricciones para la compra de bienes y servicios (como es el caso de ubicación geográfica, de tiempo, por tipo de producto o cantidad a adquirir).

1.5 Crecimiento del Comercio Electrónico

Es importante mencionar que cualquiera que sea el tipo de comercio electrónico que se ejerce tiene un crecimiento considerable, ya que en la actualidad es un medio muy utilizado para realizar cualquier tipo de compra-venta. El tipo de comercio electrónico más popular y el más usado es el B2C, por lo que se agregan diversos estudios de éste en los diferentes países.

Estudios realizados en España en el año 2011, aseguran un crecimiento anual del 17,4% en el tipo de comercio electrónico que ejercen, el B2C.

El comercio electrónico B2C en España pasa en términos absolutos de 7.760 millones de Euros en 2009 a 9.114 en 2010, lo que supone un incremento anual del 17,4%, superior al 15,9% del año anterior (ONTSI, 2011).

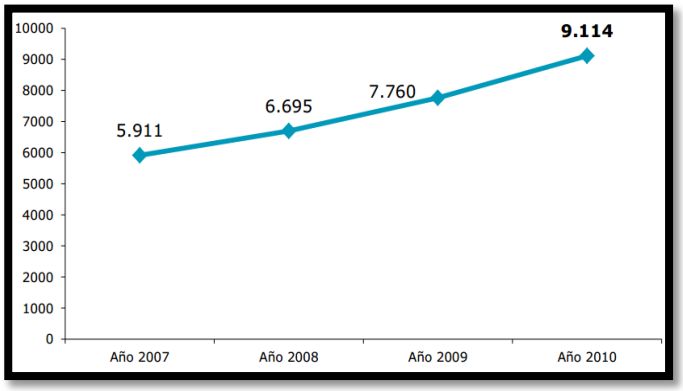

Gráfico 2: El volumen del comercio electrónico B2C (ONTSI, 2011).

Por otra parte, en el año 2012, en las empresas de la unión europea, los países que han aumentado su porcentaje de ventas se compensan con los que lo han disminuido a continuación se muestra el gráfico (Tomás, 2012).

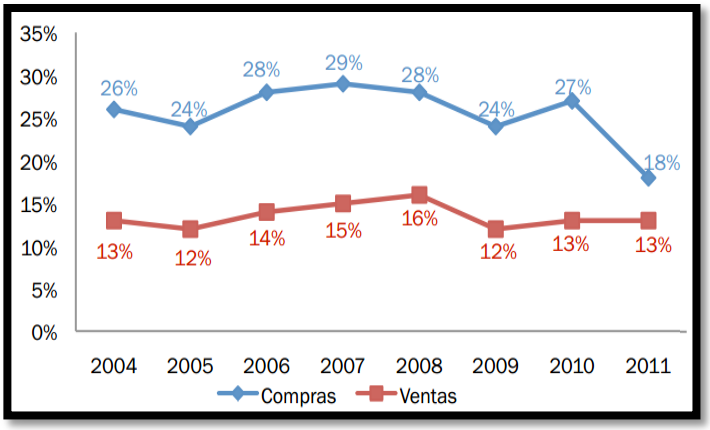

Gráfico 3: Porcentaje de empresas que compran y venden por Internet en la Unión Europea (UE-27), 2004 – 2011
(Tomás, 2012).

BAE (2013) afirma que el volumen de transacciones que se realizan en Argentina por comercio electrónico tendrá un incremento este año del 45% respecto del cierre del 2012, cuando alcanzó los $16.300 millones. Las transacciones durante el año pasado sumaron $16.300 millones; “la mayor parte correspondió a B2C –o entre empresas y consumidores finales–“aseguró.

Por su parte, el gerente de Mercado Shops, en Mercado Libre, Federico Lozano, remarcó que el 61% de la facturación de las empresas en Argentina correspondió a las ventas realizadas por Internet.

Por otra parte, en la actualidad, el crecimiento del e-commerce en 2014 se ha reflejado de manera acelerada, por lo que se anexan estudios de 3 países sobresalientes en este tema: Estados Unidos, México y España (Jannelle, 2014).

Estados Unidos: siendo USA uno de los países punteros en temas de tecnología y en el comercio electrónico ocurre lo mismo. Pese a la problemática financiera que se presentó de manera reciente en ese país, el comercio electrónico no tuvo algún tipo de retroceso y logró que tuviera un crecimiento del 16.9% durante el 2013, con ventas aproximadas a los 263,300 millones de dólares.

La consultora Emarketer tiene como expectativa que para el cierre de este 2014, las ventas generadas en tiendas online logren un crecimiento de 15.5%.

Y recordando que en este país se encuentran grandes sitios de e-commerce como Amazon y eBay, su crecimiento no puede ni debe pasar desapercibido. Además, con el aumento del uso de los dispositivos electrónicos (hablamos de los smartphone y tablets), el comercio móvil o e-commerce sigue tomando una fuerza que pocos esperaban.

Únicamente en el 2013, las ventas por medio de smartphone crecieron casi un 70% en comparación con el año 2012, alcanzando la llamativa cantidad de 42,130 millones de dólares, esperando que en el 2014 sean 57,000 millones. Hablando de tablets, en el año 2014 se espera que las ventas por estos dispositivos alcancen dos tercios de la cantidad total de ventas en el comercio móvil.

En lo que respecta de **México**, este año, las empresas que mejor participación tuvieron en el tema de comercio electrónico en el país fueron Liverpool, con un crecimiento del 15%, seguido por Famsa con un aumento en la venta de sus productos en Internet de un 16%, y para finalizar Palacio de Hierro con un 8%. La importancia de este medio radica en que multinacionales como Wal-Mart, Costco, Liverpool e Inditex han encontrado una estrategia de venta y alternativa real para el aumento de sus marcas.

Con todo esto, en el año 2013, México registró ventas en el comercio electrónico de aproximadamente 121,600 millones de pesos, representando un incremento del 42% en comparación de la cantidad registrada en el 2012.

Se nota un nivel de conocimiento y preferencia por el entorno comercial electrónico, lo que genera oportunidades de crecimiento para las tiendas virtuales que están ingresando o se han mantenido al pie.

Por otra parte, la AMIPCI (Asociación Mexicana de Internet) reporta que en 2014, aproximadamente 63% de las personas que han realizado alguna compra en Internet, lo han hecho por artículos diversos que alcanzan más de $400 pesos por compra, seguido de un 37% que consumen aproximadamente de $400 a $1,000 pesos; 18% lo hacen por artículos de $1,000 a $3,000 pesos; un 5% adquiere productos con valor de entre $3,000 y $5,000 pesos y solo 3% realiza una compra mayor a $5,000 pesos.

Si consideramos que en promedio, una persona desembolsa en promedio $200 pesos en un supermercado, podemos darnos cuenta que el crecimiento del comercio electrónico y sus volúmenes de venta son favorables. Esto se puede deber a promociones especiales realizadas por este medio, o a opciones de compra y envío con mayores facilidades de pago.

España. En el año 2013 el comercio por internet en España ha aumentado, siendo ya cerca de 11 millones de personas las que han realizado algún tipo de compra a través de la web en los últimos 12 meses. Esto supone el 31.5% de la población total.

Entre las causas por las que los consumidores prefieren comprar online el 78.0% argumenta la comodidad de este servicio como una de las principales razones para preferir esta forma de compra el 73.2% argumenta la probabilidad de encontrar ofertas y artículos a un mejor precio y el 65.5%, el ahorro de tiempo que ocasiona no tener que desplazarse físicamente (Instituto Nacional de Estadística, 2014).

(Jannelle, 2014) En este país, el comercio electrónico cerró el 2013 con un histórico en ventas que ascienden a aproximadamente 3,000 millones de euros, equivalente al 20.6% más que el año 2012. Todo lo anterior fue revelado por la Comisión Nacional de los Mercados y la Competencia o CNMC. En cuanto a operaciones totales, se registraron 45.6 millones de operaciones que representa un 24% más que el año pasado.

Las ventas provenientes del extranjero, que recaen en tiendas virtuales españolas, ascendieron a 551 millones de euros, en donde el turismo se llevó la mayor cantidad con más del 60% de los ingresos.

De manera interna, para lo que lleva de este año (2014) creció un 19.5% y supone 41.6% del volumen total del entorno, con 1,325 millones de euros. Las exportaciones españolas facturaron 1,310 millones de euros.

Con lo anterior podemos deducir que abrir una tienda en línea puede ser una oportunidad de negocio que muchas personas pueden tomar para mejorar su economía personal.

1.6 ¿Es seguro el comercio electrónico?

Después de la información acerca del e-commerce y los tipos de comercio, como usuarios y clientes o consumidores de este medio de pagos, compras o transacciones, nos hacemos la pregunta ¿es seguro el comercio electrónico?

Y la respuesta es incierta, ya que es un hecho que la seguridad total tiene un costo infinito y, por lo tanto, no es ni será nunca completamente seguro el comercio electrónico, de la misma forma que no lo es ningún tipo de comercio, lo que si es cierto, es que actualmente, la seguridad en e-commerce aumenta debido a las reglamentaciones existentes que protegen a compradores y vendedores.

En agosto de 2010, surgen informes acerca de la seguridad en e-commerce, en donde ALIGNET (2010) informa que 9 de cada 10 correos electrónicos enviados son fraudulentos “spam”. Los ataques de phishing, los correos electrónicos falsos y las formas de fraude online están aumentando a ratios 20% mensual. Un 78% de los ataques incluye un componente financiero. Los ciber-delitos podrían incluso superar los ingresos del tráfico de drogas internacional. Las tarjetas de crédito son el objetivo principal: 32% de los casos. La información de cuentas bancarias representa el 19% de todos los bienes anunciados para su venta.

A continuación se muestra este ciclo del fraude por Internet (ALIGNET, 2010):

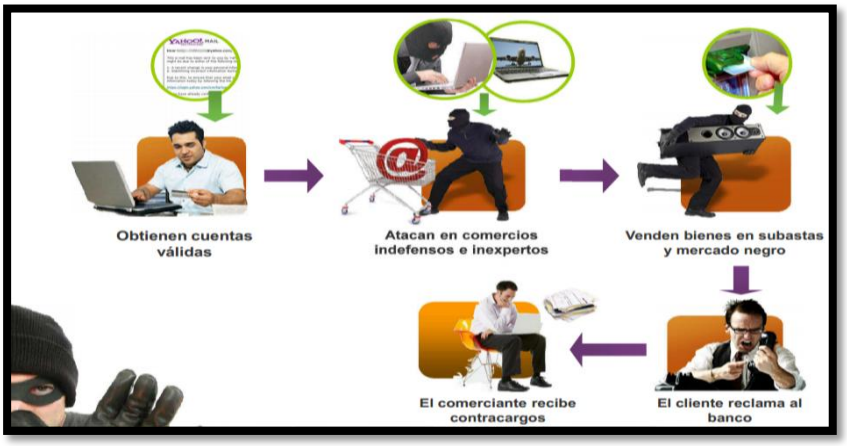

Gráfico 4: Ciclo del fraude en e-commerce
(ALIGNET, 2010)

Es por tal motivo que surge un análisis sobre las razones para no comprar Internet (ONTSI, 2011).

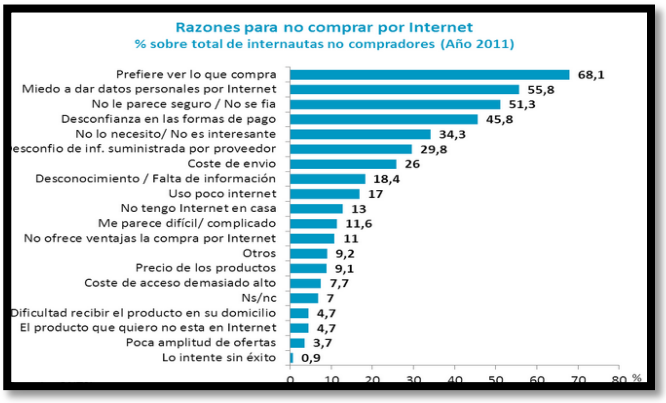

Gráfico 5: Razones para no comprar por Internet (ONTSI, 2011).

De acuerdo al análisis, ONTSI (2011) refleja que el 49.3% de los internautas no ha realizado ninguna compra on-line en el año 2011. La evolución de los datos denota un descenso significativo con respecto al año 2010.

La principal razón aportada por los internautas para no comprar por Internet es la preferencia por poder ver lo que se compra (68.1%) junto con el miedo que suscita Internet en relación a los datos personales o bancarios (55.8%) y la desconfianza en cuanto a la seguridad del comercio electrónico (51.3%).

El perfil de los grupos más alejados del comercio electrónico responde básicamente a las personas entre 15 y 24 años, y a las mayores de 65 años. Con ello, se observa que e-commerce en Internet permite una comunicación interactiva entre los diferentes usuarios que posiblemente no habían tenido ninguna relación anteriormente. Y qué lo que una empresa necesita para hacer e-commerce seguro en la red, es garantizar a los usuarios la identidad, integridad, confidencialidad y no repudio de las transacciones, pues no es muy seguro realizar compras de esta manera y surgen medidas de seguridad respecto al realizar compras por medio de Internet.

Estudios más actuales, realizados por La Procuraduría del Consumidor (PROFECO) y la Asociación Mexicana de Internet (AMIPCI) el 25 de septiembre de 2012, nos garantizan la seguridad de los usuarios al momento de realizar compras electrónicas o al momento de realizar cualquier tipo de transacción, ya sea de tipo bancaria o financiera, ya que se comprometen más a apoyar este punto y bridarnos seguridad al efectuar compras a través de Internet por el convenio firmado, el cual contempla la elaboración de manera conjunta de material informativo adecuado para los usuarios, campañas de orientación sobre el uso de las herramientas de pago, así como información acerca del riesgo de fraude a los que están sujetos los usuarios del comercio electrónico en nuestro país, lo que nos permite como usuarios e internautas estar mejor informados sobre inseguridades y el cómo prevenirlas (AMIPCI, 2012).

Y hay quienes optan por si realizar compras vía electrónica (Instituto Nacional de Estadística, 2014):

Razones para comprar a través de Internet en los últimos 12 meses. 2013

	%
Comodidad	78,0
Precio, promociones u ofertas	73,2
Ahorro de tiempo	65,5
Facilidad de compra	55,6
Facilidad para comparar entre ofertas y obtener información sobre productos	53,1
Mayor oferta, mayor gama de productos	52,8
Rapidez en el suministro	42,8
Único medio disponible	24,8
Por recomendación de otra persona	19,8
Por probar	14,0
Otras razones	9,2

Gráfico 6: Razones para comprar a través de Internet en los últimos 12 meses. (Instituto Nacional de Estadística, 2014)

Principales compras:

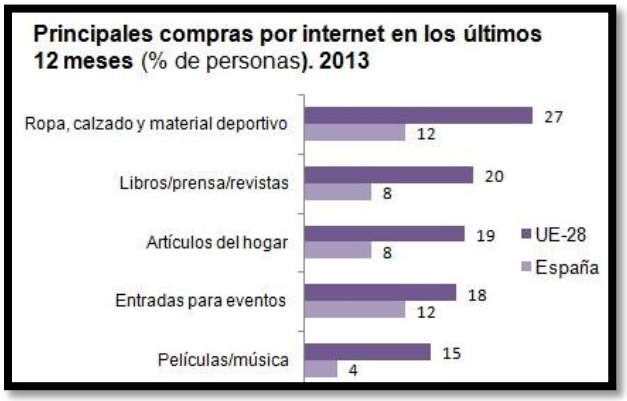

Gráfico 7: Principales compras por internet en los último 12 meses.
(Instituto Nacional de Estadística, 2014)

De igual forma, para los cibernautas que aun dudan de realizar compras electrónicamente, la AMIPCI (2012) y la PROFECO, nos dan a conocer el Decálogo de los Derechos Mínimos de los Consumidores en las Transacciones Efectuadas a través de Medios Electrónicos, que contempla los siguientes puntos:

1. Derecho a ser informado y respeto a los precios, tarifas, garantías, términos y otras condiciones que el proveedor a convenido por la entrega del servicio;
2. A que la información proporcionada al proveedor sea utilizada de manera confidencial;
3. Que el proveedor cuente con los elementos técnicos disponibles para garantizar nuestra seguridad;
4. Que el proveedor antes de realizar la transacción proporcione su domicilio físico o números de teléfono a los que se pueda acudir para presentar reclamaciones;
5. A que la información o publicidad que se difunda sea veraz, comprobable y exenta de descripciones que puedan derivar en confusión;
6. Previo a la contratación, el proveedor proporcione de manera clara, sencilla y completa el contenido de contrato de adhesión;

7. El proveedor no podrá negar ni condicionar la venta, adquisición, renta o suministro de bienes o servicios, cuando éstos se anuncien como disponibles;

8. Las leyendas que limiten el uso del bien o el servicio se presenten de forma clara, veraz y sin ambigüedades, así mismo precisar los términos de garantía;

9. A que no sean prestados servicios adicionales a los originalmente contratados, y que no sean los solicitados o aceptados;

10. Tener acceso a mecanismos de conciliación gratuitos para procurar la solución de controversias derivadas de transacciones de comercio electrónico.

Así mismo el presidente de la Asociación Mexicana de Internet, Manuel Tamez, opinó que el convenio fomenta el comercio electrónico en México, agradeció a la PROFECO por el interés para incrementar la confianza de los usuarios de internet al impulsar este medio comercial asegurando los derechos y obligaciones que permiten crear clientes mejor informados. Y aseguró que el comercio electrónico democratiza la oferta de productos y servicios en el país a través de los medios digitales.

Cabe resaltar que el acuerdo es de suma importancia, ya que de esta manera como usuarios al momento de realizar una compra, una transacción, entre otros movimientos, estaremos seguros al brindar los datos de nuestras tarjetas de crédito, pues estudios de entre el 2009 y el 2011 revelan que el valor de las operaciones de comercio electrónico en México ha crecido 49%; en 2009 registró la cifra de 24 mil millones de pesos; en el 2010 la cifra alcanzó los 36 mil 500 millones de pesos; en 2011 superó los 46 mil 500 millones y para finales de este año se espera al menos igualar esta última cifra, precisó Tamez.

Por otra parte, Bernardo Altamirano Rodríguez, titular de la Procuraduría Federal del Consumidor, menciono que “No debemos olvidar que la economía en internet es uno de los principales temas en la agenda internacional en materia de protección al consumidor, así lo demuestra que una parte importante de la OCDE está enfocada en fomentar este tipo de prácticas”.

Y es verdad, ya que en el año 2013 las sociedades nos hemos transformado en sociedades del conocimiento, es decir, nos hemos convertido en sociedades modernas que por medio de las transformaciones sociales ofrecemos un futuro con éxito, renovado, apoyado de las diferentes tecnologías existentes y de la economía, la cual aumenta gracias al uso de Internet y de los movimientos que ahí realicemos, ya que el uso de las transacciones en línea amplia los mercados.

Por otra parte, en México, D.F., el 27 de Febrero de 2013 el Consejo Directivo de la Asociación Mexicana de Internet A.C., firmó un acuerdo de colaboración entre AMIPCI y la Asociación Nacional de Tiendas de Autoservicio y Departamentales, A.C. (ANTAD), con el propósito de potenciar la adopción de las mejores prácticas en Internet para el comercio electrónico y promover un intercambio comercial ético, responsable y competitivo, que beneficie mutuamente a comerciantes y consumidores. Por lo que la seguridad aumento en estos años y podemos contestar la pregunta, que en la actualidad sí es más seguro el comercio electrónico, pues con la firma de este acuerdo, el sello de confianza aumento (AMIPCI, 2013).

De acuerdo a los artículos y la información contenida en la presente, se comenta que el comercio electrónico es más seguro actualmente ya que se basa en protocolos que proporcionan seguridad en las transacciones y brindan a su vez confianza y fiabilidad en las operaciones.

Y en 2014, el comercio electrónico está aumentando considerablemente. Adquirir productos a través de Internet tiene ciertas ventajas respecto a desplazarse a los lugares tradicionales para hacer la compra. La comodidad de no salir de casa y encargarlo todo frente al ordenador, así como la capacidad comparativa o el precio son algunas de ellas.

Comprar siempre ha sido de alguna manera un acto social. Pero ahora los mercados están cambiando e Internet está trastornando los hábitos de los ciudadanos y, por tanto, de los consumidores. El comercio electrónico tiene un papel importante en todo esto, debido a las facilidades que ofrece a los consumidores.

A continuación se hace mención de las cinco razones más sobresaliente para comprar a través de la red.

1. **Comodidad**

El comercio electrónico tiene una ventaja clara respecto al tradicional. Permite hacer la compra desde casa, sentado frente a la pantalla del ordenador (ahora incluso se puede hacer desde cualquier sitio gracias a los smartphones). De esta forma se evitan las aglomeraciones y esperas.

Además, a través de Internet las tiendas aceptan órdenes de compra las 24 horas del día, los siete días de la semana. No hay que estar pendiente de horarios. Y los que tengan jornadas laborales intensivas siempre tendrán abierta la posibilidad de adquirir un producto a través de la red.

2. **Una amplia oferta**

Te da la opción de elegir entre productos de todo el mundo. Cuando vas a un establecimiento sólo tienes a tu disposición lo que allí se vende. Si al consumidor esto no le convence o tiene necesidades de otro tipo tendrá que dirigirse a un lugar distinto.

En el caso de las compras a través de Internet el usuario puede adquirir alimentos en una página, para después visitar un sitio especializado de pinturas sintéticas y luego encontrar una impresora láser en su tienda informática de referencia. Tanto se puede elegir, que cualquiera es capaz de pedir algo que venden a miles de kilómetros de distancia.

3. **Comparar**

La compra por Internet permite comparar más fácilmente que en los grandes almacenes o tiendas. Si se trata de un portal de e-commerce la sencillez para observar las diferencias de precio y demás cualidades es obvia. Pero en caso contrario también resulta más fácil. El usuario puede visitar y tener abiertas diferentes páginas para ver al mismo tiempo lo que define a uno y otro producto.

4. **Claridad en la entrega**

Por lo general los portales de comercio electrónico, así como las tiendas online, tienen un periodo estipulado para la entrega de los productos. Esto da seguridad al cliente, que así puede saber con certeza a qué atenerse. Salvo excepciones, las compañías se preocupan de cumplir esto plazos, ya que ello es uno de los factores que crean su imagen de marca.

5. **El precio**

Esto no es exacto para todo. Existen algunos sitios que venden más caro el producto final debido al servicio que realizan. Pero muchas webs reducen los precios y, sobre todo, disponen de ofertas que no siempre coinciden con las de los establecimientos físicos. (Cooperación en Red Euro Americana para el Desarrollo Sostenible, 2014).

1.7 Seguridad

El término de seguridad es utilizado dentro de las áreas de trabajo, para evitar accidentes y proteger a los trabajadores para evitar riesgos por medio de controles que se establecen como medida preventiva. Por tal motivo (Corrales Hermoso, Beltrán Pardo & Guzmán Sacristán, 2006) definen la seguridad como la confianza, tranquilidad de una persona procedente de la idea de que no hay ningún peligro que temer.

Es importante mencionar que los riesgos son vistos como una vulnerabilidad ante un posible daño para las personas y cosas.

Riesgo. Combinación de la probabilidad de un evento y su consecuencia.

Vulnerabilidad. Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

Amenaza. Causa potencial de un incidente no deseado, el cual va resultar en un daño a los sistemas u organización (Britos, 2010).

La seguridad por tal motivo es una característica de todo sistema, la cual nos indica que cualquier sistema de información está libre de todo peligro.

Por tal motivo, podemos decir que la seguridad es un medio fiable, es decir, existe la probabilidad de que un sistema se comporte tal y como se espera de él, es decir, que sea un sistema más que seguro.

La seguridad se compone de tres aspectos importantes y actúa en conjunto con ellos para brindar protección a los usuarios y sistemas.

1.8 Aspectos de la seguridad:

1. Confidencialidad;
2. Integridad;
3. Y disponibilidad.

La confidencialidad nos dice que los elementos de un sistema deben ser accedidos únicamente por elementos autorizados; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada; y finalmente, la disponibilidad indica que los elementos autorizados de un sistema deben permanecer accesibles.

A su vez (Britos, 2010) describe la confidencialidad como la habilidad de un sistema para presentar sus recursos accesibles; la integridad como la habilidad de un sistema que permite que solo las partes autorizadas puedan modificarlo y solo en las formas que son consistentes con las funciones realizadas por el sistema. Y comenta que la disponibilidad son los derechos válidos de acceso a la información nunca deben ser denegados y deben ser satisfechos en tiempo y forma.

Por otra parte Corrales Hermoso et al. (2006) mencionan que la confidencialidad es un servicio que brinda protección para evitar que los datos sean revelados, accidental o deliberadamente, a usuarios no autorizados. Respecto al servicio de integridad de los datos, indican que garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los envidos por el emisor de los mismos. Y la disponibilidad que hace referencia a la protección que es necesario introducir para que el sistema y la red estén disponibles para ser utilizados por quienes dispongan de autorización para ello.

1.9 Informática

El término informática proviene del francés informatique, implementado por el ingeniero Philippe Dreyfus a comienzos de la década del ’60. La palabra es, a su vez, es un acrónimo de information y automatique Corrales Hermoso et al. (2006) Y es la aplicación del tratamiento automático de la información; utiliza sistemas computacionales, generalmente implementados como dispositivos electrónicos.

La informática se utiliza en la gestión de negocios, en el almacenamiento de información, en el control de procesos, en las comunicaciones, en las ciencias de la computación, como la programación, las redes como Internet, entre otras áreas. De tal forma, la informática es una ciencia que se refiere al procesamiento automático de información mediante dispositivos electrónicos y SI (sistemas de información), computacionales o sistemas informáticos.

Sistema de Información. Se define como un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos.

Sus elementos son: recursos, equipo humano, información y actividades.

Sistema Informático. Subconjunto del sistema de información que está constituido por un conjunto de elementos físicos (hardware, dispositivos periféricos y conexiones), lógicos (sistemas operativos, protocolos y aplicaciones) y por elementos humanos (personal experto en el manejo de sw y hw) (Aguilera, 2010).

Pero cual sea el término de cada autor, la informática está definida como el procesamiento automático de la información.

1.10 Seguridad informática

La seguridad informática es un elemento fundamental para realizar cualquier tipo de función computacional a nivel software o hardware, por lo que este tipo de seguridad puede ser escalón para atentar contra la seguridad.

“Una de las leyes fundamentales de la seguridad informática dice que el grado de seguridad de un sistema es inversamente proporcional a la operatividad del mismo” (Mattos Lescano).

Corrales Hermoso et al. (2006) la define como un conjunto de servicios y mecanismos que aseguren la integridad privacidad de la información que los sistemas manejen.

Mientras que (Sánchez, 2003) menciona que no existe una definición estricta de lo que se entiende por seguridad informática, porque abarca múltiples y diversas áreas relacionadas con los SI. Y añade: “sí hay tres aspectos fundamentales que definen la seguridad informática: la confidencialidad, la integridad y la disponibilidad”.

Actualmente, la seguridad informática es muy utilizada, ya que en empresas u organizaciones, o simplemente como usuarios, se acude a este recurso por la inseguridad que existe en los sistemas; por lo que se debe recurrir a técnicas de seguridad informática para fortalecer mecanismos de protección en la información y en los equipos con lo que a diario se realizan diversas actividades.

Por otra parte, se debe hacer mención a otros componentes importantes además de los que menciona (Sánchez, 2003), como son el control y la autenticación, los cuales son de vital, importancia dentro de la seguridad informática para prevenir amenazas. Con todo ello, se llega a la conclusión de que la seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional por medio de técnicas existentes, como son una serie de estándares, protocolos, métodos, reglas, herramientas y leyes para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

1.11 Componentes de la seguridad informática

A diferencia de la seguridad que se basa en tres aspectos fundamentales para su estructura (confidencialidad, integridad y disponibilidad), la seguridad informática aparte de éstos, agrega otros componentes para una estructura más completa, como son el control, la autenticación y el no repudio.

A continuación se describen:

1. Confidencialidad: como se expone en apartados anteriores, es la protección de datos e información intercambiada entre un emisor y los destinatarios, con el fin de garantizar se utilizan mecanismos de cifrado y de ocultación de la comunicación.

Algunos mecanismos de cifrado garantizan la confidencialidad durante el tiempo necesario para descifrar el mensaje son las llaves asimétricas, que son llaves privadas de autentificación distribuidas de manera segura a individuos específicos, las cuales deben ser generadas localmente y nunca ser reveladas a alguien. Estas llaves soportan todos los requisitos de servicios de seguridad (Mattos Lescano).

Por esta razón, se debe determinar durante cuánto tiempo el mensaje debe seguir siendo confidencial.

2. Integridad es garantizar que los datos no puedan ser alterados sin autorización;
3. Disponibilidad es garantizar que los usuarios autorizados tengan acceso en todo momento a la información cuando la requieran;
4. Control es asegurar que sólo los individuos autorizados tengan acceso a los recursos;
5. Autenticación es cualquier proceso mediante el cual se verifica que alguien es quien dice ser;
6. No repudio: es la imposibilidad de negar lo que el remitente final acuerda enviar como la transacción que completó;
7. Y la consistencia que debe asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

Todos los componentes de seguridad permiten proteger la información y datos de cualquier entidad o medio informático; por lo que también se les denominan necesidades de la seguridad.

1.12 Seguridad Física

Es la que tiene que ver con la protección de los elementos físicos de la empresa u organización, como el hardware y el lugar donde se realizan las actividades: edificio o habitaciones (Aguilera, 2010).

Desde el punto de vista de Alonso García et al. (2011) la seguridad física se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Se expone finalmente que la seguridad física es el medio de protección de los equipos. Éste tipo de seguridad preside problemas a nivel hardware, utilizando medios de apoyos para su protección y buen uso, estos mecanismos o medios pueden ser desde un teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

En términos generales, la seguridad física protege las propiedades físicas del sistema.

1.13 Seguridad Lógica

En cuanto a la seguridad lógica, es aquella relacionada con la protección del software y de los sistemas operativos, que en definitiva es la protección directa de los datos y de la información (López, 2010).

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista del software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera. Alonso García et al. (2011).

Pero finalmente, cual sea la definición que deseemos adoptar, la seguridad lógica siempre nos ayudará a brindar protección y control a nuestra información y datos.

1.14 Seguridad en las transacciones

Habitualmente como internautas, percibimos la falta de seguridad que coexiste en las transacciones electrónicas y surge como uno de los problemas primordiales para el desarrollo del comercio electrónico. Por tal motivo surge la seguridad en las transacciones, la cual tiene por objeto brindar protección a los datos que se manejan en la red proporcionando confianza al ejercer el comercio electrónico.

Se debe tener una excelente seguridad en todos los ámbitos, específicamente en el ámbito empresarial, que es en donde se realizan frecuentemente diferentes tipos de transacciones.

Las transacciones bancarias se realizan en su mayor parte sobre redes de conmutación de paquetes X.25 (Buch i Tarrats & Jordán). La conmutación es una función que se encarga de la distribución de conexiones, es decir, del enrutamiento de la información a través de la red hacia sus destinos precisos.

Enrutamiento se refiere a la selección del camino en una red de computadoras por donde se envían los datos.

En la conmutación de paquetes X.25 el mensaje de la fuente se descompone en pequeños mensajes, con algún formato de datos, llamados paquetes, para su transmisión a través de la red. Cabe mencionar que en este tipo de conmutación el canal de comunicaciones se comparte en forma dinámica entre diferentes usuarios (Herrera, 2003).

Buch i Tarrats et al. mencionan que este tipo de redes se consideran suficientemente seguras por estar controladas por operadores autorizados y no por presentar medidas de seguridad basadas en técnicas criptográficas, autentificación segura o integridad de la información. La red Internet es una red pública, por lo que el riesgo de que las amenazas contra la autenticidad, integridad, confidencialidad y el no repudio de las transacciones que sobre ella se realicen será mayor.

Y agrega que las nuevas tecnologías en el terreno de la seguridad en sistemas de información basadas en infraestructuras de clave pública (PKI) y en los protocolos SSL (“Secure Sockets Layer”) y SET (“Secure Electronic Transaction”) son las únicas que permiten cubrir las carencias de seguridad de la red Internet que afectan a la protección de la información que fluye a través de la red de redes.

PKI es una infraestructura de clave pública que permite garantizar requerimientos como la confidencialidad la cual se garantiza cifrando los datos que viajarán por la red. Se debe decir que mediante el uso de firmas digitales, se garantiza la autenticidad, la integridad y el no repudio de los datos.

A parte de la tecnología PKI y de los protocolos de seguridad en las transacciones, surgen otros mecanismos de seguridad para las transacciones; éstos son la encriptación de documentos, la cual es una forma de que el mensaje que se manda al receptor por parte del emisor viaje de manera segura desde la fuente al destino.

La firma digital es otro mecanismo de seguridad de los datos y las autoridades de certificación, que son quienes autentifican la firma electrónica de los usuarios.

Por otra parte, retomando el tema se seguridad en las transacciones, se expone que en la actualidad, el realizar una transacción electrónica ya es más segura que antes, debido a los mecanismos de seguridad con los que cuenta. Por ejemplo estudios actuales informan que en Agosto de 2012, el 74% de los internautas mayores de edad hace uso de servicios bancarios en línea (AMIPCI, 2012).

México, D.F., a 14 de agosto de 2012. En conferencia de Prensa celebrada en el Club de Industriales de la Ciudad de México, la Asociación Mexicana de Internet, A.C. (AMIPCI) dio a conocer los resultados de su Estudio de Banca Electrónica 2012. Entre sus principales resultados, este estudio arroja que se incrementó en un 5 por ciento la proporción de usuarios de Internet bancarizados respecto de 2011, y que el 74 por ciento de ellos usa algún tipo de servicio bancario en línea.

Al hacer la presentación del estudio, Jorge Sánchez Barceló, vicepresidente de Banca Electrónica de la AMIPCI, dijo que en esta ocasión el estudio presenta novedades, como una medición más detallada del uso de la banca en línea para transacciones de comercio electrónico, y en este mismo apartado, sobre el empleo de nuevos medios de pago.

En cifras generales, el Estudio de Banca Electrónica 2012 de AMIPCI ofrece un resumen de los datos sobre el uso de la banca en línea entre los internautas nacionales. El 42 por ciento visita portales bancarios y el 29 por ciento realiza transacciones en línea, en una proporción de 2.1 cuentas por usuario.

La edición 2012 de este análisis, cuya elaboración se realizó bajo el patrocinio de Anzen Soluciones y Everis, estuvo a cargo de Elogia, y destaca las siguientes cifras sobre el consumo de transacciones financieras en línea: Del total de entrevistados para el estudio, más de la tercera parte son usuarios de la banca desde hace más de 7 años; el 35 por ciento entre 3 y 6 años, y, finalmente, el 31 por ciento usa servicios bancarios entre menos de un año a dos años.

Entre las principales razones expuestas por el 26 por ciento de los usuarios que han decidido no usar la banca en línea, están las siguientes: el 53% prefiere acudir a una sucursal, el 43 por ciento declara que no considera suficientemente segura la banca electrónica; el 24 por ciento está en desacuerdo con el cobro de las comisiones, y el 19 por ciento no lo hace por usar computadoras compartidas.

Al cuestionar a los entrevistados sobre el lugar de conexión para realizar transacciones bancarias, aunque predomina el hogar y el trabajo con 86 y 52% respectivamente, destaca un fuerte incremento de usuarios que emplean sus dispositivos móviles para la conexión a sus bancos, con un 20%. Entre las principales actividades que realizan 6 de cada 8 usuarios emplean los servicios de banca electrónica para realizar pagos de servicios; 55% realiza traspasos entre sus cuentas y la mitad hace transferencias a terceras personas en el mismo banco.

Asimismo, un 49% hace transferencias a otros bancos y el 48% paga sus tarjetas de crédito. En proporciones menores al 20 por ciento aparecen actividades como la compra de productos, pago de impuestos federales y locales, así como el consumo de información que consideran útil en sus portales bancarios.

La presentación de los datos del estudio estuvo a cargo de Renato Juárez, Vicepresidente de Estudios de Mercado de la AMIPCI, quien destacó que el nivel de confianza en los servicios bancarios en línea expresado por los usuarios es muy alto: el 85% de quienes realizan transacciones en línea se sienten satisfechos o totalmente satisfechos con los servicios recibidos, cifra que contrasta con el 6% que se declara parcial o totalmente insatisfecho. Proporción similar, (un 86%) declara que recomendarían la banca en línea a colegas y amigos.

“Estas cifras son muy relevantes porque permite saber que los niveles de atención al cliente y de seguridad en la banca electrónica mexicana generan confianza en los usuarios y los estimulan a usar recurrentemente los servicios”, dijo Juárez.

El estudio da seguimiento al tema de la seguridad, un elemento indispensable para generar confianza en los usuarios. En este aspecto, destaca que un 69% emplea antivirus actualizado para protegerse de los riesgos en las transacciones; un 60% usa dispositivos de claves electrónicas, 55% usa firewall en su computadora y el 45 % emplea software anti spam.

A la pregunta sobre quién es el responsable de la seguridad de las transacciones, el estudio hace notar que se ha reducido la proporción de usuarios que consideran responsable sólo a los bancos, contra un 68% que considera que la seguridad es una responsabilidad compartida entre el banco y el usuario. En consecuencia, el 93% de los internautas define el no compartir sus claves como la medida de seguridad más importante para utilizar su banca por internet. Al finalizar su presentación, el Sánchez Barceló indicó que el reto para la banca es romper el paradigma de la realización de transacciones electrónicas.

“Las cifras de este estudio nos dicen que una vez que un cliente conoce y disfruta los beneficios de administrar sus cuentas a través de la banca electrónica, en su mayoría la sigue utilizando”.

Agregó: “Este paradigma lo romperemos con una estrategia integral, brindando al usuario información y herramientas necesarias para que cada día se sienta más cómodo, seguro y le demostremos las grandes ventajas de realizar operaciones bancarias electrónicas”.

Como se observa en el análisis, los usuarios tienen más seguridad al realizar cualquier tipo de transacción electrónica, pues debido a los mecanismos de seguridad existentes, el nivel de confianza en los servicios bancarios en línea expresado por los usuarios es muy alto y quienes realizan transacciones en línea se sienten satisfechos o totalmente satisfechos con los servicios recibidos.

La seguridad que actualmente existe en México, genera confianza en los usuarios y los estimulan a usar recurrentemente los servicios. El estudio da seguimiento al tema de la seguridad, un elemento indispensable para generar confianza en los usuarios, los cuales se protegen de riesgos en las transacciones, por medio de otros mecanismos de seguridad, como son los antivirus, dispositivos de claves electrónicas, firewall, software anti spam, entre otros.

Esto se afirma respecto a otro estudio expuesto en noviembre de 2012, en donde AMIPCI (2012), informa que crece el uso de la Banca Electrónica en México: 30% de los internautas hace transacciones en la banca electrónica

México, D.F., a 13 de noviembre de 2012. La Asociación Mexicana de Internet A.C. hizo la presentación de la actualización al cierre de 2012 de su Estudio de Banca Electrónica, que desarrolla Elogia, bajo el patrocinio de SafetyPay.

En un breve resumen estadístico, el estudio arroja los siguientes resultados: de los 40.6 millones de internautas mexicanos, el 64% son mayores de edad y por tanto, susceptibles de poseer algún producto bancario; el 52% efectivamente utiliza algún servicio de la banca, y el 40% visita los portales de al menos una institución bancaria. Finalmente, el 30% realizan transacciones de banca en línea. Este 30% posee un promedio de 2.1 cuentas de banca por Internet.

A partir de estas cifras generales, el corte de noviembre de 2012 del estudio refleja que el 74% de los internautas visita portales bancarios, independientemente de que realicen transacciones o no. Esta cifra es un 4% mayor que el 70% del último corte de julio de 2012.

Otros datos importantes del estudio:

Las actividades más recurrentes al hacer transacciones en línea, son:

1. Pago de servicios: 58%;
2. Transferencias entre mis cuentas: 55%;
3. Transferencias a terceros en el mismo banco, 50%;
4. Transferencias a terceros en otro banco, 49%;
5. Pago de tarjetas de crédito, 49%;
6. Compra de tiempo aire para recarga de celulares o Internet: 27%;
7. La compra de productos y servicios creció hasta un 32%, contra un 19% del periodo anterior).

En el grupo de usuarios de la banca electrónica, se ha reducido el número de visitantes frecuentes a sucursales bancarias (de 3 a 6 veces) entre 2012 y 2013 en un 2%.

Al indagar sobre las medidas de seguridad que emplean los internautas para sus transacciones en línea, el Antivirus ocupa el primer sitio (71%), superando a los dispositivos de claves electrónicas, que ocupan el 2do lugar con 59%.

El uso de Firewall, (55%), Antispam (45%), Antiespías (36%) y la actualización del sistema operativo (31%) se mantuvieron en proporciones similares que en la medición anterior.

Existe un incremento de la conciencia del usuario respecto de la responsabilidad compartida de la seguridad de las transacciones bancarias: sólo un 27%, 4% menos que en junio pasado, considera responsable sólo al banco en este aspecto. El Director de Comunicación de SafetyPay México, Ángel Aguilar Camacho comentó que “Observamos que en el entorno de los pagos electrónicos la seguridad es una preocupación de mucho peso, sin embargo podemos advertir en estos resultados un avance considerable y que el usuario de la banca en línea es un usuario cada día más informado".

En base a datos más actuales, en junio 2014, (Prezi Inc, 2014) menciona que para que una transacción electrónica sea segura, los usuarios deben usar el protocolo para transacciones electrónicas seguras para evitar información de pagos hechos con tarjetas a través de Internet.

Finalmente, se expone en el estudio que los Internautas Mexicanos mayores de edad, tomando en cuenta todos los niveles socioeconómicos, género y rangos de edad, tienen un nivel de confianza al realizar transacciones electrónicas del 95%. Y así la banca por Internet en México tiene un gran potencial de crecimiento.

1.15 Transacciones

Una transacción es una operación de compra y venta. Las transacciones las usamos cotidianamente para realizar depósitos bancarios, por ejemplo. Una transacción común de tarjeta de crédito involucra a cinco partes:

1. El cliente;
2. El comerciante;
3. El banco del cliente;
4. El banco del comerciante (que es el banco adquiriente);
5. Y la red interbancaria.

Y consta de diez pasos que se grafican a continuación (Domingo, 2002).

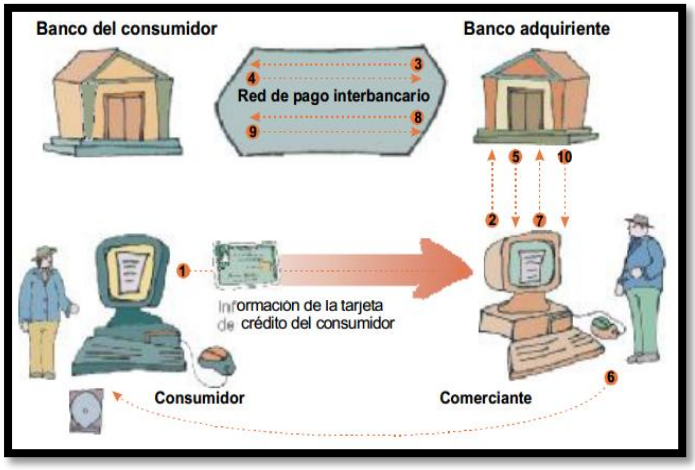

Gráfico 8: Participantes de una transacción típica con tarjeta de crédito (TDC) (Domingo, 2002)

Pasos de una transacción:

1. El cliente entrega su tarjeta de crédito al comerciante;
2. El comerciante pide autorización al banco adquiriente;

3. La red interbancaria envía un mensaje del banco adquiriente al banco del consumidor pidiendo autorización;
4. El banco del cliente envía una respuesta al banco adquiriente mediante la red interbancaria;
5. El banco adquiriente notifica al comerciante que el cargo ha sido aprobado o rechazado;
6. En caso de haber sido aprobado el comerciante realiza la orden de compra;
7. Luego el comerciante presentará cargos al banco adquiriente;
8. El banco adquiriente envía la solicitud de pago al banco del cliente mediante la red interbancaria;
9. El banco del cliente acredita el dinero en una cuenta de pagos interbancarios deduciendo algún cargo en concepto del servicio dependiendo del convenio;
10. El banco adquiriente acredita en la cuenta del comerciante debitando algún cargo en concepto del servicio dependiendo del convenio entre él y el comerciante (G. Díaz, F. Mur, E. Sancristobal, M. Castro & J. Peire, 2012).

Por otra parte, ALIGNET (2010) menciona el perfil de las transacciones:

1. Perfil Ventas Locales (despacho y entrega personal) y Perfil Ventas Internacionales (envíos por correo);
2. Perfil Ventas Clientes Recurrentes (+2 compras) y Perfil Venta a Clientes Nuevos (compras esporádicas);
3. Perfil de Ventas de Urgencia (entregas inmediatas) y Perfil de Solicitudes a futuro.

1.16 Transacción electrónica segura

Internet cuenta con una extensa gama de oportunidades para los usuarios que habitualmente realizan diversas actividades, como por ejemplo, alguna transacción electrónica para la adquisición de cualquier bien o servicio, para realizar pagos bancarios, etcétera, con redes abiertas de alcance mundial que no conocen fronteras ni sistemas jurídicos que regulen las relaciones entre las distintas partes involucradas en la población global. Y es por tal motivo que al realizar operaciones electrónicas se tiene la sensación de inseguridad, inseguridad que experimentan todos consumidores, empresarios y usuarios a la hora de transmitir datos personales y confidenciales a la red al momento de generar una transacción electrónica. Por ello, para que una transacción se efectúe de forma segura, debemos contar con los siguientes datos:

1. Nombre del cliente;
2. Número de la tarjeta de crédito;
3. Dirección del cliente;
4. Fecha de transacción;
5. Monto de la transacción;
6. Descripción de la mercadería o servicio;
7. Código de autorización;
8. Nombre del comerciante;
9. Firma del cliente.

Se solicitan siempre esos datos porque la información contenida en el comprobante que se otorga al momento de realizar la operación, es útil para consumar transacciones y combatir el fraude.

Al momento de brindar los datos, podemos elegir una de las tres formas existentes para realizar una transacción con un número de tarjeta de crédito en la Web de manera segura. Ésta formas son:

1. Fuera de línea: es un método en donde el cliente realiza la orden de compra utilizando la Web. Luego el comerciante llama por teléfono al cliente y verifica la orden de compra y le solicita los datos de la tarjeta de crédito.

Aun así, este método tiene riesgos, los cuales son equivalentes a enviar el número de tarjeta de crédito sin encriptar ya que la línea de teléfono podría estar intervenida.

2. En línea con encriptación: aquí el consumidor envía el número de tarjeta al comerciante a través de Internet mediante una transacción encriptada.

Cabe mencionar que este método es el único recomendable.

3. En línea sin encriptación: en este método el consumidor envía el número de tarjeta, ya sea utilizando correo electrónico o un comando POST o GET de HTTP.

Cabe mencionar que esta técnica es vulnerable a la intercepción.

Post y Get son comandos que indican como realizarse la transferencia de los datos. Post transmite los datos separados del URL. Mientras que Get envía los datos formando parte del URL (Cobo, Gómez, Pérez & Rocha, 2005).

Cualquiera que sea el tipo de seguridad que se emplee, debe brindar protección y garantizar fiabilidad, por lo que brinda servicios y mecanismos de seguridad. Para que una transacción electrónica sea segura, se pueden realizar transacciones basadas en SET; como informa Buch i Tarrats et al., con la ayuda de los grandes fabricantes de la industria de ordenadores y programas, Visa y MasterCard han desarrollado el que se está estableciendo en el protocolo de pago por excelencia para la práctica del Comercio Electrónico minorista (es decir, venta entre comerciante y usuario final). SET (Secure Electronic Transaction) es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito. Lo que asegura confianza a los usuarios que realizan transacciones electrónicas.

1.17 Mecanismos de seguridad en las transacciones

Los mecanismos de seguridad en las transacciones, son barreras de seguridad que ayudan a llevar a cabo una buena organización en los métodos de pago a realizar; y se consideran indispensables para una comunicación segura. Los mecanismos de seguridad son considerados por Alonso García et al. (2011) como todo aquello de naturaleza hardware como software que utilicemos para crear, reforzar y mantener la seguridad informática. Y los define de la siguiente manera:

1.17.1 Los mecanismos de software o lógicos:

Los mecanismos software o lógicos son barreas de software como los cortafuegos, antispyware, antivirus, encriptación de la información, llaves de protección de software, entre otros.

Los cortafuegos son un sistema de seguridad entre distintas redes. Es también llamado firewall y es un dispositivo que se utiliza para proteger una computadora o una red interna, de intentos de acceso no autorizados desde Internet, denegando las transmisiones y vigilando todos los puertos de red.

Su uso más común es situarlo entre una red local y la red de Internet, evitando que los intrusos puedan atacar o acceder la red de computadoras local.

Los antispyware son un tipo de aplicación que se encarga de buscar, detectar y eliminar spywares o espías en el sistema. Que suelen ser módulos o herramientas incorporadas dentro de otra aplicación mayor, como un antivirus. Otros tipos de aplicaciones "anti" son: los antivirus, los anti-intrusos (firewalls), entre otros.

En cuanto a los antivirus, son una aplicación informática encargada de detectar y eliminar virus.

La encriptación de la información son técnicas de cifrado y/o codificado, para hacerlos difíciles a intrusos que obstruyan esos mensajes o información.

Otro mecanismo que nos brinda seguridad en una transacción, y que es de gran ayuda y apoyo para proteger los datos, son las llaves de protección de sw. Éstas son un sistema de seguridad basado en hw para brindar protección al software contra la piratería y el uso ilegal, permitiendo el acceso y ejecución únicamente cuando la llave está conectada al PC.

Las llaves contienen un motor de cifrado de alta seguridad en el cual todo el proceso se realiza dentro del hardware sin abandonar en ningún momento la llave.

Como recomendación, para todos los mecanismos de seguridad lógico, se debe contar con un sistema de respaldo remoto, ya que así se tendría una copia de seguridad que tiene como fin brindar al usuario copias adicionales que puedan utilizarse para restaurar el original después de una eventual pérdida de datos (España, 2003).

1.17.2 Mecanismos hardware o físicos:

En cuanto a los mecanismos de hardware o físicos, se incluyen las cámaras de seguridad, control de acceso físico al sistema, controles de acceso con tarjetas de identificación Alonso García et al. (2011).

Todos estos mecanismos de seguridad, ya sean físicos o lógicos, ayudan a proteger nuestros sistemas y resguardar la integridad y la seguridad de nuestros equipos, permitiendo así tener actividades o alguna una transacción segura.

1.17.3 Legislación y Normas de Seguridad Informática

Existen numerosas leyes de seguridad informática que surgen como medidas para proteger los derechos al momento de realizar acciones, transacciones, entre otros aspectos, pero todas se crean con la finalidad de proteger datos personales. A continuación se mencionan algunas leyes que resultan de gran importancia para combatir diversos fraudes o inseguridades que surgen al realizar alguna transacción u otros movimientos de tipo bancarios; estas leyes, tienen como objetivo brindar respaldo y seguridad ante sucesos fraudulentos.

Alonso García et al. (2011) da a conocer las leyes y normas más sobresalientes que protegen a los internautas y les brinda seguridad informática.

A. Protección de los derechos de autor

Surge en este punto la Ley de Protección Intelectual aprobada por el real decreto legislativo 1/1996, de 12 de abril; la cual protege los derechos de autor en general, ya sea de programas informáticos, libros, etc.

B. Legislación sobre protección de datos: es la Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI-CE).

Esta ley 34/2002, de 11 de Julio, regula todo lo relativo a las comunicaciones comerciales y contrataciones vía electrónica. Es decir, las compras y e-commerce a través de Internet.

C. Ley sobre normas reguladoras de firma electrónica. Del Real Decreto- ley 14/ 199, aprobada el 17 de Septiembre con el objetivo de fomentar la incorporación de nuevas tecnologías de seguridad de las comunicaciones electrónicas.

D. Ley 59/2003, del 19 de diciembre, regula la firma electrónica, su eficacia y la prestación de sus servicios.

E. Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información. Esta ley modifica puntos de las leyes anteriores, con el fin de garantizar los derechos de los ciudadanos en la nueva sociedad de la información.

F. Ley sobre el DNI electrónico. Se aprobó en España en 1944. La ley sobre firma electrónica y el Real Decreto 1553/ 2005, de 23 de diciembre, regula los certificados de firma electrónica.

En cuanto a las normas de seguridad informática, surgen las siguientes:

A) ISO 27015: contiene guía del sector financiero y de seguros;
B) ISO 27032: guía sobre ciber-seguridad;
C) ISO 27033: norma dedicada a la seguridad en redes y comunicaciones, asegurando ambas a través de gateways, VPN y redes inalámbricas;
D) ISO 27034: norma de seguridad en aplicaciones informáticas;
E) ISO 27799: norma relativa a la seguridad de la información de datos.

Estas normas de seguridad son lineamientos que tienen por objeto respaldar y brindar seguridad a los usuarios ante algún hecho fraudulento, así como regular riesgos a los que se expone cada usuario.

1.18 Técnicas de seguridad en las transacciones

Existen diversas técnicas de seguridad en las transacciones, como son la criptografía, los protocolos de seguridad, certificados digitales, firmas digitales, entre otros, que surgen a través de la problemática y de los fraudes en las transacciones a través de Internet. Estas técnicas de seguridad en las transacciones regulan inseguridades y fraudes proporcionando a los usuarios seguridad y al mismo tiempo confianza en sus movimientos, garantizando también confidencialidad, integridad y disponibilidad de la información.

1.18.1 Criptografía

La criptografía es un elemento indispensable para proporcionar seguridad en las transacciones electrónicas, y más concretamente al pago electrónico basado en tarjeta de crédito. Por tal motivo, existen dos protocolos concretos (SSL y SET) que deberían servir para aumentar la confianza de los usuarios en los nuevos medios de contratación electrónicos (Gutiérrez Gutiérrez & J. Tena, 2003).

Domingo (2002) agrega “La criptografía es un conjunto de técnicas empleadas para conservar la información de forma segura.

Está basada en la transformación de los datos de forma tal que sean incomprensibles para los receptores no autorizados, en cambio para aquellos receptores que posean la autorización correspondiente, los datos que conforman dicha información resultarán perfectamente comprensibles”.

Y la define como un conjunto de técnicas empleadas para conservar la información de forma segura.

La criptografía se basa en la transformación de datos de forma que sean difíciles de comprender para los receptores no autorizados, pero por el contrario, para los receptores autorizados, los datos que conforman la información serán comprensibles.

En la transformación se pueden identificar 2 procesos bien definidos (Gráfico 7):

1. Encriptación: proceso mediante el cual la información se transforma en un conjunto cifrado de datos mediante una función de transformación y una llave de codificación;
2. Desencriptación: proceso mediante el cual los datos se convierten en el texto original mediante una segunda función de transformación y una llave de desencriptación.

   La llave puede ser la misma para ambos procesos o distinta.

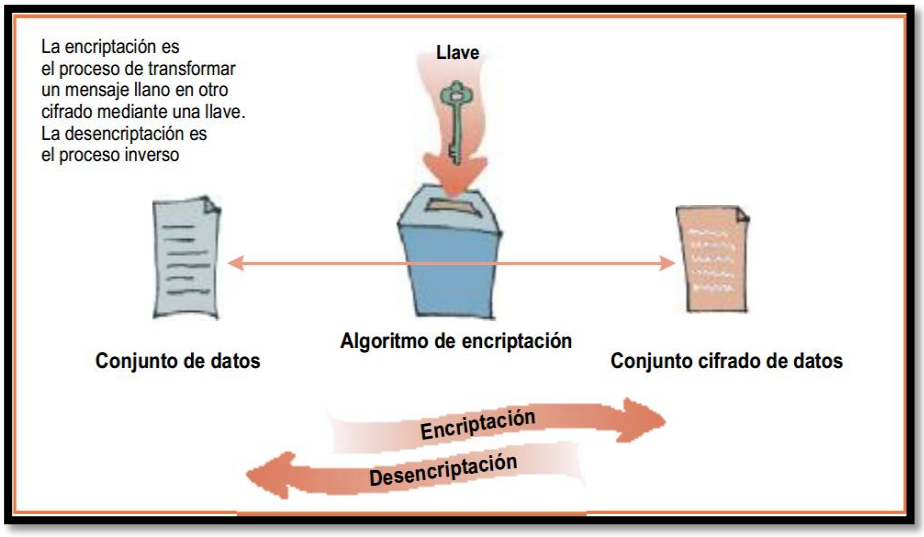

Gráfico 9: Ejemplo sencillo de encriptación desencriptación
(Domingo, 2002)

Aunque las aportaciones de diversos autores aportan diferentes ideas acerca de la criptografía, todos llegan a la definición acerca de que son técnicas de seguridad que protegen y resguardan de manera segura nuestros datos e información, por lo que se llega a la conclusión que la criptografía cubre hoy en día objetivos distintos, a veces muy alejados, del tradicional y más conocidos de la transmisión secreta de información.

Este tipo de aplicaciones se engloba dentro de lo que se denomina protocolos criptográficos (Gutiérrez Gutiérrez et al., 2003).

1.18.2 Algoritmos criptográficos

Los algoritmos criptográficos son uno de los campos de mayor auge actualmente, requiriendo continuamente algoritmos más seguros y eficientes. Y por ello, se realizan estudios que intentan mejorar la velocidad de los algoritmos existentes.

Por esa razón Ramos Álvarez & Ribagorda Garnacho (2004) mencionan el algoritmo IDEA, el cual es un algoritmo de cifrado de bloques de texto de 64 bits utilizando una clave de 128 bits que se usa para generar 52 subclaves de 16 bits.

Se ha desarrollado, mediante el lenguaje de programación Visual C++, una aplicación que permite introducir texto al usuario, gestionar ficheros, realizar funciones de codificación y decodificación, entre otras.

Algoritmo Hardware Secuencial; es un algoritmo estrictamente secuencial, con la ventaja que se ejecuta mediante el hw. Este tipo de algoritmo, antes de que se ejecute una instrucción debe haberse ejecutado la instrucción previa. Y son: SEC, SEC_R y SEG_F.

Por otra parte, Sarubbi (2008) menciona importantes algoritmos criptográficos, los define de la siguiente manera:

1. MD5: era un algoritmo de reducción criptográfico, muy pequeño y alternativo de 128 bits.
2. SHA: es un algoritmo simétrico que garantiza que no se encuentren mensajes con firmas iguales. Es un algoritmo de una sola vía y por ello es posible obtener el mensaje original.
3. DES: Algoritmo de clave privada o simétrico

Está basado en el algoritmo Lucifer, desarrollado por IBM. Es un algoritmo muy seguro pero sus costos son muy elevados.

4. Algoritmo AES o de Rijndael: fue anunciado como un estándar avanzado de cifrado para empleo de aplicaciones criptográficas no militares, potentes, eficientes y fáciles de utilizar. Es un sistema simétrico de cifrado por bloques, es decir, que opera en grupos de bits de longitud fija, aplicándoles una transformación invariante. Al realizar el cifrado, la unidad de cifrado por bloques toma como entrada un bloque de texto claro y produce un bloque cifrado de igual tamaño. Está diseñado para manejar longitudes de clave variable comprendidas entre 128 y 256 bits.

Este algoritmo está basado en la estructura de su diseño, se puede decir, que es el método más eficiente para recuperar la clave a partir de un par texto cifrado/texto claro, y es un método muy seguro.

5. RSA: Algoritmo de clave pública o asimétrica

Es un algoritmo criptográfico asincrónico que se basa en la dificultad de factorizar grandes números. Las claves pública y privada se obtienen a partir de números primos grandes.

Aunque el algoritmo RSA es bastante seguro, existen algunos puntos que se deben tener en cuenta, como ser el tamaño de la clave, que no debe ser menor a 1024 bits; y no firmar el mensaje después de codificarlo, ya que existen algoritmos que permiten manipular con éxito mensajes primero codificarlos y luego firmados.

1.18.3 Protocolos criptográficos de seguridad

La criptografía cubre hoy en día la transmisión secreta de la información. Este tipo de aplicaciones se engloba dentro de lo que se denomina Protocolos Criptográficos.

Un protocolo criptográfico es un protocolo que utiliza como herramienta algún algoritmo criptográfico.

Gutiérrez Gutiérrez et al. (2003). Describe a algunos de ellos.

1. Protocolos de Autentificación de Usuario, garantizan que el remitente de algún mensaje con el que se establece la comunicación, sea realmente el usuario mismo.
2. Protocolos de Autentificación del Mensaje, garantizan la integridad del mensaje, es decir, que el mensaje enviado no ha sido sustituido por otro ni alterado.
3. Protocolos para compartir secretos, su objetivo es distribuir secretos entre conjuntos P de participantes, de forma que los subconjuntos P puedan unir las participaciones recuperando el secreto enviado.
4. Protocolo de Needham-Schroeder, transfiere dos llaves secretas para mantener la información confidencial.

Llave secreta, es una clave secreta de seguridad.

5. Protocolo X.509, cuenta con un sistema público de cifrado y una firma digital.

Los protocolos que bridan seguridad en las transacciones electrónicas se explican en el capítulo 3.

1.18.4 Certificados digitales

Son un método más de la seguridad en las transacciones que aseguran a los usuarios de fraudes. Los certificados digitales son creados buscando cubrir las necesidades de seguridad y básicamente sirven para asegurar el envío de información entre los participantes. Principalmente, los certificados digitales se basan en dos principios: autenticidad e integridad. La autenticidad consta en que el receptor está seguro de que la información recibida pertenece al emisor, en cuanto a la integridad, garantiza al receptor que el mensaje no tuvo ningún tipo de cambio desde el envío del emisor. Sus usos más comunes son ciframiento de los datos y firmas digitales. En ambos se utilizan llaves públicas y privadas (Mauricio Pardo & Rodríguez Olivos, 2005).

Además, Buch i Tarrats et al., afirma que son la certificación electrónica generada por una autoridad de certificación, que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado tiene una validez determinada y un uso concreto.

Pero básicamente los certificados digitales sirven para asegurar el envío de información entre dos entidades (participantes). Y se basan en dos principios básicos, la autenticidad e integridad. Como menciona Mauricio Pardo & Rodríguez Olivos (2005), la autenticidad consta en que el receptor conoce y está seguro de que la información recibida pertenece al emisor, mientras que la integridad garantiza al receptor que el mensaje no tuvo ningún tipo de cambio desde el envío del emisor.

1.18.5 Firmas digitales

Firmas digitales son descritas por Buch i Tarrats et al., como una firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere.

Por otra parte Contreras (2009), expone que la firma electrónica surge debido a la necesidad de un mundo globalizado en donde las transacciones y la interacción entre los individuos son impersonales y sin vínculos físicos.

En conjunto de las definiciones, la firma digital es el conjunto de datos, en forma electrónica, adjuntos a otros datos electrónicos, utilizados como medios para identificar formalmente al autor o autores de cierta información.

1.18.6 Tecnología PKY

La tecnología PKI también se aplica a los sistemas de banca virtual sobre Internet garantizando la seguridad de las operaciones bancarias tradicionales como órdenes de compra/venta de valores, órdenes de transacciones interbancarias, gestión de cuentas, etc.

PKI es una infraestructura de clave pública que permite garantizar requerimientos como la confidencialidad la cual se garantiza cifrando los datos que viajarán por la red (Buch i Tarrats et al.).

1.18.7 Banca Virtual

Se conoce también como “banca electrónica”; se puede acceder a ella mediante Internet y pueden ser entidades físicas o entidades que sólo operan por Internet.

En banca virtual, los clientes realizan las operaciones bancarias de forma remota. El sistema se implanta sobre redes TCP/IP (Internet), WAP (comunicaciones móviles) o propietaria (por ejemplo, cajeros automáticos). En el segundo, también interviene la red Internet. El sistema de banca virtual distingue entre:

1. Autentificación de usuario;
2. Autorización de transacciones.

El sistema debe disponer de un servicio de acreditación fuerte para accesos a servicios y ofrecer la plataforma electrónica para que los usuarios puedan firmar digitalmente datos. Es importante resaltar que los sistemas actuales implantan mejoras en el sistema de autentificación, que aunque es más segura, sigue basándose en identificadores de usuario y contraseñas (Buch i Tarrats et al.).

1.18.8 Monedero electrónico seguro

Un monedero electrónico seguro usa mecanismos de seguridad simples, pero asegura que la información es verificada o registrada por el servidor.

Para que un monedero electrónico sea seguro, se puede basar también en el protocolo SET, ya que hace seguras las transacciones mediante el uso de certificados digitales y brinda mejoras en su sistema, garantizando integridad en las operaciones que realicen.

Lizama Pérez & León Oramas (2005) mencionan las ventajas de usar un monedero electrónico; éstas son:

1. Se usan herramientas multiplataforma, lo que permite portabilidad del código para implantación en otros SO;
2. Usa mecanismos criptográficos;
3. Permite la recaudación de efectivo.

CAPÍTULO 2

METODOLOGIA DE INVESTIGACION

1. Tema de Investigación

El tema del proyecto de investigación se titula:

“Propuesta para que las Empresas dedicadas a E-commerce usen el Protocolo Secure Electronic Transaction “SET” para brindar Seguridad en las Transacciones”.

2. Problemática

Mientras Internet, crece rápidamente, aumenta el intercambio de datos, y muchas empresas realizan transacciones financieras con sus clientes en Internet y necesitan asegurarse que sus transacciones sean privadas y de confianza, pues muchas veces existe inseguridad a la hora de transmitir datos confidenciales para realizar transacciones electrónicas y los usuarios demandan niveles más altos de seguridad.

3. La Justificación

Se realiza esta propuesta para implementar el uso del Protocolo Secure Electronic Transaction “SET” en Empresas dedicadas a E-commerce para brindar Seguridad en las Transacciones, ya que el principal problema al que nos enfrentamos todos los usuarios, es la carencia de un protocolo adecuado que comprenda todas las dificultades que implica el tráfico comercial en todas las operaciones electrónicas que realizamos, pues se tiene la sensación de inseguridad a la hora de transmitir datos confidenciales.

Y es por tal motivo, que el protocolo propuesto cumple con estas especificaciones, ya que proporciona y garantiza la confiabilidad de las transacciones. De este modo, el propósito de esta investigación está motivado en:

A. Identificar las necesidades de la información de los usuarios que realizan transacciones para e-commerce;
B. Realizar un estudio del comportamiento del protocolo propuesto para ser implementado.

4. Objetivos

4.1 Objetivos generales

“Proponer el protocolo SET para que las empresas dedicadas a e-commerce lo usen, ya que es el protocolo que brinda transacciones electrónicas seguras”.

4.2 Objetivos específicos

A. Analizar el entorno de aplicación del protocolo SET para ponerlo en práctica;
B. Cubrir las necesidades de los usuarios que realizan transacciones electrónicas;
C. Evaluar la calidad de los servicios que brinda dicho protocolo, es decir, cómo funciona el SET, que precisa y que seguridad proporciona.

5 Los alcances y las limitaciones

5.1 Los alcances

La trascendencia de esta investigación radica en permitir concientizar a los usuarios y empresa que utilizan e-commerce para transacciones electrónicas, sobre la importancia de implementar el protocolo “SET” para evaluar y brindar servicios de calidad. Por lo que se expone la propuesta. Las empresas dedicadas a e-commerce, deben adquirir un compromiso con los usuarios brindándoles el servicio que requieren de manera fiable, aplicando mecanismos de control y seguridad en la información como los que brinda “SET” para tener una transacción electrónica segura. De ahí que es necesario considerar que los usuarios exigen y necesitan mayores niveles de seguridad al momento de realizar sus transacciones electrónicas.

5.2 Las limitaciones

En el desarrollo de la investigación se presentaron las siguientes limitaciones:

A. La investigación sólo analiza el protocolo SET de Seguridad en las Transacciones, pero menciona algunos otros, tales como el SSL;
B. Escasez bibliográfica referida a la temática de investigación;
C. Información compleja acerca del protocolo de investigación;
D. Complejas cuestiones legales de certificación del protocolo “SET”;
E. Se expondrán sólo los factores esenciales relacionados con la propuesta del protocolo “SET” en empresas dedicadas a e-commerce para brindar Seguridad en sus Transacciones.

CAPÍTULO 3

PROTOCOLOS DE SEGURIDAD EN LAS TRANSACCIONES

1. Protocolos

Protocolo es un conjunto de etapas que realizan tareas específicas.

Un protocolo de seguridad es la parte visible de una aplicación; también se define como un conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica (Angel Angel, 2006).

2. Tipos de protocolos:

2.1 S-HTTP

Es un protocolo del cual ya no se puede esperar nada, es un protocolo orientado a proporcionar seguridad exclusivamente al protocolo HTTP, que a pesar de ser un protocolo antiguo y seguro de Internet, no es muy utilizado.

2.2 PCT

Es un protocolo compatible con SSL por Microsoft, aporta pocas cosas novedades técnicas; los servidores, por ejemplo las últimas versiones de Explorer no soportan el protocolo (Morales, 2002).

2.3 Protocolo SSL

Es el protocolo más dominante en la actualidad, en el ámbito de las transacciones y el comercio electrónico.

Secure Sockets Layer (SSL): Es un protocolo que permite la autentificación mutua de un usuario y un servidor con el propósito de establecer una conexión cifrada.

De acuerdo a artículos leídos, todos coinciden en que la gran mayoría de transacciones comerciales que se realizan hoy en día en la red se protegen mediante SSL.

Martínez López et al. (2009), describen a SSL como el protocolo de seguridad más extendido en la Red. Se trata de una tecnología diseñada por Netscape Communications Inc., con el propósito de conseguir un sistema de intercambio de información seguro tanto en el transporte de la información como en la autenticación del servidor de comercio electrónico.

El protocolo SSL combina sistemas de encriptación simétrica con sistemas de encriptación asimétrica. El intercambio de información tiene lugar en dos fases: primero se negocia entre el cliente y el servidor una clave simétrica sólo válida para esa sesión, después se transfieren los datos cifrados con dicha clave. Estas fases son transparentes para los usuarios finales que sólo saben que el canal de transmisión de la información es seguro y proporciona confidencialidad entre los extremos, haciéndolo simple de usar.

Aunque es un protocolo muy usado en las transacciones y en e-commerce, Morales (2002), nos indica que es un estándar que no contempla la implementación del No Repudio de mensajes. Y agrega que es un protocolo que no está diseñado específicamente para esas operaciones, por ejemplo, en una transacción comercial electrónica existe una tercera parte involucrada que no se contempla en SSL: el banco.

Cuando se realiza una transacción comercial usando SSL el cliente escoge la mercancía, realiza la orden de pedido y envía la información de pago (típicamente un número de tarjeta de crédito o débito) al vendedor. Este realiza las comprobaciones oportunas en el banco y una vez que obtiene la validez del medio de pago procesa el pedido.

Y todo se ve muy seguro en la transacción usando este protocolo, pero se hace la pregunta ¿Cuál es el problema en este esquema? Es evidente: el vendedor no compromete ante el cliente ningún tipo de información sensible y, además, está protegido contra posibles fraudes (tarjetas falsas o caducadas). El comprador, sin embargo, tiene que enviar información sensible al vendedor comprometiendo la misma ante la honestidad de este.

La gran difusión del protocolo, la facilidad de implantación por parte de administradores de sistemas y la transparencia para el usuario que, en la mayoría de los casos ni siquiera se entera de que lo está usando lo ha convertido en el protocolo dominante en un terreno en el que existen opciones mucho mejores. Por ejemplo, el sucesor de éste, el protocolo TLS.

Por otra parte, Mauricio Pardo et al. (2005) mencionan que SSL es un protocolo creado por Netscape a mediados de los 90´s, con el fin de garantizar de modo seguro la transmisión de datos por Internet. SSL utiliza un sistema de codificación a través de dos llaves: pública y privada. Además, indican que para que se pueda establecer una comunicación con SSL, es necesario que el servidor, ya sea un comerciante o empresa que tenga instalado un certificado digital, con el fin de garantizar una comunicación estable con alguien legítimo.

Así mismo SSL, proporciona seguridad en el proceso de comunicación mediante la autenticación del servidor y la codificación de mensajes, en donde solo el receptor pueda entenderlo.

Dentro de e-commerce, SSL juega un papel importante, ya que se encarga de transmitir de manera segura datos del cliente y el servidor por la red, garantizando así la integridad, autenticidad y bloqueo de información a terceros. Sin embargo, coincide con el autor anterior, SSL no realiza operaciones que son de gran importancia en una transacción de comercio electrónico, pues por mencionar algún ejemplo, no verifican la validez del número de TDC del cliente.

Proceso SSL entre cliente y servidor:

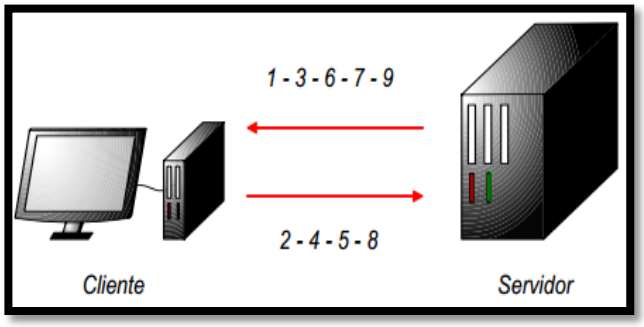

Gráfico 10: Proceso SSL

Mauricio Pardo et al. (2005)

El proceso se describe de la siguiente forma Mauricio Pardo et al. (2005):

1. El cliente hace una petición para establecer un canal de seguridad;
2. El servidor envía la llave pública en un certificado digital y un resumen;
3. El cliente valida la autenticidad del certificado. Con la llave pública se descifra el resumen: si son iguales confía en la comunicación, sino rompe la comunicación;
4. El cliente genera una llave simétrica, es decir, una llave de sesión;
5. Cifra la llave de sesión con la llave pública del servidor y se guarda en un sobre digital;
6. El cliente envía sobre digital;
7. El servidor abre el sobre digital con su llave privada y descifra el mensaje;
8. El servidor envía mensajes cifrados con la llave de sesión;
9. El cliente descifra los mensajes con la llave de sesión.

2.4 TLS

Es la versión 3.1 de SSL; se conoce también como SSL 3.1; es un SSL mejorado que posee mecanismos compatibles con SSL y viene incluido en la mayoría de los navegadores, pero es un protocolo que no acaba de realizarse.

Apache e IIS son los dos servidores que bridan soporte a este protocolo.

2.5 IPSEC

Ha sido postulado como el competidor de SSL, sim embargo es un protocolo muy complejo en cuanto a implantación y mantenimiento y es por eso que se reduce su ámbito de trabajo en las transacciones y el e-commerce.

De acuerdo a la información anterior, y al punto de vista expuesto por los diferentes autores, se puede decir que el protocolo más usado actualmente pero que es un protocolo que carece de mecanismos seguros para efectuar transacciones, es el protocolo SSL; pero aparte de este protocolo, surgen otros dos protocolos, los cuales Morales (2002) los define como protocolos realmente orientados a las transacciones comerciales electrónicas; estos protocolos son:

2.6 CYBERCASH

Es el protocolo más antiguo que se introdujo en el panorama de los protocolos seguros dentro de la pasarela de pago y de los mecanismos para proteger no sólo al vendedor, sino también al comprador.

Cybercash quedo fuera del mercado debido a la inmadurez de los sistemas PKI que manejaba, acompañado de una serie de cambios y adaptaciones inadecuadas.

2.7 SET

El más poderoso protocolo, utiliza un esquema muy similar al Cybercash, y los respaldan los gigantes del pago electrónico y las grandes compañías de informática y telecomunicaciones. En cuanto a las PKI que utiliza, tienen un excelente reconocimiento.

El principal problema de SET es la complejidad de su infraestructura, pero a pesar de este factor, es el mejor de los protocolos, brinda confidencialidad, integridad, no repudio, etc., y cumple con los requisitos de seguridad. Aunque por ahora la única competencia que tiene SET es SSL, un protocolo que debe salir del mercado y dar ese lugar a SET.

Tal y como afirma Morales (2002) “el comercio electrónico es hoy en día, un mecanismo impulsivo y espontáneo y sería muy difícil convencer al usuario de la necesidad de obtener una certificación para realizar sus compras en Internet. Hay, de todas formas, muchos factores que pueden cambiar este punto: la inminente implantación del DNI digital hará que todos tengamos en el bolsillo un certificado digital con las máximas garantías. Quizás sea ese el ‘pistoletazo’ de salida que necesita SET y represente la definitiva salida de SSL de un mundo que no le corresponde por derecho”.

Todos los protocolos de seguridad a los que se hacen referencia, tienen por objetivo, resolver problemas de seguridad, como son la integridad, la confidencialidad, la autenticación y el no repudio, mediante sus diferentes características.

Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

Por otra parte, Martínez López et al. (2009) hacen referencia a nivel mundial de tres protocolos que ofrecen garantías de seguridad e integridad en los sistemas de pago electrónico o en transacciones de una forma fiable, brindando confianza a los usuarios. SSL, SET y 3D Secure, los cuales tienen el propósito de disipar las posibles dudas en cuanto a la falta de seguridad en las transacciones electrónicas a través de Internet.

Y de acuerdo a ello, y a lo expuesto en la información contenida de cada protocolo, se llega a la conclusión de que el protocolo más completo que brinda mayor seguridad a las empresas que emplean e-commerce y a usuarios que realizan cualquier tipo de transacción electrónica es el protocolo Secure Electronic Transaction “SET”, y se añaden algunas ventajas de este en comparación de SSL que es el protocolo con el que actualmente compite.

3. Comparativa de los protocolos SSL y SET

En este apartado se explican algunas ventajas y funcionalidades de SET ante SSL, con el fin de dar a conocer a las empresas dedicadas a e-commerce que actualmente usan el protocolo SSL en sus sistemas pago o lo usan para realizar transacciones electrónicas, que SET es un protocolo completo capaz de realizar múltiples operaciones electrónicas de manera segura, siendo un protocolo especializado para este tipo de operaciones en Internet; y así mismo, realizar una innovación ante este y utilicen el protocolo SET para brindar seguridad, integridad, confidencialidad, fiabilidad y autentificación en las operaciones que se realizan ya que en muchas ocasiones no lo cambian porque la infraestructura de cambio de protocolos es costosa, o porque es un protocolo famoso que se ha utilizado de años atrás, pero a pesar de estos aspectos, SET es un protocolo especial para las transacciones y SSL no.

Como menciona Mauricio Pardo et al. (2005) SSL se encarga de transmitir de manera segura datos del cliente y del servidor por la red, garantizando así la integridad, autenticidad y bloqueo de información a terceros, pero no realiza operaciones que son de gran importancia en una transacción de comercio electrónico, pues por mencionar algún ejemplo, no verifican la validez del número de TDC del cliente, lo que SET si proporciona.

Algunas otras ventajas que tiene SET en comparación de SSL se muestran en el siguiente gráfico (Martínez López et al, 2009).

VENTAJAS	SSL	SET
Confidencialidad	X	X
Integridad	X	X
Autentifica los titulares de las tarjetas de crédito	X	X
Autentifica los comerciantes	X	X
Autentifica los bancos		X
Verifica que el comprador está autorizado a utilizar la tarjeta de crédito que le proporciona al vendedor		

Gráfico 11: Ventajas de SET ante SSL
(Martínez López et al, 2009)

SSL: Para la mayoría de las transacciones, este protocolo es válido, práctico y fácil de implantar además de asegurar las transacciones de una forma similar al comercio tradicional. Sin embargo, SSL deja de lado ciertos aspectos como para ser considerado una solución definitiva:

A. Sólo protege transacciones entre dos puntos (el servidor web comercial y el navegador del comprador). Cuando toda operación de pago con TDC involucra como mínimo tres partes: el consumidor, el comerciante y el emisor de tarjetas;

B. No protege al comprador del riesgo de fraude de su tarjeta;

C. Los comerciantes corren el riesgo de que el número de tarjeta de un cliente sea fraudulento o no tenga saldo (Martínez López et al, 2009).

Funcionamiento del protocolo SSL:

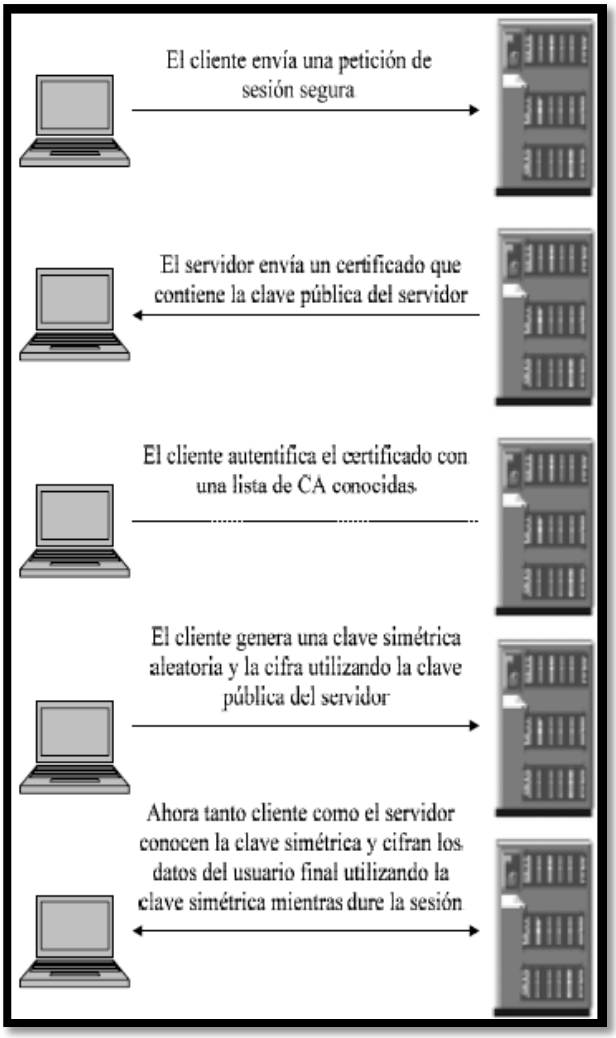

Gráfico 12: Funcionamiento de SSL

(Martínez López et al, 2009)

SET: Como complemento al protocolo SSL, MasterCard y Visa junto con American Express, se unieron y desarrollaron con esfuerzos un único protocolo para el pago electrónico con tarjetas, denominado SET (Transacción Electrónica Segura), el cual Luis Martínez et al, (2009) lo definen como un conjunto de normas o especificaciones de seguridad que constituyen una forma estándar para la realización de transacciones de pago a través de Internet.

Este protocolo a diferencia de SSL, sí es exclusivo para transacciones electrónicas y fue desarrollado para:

A. Proteger el sistema de TDC cuando es utilizado a través de Internet;
B. Generar en la mente del consumidor una opinión de confianza respecto al nuevo concepto de Internet como mercado,
C. Y generar nuevos tipos de transacciones financieras seguras.

SET se basa en el uso de una firma electrónica del comprador y una transacción que involucra, no sólo al comprador y al vendedor, sino también a sus respectivos bancos.

Cuando se realiza una transacción segura por medio de SET, los datos del cliente son enviados al servidor del vendedor, pero dicho vendedor sólo recibe la orden. Los números de la tarjeta del banco se envían directamente al banco del vendedor, quien podrá leer los detalles de la cuenta bancaria del comprador y contactar con su banco para verificarlos en tiempo real (gráfico 13).

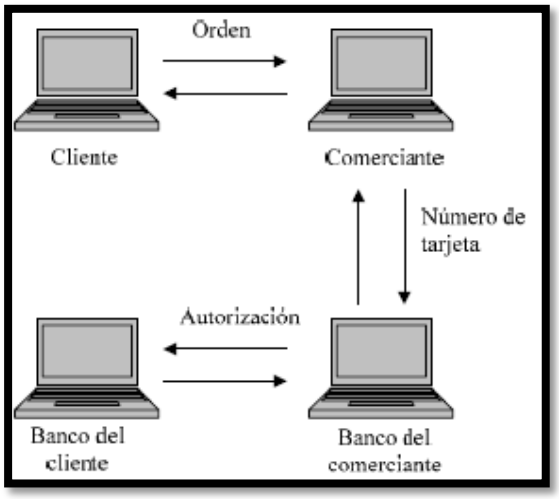

Gráfico 13: Funcionamiento de SET

Luis Martínez et al, (2009)

A continuación se agrega una gráfica con otras ventajas de SET ante SSL:

SSL	SET
El comercio puede conocer los datos de la tarjeta de crédito del comprador.	El comprador nunca introduce los datos de su tarjeta de crédito en la Red.
El comercio no puede comprobar si la compra se realiza con una tarjeta robada.	Se elimina la posibilidad de comprar con tarjeta robada.
El comercio no tiene ninguna prueba de que el titular de la tarjeta ha autorizado esa compra, lo que permite a éste repudiarla posteriormente sin que el comercio pueda hacer nada.	El comercio se garantiza que el comprador nunca podrá repudiar la transacción (la firma digital, correctamente emitida, tiene mayor validez legal que la propia firma manuscrita).
En caso de repudio, los gastos corren a cargo del comercio.	El banco nunca sabe qué está comprando el titular de la tarjeta.

Gráfico 14: Ventajas de SET ante SSL

(Nociones de comercio electrónico, 2007)

CAPÍTULO 4

PROTOCOLO PROPUESTO

1. Protocolo SET “Secure Electronic Transaction”

Secure Electronic Transaction (SET), o bien, Protocolo de Seguridad Electrónica en las Transacciones, es un protocolo que asegura la confidencialidad y la integridad de los pagos basados en tarjeta hechos por Internet, con independencia de quien sea el comprador y el vendedor del producto.

El Protocolo SET es un sistema de comunicaciones que permite gestionar de una forma segura las transacciones comerciales en la Red. Y cuando decimos de una forma segura nos referimos a que aporta un mayor nivel de seguridad que su antecesor el SSL (que surgió en 1994 por Netscape). Precisamente esa fue la razón que dio origen a su nacimiento.

Con la ayuda de los grandes fabricantes de la industria de ordenadores y programas, Visa y MasterCard se desarrolló el protocolo de pago por excelencia para la práctica del Comercio Electrónico minorista (es decir, venta entre comerciante y usuario final). SET (Secure Electronic Transaction); el cual lo describen como un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito (Buch i Tarrats et al).

El protocolo SET surge de la necesidad de las empresas y usuarios que realizan transacciones electrónicas de tener confianza y seguridad en las operaciones que realiza; así mismo fiabilidad e integridad de su información.

El temor al fraude con tarjetas de crédito retrae por igual a consumidores (que quieren estar seguros de comprar en una tienda real y que el comerciante no utilizará ilícitamente su tarjeta de crédito) y comerciantes (que de hecho se encuentran más desprotegidos que los clientes, ya que deben asumir los costes de transacciones ilícitas si más tarde el titular legítimo de la tarjeta rechaza el pedido), y este temor afecta tanto a los intereses económicos de los comerciantes, que ven reducidas sus ventas, como de las instituciones financieras, que ven disminuir sus comisiones por pagos con tarjeta.

El protocolo usado por la mayoría de las empresas era el protocolo SSL, y que actualmente es mucho más extendido en Internet que SET, pero este protocolo SSL no fue diseñado para interacciones entre múltiples partes, como las transacciones comerciales, que pueden llegar a involucrar hasta seis partes. SSL se limita a cifrar el número de tarjeta de crédito cuando es transmitido desde el navegador del cliente hasta el servidor del comerciante, resultando insuficiente para los requisitos de seguridad de un comercio electrónico fiable. Por esta razón, se menciona que el protocolo SSL no brindaba seguridad en las transacciones por Internet y no se podía mantener por más tiempo; por lo que en 1995 Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, o VeriSign, unieron sus fuerzas para desarrollar Secure Electronic Transaction (SET), un protocolo estandarizado y respaldado por la industria, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas, incluyendo Internet.

SET es un protocolo que surge debido a defectos en SSL a la hora de implementar alguna transacción segura. Estas carencias hicieron que diferentes empresas y organismos buscaran un nuevo sistema que permitiera realizar operaciones sensibles por Internet de forma segura, con el objeto de estimular la confianza de los consumidores en el comercio electrónico.

El protocolo SET fue desarrollado en 1996 por un grupo de empresas del sector financiero, informático y de seguridad: Visa International y MasterCard, con la colaboración de American Express, Microsoft, IBM, Netscape, VeriSign, RSA y otras empresas para dotar al comercio electrónico de mayores garantías de seguridad de las que tenía hasta entonces.

Estas empresas anunciaron el desarrollo de una nueva tecnología común destinada a proteger las compras a través de redes abiertas como Internet basadas en el uso de tarjetas de crédito. Esta nueva tecnología se conoce con el nombre de Secure Electronic Transaction (Transacciones Electrónicas Seguras), SET, y ha sido creada exclusivamente para la realización de comercio electrónico usando tarjetas de crédito. (Moreno, 2003).

SET se basa en el uso de certificados digitales (un certificado digital contiene un número de identificación de la entidad certificadora, el NIP del titular del certificado) para asegurar la perfecta identificación de todas aquellas partes que intervienen en una transacción on-line basada en el uso de tarjetas de pago, y en el uso de sistemas criptográficos de clave pública para proteger el envío de los datos sensibles en su viaje entre los diferentes servidores que participan en el proceso. Con ello se persigue mantener el carácter estrictamente confidencial de los datos, garantizar la integridad de los mismos y autenticar la legitimidad de las entidades o personas que participan en la transacción, creando así un protocolo estándar abierto para la industria que sirva de base a la expansión del comercio electrónico por Internet.

Las especificaciones formales del protocolo SET se hicieron públicas el 31 de mayo de 1997, y se pueden encontrar en el sitio web oficial de SETco, organismo encargado de homologar los módulos de programación y los certificados desarrollados por empresas privadas que se usen en implementaciones del protocolo SET.

Algunas de estas especificaciones son que el protocolo SET usa criptografía asimétrica (RSA) para las firmas y para el cifrado de las claves de cifrado simétrico y de los datos bancarios y criptografía simétrica (DES) para la transmisión del resto de los datos involucrados en la transacción. Las claves usadas son de 128 bytes y SHA-1 la función hash usada para la verificación de integridad de los mensajes (Vázquez, 2002).

Sus metas son (Prezi Inc, 2014):

1. Permitir la transmisión confidencial;
2. Autenticar a las partes involucradas;
3. Asegurar la integridad de las instrucciones de pago por bienes y servicios;
4. Autenticar la identidad del tarjeta ambiente y del comerciante entre sí.

2. Arquitectura de SET

La arquitectura de SET permite efectuar metas que el protocolo propone; entre las más importantes Lemos Ponce, Moran Vera & Cabrera Sarmiento, (2006) mencionan:

A. Permitir la transmisión confidencial;
B. Autenticar a las partes involucradas;
C. Asegurar la integridad de las instrucciones de pago por bienes y servicios;
D. Autentificar la identidad del tarjeta habiente y del comerciante entre sí.

Arquitectura de SET:

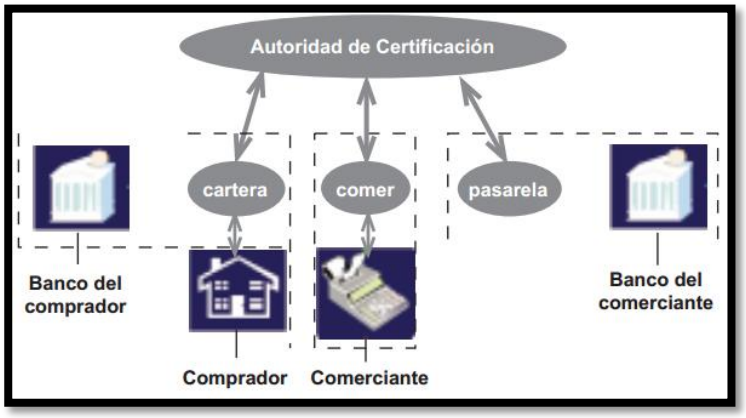

Gráfico 15: Arquitectura SET

Lemos Ponce, Moran Vera & Cabrera Sarmiento, (2006)

3. Componentes de SET:

Éste protocolo se compone de 3 entidades: comerciante, titular y pasarela (Buch i Tarrats et al).

A. Entidad “Merchant” SET o Comerciante SET: es la entidad que se encarga de gestionar el pago del bien o servicio iniciado por un comprador.

Y cabe mencionar que el pago siempre lleva asociado una transacción con un aceptador (“acquirer”) para la autorización del importe a pagar por el comprador. Habitualmente a esta entidad se le denomina POS (“Point Of Sale”) o TPV (Terminal Punto de Venta) virtual ya que su comportamiento, entre otras funciones, simula el de los sistema tradicionales.

B. Entidad “Cardholder” SET o Titular SET: es la encargada de actuar en nombre del titular de la tarjeta virtual para realizar el pago.

Habitualmente a esta entidad se le conoce como Wallet o Cartera ya que su funcionalidad es muy similar a una cartera en la cual se almacenan las tarjetas.

C. Entidad “Gateway” SET o Pasarela SET: su función es la de hacer de puente entre el sistema aceptador SET y el sistema financiero propietario ya existente.

Esta entidad es muy importante en cuanto supone la conexión de los sistemas y redes de autorización privados existentes con el mundo de Internet.

Son muy importantes éstas tres entidades, ya que forman parte de la arquitectura del protocolo SET; el cual define los mensajes e interacciones entre las entidades SET (comprador, comerciante y pasarela de pago) para llevar a cabo una transacción de pago desde que el comprador acepta pagar hasta que dicho pago, se realiza mediante un abono en la cuenta del comerciante desde la cuenta del comprador de manera segura. La siguiente figura muestra un esquema en el que aparecen los mensajes e interacciones típicas de un pago:

4. Proceso de pago para transacciones electrónicas con SET:

El proceso de pago que se realiza con el protocolo SET para efectuar cualquier transacción electrónica, consta de diez fases (Vázquez, 2002):

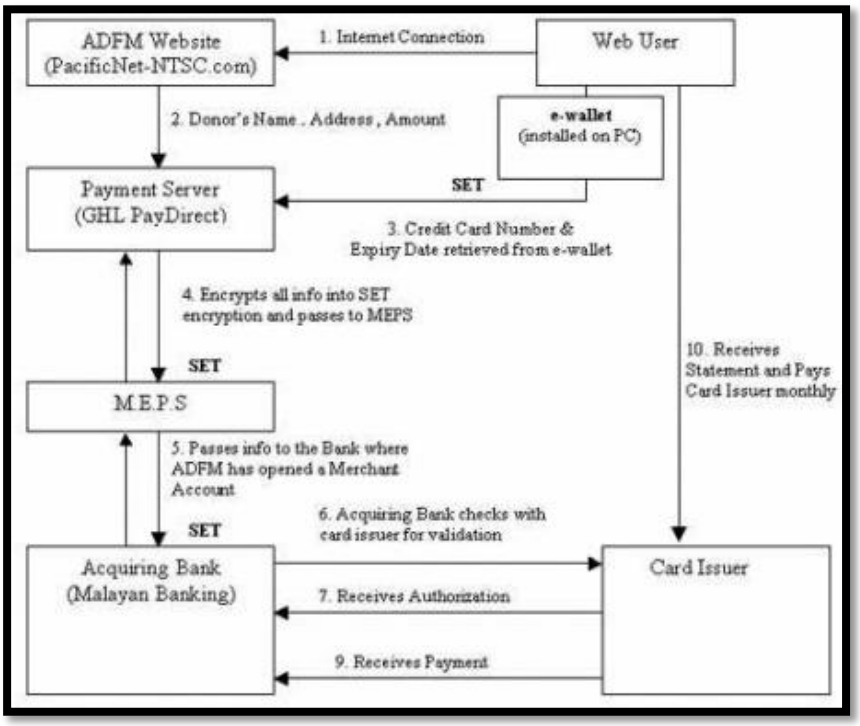

Gráfico 16: Proceso de pago SET
(Vázquez, 2002):

A. El cliente elige el producto o servicio que desea comprar y el vendedor le presenta en la web una página en la que detalla los precios y condiciones y le pide confirmación de la transacción;

B. El cliente acepta las condiciones y elige SET como forma de pago. En este momento se inicia el protocolo mediante el envío por parte del vendedor de una descripción del pedido al cliente que arranca en el ordenador de este la aplicación de 'cartera' electrónica;

C. El cliente comprueba la orden de pedido recibida, elige la forma de y transmite la orden de pago al vendedor.

La aplicación de cartera electrónica crea, a tal efecto, dos mensajes que envía al vendedor: uno de ellos contiene los datos del pedido, dirección de entrega, etc. y el otro las instrucciones de pago (número de tarjeta, banco emisor, etc.).

El software de cartera genera un mensaje cifrado y firmado dualmente de forma que el vendedor pueda acceder tan sólo al primer mensaje y el banco a la segunda.

D. El vendedor (en realidad el software de SET en su servidor) retransmite este mensaje, una vez recibido, a su banco;
E. El banco del vendedor descifra y valida la petición obteniendo las instrucciones de pago del cliente y verificando la integridad de los datos, la identidad del vendedor y la validez de la transacción.

Si todo es correcto se envía una petición de autorización al banco del cliente por los canales dedicados a tal efecto;

F. El banco del cliente verifica la identidad del mismo, la validez de la tarjeta, la existencia de crédito y, si todo está en orden, autoriza la transacción;
G. Cuando el banco del vendedor recibe la autorización genera y firma digitalmente un mensaje con el testigo de la autorización y transferencia de fondos que, una vez cifrado, se envía al vendedor;
H. Cuando el vendedor recibe este mensaje y lo verifica, almacena el testigo de la transferencia, autoriza el suministro o proceso de los servicios demandados por el cliente y le envía a este un recibo de la compra que recoge la aplicación de “cartera” electrónica y que actúa como justificante de la misma;
I. Una vez procesado con éxito el pedido, el vendedor genera una petición de transferencia a su banco;
J. Se hace efectivo el cargo en la cuenta del cliente.

De acuerdo con Moreno (2003):

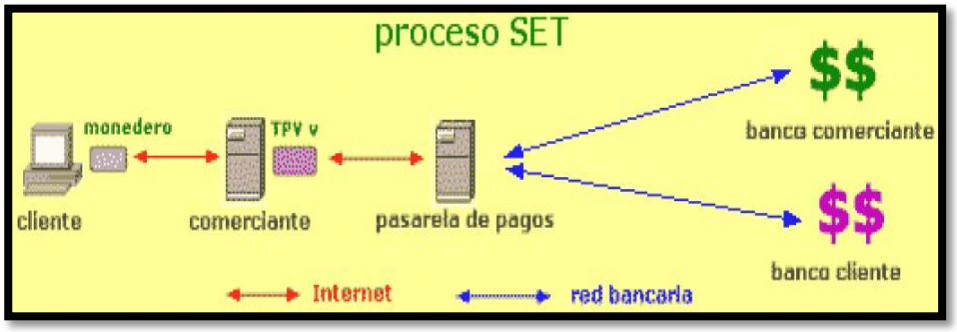

Gráfico 17: Proceso de Pago con SET

Moreno (2003)

El proceso de pago en una transacción electrónica usando el protocolo SET admite un gran número de opciones diferentes pero, consta de los siguientes pasos:

A. El cliente, tras seleccionar los artículos a comprar en el sitio web del vendedor, envía a éste un formulario de pedido, siendo respondido por el comerciante con el envío de su certificado digital y el de la pasarela de pago.

El cliente comprueba la validez de los certificados y envía entonces al comerciante una orden de pago, que está dividida en dos secciones o documentos diferentes: la información de pedido (OI), en la que figuran los datos de los productos comprados, su precio y las demás informaciones necesarias para la compra, y la instrucción de compra (PI), en donde se describen sus datos bancarios y se dan instrucciones para el pago a la entidad vendedora;

B. Esta orden de pago se firma digitalmente por medio de un algoritmo especial, denominado firma dual, que se realiza concatenando primero los resúmenes hash de los dos documentos generados y encriptado esta concatenación después con su llave privada, para seguidamente encriptar la firma dual mediante una clave simétrica generada por su software SET.

Por último, se encriptan la clave simétrica generada y el número de la tarjeta de crédito con la llave pública de la pasarela de pago.

C. El vendedor recibe la orden de compra y la firma dual del cliente, se queda con la descripción de la compra y tras comprobar la autenticidad del comprador, utilizando para ello la firma digital de éste y su certificado, y la integridad de los datos recibidos envía los datos financieros a la Pasarela de Pago encriptados con la clave pública de la misma.

D. La Pasarela de Pago comprueba la autenticidad del comprador y la integridad del PI del mismo, y con el mensaje del vendedor comprueba la relación existente entre la descripción de la compra enviada al vendedor y la usada para la firma dual recibida;

E. Si todo es correcto, la Pasarela de Pago envía mediante las redes de comunicación bancarias el PI al banco del vendedor y solicita autorización para realizar el pago, mediante un documento denominado petición de autorización de pago;

F. El banco del vendedor comprueba entonces que la tarjeta de crédito es válida y permite el cargo del importe de la compra, enviando entonces un documento a la pasarela, denominado autorización de pago, que autoriza el proceso de compra;

G. Una vez informado el vendedor de la autorización procede al envío de los artículos comprados al cliente, y después de la entrega física del producto pide el importe de la venta a la Pasarela de Pagos, proceso que se conoce con el nombre de solicitud de pago;

H. Entonces la Pasarela de Pagos pide al banco del comprador la transferencia del importe de la venta al banco del vendedor, petición que recibe el nombre de solicitud de compensación. Entonces se le hace efectivo al vendedor el importe, con lo que se cierra el proceso total de compra.

De manera resumida se describe el proceso de pago para realizar transacciones electrónicas seguras con SET en 3 fases:

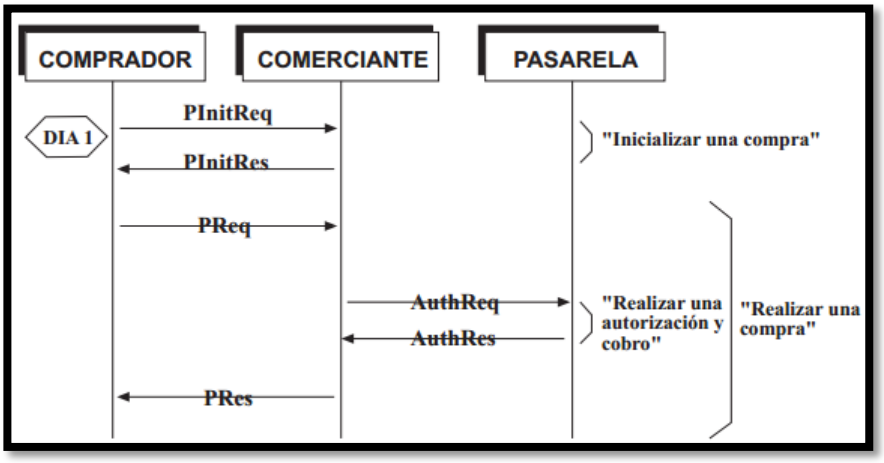

Gráfico 18: Protocolo de pago SET

Moreno (2003)

1. La fase de inicialización: que corresponde al mensaje PInit y en la que el comprador contacta con el comerciante.

El comprador informa de la marca de tarjeta que va a utilizar en el pago y el comerciante responde con un mensaje firmado que contiene el certificado de cifrado de la pasarela de pago asociada;

2. En la fase de pago: que corresponde al mensaje P y en la que el comprador, si acepta el pago después de verificar la identidad del comerciante y las condiciones, realizara la orden de pago. La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago proveniente de la autorización;
3. La última fase, que es la de Autorización: corresponde al mensaje Auth y en el que el comerciante solicita a la pasarela de pago (que a su vez solicitará al sistema financiero tradicional) si el comprador puede hacerse cargo de dicho pago (tiene crédito o saldo, la tarjeta no está revocada, etc.). La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago.

SET implementa el sistema de firma dual en el que el comprador en el mensaje PReq incluye datos protegidos para el comerciante y para la pasarela de forma que, el comerciante sólo puede ver los datos de la compra (pedido, modo de pago, cantidad, etc.) y la pasarela sólo puede ver los datos de pago (número de tarjeta, modo de pago, cantidad, etc.) que se enviarán en el mensaje AuthReq. De esta forma el comerciante nunca tendrá el número de tarjeta del comprador y la entidad financiera (a través de la pasarela) nunca tendrá los datos de la compra.

Cabe mencionar que además de las fases y mensajes vistos, SET proporciona también servicios para retrocesos o cambios de autorizaciones realizadas y administración de “batchs”.

5. Características de SET

El uso del protocolo SET aporta una serie de beneficios de carácter inmediato:

A. Autentica los titulares de TDC, comerciantes y bancos que intervienen en operaciones electrónicas por Internet;
B. Garantiza la máxima confidencialidad de la información del pago;
C. Asegura que los mensajes financieros no serán manipulados dentro del circuito del proceso de pago; y de esta manera evitar fraudes;
D. Proporciona inter-operatividad entre distintas plataformas HW y SW;

Con ello, el protocolo evita:

A. El pago de compras mediante tarjetas de crédito no autorizadas;
B. El robo de información financiera del comprador.

Por otra parte, Lemos Ponce et al. (2006) mencionan:

E. SET utiliza encriptación para brindar confidencialidad en la comunicación, y firmas digitales para autenticación;
F. Con SET, se pide a los comerciantes certificados digitales emitidos por sus bancos adquirientes, para los consumidores es opcional;
G. SET permite incluir información privada entre el consumidor y el comerciante y entre el consumidor y el banco en una sola transacción firmada mediante una estructura criptográfica conocida como firma dual.

Y Moreno (2003), hace mención a las siguientes características:

H. Es un estándar abierto y multiplataforma; de mensaje, certificados, etc., sin limitación alguna respecto al lenguaje de programación o S.O.;
I. Su principal objetivo es la transferencia segura de números de TDC;
J. Utiliza codificación estándar;
K. Es independiente del medio de comunicación utilizado. Fue diseñado para su uso en Internet, pero permite la conexión a través de cualquier tipo de red siempre que se definan los interfaces adecuados. Además, el protocolo SET se puede transportar directamente mediante TCP y HTTP en páginas web;
L. Utiliza estándares criptográficos reconocidos y ampliamente usados;
M. Se basa en el uso de la Criptografía de Clave Pública;
N. Realiza una Autenticación de todas las partes participantes en la transacción usando certificados digitales;
O. A diferencia del proceso de SSL (en donde solo intervienen dos entidades: el Comprador (Cardholder) y el Vendedor (Merchand)). SET incluye otras entidades adicionales necesarias para la transacción:
  i. La Pasarela de Pago (Gateway Payment), que permite la comunicación directa a través de Internet entre el comerciante y las Redes Bancarias, con lo que el papel del vendedor queda limitado a un mero intermediario entre el cliente y su banco.

Puede ser una entidad independiente o el mismo banco del comerciante. Y son las encargadas de conectar a los comerciantes con las entidades financieras. Reciben peticiones de autorización, liquidación o reconciliación de pagos de los sistemas comerciales TPV Virtuales y las encaminan hacia los sistemas autorizadores de pago tradicionales.

j. El Banco o entidad financiera (Issuer) que ha emitido la tarjeta de crédito que va a usar el cliente en el proceso de pago;

k. El Banco del comerciante (Adquirer), en el que éste tiene su cuenta.

Además de estas entidades principales existen otras dos relacionadas con ellas:

l. La empresa propietaria de la marca de la tarjeta de crédito, como Visa, MasterCard, American Expres, etc., que avalan las tarjetas;

m. Y las autoridades de certificación, que emiten los certificados digitales usados como medio de autenticación de las entidades que intervienen directamente en la operación.

Pueden ser entidades independientes autorizadas, bancos o los mismos propietarios de la marca de la tarjeta.

6. Las ventajas del protocolo SET

Luis Martínez et al (2009) hacen referencia a las siguientes:

A. Los compradores, los comerciantes, los intermediarios financieros y los bancos tendrán la confianza de saber que cada transacción electrónica está protegida por un protocolo de validación aceptado;
B. La principal aportación del protocolo SET es la garantía de la confidencialidad y la no manipulación de la información financiera personal;

Por otra parte:

SET brinda autenticación, privacidad e integridad en los sistemas de pago y operaciones que se realizan vía electrónica; es decir:

C. Proporciona seguridad en las transacciones electrónicas;
D. Brinda autenticidad en las transacciones;
E. Y no repudio en las operaciones.

A pesar de las diferentes ventajas que exponen a continuación los autores, SET se caracteriza por brindar autenticación y privacidad de la información, a través de las redes abiertas donde pueden ser interceptados los mensajes. Se debe asegurar que la información transmitida, tanto en la orden de pedido, como en la orden de pago, sólo sea leída por el destinatario autorizado. Así mismo, proporciona integridad de los mensajes, asegurándose que no se alteren los datos del mensaje durante su transmisión.

7. Desventajas de SET

A pesar de que SET es un protocolo muy completo, el más completo y seguro de todos los que existen actualmente, también cuenta con algunas desventajas. Desventajas de porque algunas empresas no lo implementan. Éstas son:

A. Debido a su gran contenido de funcionalidad y sus altos grados de seguridad,

SET es un sistema complejo y ha hecho que los fabricantes tardaran mucho en tener un sistema completo y estable en el mercado.

La misma causa ha hecho que los distintos desarrollos comerciales se encontraran ciertos aspectos de incompatibilidad a nivel de protocolo y funcionalidad.

B. Las grandes inversiones de los fabricantes de sistemas SET en el desarrollo han hecho que los precios de los productos sean elevados frenando de este modo su adquisición masiva.

Además, coyunturalmente tampoco parece que el comercio electrónico (minorista en este caso) haya despegado masivamente así que las inversiones en infraestructura no suponen una de las prioridades inmediatas y se hacen a un ritmo lento.

C. Existe algún problema de aceptación en el usuario final (sobre todo del comprador). Debido también a la complejidad del sistema, en la mayoría de los casos el producto final resulta complejo de instalar y administrar.

Mientras que Moreno (2003) menciona:

SET proporciona buenas cualidades de seguridad, integridad, autenticidad y no rechazo en las transacciones comerciales por redes abiertas basadas en el pago mediante tarjetas de crédito, y que existe un gran empuje por parte de las principales empresas financieras y expendedoras de tarjetas de crédito para estandarizar su uso, pero el caso es que no se ha logrado un desarrollo e implementación masivo del mismo por las siguientes desventajas:

A. La complejidad intrínseca del mismo. Con SSL el usuario no tiene que hacerse con certificado alguno (normalmente), ni tiene que andar instalando en su ordenador software adicional; tan sólo debe seleccionar los productos que desea comprar y aceptar el pago.

B. La relativa lentitud de proceso de SET, al tener que realizarse diferentes verificaciones de identidad e integridad por parte de diversas entidades a lo largo de una transacción.

Por todo esto, y aunque cada vez se pueden encontrar más tiendas virtuales que usan SET, sigue siendo SSL el protocolo más usado en las transacciones por Internet. (Moreno, 2003).

8. Uso y funcionamiento del protocolo SET en la actualidad:

En 1996, las compañías emisoras de medios de pago, Visa y MasterCard, desarrollaron el sistema SET, una aplicación de certificación digital para el pago con tarjeta de crédito a través de Internet, que nació con grandes expectativas de crecimiento, aunque su implantación ha sido mucho más lenta de lo esperado, ya que las inversiones que requiere por parte de las entidades financieras son muy elevadas y porque la tecnología resulta pesada y su utilización algo compleja para el usuario.

A pesar de todo, la apuesta de Visa Internacional por SET es firme en Europa, donde se está buscando una solución para que, en un plazo de dos años, converjan los sistemas que se tratan de instalar en Europa y los que están implantando en EEUU. La empresa ha anunciado que ya se ha ideado un sistema que posibilita la implantación de SET de una forma no tan costosa ni tan compleja de utilización para el cliente final, mediante la creación de servidores por parte de los bancos que almacenen de forma segura los certificados personales de sus usuarios.

En esencia, los planes de Visa pretenden que ningún titular de una tarjeta pueda realizar una compra online y posteriormente repudiarla. Para ello, la multinacional obligará a aquellos bancos que no certifiquen a sus usuarios a cargar con el peso de la operación en vez del comercio, al que se le garantizará el pago de la compra siempre que permita a sus clientes pagar mediante SET.

Otro de los grandes cambios que introduciría SET es el de las comisiones. Con el sistema actual los bancos, para cubrirse las espaldas ante el riesgo de fraude, cobran a los comercios comisiones que oscilan entre el 2.75% y el 6%, cifras mucho más altas que las del mundo tradicional, donde se aplican tarifas distintas a cada tipo de producto pero la media ronda el 1.3%.

Los expertos coinciden en que con SET se equipararán las transacciones de Internet a las presenciales, por lo que las comisiones también deberían igualarse.

Ya que es un protocolo seguro, Bancos como Banesto y Banco Sabadell, ya están emitiendo certificados digitales para sus clientes. El primero para particulares de banca online (donde ya se puede operar y firmar las operaciones tanto con el sistema tradicional de contraseña como por un certificado emitido por el propio banco) y el segundo para las empresas clientes que hagan uso de su servicio de banca online (actualmente un 35%).

SET se basa en el estándar de certificación digital ISO X—509 V3, que es la norma internacional que dicta el formato estándar que tiene un certificado digital: cómo debe estar ordenado y qué elementos debe contener. *SET* utiliza este formato con algunos añadidos. Todos los sistemas de certificación digital deben adecuarse a estas directrices.

CONCLUSIONES

El presente proyecto pretende mostrar a las empresas dedicadas a e-commerce, que existen protocolos para llevar a cabo transacciones electrónicas de forma segura, con el objetivo de incrementar su confianza en este tipo de transacciones por internet.

Para ello, se muestran algunas comparaciones de los protocolos existentes en la actualidad, siendo SET el protocolo que proporciona mayor seguridad, fiabilidad, confianza e integridad en las operaciones que se realizan, a través de los sistemas de autenticación y de encriptación de información que maneja.

Se propuso este protocolo “SET” porque a diferencia de otros protocolos, SET es el protocolo que aporta e implanta mayor seguridad en las transacciones realizadas sobre la red Internet, aunque es demasiado complejo.

Finalmente, es importante resaltar la importancia de utilizar este protocolo; y se realiza esta propuesta para impulsar a las empresas dedicadas a e-commerce adopten este protocolo, ya que:

A. Se pueden mejorar los sistemas de pago si las empresas usan SET;
B. Con el uso del protocolo SET, existen mejoras en los procesos generales de pago y al mismo tiempo, se reducen fraudes al realizar este tipo de transacciones;
C. SET es el protocolo que actualmente aporta el mayor grado de seguridad;
D. SET facilita la realización de transacciones de comercio electrónico de forma al menos, tan simple y segura como en el comercio tradicional;
E. El uso del protocolo SET aporta una serie de beneficios de carácter inmediato;

F. Autentica los titulares de las tarjetas de crédito, los comerciantes y los bancos que intervienen en las operaciones comerciales por Internet;
G. Garantiza la máxima confidencialidad de la información del pago.

Por otra parte, las empresas dedicadas a e-commerce que usan el protocolo SSL para realizar transacciones electrónicas, deben cambiar este protocolo y comenzar a basar la seguridad de sus operaciones en SET, ya que:

H. SSL no protege al comprador del riesgo de que un comerciante utilice ilícitamente su tarjeta;
I. Los comerciantes corren el riesgo de que el número de tarjeta de un cliente sea fraudulento o que ésta no haya sido aprobada;
J. SSL no ofrece su seguridad ni sus garantías.

Finalmente, como conclusión en general, la hipótesis planteada en la investigación es correcta, ya que SET cumple con los requisitos de ser el mejor protocolo que las empresas dedicadas a e-commerce pueden adquirir. Además:

1. Permite la transmisión confidencial;
2. Autentica a las partes involucradas;
3. Es un protocolo que asegura la integridad de las instrucciones de pago por bienes y servicios;
4. Y autentica la identidad del tarjeta ambiente y del comerciante entre sí.

BIBLIOGRAFÍA

1. Alberto Luis Corrales Hermoso, Corrales Hermoso, Alberto Luis, Beltrán Pardo, Marta, Guzmán Sacristán Antonio, Marta Beltrán Pardo, Antonio Guzmán Sacristán. Diseño e implantación de arquitecturas informáticas seguras. Una aproximación práctica. Madrid: Dykinson (2006).
2. Alonso García- Cervigón Hurtado, María del Pilar Alegres Ramos. Seguridad Informática. Madrid, España: Paraninfo (2011).
3. Amipci. El 74 por ciento de los internautas mayores de edad hace uso de servicios bancarios en línea. Obtenido de http://www.amipci.org.mx/?P=articulo&Article=131. (14 de Agosto de 2012). Fecha de Consulta: 21 de Septiembre de 2013.
4. Ana Belén Alonso Conde. Comercio Electrónico: Antecedentes, Fundamentos y Estado Actual. Madrid: Dykinson (2004).
5. Ángel Cobo, Patricia Gómez, Daniel Pérez, Rocío Rocha. Php y MySql. Tecnologías para el desarrollo de aplicaciones web. España: Díaz de Santos (2005).
6. Carolina Droguett Ibarra, Tania Paine Cabrera Eliana Riveros Contreras. Tesis Electrónica. E-commerce en el Turismo: Modelamiento del perfil de clientes que prefieren comprar servicios turísticos por internet Obtenido de http://www.tesis.uchile.cl/tesis/uchile/2010/ec-droguett_ca/pdfAmont/ec-droguett_ca.pdf (2010).
7. Copyright. Negocios Virtuales. E-commerce. Obtenido de http://www.negociosvirtualesweb.com/ecommerce.php (2013).
8. Daniel Arias Figueroa. Herramientas de Gestión basada en Web. Tesis Magister en Informática. Obtenido de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Arias_Figueroa.pdf (Diciembre de 1999).
9. Diario Bae Negocios. Proyectan un crecimiento del 45% en el comercio electrónico local. (20 de Mayo de 2013).

10. Gabriel Díaz, Francisco Mur, Elio San cristóbal, Manuel- Alonso Castro, Juan Peire. Seguridad en las comunicaciones y en la información. Madrid (2012).

11. Irma Contreras López. Tesis: La firma electrponica y la función notarial en Jalisco. Obtenido de http://www.revistanotarios.com/files/La-Firma-electronica.pdf (2009).

12. Jaime Gutiérrez, Juan Tena. Protocolos criptográficos y Seguridad en Redes. Universidad de Cantabria (2003).

13. Javier Draxl – Alignet. Cómo bajar el fraude y mejorar la seguridad de las transacciones. Obtenido de http://www.ecommerceday.pe/wp-content/uploads/2010/11/Draxl.pdf (Noviembre de 2010).

14. Javier Mauricio Pardo, Santiago Rodriguez Olivos. Tesis de Ingenieria en Sistemas. Análisis de la problemática de los medios de pago en el comercio electrónico. Obtenido de http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis211.pdf (2005).

15. Jordi Buch i Tarrats, Francisco Jordán. La seguridad de las transacciones bancarias en Internet. Obtenido de http://www.seis.es/documentos/informes/secciones/adjunto1/6BuchTarrats.pdf

16. Jose Daniel Britos. Tesis de Maestria en Redes de Datos. Detección de Instrucciones en redes de datos con captura distribuida y procesamiento estadístico. Obtenido de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Britos_Jose_Daniel.pdf (1 de Septiembre de 2010).

17. José María Morales Vázquez. Master de Seguridad Informática SSL, Secure Socket Layers y Otros Protocolos Seguros para el Comercio Electrónico. Obtenido de http://pics.unlugarenelmundo.es/hechoencasa/ssl%20secure%20sockets%20layer%20y%20otros%20protocolos%20seguros%20para%20el%20comercio%20electronico.pdf (2002).

18. Lenin Lemos Ponce. Tesis de Grado “Seguridad en el comercio electrónico a través de redes provadas virtuales”. (2006).

19. Lic. Gonzálo Ernesto Domingo Tesis de Grado “Seguridad en las transacciones on line de coemrcio electrónico”. Obtenido de http://campus.dokeos.com/courses/0025/document/certificates/comercio.pdf?cidReq=0025 (2002).

20. Luis Martínez López. Revista de Estudios Empresariales. Sistemas de Pago Seguro. Seguridad en el commercio electrónico (2009).

21. Mattos Lescano, Elisa Zoraida. Tesis “Seguridad en el comercio electrónico”. Obtenido de http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/mattos_le/cap3.PDF.

22. Ontsi. Razones del consumidor final para no comprar por Internet. Obtenido de http://www.ontsi.red.es/ontsi/es/indicador/razones-del-consumidor-final-para-no-comprar-por-internet (2011).

23. Profeco. Comercio Eletronico. Obtenido de http://www.profeco.gob.mx/internacionales/com_elec.asp (2 de Julio de 2012).

24. Purificación Aguilera López. Seguridad Informática. Madrid: Editex, S.A (2010).

25. Victoria del Rosario Pivaral Leal, Giovanni Obdulio Chajón Arriaza. Tesis de Comercio Electrónico en Internet: E-commerce. Obtenido de http://www.tesis.ufm.edu.gt/pdf/2998.pdf (2 de Agosto de 2000).

26. Jannelle, P. (21 de Abril de 2014). *Situación actual del comercio electrónico en EE.UU, México y España*. Obtenido de Ecommerce, shopify: http://es.shopify.com/blog/13815633-situacion-actual-del-comercio-electronico-en-ee-uu-mexico-y-espana#axzz38ajEcKe6

27. Instituto Nacional de Estadística. (01 de 2014). *El comercio electrónico y el uso de las nuevas tecnologías.* Obtenido de Compras por Internet: http://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259943296411&p=1254735116567&pagename=ProductosYServicios/INECifrasINE_C/PYSDetalleCifrasINE

28. Cooperación en Red Euro Americana para el Desarrollo Sostenible. (28 de Julio de 2014). *Cinco razones para comprar por Internet.* Obtenido de http://www.creadess.org/index.php/informate/sostenibilidad-empresarial/marketing-digital/6093-cinco-razones-para-comprar-por-internet

29. Prezi Inc. (2014). *Seguridad en las Transacciones Electrónicas*. Obtenido de http://prezi.com/swf_oozkmytm/seguridad-en-las-transacciones-electronicas/

VOTO APROBATORIO

Toda vez que el trabajo de evaluación profesional, ha cumplido con los requisitos normativos y metodológicos, para continuar con los trámites correspondientes que sustentan la evaluación profesional, de acuerdo con los siguientes datos:

Nombre del pasante	Yoselin Monserrat Sánchez Casas		
Licenciatura	Informática Administrativa	Nº de cuenta	0550101
Opción	TESIS	Escuela de Procedencia	Facultad de Contaduría y Administración
Nombre del Trabajo para Evaluación Profesional	Propuesta para que las Empresas dedicadas a E-commerce usen el Protocolo Secure Electronic Transaction "SET" para brindar Seguridad en las Transacciones. 160/11/13		

NOMBRE		FIRMA DE VOTO APROBATORIO	FECHA
ASESOR	M. en A. Juan Carlos Montes de Oca López		18-08-2014

NOMBRE		FIRMA Y FECHA DE RECEPCIÓN DE NOMBRAMIENTO	FIRMA Y FECHA DE ENTREGA DE OBSERVACIONES	FIRMA Y FECHA DEL VOTO APROBATORIO
REVISOR	L.I.A. Alejandro Domínguez Bond	03-09-2013		17-09-2014
REVISOR	MTI Jorge Ignacio Pérez Morales	03-09-2013		22/09/14

Derivado de lo anterior, se le **AUTORIZA LA REPRODUCCIÓN DEL TRABAJO DE EVALUACIÓN PROFESIONAL** de acuerdo con las especificaciones del anexo 8.7 "Requisitos para la presentación del examen de evaluación profesional".

NOMBRE		FIRMA	FECHA
ÁREA DE EVALUACIÓN PROFESIONAL	C.P. Angela Cecilia Orozco Solano		23/09/14

FACULTAD DE CONTA... Y ADMINISTRACIÓN
DEPARTAMENTO DE ... ACADÉMICO

CARTA DE CESIÓN DE DERECHOS DE AUTOR

El que suscribe Yoselin Monserrat Sánchez Casas Autor del trabajo escrito de evaluación profesional en la opción de Tesis con el título "Propuesta para que las Empresas dedicadas a E-commerce usen el Protocolo Secure Electronic Transaction "SET" para brindar Seguridad en las Transacciones", por medio de la presente con fundamento en lo dispuesto en los artículos 5, 18, 24, 25, 27, 30, 32 y 148 de la Ley Federal de Derechos de Autor, así como los artículos 35 y 36 fracción II de la Ley de la Universidad Autónoma del Estado de México; manifiesto mi autoría y originalidad de la obra mencionada que se presentó en Toluca Estado de México para ser evaluada con el fin de obtener el Título Profesional de Licenciado en Informática Administrativa.

Así mismo expreso mi conformidad de ceder los derechos de reproducción, difusión y circulación de esta obra, en forma NO EXCLUSIVA, a la Universidad Autónoma del Estado de México; se podrá realizar a nivel nacional e internacional, de manera parcial o total a través de cualquier medio de información que sea susceptible para ello, en una o varias ocasiones, así como en cualquier soporte documental, todo ello siempre y cuando sus fines sean académicos, humanísticos, tecnológicos, históricos, artísticos, sociales, científicos u otra manifestación de la cultura.

Entendiendo que dicha cesión no genera obligación alguna para la Universidad Autónoma del Estado de México y que podrá o no ejercer los derechos cedidos.

Por lo que el autor da su consentimiento para la publicación de su trabajo escrito de evaluación profesional.

Se firma presente en la ciudad de Toluca, Estado de México, a los 23 días del mes de Septiembre de 2014.

Yoselin Monserrat Sánchez Casas

Nombre y firma de conformidad