UNIVERSIDAD DE SOTAVENTO A.C.
FACULTAD DE INFORMATICA
INCORPORADA A LA UNAM

" SEGURIDAD EN TRANSACCIONES ON-LINE"

TESIS PROFESIONAL

PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA ADMINISTRATIVA

QUE PRESENTA:

JOSE DANIEL MENDEZ GONZALEZ

ASESOR DE TESIS:

LIC. RAUL DE JESUS OCAMPO COLIN

COATZACOALCOS, VER MARZO DE 2008

AGRADECIMIENTOS

Agradezco en primer lugar profundamente a Dios por todas las bendiciones que me da a mí y a mi familia.

En segundo lugar agradezco profundamente a mi familia por todo el apoyo que me han brindando durante esta larga jornada que es la vida de estudiante y sus acertados consejos y llamadas de atención.

En tercer lugar, por ultimo y no menos importante agradezco de todo corazón a mis maestros que durante todos un cada uno de los semestres cursados me brindaron su confianza y amistad además de los conocimientos necesarios para ser parte del mundo laboral.

INDICE

CAPITULO I

Capitulo II (Marco Teórico)

Capitulo III

CAPITULO IV

CAPITULO V

ENUNCIADO PROBLEMA

¿Cómo se sabe que una transacción electrónica ha sido realizada de manera segura?

HIPOTESIS

En los últimos 15 años se ha expandido el Internet a nivel mundial y con esto el crecimiento del comercio electrónico el cual ha sido bien recibido por los millones de usuarios que navegan en Internet. Esta forma de comercio ha sido adoptada por un gran número de empresas que han encontrado en el comercio electrónico una herramienta que genera importantes utilidades para sus negocios. Sin embargo los sitios donde se ofrecen dichos productos y servicios no siempre seguros y se pude poner en riesgo los datos personales de los usuarios.

OBJETIVO GENERAL

Asegurar que una transacción on-line se lleve a cabo correctamente.

OBJETIVOS DEL PROYECTO

- Conocer los conceptos relacionados a las transacciones on-line.
- Conocer como se garantiza la seguridad de los datos y la manipulación de los estos.
- Conocer las arquitecturas que se usan.
- Identificar un sitio seguro
- Empresas que ofrecen seguridad de datos en referencia a las transacciones on-line.

JUSTIFICACIÓN

Este trabajo de investigación se realiza para mostrar de forma general el funcionamiento de la seguridad en las transacciones on-line, así como también se hace mención a una serie de pasos que orientan a los usuarios como llevar a cabo una transacción on-line de manera segura. Ya que dichas operaciones se han vuelto acciones cotidianas en la vida diaria de las personas.

INTRODUCCION

El trabajo de investigación que se presenta en las siguientes páginas trata sobre un tema de interés común en todo el mundo que son las transacciones on-line y en que en la actualidad y en futuro muy próximo regirán nuestra forma de vida en el aspecto de la adquisición de bienes y servicios vía on-line. Por esa razón esta investigación trata de una manera general los aspectos de seguridad involucrados en una transacción electrónica dándonos a conocer los protocolos, encriptación o programas de seguridad especializados para transacciones electrónicas.

Las transacciones electrónicas surgen de una solicitud de un estándar de seguridad por VISA y MasterCard en febrero de 1996 y la especificación inicial involucro un amplio rango de compañías tales como: GTE, IBM, Microsoft, Netscape, RSA y VeriSing.

Todo este fenómeno nace a partir de la aparición del Internet, que comienza como un proyecto militar denominado ARPANET el cual pretendía crear una red de comunicación de tal forma que si un sector de la red colapsaba totalmente los mensajes pudieran encontrar el camino hasta su destino de cualquier manera.

Pero el verdadero cambio llega en el año de 1983, es en este año que se divide ARPANET en dos sistemas diferentes. El primero conocido como ARPAnet de uso civil y el segundo conocido como MILInet de uso exclusivo para la milicia. Las redes se conectaron de tal manera que los usuarios pudieran intercambiar información lo que acabo conociéndose como Internet.

Otro parte aguas fue en 1986 cuando los Estado Unidos de Norte América fundaron el NFSNET con el propósito de conectar varias supercomputadoras de gran velocidad a lo largo del país. Después de esto ARPAnet se cancelo y NFSNET fue el principal servidor de Internet.

En 1992 aparece lo que se conoce como la Web que agrupo todos lo servicios que estaban separados y da la oportunidad de crear un entorno en el cual se puedan combinar imágenes, sonido y textos.

Pero no fue hasta el año de 1996 que se pude decir que se estableció un protocolo estándar para la seguridad de las transacciones electrónicas solicitados por VISA y MASTERCARD, esta solicitud involucro a otras grandes compañías tales como GTE, IBM, Netscape, RSA y Verising.

Se pude decir de alguna manera que el primer protocolo de seguridad o el pionero de los protocolos de seguridad fue el SET que quiere decir transacción electrónica segura.

En los años subsiguientes salieron nuevos protocolos o programas de seguridad para garantizar la seguridad en las transacciones on-line. De los cuales se hablara mas adelante tales como el 3D Secure, protocolos SSL, Norton Confidencial etc.

CAPITULO
I

1.1 CONCEPTO SEGURIDAD

Comencemos definiendo el concepto de seguridad desde el punto de vista de la informática que consiste en mantener la integridad de los recursos de un sistema de información de una organización para que sean utilizados de manera que se decidió y que la información que se considere importante no sea fácil de acceder por cualquier persona que no se encuentre acreditada.
Su objetivo principal es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora.

1.2 Antecedentes de las transacciones on-line.

En el año de 1969 el departamento de defensa crea la agencia para proyectos avanzados de investigación (ARPA, Advanced Research Proyect Agency). El objetivo del departamento de Defensa era crear un red de comunicación de tal forma que si un sector de la red colapsaba totalmente los mensajes pudieran encontrar el camino hasta su destino de cualquier manera, lo que dio como ha ARPANET.
En el año de 1983 ARPANET se divide en dos sistemas diferentes llamados ARPAnet y MILInet, siendo la primera de uso civil y la segunda de uso exclusivo para

la milicia. Las redes se conectaron de tal manera que los usuarios pudieran intercambiar información lo que acabo conociéndose como Internet.

Uno de los avances más importantes para el Internet fue en 1986 cuando la fundación Nacional de la Ciencia (NFS, Nacional Foudation of Science) de los Estados Unidos creo el NFSNET con el propósito de conectar varias supercomputadoras de gran velocidad a lo largo del país. Después de esto ARPAnet se cancelo y NFSNET fue el principal servidor de Internet.

En el año de 1992 aparece el World Wid Web inventado por Tim Bernes-Lee.

La Web agrupó todos los servicios de Internet que antes estaban separados y les da un entorno capaz de combinar imágenes, texto y sonido. Apartir de este punto se puede decir que es que se comienza a introducir el comercio on-line lo cual provoca forzosamente la entrada de las transacciones on-line o también llamadas transacciones electrónicas.

Imagen 1.- Simbolización de ARPAnet.

1.3 ¿Qué es una transacción on-line?

Una transacción on-line o transacción electrónica es un protocolo estándar para proporcionar seguridad a transacciones con tarjeta de crédito en redes de computadoras inseguras comúnmente en Internet.

Este concepto surge por la necesidad de establecer un estándar de seguridad por parte de VISA y MASTERCARD en febrero de 1996, tal especificación involucro a un gran grupo de compañías tales como son GTE, IBM, Netscape, RSA y Verising.

SET utilizo técnicas criptográficas tales como certificados digitales y criptografía de clave publica para el uso de tarjetas de crédito vía Internet, sin embargo no logro el éxito esperado ya que el software que requería era complejo y costoso.

A partir del año 2000 las compañías de crédito comenzaron a proporcionar un nuevo estándar para reemplazar el SET denominado 3D Secure.

1.4 PROTOCOLOS DE SEGURIDAD EN TRANSACCIONES ON-LINE

1.4.1 3D Secure

3D Secure es protocolo basado en XML para permitir l autentificación de los titulares de las compañías de tarjetas de crédito en las transacciones epayment. Este protocolo fue desarrollado por VISA para garantizar la seguridad en los pagos vía Internet. Se aprobó y se ofrece con el nombre de servicio verificado por VISA y Mastercard SecureCode. La principal diferencia en Visa y MasterCrad implementaciones es en el método para generar el EVA (Valor Accountholder autentication) MasterCard utiliza UCFA (Universal titular de la tarjeta de autentificación de campo) y Visa usos Atlanta (Valor de Verificación de la tarjeta de autentificación). El protocolo también ha sido adoptado por JCB Internacional en el marco del servicio denominado J / Secure.

1.4.2 Caracteristicas de 3D Secure

Este protocolo consiste en vinvular el proceso de autorizacion finanaciera con una linea de autentificacion. Esta autententificacion esta basada en un modelo de dominio 3 (que es lo que hace referencia al 3D). Los 3 dominios son los siguientes: adquiriente del dominio (el comercio), la emisora del dominio (el banco emisor de la tarjeta de credito) y la interoperabilidad del dominio (el mundo de tarjetas de credito).

Este protocolo utiliza XML mensajes que son enviados a travez de conexiones SSL con la autentificacion de clientes, lo cual garantiza la autenticidad de los compañeros, el cliente y el servidor, utilizando certificados digitales.

Cada emisora podrá utilizar cualquier tipo de método de autenticación (el protocolo no es aplicable a este), pero típicamente, una contraseña basada en el método utilizado, de manera eficaz a comprar en Internet conlleva el uso de una contraseña secreta vinculada a la tarjeta.

Con el fin de que un miembro de Visa o MasterCard Banco a utilizar el servicio, se tiene que utilizar un software que cumple con las últimas especificaciones del protocolo. Actualmente, las especificaciones están en la versión 1.0.2. Las versiones anteriores 0.7 (sólo se utiliza en Visa EE.UU.) y 1.0.1 se han convertido en

redundante y ya no son compatibles. MasterCard y JCB han adoptado la versión 1.0.2 del protocolo.

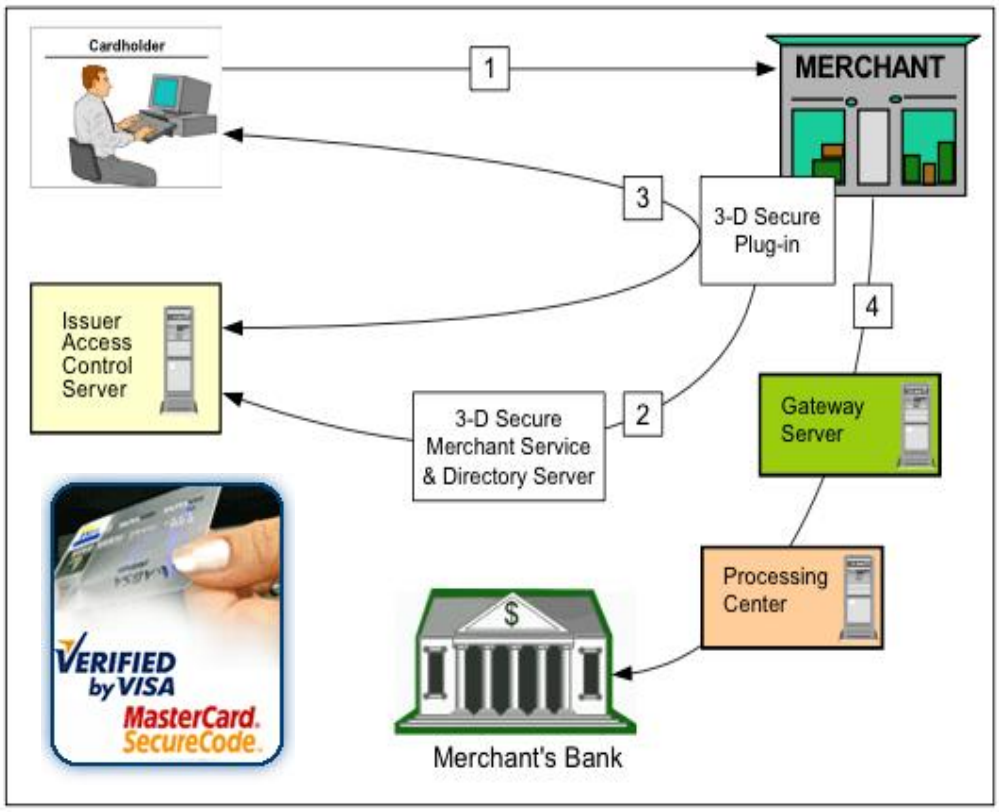


Imagen 2.- Representacion grafica del funcionamiento de 3D Secure

1.5 Secure Sockets Layer

Seguridad dela capa de transporte, su sucesor, son protocolos criptograficos que proporcionan comunicaciones seguras en Internet.
SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.
Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente (phishing) y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.

1.5.1 Cómo funciona

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autentificación del mensaje (MAC). Cada registro tiene un campo de content_type que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo handshake, que tiene el content_type 22.

El cliente envía y recibe varias estructuras handshake:

- Envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados Challenge de Cliente o Reto). Además puede incluir el identificador de la sesión.

- Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.

- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

- El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.

- Cliente y servidor negocian una clave secreta común llamada master secret, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una

clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función seudo aleatoria cuidadosamente elegida.

SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).
- Protección contra varios ataques conocidos (incluidos ataques man in the middle attack), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.

1.5.2 Aplicaciones de SSL

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

Aunque un número creciente de productos clientes y servidores pueden proporcionar SSL de forma nativa, muchos aún no lo permiten. En estos casos, un usuario podría querer usar una aplicación SSL independiente como Stunnel para proporcionar cifrado. No obstante, el Internet Engineering Task Force recomendó en 1997 que los protocolos de aplicación ofrecieran una forma de actualizar a TLS a partir de una conexión sin cifrado (plaintext), en vez de usar un puerto diferente para cifrar las comunicaciones esto evitaría el uso de envolturas (wrappers) como Stunnel.

SSL también puede ser usado para tunelar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

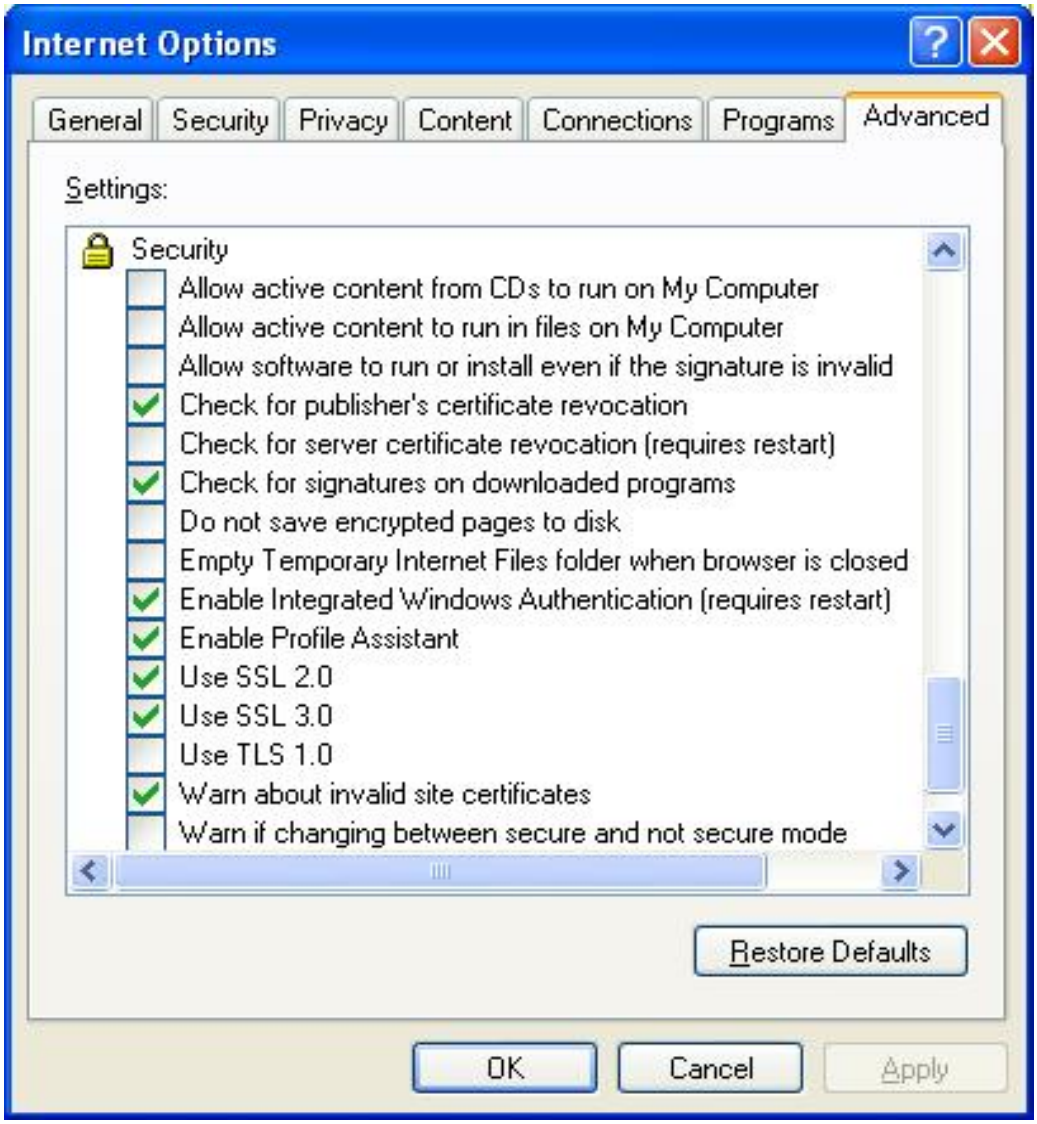


Imagen 3.- Aplicaciones SSL en Internet Explore.

1.6 Historia y desarrollo de SSL

Desarrollado por Netscape, SSL versión 3.0 se publicó en 1996, que más tarde sirvió como base para desarrollar TLS versión 1.0, un estándar protocolo IETF definido por primera vez en el RFC 2246. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

SSL opera de una manera modular: sus autores lo diseñaron extensible, con soporte para compatibilidad hacia delante y hacia atrás, y negociación entre las partes (peer-to-peer).

CAPITULO
II

MARCO TEORICO

2.1 Primeras claves débiles

Algunas primeras implementaciones de SSL podían usar claves simétricas con un máximo de sólo 40-bit debido a las restricciones del gobierno de los Estados Unidos sobre la exportación de tecnología criptográfica. Dicho gobierno impuso una clave de 40-bit lo suficientemente pequeña para ser “rota” por un ataque de fuerza bruta por las agencias de seguridad nacional que desearan leer el tráfico cifrado, a la vez que representaban un obstáculo para atacantes con menos medios. Una limitación similar se aplicó a Lotus Notes en versiones para la exportación. Después de varios años de controversia pública, una serie de pleitos, y el reconocimiento del gobierno de Estados Unidos de cambios en la disponibilidad en el mercado de 'mejores' productos criptográficos producidos fuera del país, las autoridades relajaron algunos aspectos de las restricciones de exportación. La limitación de claves de 40-bit en su mayoría ha desaparecido. Las implementaciones modernas usan claves de 128-bit (o más) para claves de cifrado simétricas.

2.2 Criptografía asimétrica

Método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

2.2.1 Seguridad

Como con los sistemas de cifrado asimétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 2^{81}-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con un clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

2.2.2 Desventajas respecto a las cifras asimétricas

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

El sistema de criptografía de curva elíptica representa una alternativa menos costosa para este tipo de problemas.

Herramientas como PGP, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información.

2.3 Criptografía de curva elíptica

La Criptografía de Curva Elíptica (CCE) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que los métodos antiguos como RSA al tiempo que proporcionan un nivel de seguridad equivalente. La utilización de curvas elípticas en criptografía fue propuesta de forma independiente por Neal Koblitz y Víctor Miller en 1985.

La criptografía asimétrica o de clave pública utiliza dos claves distintas: una de ellas puede ser pública, la otra es privada. La posesión de la clave pública no proporciona suficiente información para determinar cuál es la clave privada.

Existen varias versiones de criptografía de curva elíptica con pequeñas variaciones, todas ellas basadas en la creencia ampliamente extendida de la dificultad de resolver el problema de un logaritmo discreto para el grupo de una curva elíptica sobre algunos grupos finitos. Los grupos finitos más usados para ello son los enteros módulo un número primo (véase aritmética modular), o un grupo de Galois de tamaño potencia de dos. También se han propuesto grupos de Galois de tamaño de la

potencia de algún otro primo, pero son considerados dudosos entre los criptoanalistas.

La CCE ha sido ampliamente reconocida como el algoritmo más fuerte para una determinada longitud de clave, por lo que podría resultar útil sobre enlaces que tengan requisitos muy limitados de ancho de banda.

NIST y ANSI X9 han establecido unos requisitos mínimos de tamaño de clave de 1024 bits para RSA y DSA y de 160 bits para ECC, correspondientes a un bloque simétrico de clave de 80 bits. NIST ha publicado una lista de curvas elípticas recomendadas de 5 tamaños distintos de claves (80, 112, 128, 192, 256). En general, la CCE sobre un grupo binario requiere una clave asimétrica del doble de tamaño que el correspondiente a una clave simétrica.

Certicom es la principal empresa comercial de CCE, esta organización posee 130 patentes, y ha otorgado licencias sobre tecnología a la National Security Agency (NSA) por 25 millones de dólares. Certicom también ha patrocinado varios desafíos al algoritmo CCE. El más complejo resuelto hasta ahora, es una clave de 109 bits, que fue roto por un equipo de investigadores a principios de 2003. El equipo que rompió la clave utilizó un ataque masivo en paralelo basado en el 'birthday attack', mediante más de 10000 PC's de tipo Pentium funcionando continuamente durante 540 días. Se estima

que la longitud de clave mínima recomendada para CCE (163 bits) requeriría 10^8 veces los recursos utilizados para resolver el problema con 109 bits.

Imagen 4.- Logotipo de certimom.

CAPITULO
III

3.1 MasterCard SecureCode

MasterCard SecureCode es un programa de alta tecnología por medio del cual el pago de transacciones remotas serán más seguras. Este sistema será presentado en la Convención Bancaria de Cartagena.
Desde hace algún tiempo, el mundo de los negocios ha dado un vuelco significativo en la manera de realizar las transacciones. El comercio electrónico se ha convertido en una herramienta útil en la industria del comercio masivo y en la medida que ha ido evolucionando se han creado sistemas que garantizan la seguridad de estas transacciones remotas.

Tal es el caso de MasterCard SecureCode, un nuevo programa por medio del cual MasterCard asegura el pago y la transparencia de transacciones hechas a través de Internet. Este sistema ofrece a los bancos emisores la flexibilidad de seleccionar la tecnología de autenticación más conveniente a sus necesidades.

MasterCard SecureCode integra la infraestructura de UCAF (Universal Cardholder Authentication Field) al esquema de autenticación seleccionado por el emisor, así se facilita el transporte de datos relativos a la autenticidad del cliente entre el comercio que realiza la venta y la entidad que emitió la tarjeta. La finalidad de MasterCard SecureCode es otorgar a las transacciones

efectuadas por medio de Internet la seguridad presente en una transacción realizada en el mundo real.

Dado que en una compra virtual, ni el tarjethabiente ni su tarjeta están físicamente presentes, el reto hasta el día de hoy era precisamente la verificación de la autenticidad de la persona que realiza la transacción. Antes de tener estos sistemas de seguridad, en la mayoría de los casos los establecimientos tuvieron que asumir las pérdidas por fraude que se presentaban en las transacciones.

Ahora todo es más fácil y seguro porque SecureCode facilita la autenticación del usuario de la tarjeta eliminando así el riesgo de que se presenten transacciones fraudulentas por medio de la red y sus beneficios no sólo están dirigidos al comercio, sino también al tarjeta habiente y al banco emisor de las tarjetas.

De acuerdo con Wilson Castellanos, gerente general de MasterCard para Colombia y Ecuador, “los participantes en una transacción en línea utilizando MasterCard SecureCode pueden sentirse más confiados de que el mundo virtual sus transacciones serán más seguras”

Los objetivos de MasterCard SecureCode no están limitados a las transacciones por medio de Internet. El esquema de autenticación es también aplicable a las transacciones de comercio móvil y otros medios transaccionales remotos como lo son las órdenes por correo o teléfono, entre otros.

Este sistema se encuentra en uso en varias partes del mundo con importantes resultados en el control de riesgo. En América Latina el concepto se ha sido presentado a todos los países y se estima que en un corto plazo todos los bancos emisores de tarjetas de crédito MasterCard® y débito Maestro® se vean beneficiados de esta aplicación, ya que la autenticación del tarjeta habiente durante las transacciones por Internet generará una confianza entre los establecimientos que comercializan sus productos por Internet.

De esta manera, SecureCode es la alternativa que ofrece beneficios tangibles en la eliminación del fraude y en la medida que todos los participantes se sientan confiados en que sus transacciones por Internet se están efectuando de manera segura el comercio electrónico será aún más estimulado.

MasterCardDelivery™, el complemento perfecto para sus compras por Internet.

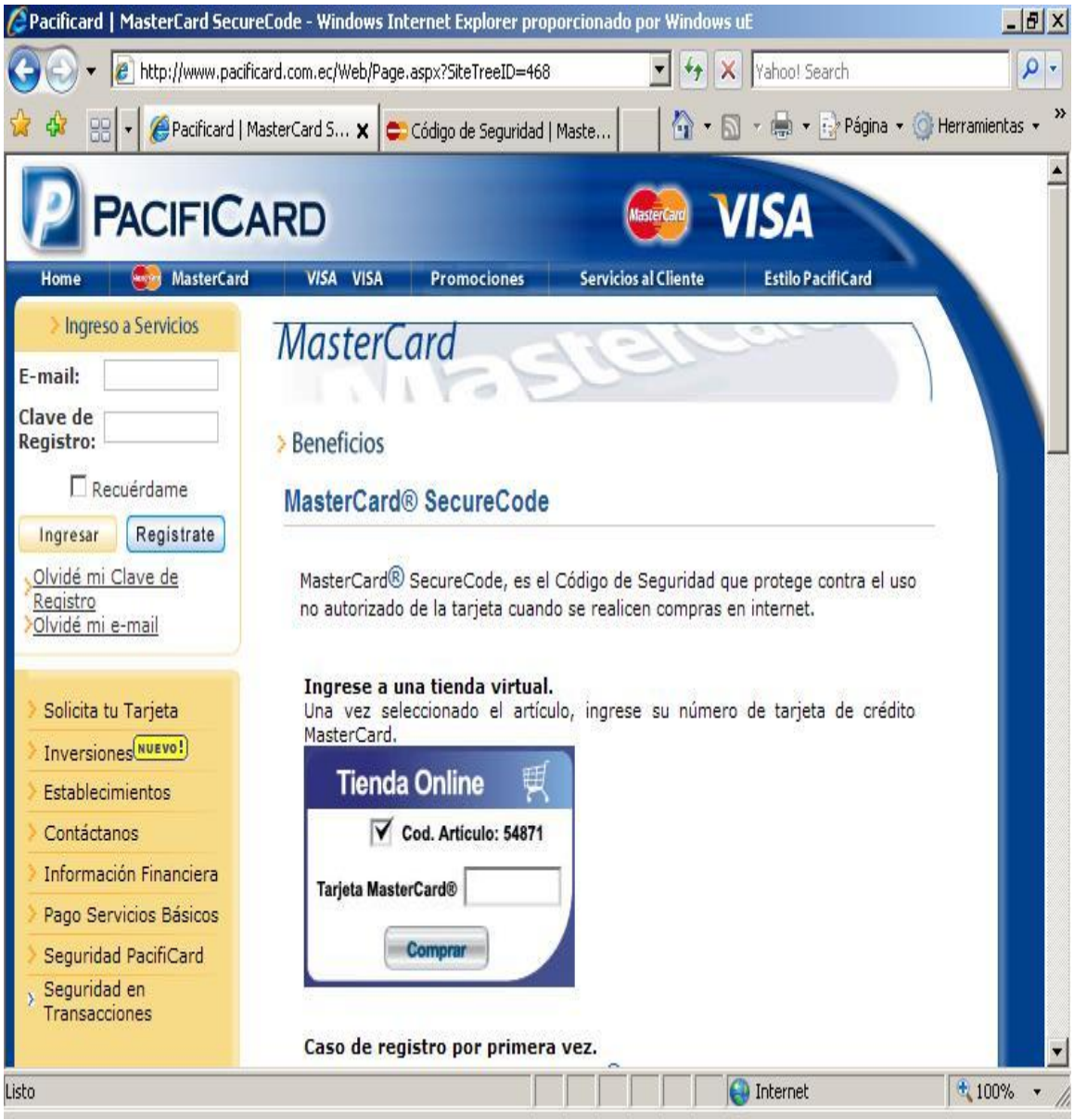
Varias son las novedades que se presentan durante las Convención Bancaria que se lleva a cabo en Cartagena. Como un complemento ideal a las compras por Internet se creo MasterCardDelivery, el exclusivo servicio de MasterCard Internacional para el envío de artículos comprados por comercio electrónico desde los Estados Unidos a cualquier país de América Latina.

Con MasterDelivery, el tarjeta habiente MasterCard puede traer fácilmente a Colombia artículos y mercancías adquiridas a través de Internet, conforme los términos y condiciones del servicio, con la garantía de una rápida entrega, ya que este servicio está diseñado para facilitar el envío de productos y le proporciona al cliente una dirección física y postal en los Estados Unidos, localizada en la ciudad de Miami, Florida.

MasterDelivery recibe, clasifica, codifica, empaca y envía toda la mercancía diariamente hacia Colombia, cargando con los costos relacionados al envió y manejo a la tarjeta de crédito MasterCard. Entrando a www.masterdelivery.com cada usuario que se registre recibirá una clave y un número de cuenta en tiempo real para acceder al servicio. Su información de cuenta es

actualizada constantemente, los costos y trámites aduaneros están incluidos, así como el rastreo electrónico de todos los paquetes desde el momento en que llegan a la dirección de MasterDelivery en Miami hasta la dirección final de destino.

Imagen 5.-Ejemplo de compra con MasterCard SecureCode:



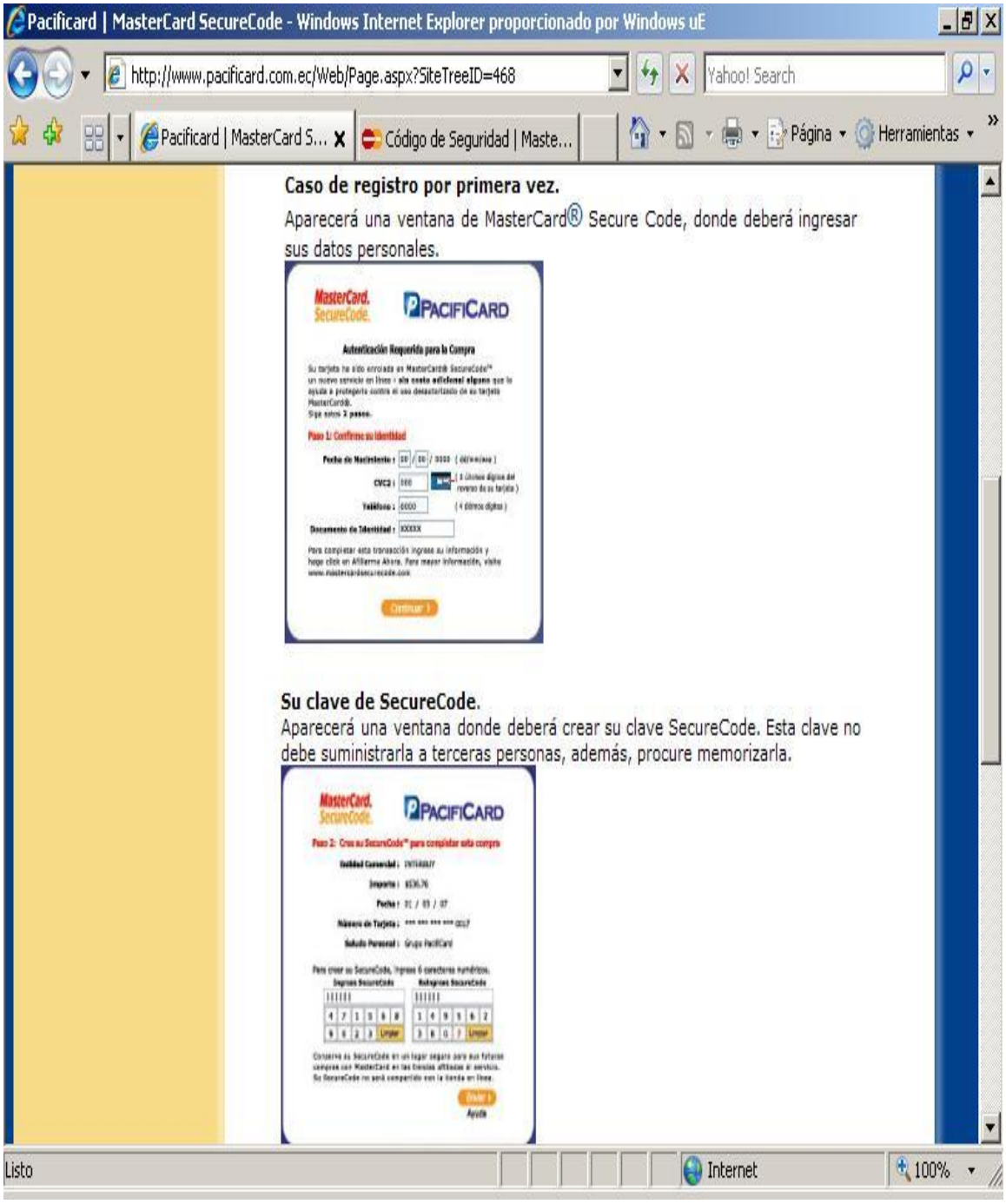


Imagen 5.1.- Ejemplo de compra con MasterCard SecureCode

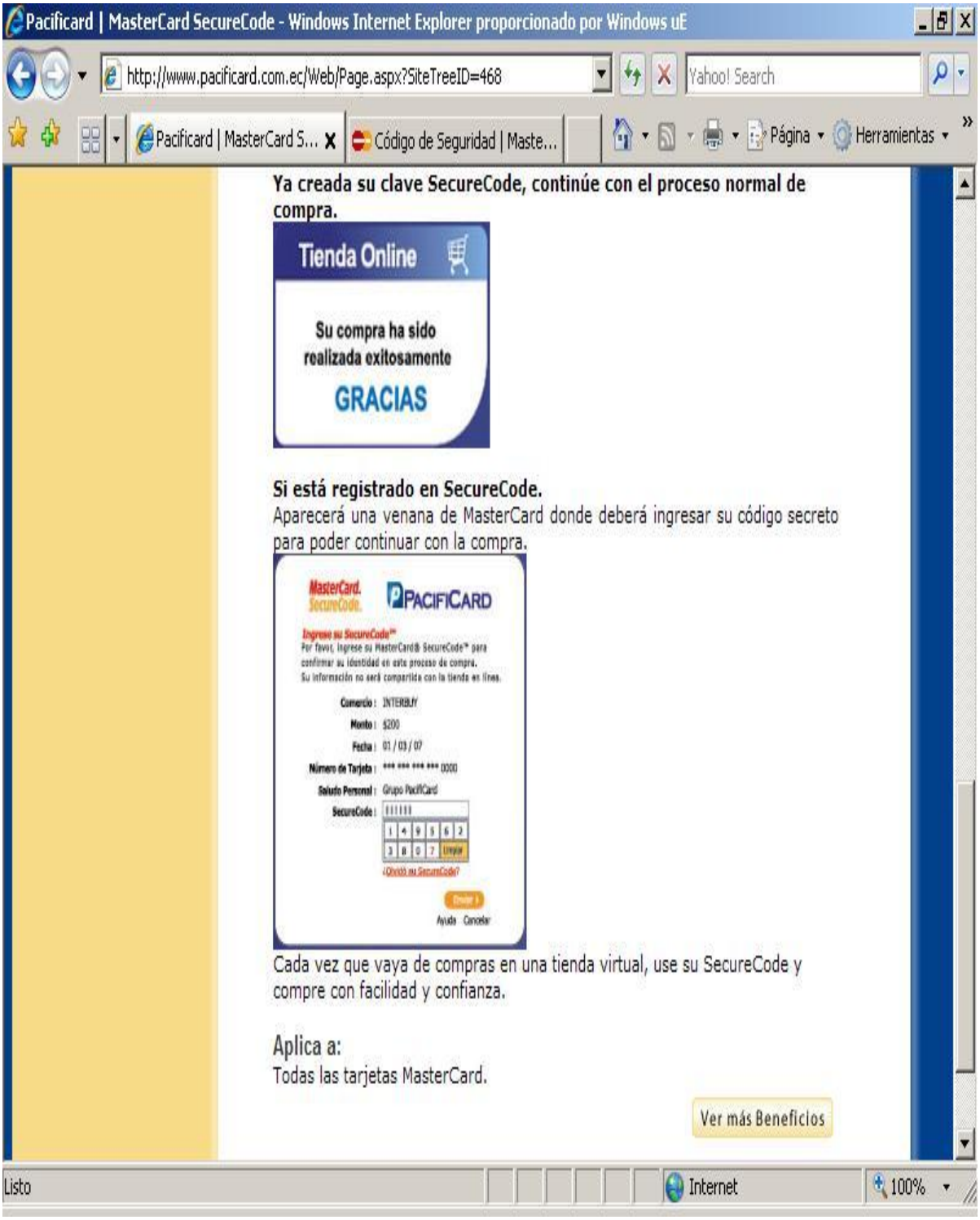


Imagen 5.1.- Ejemplo de compra con MasterCard SecureCode

3.2 Norton Confidential para usuarios de plataforma Macintosh

Norton Confidential para usuarios de plataforma Macintosh, es una solución que les permitirá realizar transacciones y compras más seguras, enviar contraseñas, números de cuenta u otra información personal en Internet de manera protegida.

Norton Confidential inspecciona los sitios Web antes de que los usuarios interactúen con ellos y bloquea automáticamente la información privada de los ataques al buscar amenazas conocidas y comportamientos sospechosos.

De acuerdo con el más reciente Informe sobre Amenazas a la Seguridad en Internet de Symantec (ISTR X), durante el primer semestre de 2006, la Red de investigación de Symantec “Symantec Probe Network” detectó 157,477 mensajes de estafa electrónica. Esto significa un aumento de 81% con respecto a los 86,906 mensajes de estafa en Internet que se detectaron en el último semestre de 2005.

“A diferencia de los virus y software espía, los usuarios de Macintosh enfrentan los mismos peligros de estafa electrónica que los consumidores que usan las PC, por ello deben tomar las mismas precauciones de seguridad cuando realicen transacciones en línea. Norton

Confidential brinda a los usuarios de Macintosh tranquilidad y confianza para realizar operaciones bancarias, hacer compras u otras actividades confidenciales sin preocuparse de exponer su información personal", señaló Enrique Salem, vicepresidente de Soluciones y Productos de Consumo de Symantec Corporation.

Norton Confidential para Macintosh ofrece protección de vulnerabilidades con el fin de evitar que los ladrones de identidad aprovechen vulnerabilidades en el sistema operativo y en las aplicaciones recientemente descubiertas. Adicionalmente, evita que la información personal como números de identificación y de tarjetas de crédito sea enviada sin permiso de los usuarios. También permite a los usuarios bloquear personalmente importantes archivos en su Mac, para que no sean eliminados o alterados de forma deliberada por los hackers o accidentalmente por amigos o familiares, e incluso, para que no sean abiertos sin autorización del usuario.

Norton Confidential para Macintosh funciona conjuntamente con las actuales soluciones antivirus y de seguridad en Internet de Symantec y de otros proveedores para brindar seguridad contra nuevos tipos de amenazas.

Para proteger mejor al usuario, en la barra del navegador de Internet se puede ver una ventana de Norton Confidential que alerta sobre los niveles de amenaza de fraudes; cuando los usuarios entran a una página Web confiable, inmediatamente aparece un indicador que dice “sitio seguro”. Las funcionalidades clave de Norton Confidential para Macintosh son:

Protección contra la estafa electrónica.- evita que los usuarios visiten y/o envíen información confidencial a los sitios Web de estafa electrónica conocidos y desconocidos;

Protección de archivos.- bloquea archivos importantes para impedir que la información de los usuarios sea alterada por un hacker o que sea eliminada accidentalmente por un amigo o familiar;

Protección de la información.- garantiza que la información confidencial del usuario no salga sin su autorización, esto incluye números de identificación expedidos por el gobierno, tarjetas de créditos, direcciones o números telefónicos.

Protección de las vulnerabilidades.- este tipo de protección es generalmente descrita por los profesionales en seguridad como un “sistema de protección de intrusos en la Red” o un Sistema de Prevención de Intrusos (IPS). La protección de las

vulnerabilidades proporciona protección el mismo día contra ataques al sistema operativo y a las aplicaciones, en lugar de semanas después como sucede con los parches de las aplicaciones y sistemas operativos.

Symantec es el líder global en soluciones que permiten a las personas y empresas garantizar la seguridad, disponibilidad e integridad de su información. Con sede en Cupertino, California, Symantec opera en más de 40 países.

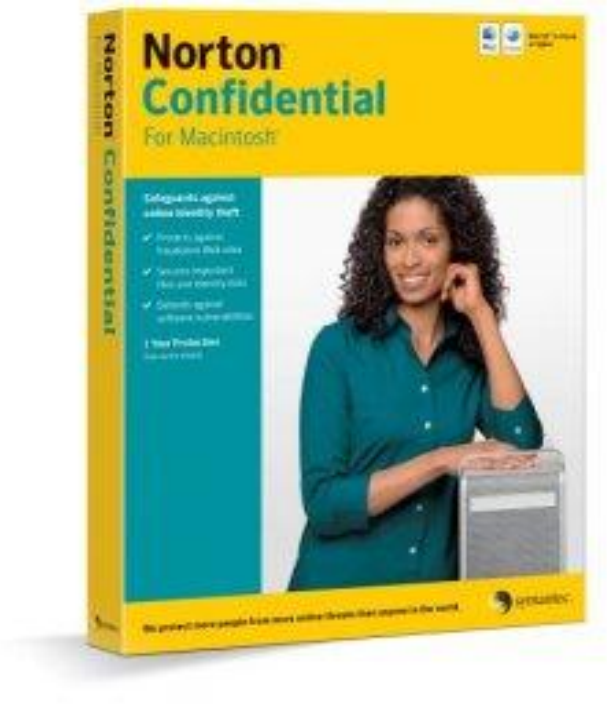


Imagen 6.- Norton Confidential para Macintosh.

3.3 Sistemas de informacion mas frecuente en las transacciones on-line

Con la puesta en marcha de diversos medios de pago digitales, se está incrementando la existencia de transacciones electrónicas llevadas a cabo en su totalidad a través de la red.

Entre los sistemas de seguridad más utilizados actualmente, encontramos los siguientes:

3.4 Servidores seguros

Un servidor seguro es un procesador que permite que la información que viaja entre el Servidor y el PC del usuario vaya "encriptada" y "controlada" de forma que no pueda ser leída ni manipulada por terceras personas.

3.4.1 Funcionamiento

Al conectarse a un servidor seguro, éste le obliga a que se autentifique. La seguridad de estar en un servidor seguro se obtiene mediante un certificado digital, el cual es expedido por una compañía independiente, la cual está autorizada legalmente para garantizar que un determinado servidor pertenece a una compañía determinada. A través del certificado de seguridad el

usuario obtiene la confirmación de que está enviando la información al lugar correcto.

3.4.2 Finalidad

Incrementar la confidencialidad y la fiabilidad de las transacciones on-line y mantener en todo momento la privacidad de los datos emitidos.

Este sistema de protección criptográfica impide que los datos transmitidos puedan ser reconocidos por un tercero ajeno a la transacción que logre infiltrarse ilegalmente en la comunicación (como puede ser el caso de un hacker).

Imagen 7.- Conjunto de servidores.

3.5 Pasarelas de pagos

Las pasarelas de pago son plataformas que realizan la función de procesamiento de tarjetas de crédito desde Internet a las redes privadas de los sistemas VISA, Mastercard, American Express, etc.

Las pasarelas de pago, generalmente conocidas como aplicaciones TPV (Terminal Punto de Venta) virtual, permiten que los clientes puedan realizar una compra utilizando una tarjeta de crédito y validando la operación de forma automática y en línea.

3.5.1 Funcionamiento

La operación de pago a través de una TPV consta de las siguientes fases:

- El cliente utiliza una aplicación de comercio electrónico para elegir los artículos que desea adquirir; la aplicación calcula el importe total de la compra.
- Cuando el cliente decide pagar, la aplicación de comercio electrónico le redirige al servidor seguro del banco y le indica al TPV la cantidad total a cobrar para que procese el pedido.

- El cliente introduce el número de su tarjeta de crédito en un formulario del servidor seguro del banco (los datos viajan debidamente encriptados).
- El banco realiza una comprobación (en segundos) de la validez de la tarjeta de crédito y de la existencia de fondos. Si la respuesta es afirmativa, se realiza el cobro ingresando el dinero en la cuenta bancaria del vendedor.
- El servidor seguro del banco redirige al cliente de vuelta a la aplicación de comercio electrónico indicando si la operación se ha realizado o no con éxito.

3.5.2 Finalidad

La función básica de las paralelas de pago es evitar que la información sobre la tarjeta de crédito del comprador llegue directamente al vendedor, siendo utilizada únicamente por la entidad bancaria. El vendedor únicamente recibe una notificación informándole de si el pago ha sido hecho efectivo o no.

3.5.3 Ventajas

Este sistema de pago ofrece diversas ventajas, tanto para los compradores como para los vendedores.

a. Para el comprador:

- El pago se realiza directamente en los servidores de cada banco.
- El número de la tarjeta viaja encriptado, con lo cual, el vendedor nunca llega a saber cual es el número de la tarjeta de crédito del cliente.
- El vendedor debe tener una cuenta en un banco donde consten sus datos auténticos. Esto elimina en la práctica las posibilidades de ventas fraudulentas.
- El cliente puede elegir entre varias tarjetas de crédito para efectuar el pago.

b. Para el vendedor:

- Disponer de la TPV de un banco significa seguridad total para sus clientes.
- El cobro se ingresa al instante.

- El banco verifica que la tarjeta de crédito del comprador sea válida y de que el cliente tenga fondos suficientes.
- El sistema permite cobrar a clientes desde cualquier lugar del mundo.

3.5.4 Desventajas

El sistema TPV también conlleva ciertas desventajas:

- Las comisiones por este sistema de cobro son muy altas, alrededor de un 4% del importe total de la operación, a diferencia del 2% que se carga por los pagos realizados con la tarjeta en tiendas físicas.
- Otro inconveniente que pueden encontrar los comerciantes que utilicen este sistema es la posibilidad de reclamaciones a Visa u otra entidad emisora por parte de compradores insatisfechos o con mala fe. Por ello, es conveniente conservar toda la información posible que pruebe el envío real de la mercancía vendida (por ejemplo, los resguardos de las agencias de transporte).

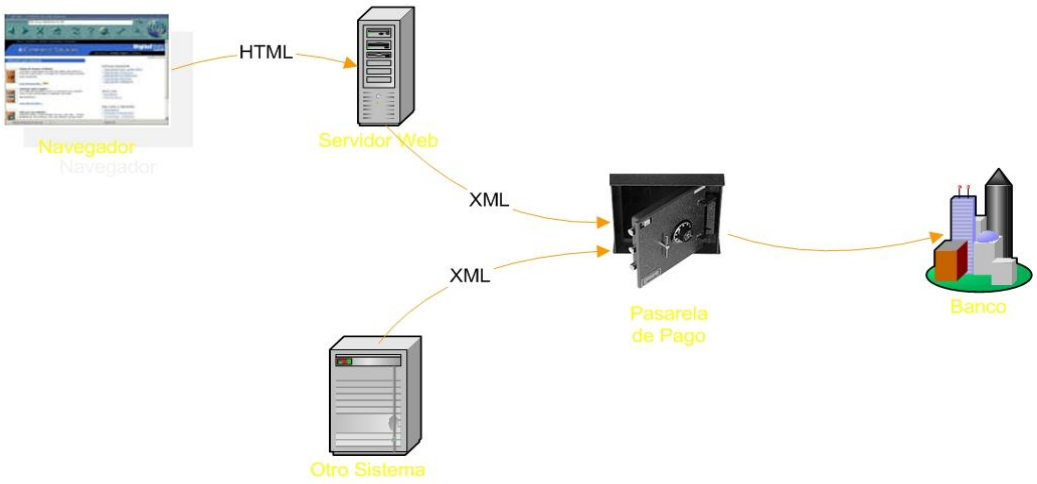


Imagen 8.-Representacion grafica de una pasarela de pago.

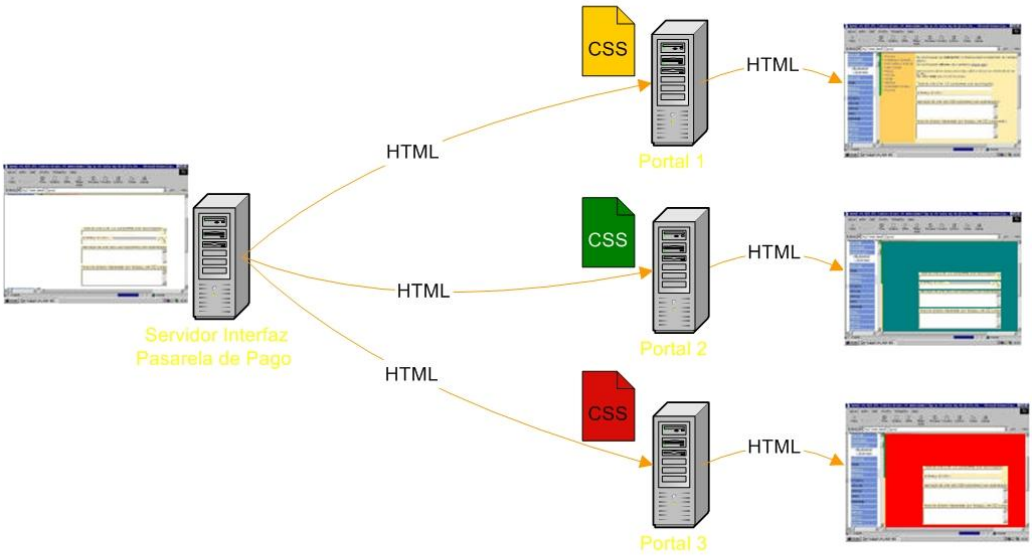


Imagen 8.1.- Representación grafica de pasarelas de pago CSS.

3.6 Protocolos de seguridad

Existen dos protocolos estándar de seguridad: el SET y el SSL, sistemas que encriptan nuestros datos para que nadie pueda acceder a ellos.

El SET, es un conjunto de normas de seguridad que adjunta un certificado al pago que se realiza mediante tarjeta de crédito. Mientras que, el SSL (más conocido y más utilizado), tiene como función principal cifrar el número de las tarjetas de crédito antes de que el mismo sea enviado.

3.7 Protocolo SET (Transaccion Electronica Segura)

Este protocolo fue diseñado con la intención de asegurar y autenticar la identidad de las personas que participan las transacciones efectuadas a través de cualquier red en línea.

Fue desarrollado por iniciativa de Visa y Mastercard, y con la participación de diversas empresas como Microsoft, IBM, Netscape, SAIC, GTE, RSA, VeriSign y otras empresas líderes en tecnología.

3.7.1 Finalidad

El objetivo primordial de SET es mantener la confidencialidad de la información intercambiada en una transacción, así como garantizar la integridad del mensaje y la identidad de los participantes, con objeto de evitar los fraudes, falsificaciones y uso ilegitimo de tarjetas de crédito en Internet.

3.7.2 Funcionamiento

El SET proporciona los medios para que consumidores y comerciantes se identifiquen entre ellos antes de la realización de la transacción. Su funcionamiento se basa en la utilización de certificados digitales[1] y de la encriptación de claves públicas para proteger la información financiera de los participantes.

Es importante recalcar que, para evitar cualquier clase de fraude, SET esta diseñado de tal forma que la empresa, en cuyo favor se realiza la transacción, nunca podrá tener acceso ni conocerá el número de la tarjeta usada por el consumidor.

El mecanismo de una transacción realizada utilizando el SET es similar al de las transacciones ordinarias,

celebradas utilizando como medio de pago una tarjeta de crédito. Una transacción SET se desarrolla de la siguiente manera:

1. El protocolo SET da inicio en el momento en que el cliente decide adquirir un determinado artículo o servicio.
2. El servidor del comerciante realiza una descripción del pedido, con lo cual pone en marcha la aplicación "cartera del cliente".
3. Se cifra y se transmite la orden de pago. Se incluyen tanto los datos del pedido como las instrucciones de pago.
4. Se envía la petición del pago al banco del comerciante.
5. El banco descifra la información recibida, verifica la identidad del comprador y del comerciante, y comprueba la integridad de los datos. Si todo es correcto, envía una petición de autorización de pago al banco emisor (banco del cliente).
6. El banco del emisor verifica los datos y si todo es correcto autoriza la transacción.

7. Después, se envía al comerciante un testigo de transferencia de fondos, el cual comprueba que todo se ha desarrollado correctamente.

8. El software del cliente prepara y envía a éste un recibo de la transacción. A continuación se completa el procesamiento del pedido (envío de mercancías o suministro de servicios).

9. Realizada con éxito la transacción, el comerciante genera una petición de transferencia a su banco solicitando el abono en su cuenta del precio pactado.

10. Se hace el cargo en la cuenta correspondiente a la tarjeta de crédito utilizada.

3.7.3 Desventajas

El SET aún no esta completamente implantado en Internet debido, en primer lugar, a la necesidad de utilizar un software especial (tanto para compradores como para comerciantes) cuya distribución y comercialización se está desarrollando muy lentamente.

La segunda y más importante razón es que el funcionamiento del SET resulta complejo y confuso para los usuarios.

Desde el punto de vista de los especialistas, SET es un mecanismo que irá creciendo paulatinamente, pero de momento seguirá coexistiendo con el protocolo SSL.

3.8 Protocolo SSL (Secure Sockets Layer)

Este protocolo fue diseñado en el año de 1994 por Netscape con el objetivo de proteger el acceso de personas no autorizadas a determinada información confidencial.

El protocolo SSL proporciona los servicios de cifrado de datos, autenticación de servidores, integridad de mensajes y, en menor grado, la identificación del cliente para conexiones TCP/IP (Transmission Control Protocol/ Internet Protocol).

El protocolo SSL proporciona un canal de comunicaciones entre los servidores y los navegadores a través del cual, cifrando los datos intercambiados, las partes pueden celebrar transacciones electrónicas con seguridad.

3.8.1 Funcionamiento

El SSL funciona de forma sencilla, se basa en la encriptación de los datos mediante la utilización de una clave de sesión y la aplicación de una clave pública (normalmente la RSA).

El funcionamiento del protocolo SSL puede resumirse en 4 fases:

1. La denominada "Fase Hola", momento en el cual el navegador y el servidor se deben poner de acuerdo respecto a los algoritmos necesarios para mantener la confidencialidad y la autenticación.

2. Una vez alcanzado el acuerdo se inicia la "Fase de Autentificación", etapa en la cual el servidor envía al navegador el certificado que contiene su clave pública, solicitando al mismo tiempo el certificado del cliente.

3. Después, el cliente envía al servidor una clave maestra, con la cual se genera la clave de sesión que cifrará los datos que las partes intercambien a través del algoritmo de cifrado acordado. La clave de sesión es remitida por el usuario debidamente cifrada gracias a la utilización de la clave pública del servidor. Esta

parte del proceso se conoce como "Fase de Creación de Clave de Sesión".

4. Por último, en la "Fase de Verificación" se comprueba tanto la autenticidad del servidor y del usuario, como la seguridad del canal establecido. Concluida esta última fase, se da inicio a una sesión segura entre las partes.

3.8.2 Desventajas

Si bien es cierto que ofrece un sistema seguro para el envío y cifrado de los números de tarjetas de crédito, también lo es que carece de la capacidad para proteger otros aspectos de la actividad comercial (verificar que la tarjeta sea valida, autorizar la transacción con los bancos, etc.)

Otra desventaja es la protección parcial que concede, ya que garantiza la integridad y confidencialidad de los datos únicamente durante el tránsito de los mismos, pero no los protege una vez que los mismos son recibidos por el servidor.

A pesar de estas deficiencias, el SSL es un protocolo seguro cuya utilización es altamente recomendable para proteger las transacciones electrónicas.

Sin embargo, para lograr una óptima protección, lo mejor es utilizar tanto el protocolo SSL como el protocolo SET, pues así se gozaría al mismo tiempo de la seguridad proporcionada por ambos sistemas.

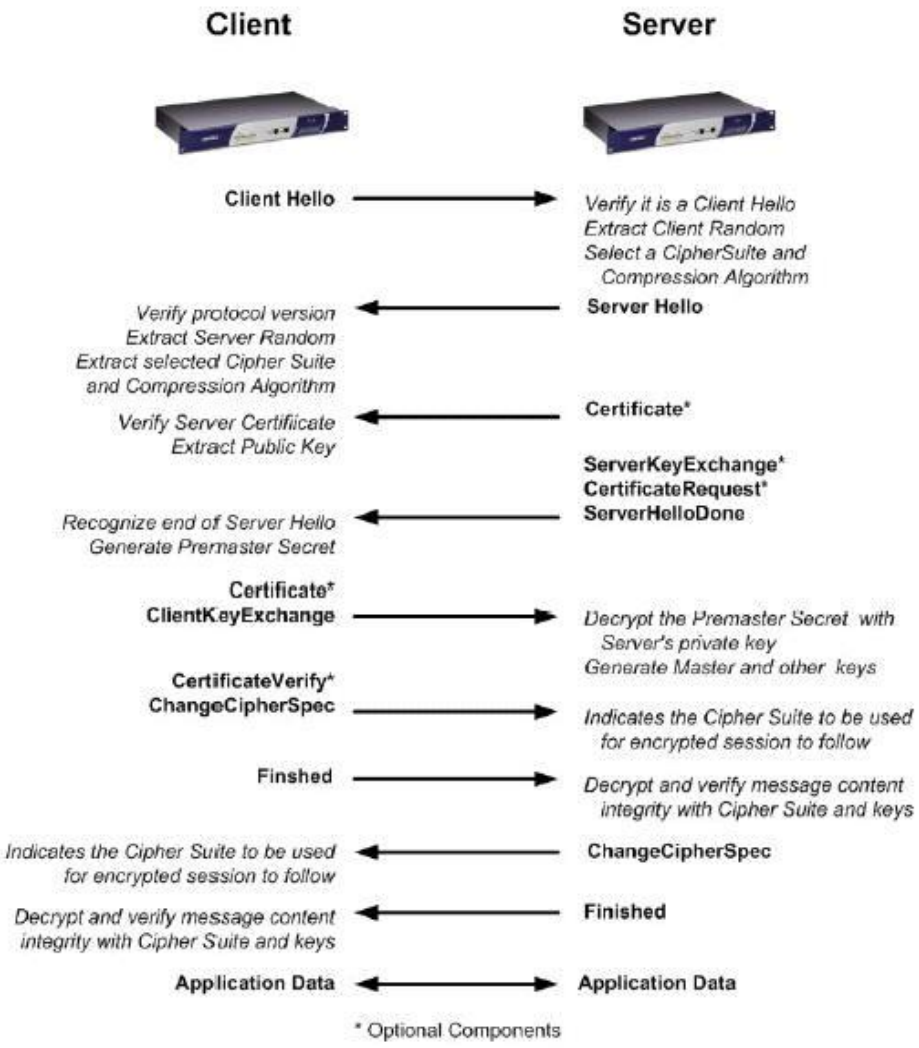


Imagen 9.- representación grafica del funcionamiento del protocolo SSL.

CAPITULO
IV

4.1 COMO LLEVAR A CABO TRANSACCIONES ON-LINE DE FORMA SEGURA

El mundo moderno de hoy en día nos brinda la forma de realizar compras desde la comodidad de nuestros hogares, oficina o de cualquier lugar donde haya un computadora con acceso a Internet. Se pueden adquirir bienes o servicios desde cualquier parte del mundo y en cualquier momento.

A pesar de todas estas ventajas cuando se realiza la adquisición de un producto o servicio vía Internet hay que estar conciente de lo implica esto, y preocuparse de buscar siempre sitios que den confianza y que no sean sospechosos.

La mayoría de los comercios que cumplen con la especificación de transacción electrónica segura despliegan un candado, con el logotipo Verified by Visa, u otro tipo de símbolos que permiten identificar al sito como confiable.

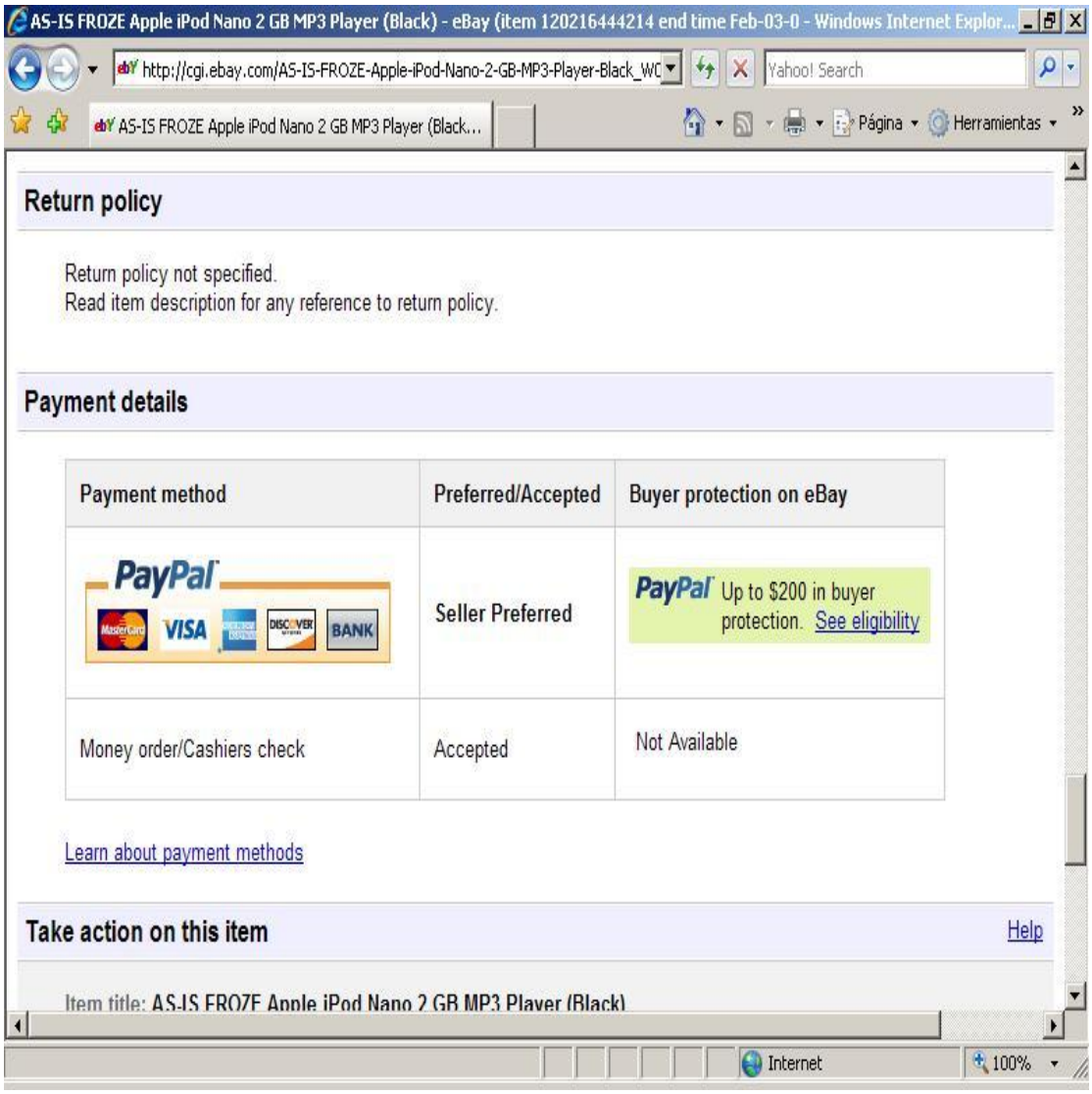


Imagen 10.- Logotipos que permiten autentificar que un sito es seguro, en este caso corresponde al sitio de ebay.

Otra manera de realizar una transacción on-line de forma segura es con el uso de un explorador confiable para navegar en la red como el Netscape Navigator (V 2.0 o superior), Microsoft Explorer y América Online, estos navegadores reducen el riesgo de que la información que se envié por Internet sea interceptada por un tercero cuando esté comprando en un sitio Web.

Imagen 11.- Software recomendados para una navegación segura en Internet.

Se debe verificar que el sitio haya implementado las normas de seguridad de la industria. Esto lo verificamos por medio del símbolo del candado con llave lo cual indica que el sitio utiliza la tecnología SSL, la cual garantiza la seguridad de la transacción.

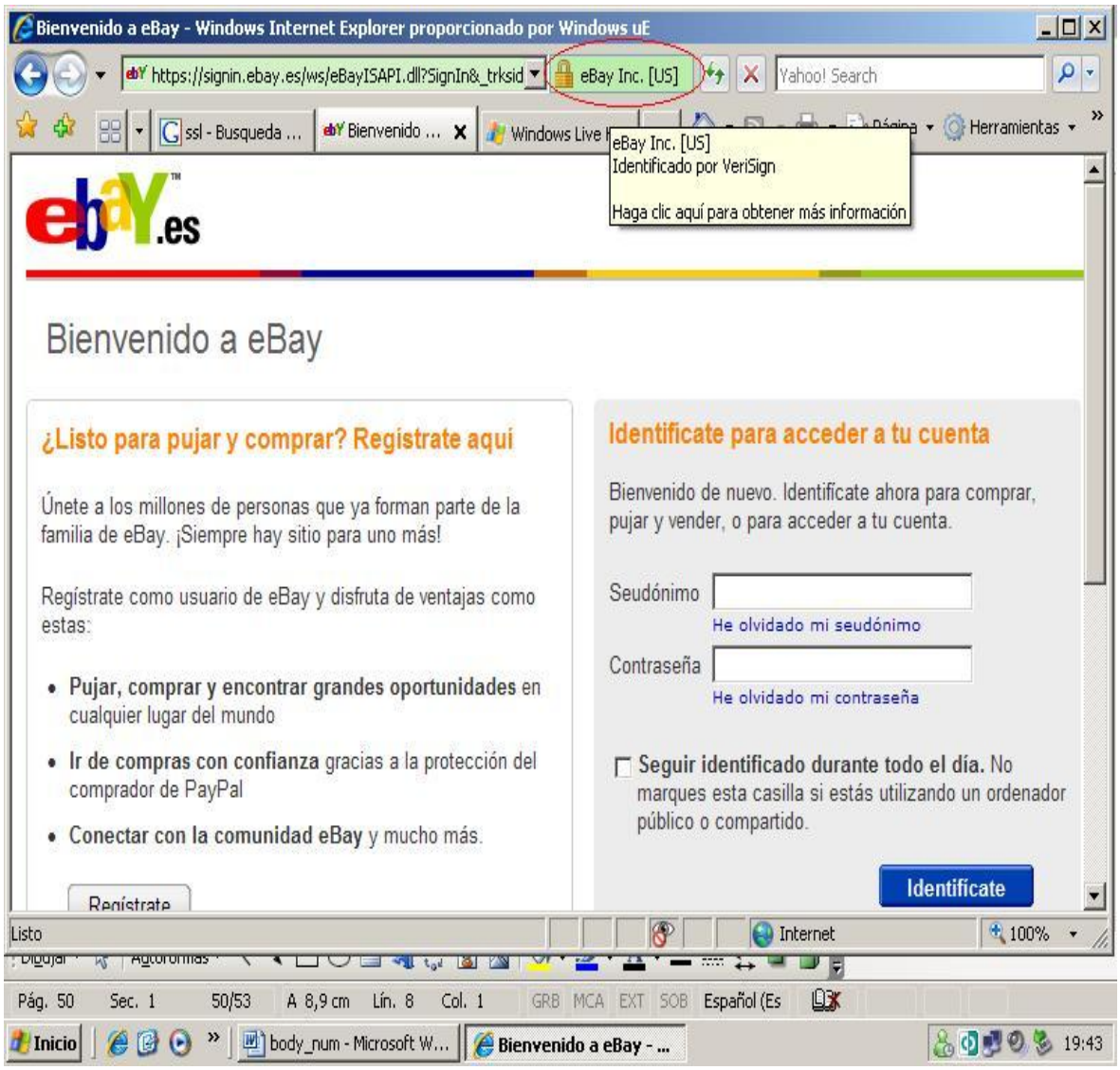


Imagen 12.- Observar el símbolo del candado lo cual indica tecnología SSL.

Se debe de obtener toda la información acerca de la política de devolución y reembolso del sitio, estas políticas generalmente se encuentran el la misma pagina del sitio. En caso de que el sitio no proporcione dicha información es recomendable no realizar ningún tipo de transacción.

Se debe buscar la declaración de privacidad, es esta se nos explica las políticas de privacidad de la empresa.

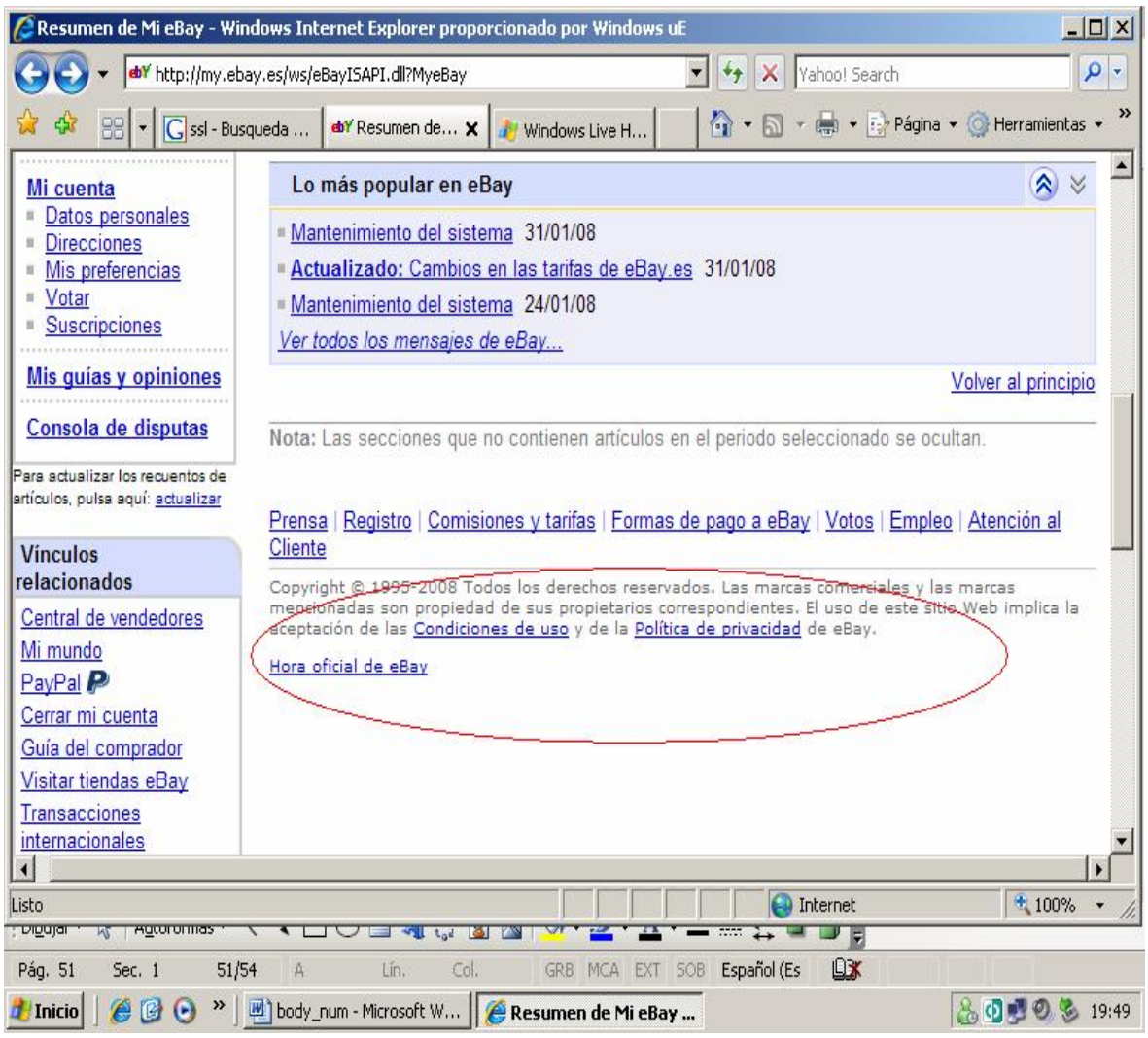


Imagen 13.- Obsérvese que el sitio contenga condiciones de uso y políticas de privacidad.

A pesar de ser un tema de cierta forma complicado estos son los puntos mas importantes o básicos que uno debe tener en cuenta cuando realice una transacción on-line, ya que detrás de una transacción on-line existe una gran estructura lógica que es la encargada de salvaguardar la información confidencial que se maneja en este tipo de operaciones, además de que en ella se invierten miles de millones de dólares, y que es también generadora de grandes ganancias anuales para empresas de diferentes actividades económicas.

Una de las grandes ventajas para los usuarios de este tipo de servicio es la estandarización de protocolos y aplicaciones lo cual facilita el entendimiento de como funciona una transacción y de cierta forma brinda una tranquilidad a los usuarios de que la integridad de sus datos no será violada.

CAPITULO
V

5.1 WEBS MÁS USADOS PARA TRANSACCIONES ELECTRONICAS

Existen innumerables sitios Web en todo el mundo para realizar compras a continuación se mencionaran algunos de los sitios mas usados por su confiabilidad y variedad de artículos que ofrecen.

Se comenzara con uno de los sitios más conocidos y utilizados en la actualidad conocido como ebay.
Ebay es un sitio destinado a la subaste de productos a través de Internet. Es uno de los primeros en este tipo de transacciones, dado que su presencia en la comunidad en línea es de varios años.
Actualmente se aplica una cita muy común en los enlaces de ebay, ¿no encuentra lo que busca? Búsquelo en ebay.

Ahora veamos un porco de la historia de este sito. Ebay fue fundada en 1995 por Pierre Omidyar en San José, California con la idea de completar su colección de caramelos "Pez", no obstante se dio cuenta que podía usarlo para que otras personas vendieran cosas que ya no usaran, el primer articulo que se vendió en ebay fue un puntero láser inservible por un costo de $13,83 dólares.

En el año de 1999 comienza su transacción bursátil en el índice Nasdaq. En el 2002 compra la empresa PayPal y en mayo del 2005 compra el portal de clasificados Loquo.

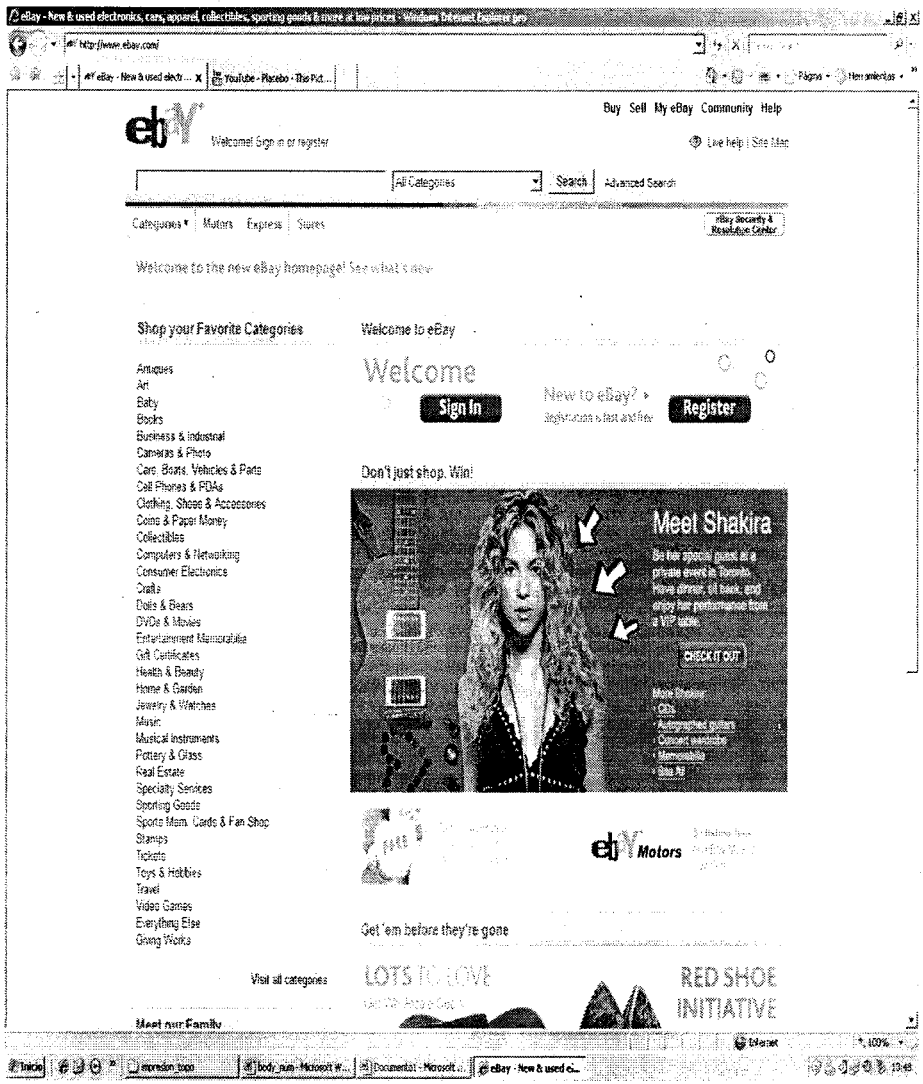


Imagen 14.-Portal Ebay.

Otro sitio de gran auge mundial es Amazon conozcamos mas de este sitio a continuación.

Amazon.com, Inc. es una compañía estadounidense de comercio electrónico con sede en Seattle, Washington. Su eslogan es and you're done (Traducido al español: y listo o estás listo). Fue una de las primeras grandes compañías en vender bienes a través de Internet. Amazon también posee Alexa Internet, a9.com, Shopbop e Internet Movie Database (IMDb).

Amazon ha establecido sitios web separados para Canadá, el Reino Unido, Alemania, Austria, Francia, China y Japón, para poder ofrecer los productos de esos países.

Ahora veamos algo se su historia. Fundada como Cadabra.com por Jeff Bezos en 1994 y lanzada en 1995, cadabra.com comenzó como una librería online. Tenía más de 200.000 títulos y estos se podían pedir también por e-mail. Tiempo después la bautizó amazon, por el río sudamericano del mismo nombre, y ya que en ese momento circulaban listas ordenadas alfabéticamente, Amazon aparecería en los primeros lugares.

El 15 de mayo de 1997 amazon.com salió a la bolsa, específicamente a la NASDAQ con el símbolo AMZN y a un precio de 18 dólares la acción.

El primer plan económico de amazon era inusual: la compañía no cambió nada en 4 o 5 años; tiempo después, pensando en retrospectiva, la estrategia funcionó bien. Tiempo después, la compañía se decidió

a crecer, y lo hizo bien: En 2002 logró un beneficio de 3900 millones de dólares, 5300 millones en 2003, 6900 millones en 2004, 8500 millones en 2005 y 10700 millones en 2006. Además, la prestigiosa revista Time Magazine calificó a Bezos como la persona del año en 1999, por ser dueño de Amazon, que se había vuelto muy popular.

En la actualidad está totalmente diversificada en diferentes líneas de productos, ofreciendo DVDs, CDs de música, software, videojuegos, electrónica, ropa, muebles, comida, libros, etc.

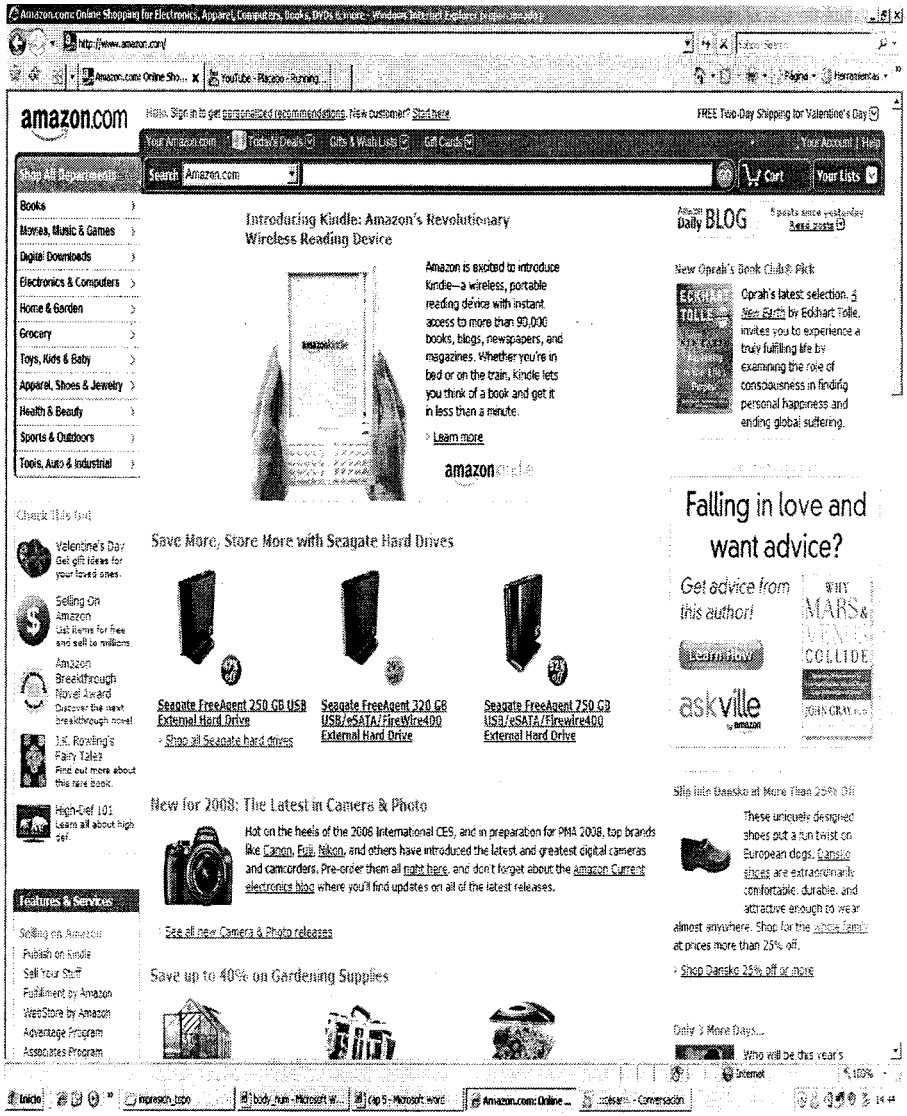


Imagen 15.- Portal Amazon.

Otro sitio de gran uso pero orientado al mercado de habla hispana es MercadoLibre.com. MercadoLibre.com (NASDAQ:MELI) es un sitio web de América latina dedicado a las compras, ventas y subastas por Internet. Cuenta con operaciones en Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Perú, República Dominicana, Uruguay y Venezuela. Los usuarios de MercadoLibre.com pueden vender tanto productos nuevos como usados a precio fijo o en la modalidad de subastas. MercadoLibre también posee MercadoPago, una compañía que ofrece diversas modalidades de cobro a los vendedores. MercadoLibre.com está asociado con eBay, la mayor tienda en Internet de Estados Unidos. Sus oficinas centrales se encuentran en Miami, Florida, Estados Unidos.

Ahora conozcamos algo sobre el origen de MercadoLibre. En marzo de 1999, mientras Marcos Galperín terminaba su MBA en la Universidad de Stanford escribió el plan de negocios de MercadoLibre. Una vez terminado el MBA, se dedicó a conformar la compañía que fue presentada en sociedad el 2 de agosto de 1999 y que rápidamente se expandió a los siguientes países: Argentina, Brasil, Colombia, Chile, Ecuador, México, Perú, Uruguay y Venezuela.

MercadoLibre tuvo dos rondas de financiamiento, la primera en noviembre de 1999 y la segunda en mayo de 2000. Las rondas incluyeron a los siguientes socios: JP

Morgan Partners, Flatiron Fund, y Hicks, Muse, Tate & Furst, Goldman Sachs, Fondo CRI Banco Santander Central Hispano y GE Equity

A dos años de su lanzamiento, en octubre de 2001, MercadoLibre firmó un acuerdo con eBay mediante el cual eBay se convirtió en el principal accionista de la compañía, MercadoLibre tomó las operaciones de Ibazar de Brasil y ambas compañías se convirtieron en socias exclusivas para América latina. En noviembre de 2005, MercadoLibre.com adquirió operaciones de DeRemate.com en Brasil, Colombia, Ecuador, México, Perú, Puerto Rico, Uruguay, y Venezuela.

A fines de 2006, MercadoLibre.com comenzó a operar en Costa Rica, Panamá y República Dominicana.

Imagen 16.- Portal de MercadoLibre MX.

Estos tres sitios que se mostraron en las páginas anteriores son los sitios mas utilizados en la mayor parte del mundo y América latina por su confiabilidad y antigüedad en el Internet como sitios de comercio electrónico.

CONCLUSION

Se ha logrado demostrar de manera clara las aplicaciones de seguridad que hay de tras al momento en que se realiza una transacción on-line.
Se ha explicado de forma general los protocolos y estándares que garantizan que una transacción on-line se realice correctamente y así se logre la integridad de los datos implicados en ella.
También se ha hecho referencia a empresas que desarrollan software de seguridad para transacciones on-line y los servicios que proporcionan dichos software.

En conclusión hoy en día la seguridad de las transacciones on-line son de suma importancia puesto que la información que se maneja debe mantenerse confidencial ya que si esta información llega a ser obtenida por gente ajena a esta, se podría ver afectado una persona, familias u organizaciones.

También debemos estar concientes de que en un futuro muy próximo la mayoría de los servicios sean públicos o privados serán y están siendo adquiridos por medio del Internet, gran parte de esta corriente de adquisición de bienes o servicios vía on-line es por que el Internet los globalizo y puso al alcance de un clic a todos los usuarios de obtener diferentes bienes o servicios sin importar en que parte del mundo se encuentre uno.

Por eso es importante que las personas estén concientes de la forma en que se llevan las transacciones on-line, ya que se volverán en parte de nuestra de vida diaria.

Otro punto muy importan es que como el documento a mostrado en sus paginas anteriores la gran variedad de productos que ofrecen específicamente seguridad para las transacciones on-line y también la implementación de protocolos de seguridad en la mayor parte de la Web.

Para finalizar se espera a ver logrado mostrar de manera muy general el funcionamiento y las características principales de la seguridad en las transacciones on-line.

GLOSARIO

A

AES.- Estándar de Encriptación Avanzado.

ANSI.- Instituto Norteamericano de Estándares.

ARPA.- Agencia de Proyectos de Investigación Avanzada.

D

DSA.- Algoritmo de Firma Digital.

H

HTTP.- Protocolo de Transmisión Hipertexto.

HTTPS.- Protocolo de Transmisión Hipertexto Seguro.

I

IDEA.- Algoritmos de Encriptación de Datos Internacional.

N

NFS.- Fundación Nacional de Ciencia.

NIST.- Instituto Nacional para Estándares y Tecnologías.

R

RSA.- Algoritmo de encriptación de clave publica desarrollado por Rivest, Shamir y Adelman.

S

SET.- Transacción Electrónica Segura.

SMTP.- Protocolo Simple de Transferencia de Correo.

T

TCP/IP.- (Protocolo de Control de Transmisión/Protocolo Internet).

TO.- Transacción on-line.

TPV.- Terminal Punto de Venta.

BIBLIOGRAFIAS

http://es.wikipedia.org/wiki/Transacci%C3%B3n_electr%C3%B3nica_segura

http://es.wikipedia.org/wiki/Transport_Layer_Security

http://es.wikipedia.org/wiki/Internet

http://en.wikipedia.org/wiki/3-D_Secure

http://es.wikipedia.org/wiki/Cifrado_sim%C3%A9trico

http://es.wikipedia.org/wiki/Criptograf%C3%ADa_de_curva_el%C3%ADptica

http://www.channelplanet.com/index.php?idcategoria=14782

http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20061122_01

http://209.85.165.104/search?q=cache:L-4kn6R5me4J:www.ipr-helpdesk.org/docs/docs.ES/securityOLTransactions.pdf+MasterCard+desarrolla+un+sistema+que+permite+mayor+seguridad+en+las+transacciones+electr%C3%B3nicas&hl=es&ct=clnk&cd=2&gl=mx

http://www.isocmex.org.mx/kiyoshi.html

http://www.eupmt.es/imesd/telematica/xarxes_i_serveis/documents/comercio_electronico.pdf

ANEXO

Legislación del Comercio Electrónico

Hablar de leyes que regulen Internet se ha convertido en el último grito de la moda entre nuestros legisladores, fenómeno que probablemente ha sido sólo superado por la magnitud con que los medios han abordado este acontecimiento.

El tema pareciera novedoso, pero la realidad es que lleva ya algún tiempo sobre la mesa. En mayo de 2000 entraron en vigor una serie de reformas al hoy Código Civil Federal (CC), Código de Comercio (CCom), Código Federal de Procedimientos Civiles (CFPC) y Ley Federal de Protección al Consumidor (LFPC). Su finalidad era habilitar la contratación electrónica, de manera que los acuerdos celebrados por “medios electrónicos ópticos o cualquier otra tecnología”1 pudieran considerarse legalmente válidos y por consiguiente plenamente obligatorios y exigibles entre las partes que concurrieron a su celebración.

El texto de estas reformas estaba inspirado a su vez en la ley modelo de CNUDMI2 de diciembre de 1996. La adopción de un lenguaje universal y uniforme en nuestra legislación nacional fue un acierto del legislador mexicano, pues sentó las bases para lanzar una plataforma sostenible de negocios electrónicos mexicanos en la arena global. Sobra mencionar que la red de redes no toma muy en cuenta las divisiones

geopolíticas y que por ende cualquier jurisdicción que decida separarse de los estándares y reglas uniformes aceptados internacionalmente está condenada al ostracismo comercial, con las consecuencias que ello implica para la economía local.

Con objeto de mantener nuestras leyes en armonía con el concierto mundial, los términos de la reforma necesitaban ser lo suficientemente generales y amplios como para mantener la uniformidad con legislaciones de otros países. Sin embargo, también eran necesarios una serie de lineamientos y reglas que permitieran aplicar e interpretar esta legislación. Lo idóneo hubiera sido la creación de documentos del tipo que tradicionalmente son usados en Derecho Mexicano para llevar a cabo la ejecución de leyes, tales como los Reglamentos, las Normas Oficiales Mexicanas (NOMs), los Decretos, etcétera.

El comercio electrónico aún lejos en México

La realidad es que ninguno de estos documentos ha entrado en vigor, por lo que el comercio electrónico no ha despegado en México con la intensidad o difusión esperada.

¿Cuál es la razón para que el desarrollo de las transacciones en línea se encuentre en una fase tan incipiente en nuestro país? La respuesta es simple: los

empresarios, directivos y demás personas con poder de decisión dentro de las corporaciones mexicanas no saben qué esperar, pues enfrentan riesgos considerables y difíciles de determinar en la mayoría de los casos; a su vez, sus consejeros y abogados no saben con precisión cuál será la reacción de las autoridades judicial y administrativa al aplicar la ley en operaciones, mensajes de datos y/o medios de autenticación electrónicos. Después de todo, la autoridad tampoco cuenta con los medios indispensables para llevar a cabo tal interpretación.

Y es precisamente en este escenario donde aparece la iniciativa de "Ley Federal de Firma y Comercio Electrónicos, Mensajes de Datos y Servicios de la Sociedad de Información" del diputado Barbosa, presentada el mes pasado ante la H. Cámara de Diputados, justamente dos años después de la entrada en vigor de las reformas mencionadas en párrafos anteriores. Sin duda se trata de un proyecto ambicioso y seguramente el mismo se encuentra motivado en beneficio de la nación en su conjunto.

Sin embargo, la ambición, tan importante ingrediente en los negocios electrónicos, no es la mejor consejera cuando se trata de elaborar leyes concisas, claras, cuya aplicación sea factible.

Iniciativa de ley en el Congreso

La propuesta Barbosa aglomera demasiados y muy diversos tipos de regulación, pertenecientes a ramas muy distintas del Derecho, en una sola iniciativa de ley. Al leerla, saltan a la vista temas tan disímbolos como: la prestación de servicios de la sociedad de la información (con regulación parecida a la contenida en la Directiva de la Unión Europea No. 2000/31/EC, relativa a dichos prestadores y al ejercicio del comercio electrónico); la regulación de contenidos (tema relacionado con nuestra garantía constitucional de libertad de expresión); algunas excluyentes de responsabilidad para aquellos casos en que el Proveedor de Servicios de Internet (por sus siglas en inglés: ISP) es un simple medio “pasivo” en la transmisión de datos, casos de almacenamiento de copias de información o “caching”, servicios de alojamiento de páginas Web o “hosting” y ciertos casos en donde se encuentre involucrado un motor de búsqueda (el plantea-miento, orden y tratamiento de estas excluyentes parece indicar que las mismas fueron moldeadas con base en los famosos “safe harbors” contenidos en la legislación norteamericana de derecho de autor). Por si fuera poco, la iniciativa toca asuntos como el valor probatorio de mensajes electrónicos (el cual ya ha sido regulado en el CFPC); privacidad de la información (un poco a la manera de la Directiva No. 95/46/EC de la Unión Europea); comunicaciones

publicitarias no solicitadas o “spamming”; firma electrónica y medios de certificación de la misma; contratación electrónica y formación del consentimiento por medios electrónicos (tema que también ya ha sido regulado en nuestro CC y CCom), así como capacidad jurídica de las personas (problema ya resuelto por los civilistas).

Ahora bien, si la lectura de esta lista casi interminable de temas complejos que constituyen la iniciativa de ley resulta rebuscada, eso es sólo una muestra de lo difícil que puede ser para nuestras autoridades aplicarla y lo inseguro que puede ser para los gobernados intentar conocer cuál es su alcance y consecuencias jurídicas. Pero más preocupante aún resulta que no todos los actores que pudieran resultar afectados por una legislación de esta magnitud han sido consultados por los redactores de la propuesta.

En los países donde ya se han creado leyes relacionadas con el entorno digital, la técnica legislativa es ordenada. En dichas jurisdicciones es común encontrar una serie de leyes separadas entre sí, de manera que cada una regula en forma concisa, sólida y clara una materia normalmente bien delimitada. Antes de la entrada en vigor de dichas leyes, los respectivos órganos legislativos sostuvieron consultas detalladas con miembros de la industria relevante y la sociedad

civil, con objeto de identificar necesidades y buscar soluciones que resultaran en el bien común. El proceso ha tomado una cantidad considerable de tiempo, pero parece que está rindiendo frutos. Si nuestros legisladores optan por adoptar preceptos jurídicos tomados de sistemas legales extranjeros, sería recomendable que también adoptaran una técnica legislativa mesurada. Por supuesto, mucho mejor sería que en lugar de importar principios legales extranjeros, pudiéramos los mexicanos encontrar aquellas reglas que más se ajustan a nuestra realidad nacional, cuidando de mantener nuestro sistema jurídico en armonía con los del resto del mundo.

En este sentido, la Comisión de Comercio de la H. Cámara de Diputados ha venido llevando a cabo un proceso incluyente y serio de consulta con la comunidad interesada en el desarrollo de Internet en México, los representantes de la industria informática, los especialistas en la materia, los posibles usuarios del sistema y la sociedad civil, lo cual ha generado una serie de consensos que a su vez han desembocado en una iniciativa de reforma al CCom que se nos presenta en un formato simple, conciso y de fácil aplicación al interpretarla. Dicha propuesta busca regular la firma electrónica de forma precisa, bien delimitada y empleando conceptos claros, al mismo tiempo que intenta mantener nuestra legislación nacional en

consonancia con las leyes modelo y principios uniformes adoptados por la mayoría de los países que hoy son socios comerciales de México, de modo que nuestros empresarios puedan hacer negocios de forma predecible y segura.

Si bien esta última propuesta no es la panacea para regular la amplia gama de relaciones jurídicas que pueden suscitarse a través de medios electrónicos, y aun cuando hacen falta
muchas leyes e instrumentos que permitan interpretar dichas leyes, la propuesta de la Comisión de Comercio es a todas luces una alternativa más viable como parte de los esfuerzos para impulsar el crecimiento del comercio electrónico en México.