I DESARROLLO Y FUNCIONAMIENTO DEL COMERCIO ELECTRONICO, Y LA SEGURIDAD QUE ESTE BRINDA AL USUARIO.

I.1 DEFINICION DE COMERCIO ELECTRONICO

El comercio electrónico es cualquier actividad de intercambio comercial en la que las órdenes de compra / venta y pagos se realizan a través de un medio telemático, los cuales incluyen servicios financieros y bancarios suministrados por Internet. El comercio electrónico es la venta a distancia aprovechando las grandes ventajas que proporcionan las nuevas tecnologías de la información, como la ampliación de la oferta, la interactividad y la inmediatez de la compra, con la particularidad que se puede comprar y vender a quién se quiera, y, dónde y cuándo se quiera. Es toda forma de transacción comercial o intercambio de información, mediante el uso de Nueva Tecnología de Comunicación entre empresas, consumidores y administración pública.

El comercio moderno está caracterizado por un incremento de la capacidad de los suministradores, de la competitividad global y de las expectativas de los consumidores. En respuesta, el comercio mundial está cambiando tanto en su organización como en su forma de actuar. Se están sobrepasando las estructuras jerárquicas antiguas y erradicando las barreras entre divisiones de empresas, así como las existentes entre las empresas y sus suministradores y clientes. Los procesos comerciales se están rediseñando de manera que atraviesen estos límites. Existen ya muchos ejemplos de procesos que afectan a una empresa entera e incluso algunos que llevan a cabo de manera conjunta las empresas y sus consumidores o suministradores.

El comercio electrónico es un medio de hacer posible y soportar tales cambios a escala global. Permite a las empresas ser más eficientes y más flexibles en sus operaciones

internas, trabajar más estrechamente con sus suministradores y dar mejor respuesta a las necesidades y expectativas de sus clientes. Les permite seleccionar los mejores proveedores, sin tener en cuenta su localización geográfica, y vender en un mercado global.

Un tipo especial de comercio electrónico es la venta electrónica, en la que un suministrador provee bienes o servicios a un cliente a cambio de un pago. Como caso especial de venta electrónica estaría aquel en el que el cliente es un consumidor ordinario en lugar de otra empresa.

Sin embargo, aunque estos casos especiales tienen una considerable importancia económica, son sólo casos particulares del caso más general de cualquier forma de operación o transacción comercial llevada a cabo a través de medios electrónicos. Otros ejemplos igualmente válidos son las transacciones internas dentro de una misma empresa o el suministro de información a una organización externa con o sin cargo.

El comercio electrónico es tecnología para el cambio. Las empresas que lo miren como un "añadido" a su forma habitual de hacer negocio obtendrán sólo beneficios limitados, siendo el mayor beneficio para aquellas que sean capaces de cambiar su organización y sus procesos comerciales para explotar completamente las oportunidades ofrecidas por el comercio electrónico.

I.2 TIPOS, NIVELES Y APLICACIONES DEL COMERCIO ELECTRÓNICO

El comercio electrónico, según los agentes implicados, puede subdividirse en cuatro categorías diferentes:

* empresa-empresa
* empresa-consumidor
* empresa-administración

* consumidor-administración

Un ejemplo de la categoría empresa-empresa sería una compañía que usa una red para ordenar pedidos a proveedores, recibiendo los cargos y haciendo los pagos. Está establecida desde hace bastantes años, usando en particular Intercambio Electrónico de Datos (EDI, Electronic Data Interchange) sobre redes privadas o de valor añadido.

La categoría empresa-consumidor se suele igualar a la venta electrónica. Se ha expandido con la llegada de la Word Wide Web. Hay ahora galerías comerciales sobre Internet ofreciendo todo tipo de bienes consumibles, desde dulces y vinos a ordenadores y vehículos a motor.

La categoría empresa administración cubre todas las transacciones entre las empresas y las organizaciones gubernamentales. Por ejemplo, en USA las disposiciones gubernamentales se publicitan en Internet y las compañías pueden responder electrónicamente. Generalmente esta categoría está empezando, pero puede crecer rápidamente si los gobiernos la usan para sus operaciones para promover la calidad y el crecimiento del comercio electrónico. Además, las administraciones pueden ofrecer también la opción del intercambio electrónico para transacciones como determinados impuestos y el pago de tasas corporativas.

La categoría consumidor-administración, no acaba de emerger. Sin embargo, a la vez que crecen tanto las categorías empresa-consumidor y empresa-administración, los gobiernos podrán extender las interacciones electrónicas a áreas tales como los pagos de pensiones o el autoasesoramiento en devoluciones de tasas.

Los negocios en internet

En el comercio electrónico se puede distinguir diferentes niveles, que pueden ir desde la forma más sencilla de su aplicación, hasta llegar al principio o esencia de lo que éste representa, así:

1. En el primer nivel, encontramos la simple transferencia de fondos y transferencia de tarjetas de crédito.
2. En este segundo nivel, se incluye la infraestructura que apoya al comercio electrónico (proveedores de servicio y acceso, fabricantes de quipos, etc.)
3. Luego encontramos, el nivel que contiene transacciones electrónicas de compañía a compañía.
4. Luego está, el nivel empresa - consumidor sin transacciones.
5. Por último, empresa consumidor con pagos electrónicos

Aplicaciones del comercio electrónico

Dentro del nivel organizacional el comercio electrónico juega un papel muy importante dentro de la reingeniería de procesos de negocios, es una manera natural de automatizar los procesos entre departamentos o divisiones de una organización. Es aplicable a estrategias del Marketing Directo, a video conferencias, cursos y seminarios virtuales, y con la aparición del EDI, alcanza una magnitud insospechada, abarcando temas legales, contables, financieros, de seguros, incluso en las actividades del sector gubernamental; constituye el eje sobre el cual gira el comercio internacional y su registro en las cuentas del Estado, como Banco Central, Ministerio de Finanzas o Hacienda, de Comercio Exterior, Aduanas, etc.

I.3 HERRAMIENTAS DEL COMERCIO ELECTRÓNICO

Sabemos que el comercio electrónico es toda forma de transacción comercial (compra-venta, pago-cobro) a través de medios electrónicos, y para llevar adelante estas transacciones se hace imprescindible la presencia de varias herramientas tecnológicas utilizadas por el comercio electrónico para su desarrollo.

Internet es una gran base de datos, representada en tablas, textos libres, textos enriquecidos, documentos con audio y video, etc., es decir, una fuente de información incalculable, a disposición del comercio electrónico.

Sin embargo nada de esto podría ser transmitido a los usuarios de Internet, sin la aplicación de la World Wide Web o comúnmente conocida como la WWW, ya que se constituye en la ventana de acceso a la red de redes, y a otras aplicaciones como el correo electrónico, news, FTP, etc.

La WWW es un sistema de información que utiliza el formato de hipertexto o lenguaje HTML (HyperText Markup Language), para la creación de páginas o sitios Web, dicho formato nos permite escoger las opciones que más nos interesen entre textos, sonidos e imágenes, facilitándonos la elaboración de párrafos, cabeceras, la inclusión de imágenes y de hiperenlaces o links, los cuales pueden ser una, varias palabras o imágenes resaltadas, normalmente subrayadas en color azul, que nos conducen a otra parte del mismo documento o a otros documentos.

La WWW facilita la localización de información a través de los URL (Universal Resource Locator), que son direcciones únicas o identificaciones universales para acceder a la red. Si no conocemos las direcciones a las que queremos acceder, tendremos que utilizar

un "buscador o search engine" (bases de datos de páginas recopiladas por máquinas) o un "índice" (directorios de páginas recopiladas manualmente).

Pero en la red no solo podemos obtener información, sino también es posible comunicarnos con cualquier usuario de manera similar como en un correo postal, pero de manera casi instantánea; esto es posible gracias al correo electrónico o e-mail, que es un mecanismo de intercambio de información y mensajes, que va desde nuestro ordenador personal hasta el ordenador del destinatario. Para llevar a cabo este proceso, es necesario conocer la dirección de correo electrónico a la cual queremos enviar la información, la misma que está formada por una parte que identifica al usuario y otra que identifica al ordenador, separados por el símbolo @ (arroba). Por ejemplo:

usuari@ps.uib.es

Con ayuda del e-mail, hoy es posible entablar auténticas tertulias internacionales en la red, es decir charlar electrónicamente mediante el uso de fórums de debate, los que pueden ser listas de correos y news .

Las listas de correos son direcciones electrónicas en los cuales los usuarios pueden participar únicamente al suscribirse con su dirección de e-mail, de esta manera reciben o envian mensajes desde y hacia todos los suscriptores de estas listas.

Los grupos de noticias o News es el sistema más sencillo para localizar colectivos y personas relacionadas con nuestros intereses. Son grupos de debate o trabajo en grupo organizados temáticamente que tratan cualquier tema que imaginemos. Es algo similar a las listas, pero con la diferencia de que los mensajes no son depositados en su buzón de correo, sino en un tablón público que lo puede mirar cuando lo desee.

Nos hemos referido, a la WWW, como una ventana de acceso a todas estas herramientas: e-mail, news, tablón de anuncios, veamos ahora cómo se relaciona con el FTP. En primer lugar FTP (File Transfer Protocol) es una aplicación estándar utilizada por internet para transferir ficheros de un programa cliente de FTP de cualquier usuario a un servidor de FTP. Al establecer una sesión de FTP, el usuario debe disponer de una cuenta de usuario en el ordenador remoto, para que éste le permita acceder. Sin embargo existen también servidores de FTP públicos, para usuarios que no mantienen cuenta. Estos últimos nos permiten bajar o descargar información de los sitios FTP públicos a nuestro ordenador.

Otra de las herramientas que contribuye al desarrollo del comercio electrónico, son las tiendas virtuales, las mismas que residen en un servidor de Internet especialmente adaptado para ello. En ellas usuarios y proveedores participan interactivamente en la compra-venta de innumerables artículos, que van desde CDs, libros, prendas de vestir, alimentos, autos, casas, etc.

A través de este revolucionario sistema de compras, podemos acceder desde casa, oficina o negocio, a tiendas on line, y realizar nuestras órdenes de compra y pagos electrónicos mediante el uso de la tarjeta de crédito hasta sitios seguros reconocidos en Internet como "save servers", que es un lugar que soporta el protocolo Secure Sockets Layer (SSL) de encriptación de información basado en claves públicas, de manera que la información enviada por la red es segura y en principio no accesible por un usuario no autorizado.

Si queremos enviar nuestros datos personales y número de tarjeta, debemos asegurarnos que este sea un sitio seguro, así, cuando navegamos en Internet Explorer, aparecerá un candado en la barra inferior, lo cual significa que el sitio trabaja con el protocolo SSL, en cambio si lo hacemos por Netscape, la barra nos mostrará una llave.

Existen además otros métodos de pago como el Dinero Digital o Digital Cash, su desarrollo será indudablemente más lento que el dinero plástico o tarjetas de crédito. Se trata de unidades con valor monetario, sin necesidad de estar vinculadas a una cuenta bancaria. Están destinados a transacciones de valor más bajo en principio que las tarjetas y permitirán el intercambio de dinero entre dos particulares. En algunos casos se ha puesto bastante énfasis en que permitan el anonimato (al menos del que paga) sin que pierdan seguridad. Son planteamientos muy innovadores, y por tanto generan muchas más reservas y recelos en el entorno financiero.

Además las grandes entidades financieras del sector están muy interesadas y ya están creando estándares apoyados por otras empresas, en el momento actual hay hasta siete formas de dinero digital que se disputan entre sí la primacía : Checkfree, CyberCash, DigiCash, First Virtual Holdings, Net Bill, Netscape Communications y Open Market.
Se han formado dos grandes consorcios que parece que van ser los que se enfrenten por la supremacía en este sector:

1. SEPP (Secure Electronic Payment Protocol). Creado por Mastercard, incluye también a GTE Corp. e IBM, a Netscape (quizás la empresa de software más influyente en temas relacionados con el WWW, ya que más del 60% de clientes Web presentes en Internet son Netscape Navigator) y a CyberCash (una de las empresas pioneras en sistemas de pago electrónicos).
2. STT (Secure Transaction Technology). Liderado por VISA y Microsoft, y con otros socios como Spyglass, una empresa de software que fue una de las pioneras en clientes WWW comerciales.

Con todo esto, sin duda podemos entrever que las gestiones bancarias cibernéticas han sido siempre las pioneras y quienes han concientizado el uso de "cajeros virtuales". Las operaciones con bancos a través de Internet son posibles desde hace tiempo. Entre otros, ya es posible operar con: Banco Santander, Bankinter, La Caixa, Banesto, Banco Central Hispano, Caja de Arquitectos (España), BBV, First Virtual (Primer banco creado en la propia Internet), First Bank of Internet (FBOI), Wells Fargo Bank, Natwest Bank y Bank of America.

Las operaciones que se pueden realizar dependen de cada entidad. Las más habituales son: consultas de saldo, extractos de operaciones, transferencias, compra / venta de acciones y de fondos, cambio de condiciones de tarjetas de crédito.

Como es obvio, los datos que circulan sobre estas operaciones están altamente protegidos a través del protocolo SSL, estos se conocen porque sus URL son una dirección de tipo: https:// en lugar del clásico http://.

Proporcionar toda la seguridad y confianza posible tanto para el cliente como para su proveedor en Internet, son la herramienta clave del comercio electrónico, y para ello se ha creado el protocolo SET (Security Electronic Transaction , conjunto de especificaciones que permite a los involucrados realizar transacciones seguras) y los sistemas de encriptación de mensajes, basados en el uso de algoritmos criptográficos que son de doble naturaleza (una de clave pública y otra de clave privada), los cuales facilitan la emisión de certificados y la generación de firmas digitales, simplificando las operaciones de pago y cobro en Internet.

Con la encriptación, la información transferida solo es accesible por las partes que intervienen (comprador, vendedor y sus dos bancos). La firma digital evita que la

transacción sea alterada por terceras personas sin saberlo. El certificado digital, que es emitido por un tercero, garantiza la identidad de las partes.

Desde el punto de vista del usuario, es importante que se lleve un tipo de control para asegurar en primer, lugar que la información recibida realmente proviene de la persona que dice que la envía y que la información enviada llegue a su destino, esto se conoce con el nombre de autenticación.

En segundo lugar, asegurar que la información que se envía o se recibe, no haya sido alterada por el camino por terceras personas, conocida como integridad de la información.

Y finalmente asegurar que la información no sea interceptada o copiada por otras personas y se conoce con el nombre de privacidad y confidencialidad de la información.

I.4 SEGURIDAD Y CRIPTOGRAFIA

La seguridad es uno de los elementos clave en el desarrollo positivo de las redes de información mundial y particularmente en el comercio electrónico, ésta genera confianza, y hace que los usuarios al depositar sus datos en la red, esten seguros de que no serán alterados ni desviados a usuarios no autorizados. Todo esto hoy es posible gracias a la utilización de métodos criptográficos cuyo objetivo es garantizar la seguridad en la difusión de los mensajes que son transmitidos por la red.

Es muy importante, por consiguiente, reducir los riesgos que la distancia impone a compradores y a vendedores; y como primer paso es necesario garantizar la confidencialidad , es decir que los datos necesarios para hacer el pago, como son número de tarjeta o cuenta, y su fecha de vencimiento, no sean vulnerables a receptores no autorizados en la red, lo cual se alcanza mediante la encriptación de mensajes .

El segundo paso, es garantizar que la integridad de los datos que llevan las instrucciones de pago, no sean modificados a lo largo de su trayecto, esto se logra mediante el uso de firmas digitales.

Por último, la autentificación tanto del comprador como del comerciante, el primero, como usuario legítimo de la tarjeta para el pago del bien adquirido, y el segundo garantizando que mantiene una relación bancaria con una institución financiera que acepta el pago con tarjetas, lo cual se consigue con la emisión de certificados digitales y la generación de firmas digitales.

Niveles de seguridad y de autenticación:

* Contraseña/prueba: registro/confianza basada en la primera transacción.

* Transmisión segura: cifra el contenido mientras éste es transmitido por la Internet.

* Cifrado de tecla doble: asegura que solamente el destinatario deseado pueda abrir el mensaje. Las partes se pasan entre ellas las teclas de cifrado.

* Autenticación: Una tercera parte en la que se tiene confianza emite certificados digitales a las partes conocidas, examina las transacciones en tiempo real, provee al comerciante recibidor válido la llave para que descifre la transmisión, certifica que la transacción tuvo lugar entre el comprador y el vendedor mediante un comprobante independiente de la transacción.

* Transacción electrónica segura, (Secure Electronic Transaction [SET]): El protocolo común de los servicios de autenticación, permite que emisores múltiples de certificados digitales cooperen en la transacción, integra los servicios de compensación de tarjetas de crédito, débito y otras con el servicio de autenticación. No revela al comerciante la información de la tarjeta.

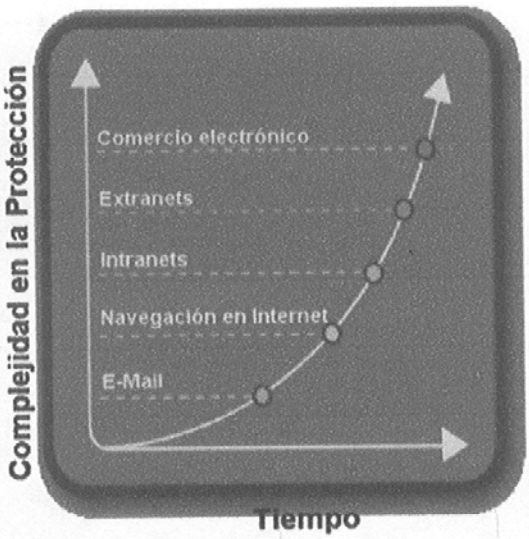

Fig. 1 Relación entre tiempo y complejidad de protección

Proceso de encriptación

Internet es prácticamente una puerta abierta, sobre la cual ninguna entidad ejerce un control en cuanto a qué publicar o no, pero si es posible monitorear desde que lugar se conectan los usuarios a la red, con qué frecuencia lo hacen, incluso lograr apoderarse de alguna información. Naturalmente, como usuarios tememos por el peligro que al enviar nuestros datos personales, caigan en manos de un extraño o los llamados hackers, sin embargo, un servidor seguro nos garantiza que la información llegará protegida a su destino, mediante un proceso de encriptación:

a. Nuestra información se encripta desde el momento en que pulsamos el boton "enviar", al llenar un formulario de compra, y es nuestro ordenador el encargado de cifrar y "esconder" los datos.

b. Todo dato que se digitalice se codifica en binario, es decir en ceros y en unos.

c. Para encriptarlo, se aplica al mensaje un algoritmo u operación matemática que devuelve un mensaje indescifrable, también en binario.

d. Para decifrar el mensaje original, se aplica el mismo algoritmo al llegar al lugar destino.

e. Solamente el emisor y el receptor podrán decifrar el algoritmo y el mensaje contenido con una información en clave que cada uno de ellos conoce. Estas claves pueden ser privada (que conocerá solo el emisor) y pública (que conocerán los destinatarios).

f. Cada usuario deberá disponer de este par de claves que van asociadas. De esta manera si alguien quiere enviar un mensaje cifrado a un usuario, tendría que conocer su clave pública y solo la clave privada podría descifrarlo.

g. Si quien envía un texto es un usuario cualquiera, el emisor podrá verificar a través de la clave pública (correspondiente solo a ese usuario) que el mensaje ha sido enviado por el usuario correcto. De este modo el usuario no podrá negar el hecho pues solo puede haber sido firmado con la clave privada por él conocida.

En la práctica, si nuestro objetivo es realizar una compra en línea utilizando el navegador Internet Explorer, primeramente debemos asegurarnos de que estamos conectados con un servidor seguro; de ser así, tendremos en pantalla la opción de entrada a este sitio, y al hacer click sobre ésta aparecerá inmediatamente la siguiente alerta de seguridad:

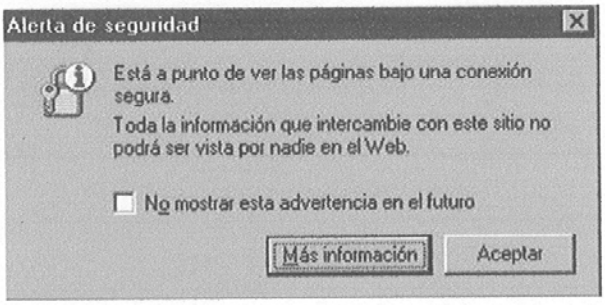

Fig. 2 Alerta de seguridad

Al dar un click sobre la celda que dice "Más información", tendremos el sigiente recuadro, que señala la garantía de estar ingresando a un sitio seguro:

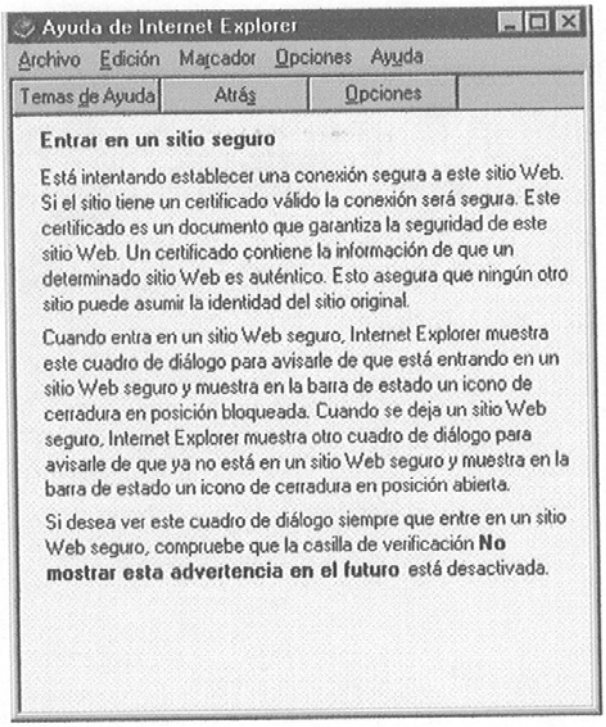

Fig. 3 Recuadro de sitio seguro

Si escogemos la opción "Aceptar", podremos darnos cuenta que el URL o dirección de la página ya no es http:// sino https://, y en nuestro ordenador aparecerá un candado en la barra inferior de controles:

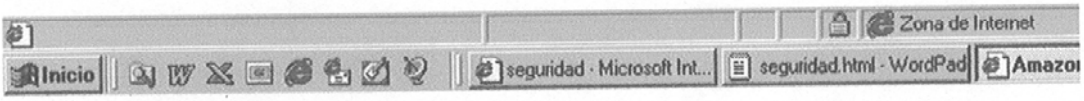

Fig. 4 Icono del candado

Al hacer un click sobre el ícono del candado, Internet Explorer nos muestra una ventana con las propiedades del certificado de validez, que esa tienda virtual posee para el cobro mediante tarjeta de crédito; en dicho certificado se especifica quien es la autoridad emisora, la fecha en la que se emitió el certificado y la de caducidad, la huella digital

representada por una serie de números y letras, el protocolo de seguridad utilizado (Secure Socket Layer SSL) y otros aspectos necesarios para su identificación:

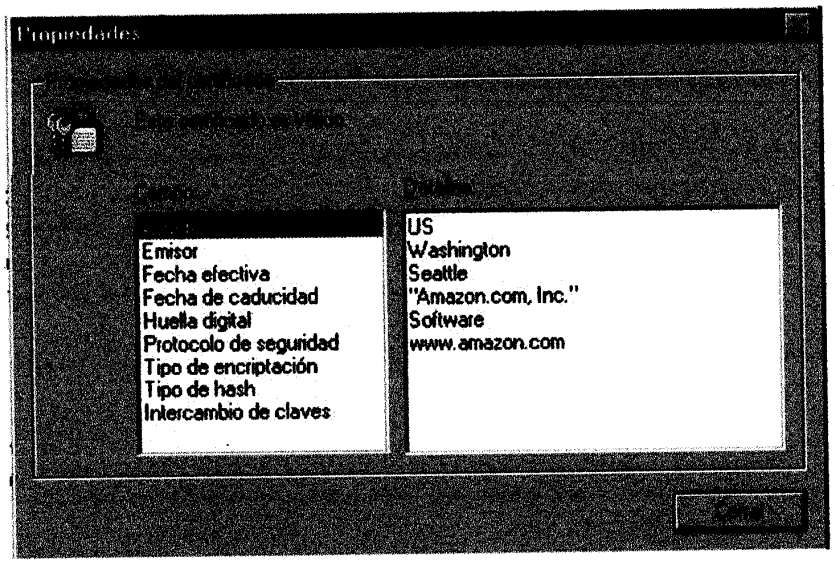

Fig. 5 Ventana del certificado de validez

Si la compra la queremos hacer empleando el navegador Netscape, observamos un proceso similar al de Internet Explorer; por consiguiente, cuando elegimos la opción de entrada al sitio seguro, la pantalla nos muestra la información de seguridad:

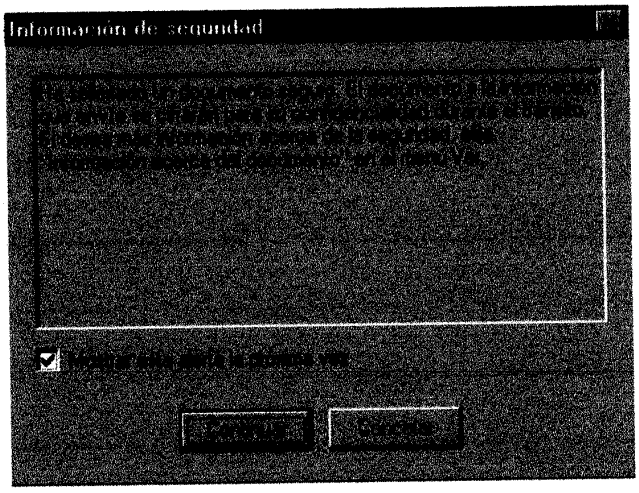

Fig.6 Ventana de información de seguridad

En este cuadro podemos distinguir la opción "Continuar", al elegirla, entraremos al sitio seguro para efectuar la compra, esto lo podemos comprobar cuando se presente un pequeño candado en la parte inferior de la barra de controles:

Fig. 7 Candado en barra de controles

Al dar un click sobre este candado, el certificado que valida la existencia del sitio seguro aparecerá inmediatamente, el mismo que nos presenta una serie de opciones referentes a los requisitos de seguridad empleados por la tienda virtual y el seleccionados por el navegador.

Protocolo set

Los principales bancos y corporaciones involucrados con tarjetas de crédito en el mundo, han formado un consorcio con el objetivo de crear un conjunto de especificaciones que permitan el desarrollo del comercio electrónico en el seno de Internet, llamado SET, Secure Electronic Transaction o Protocolo de Transacción Electrónica Segura.

Definición de Protocolo SET

Secure Electronic Transactions es un conjunto de especificaciones desarrolladas por VISA y MasterCard, con el apoyo y asistencia de GTE, IBM, Microsoft, Netscape, SAIC, Terisa y Verisign, que da paso a una forma segura de realizar transacciones electrónicas, en las que están involucrados: usuario final, comerciante, entidades financieras, administradoras de tarjetas y propietarios de marcas de tarjetas.

SET constituye la respuesta a los muchos requerimientos de una estrategia de implantación del comercio electrónico en Internet, que satisface las necesidades de consumidores, comerciantes, instituciones financieras y administradoras de medios de pago.

Por tanto, SET dirige sus procesos a:

* Proporcionar la autentificación necesaria.

* Garantizar la confidencialidad de la información sensible.

* Preservar la integridad de la información.

* Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

SET utiliza para sus procesos de encriptación dos algoritmos:

* De clave pública RSA (algoritmo simétrico), diseñado por Rivest, Shamir y Adleman, cuyas iniciales componen su nombre.

* De clave privada DES (Data Encryption Standard), de fortaleza contrastada y excelente rendimiento, conocido también como algoritmo asimétrico ya que emplea dos claves diferentes: una para encriptación y otra para desencriptación.

La base matemática sobre la cual trabajan los algoritmos, permite que, mientras un mensaje es encriptado con la clave pública, es necesaria la clave privada para su desencriptación.

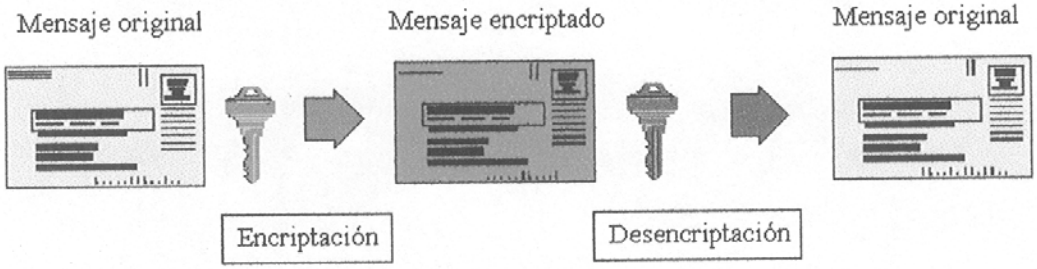

Fig. 8 Encriptación y desencriptación de mensajes

El mensaje original es encriptado con la clave pública del destinatario; este podrá obtener el mensaje original después de aplicar su clave privada al mensaje cifrado.

Para evitar que la clave pública de un usuario sea alterada o sustituida por otro no autorizado, se crea una entidad independiente llamada Autoridad Certificadora (Certifying Authority, CA), cuya labor consiste en garantizar y custodiar la autenticidad de la claves públicas de empresas y particulares, a través de la emisión de certificados electrónicos.

Sobres electrónicos :

Como hemos visto SET, se encarga de proporcionar la confidencialidad de los mensajes y para cifrarlos utiliza dos claves simétricas, las que al ser generadas aleatoriamente, son cifradas a su vez con el componente público del par de claves asimétricas del destinatario. Por tanto, sobre electrónico (digital envelope) es la unión de la clave simétrica cifrada, con los datos del mensaje cifrados por esta.

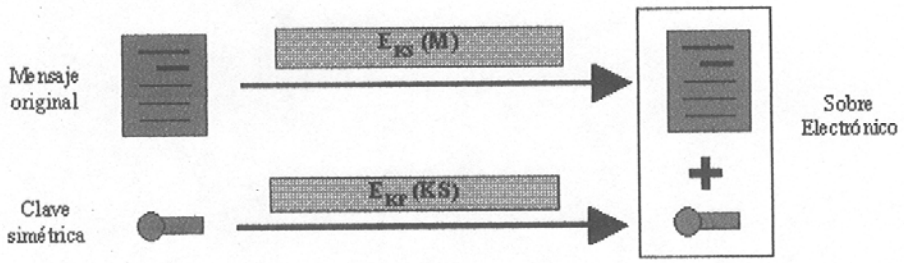

Fig. 9 Sobre Electrónico

Al llegar a su destino, el componente privado del par de claves asimétricas de quien recibe el mensaje, descifra la clave simétrica y los datos del mensaje.

Firmas electrónicas :

Las relaciones matemáticas entre la clave pública y la privada del algoritmo asimétrico utilizado para enviar un mensaje, se llama firma electrónica (digital signatures). Quien envía un mensaje, cifra su contenido con su clave privada y quien lo recibe, lo descifra con su clave pública, determinando así la autenticidad del origen del mensaje y garantizando que el envío de la firma electrónica es de quien dice serlo.

La integridad del contenido del mensaje es garantizada al hacer pasar los datos a través de una función irreversible, como MD5, que produce un destilado del original que es único para un contenido dado y jamás podrá darse un destilado igual partir de dos mensajes diferentes. Este proceso se conoce como digestión del mensaje (message digest).

Fig.-10 Digestión del mensaje

La clave privada del emisor destila el mensaje, y el resultado se añade al mensaje original enviado, formando la firma electrónica, mientras que el receptor descifra el destilado con la clave pública del emisor. Si al aplicar el receptor, la misma función al mensaje original, los resultados son iguales, la integridad y autenticidad del mensaje son correctas. Si el "destilado" generado no es coincidente con el extraído de la firma electrónica, se ha producido una modificación en el contenido del mensaje.

Certificados de autenticidad :

Como se ha visto la integridad de los datos y la autenticidad de quien envia los mensajes es garantizada por la firma electrónica, sin embargo existe la posibilidad de suplantar la identidad del emisor, alterando intencionalmente su clave pública. Para evitarlo, las claves públicas deben ser intercambiadas mediante canales seguros, a través de los certificados de autenticidad, emitidos por las Autoridades Certificadoras.

Para el efecto SET utiliza dos grupos de claves asimétricas y cada una de las partes dispone de dos certificados de autenticidad, uno para el intercambio de claves simétricas y otro para los procesos de firma electrónica.

Las Autoridades Certificadoras poseen un sistema jerárquico para la emisión y verificación de Certificados de Autenticidad hacia autoridades de niveles inferiores, en este sistema intervienen:

7. Asociación de emisores de medios de pago o propietarios de las marcas de tarjetas.

* Issuer, entidad financiera del comprador, la cual posee certificados para actuar como Autoridad Certificadora, lo que le permite emitir otros hacia los compradores.

* Acquirer, entidad financiera del comerciante, de igual forma posee un certificado de Autoridad Certificadora, para la emisión de otros hacia los comerciantes.

* Compradores, que obtienen su certificado de la entidad financiera o issuer, para su completa identificación, el mismo que reemplazará a la tarjetas de crédito.

* El comerciante, que obtiene su certificado de la entidad financiera o acquirer, con la cual firma un contrato de adhesión para la aceptación de tarjetas de crédito o débito; el comerciante poseerá tantos certificados como marcas de tarjetas acepte como medio de pago.

Programas para Encriptación -Desencriptación :

En la actualidad hay varios métodos de encriptación y cada vez se utilizan más programas de correo electrónico coordinadamente con programas de encriptación-desencriptación compatibles, que aseguran sus relaciones en operaciones comerciales, entre todos ellos podemos mencionar algunos:

Pretty Good Privacy (PGP): Es un programa de encriptación de documentos a través de redes, creado por Philip Zimmermann, combinando el mejor algoritmo existente de clave única, el IDEA (International Data Encription Algorithm), con el mejor de clave pública, el RSA, y añadiendo el MD5 para las firmas digitales. Este combina criptografía de clave pública con criptografía convencional, ofreciendo encriptación, autenticación de documentos con firmas digitales, comprobación de integridad y opciones de manejo de claves. Por sus gran ductilidad y adaptabilidad a las diferentes arquitecturas informáticas puede ser utilizado con la mayoría de los sistemas operativos comerciales como Windows,

Windows NT, Mac, etc. Asimismo, puede ser utilizado conjuntamente con programas de correo electrónico tradicionales como Eudora.

La compañía de Zimmermann ha creado diversos programas comerciales cuya venta está restringida por la normativa ITAR a Estados Unidos y Canadá. Entre ellos cabe destacar PGPMail, un programa que integra PGP como una parte más del programa de e-mail Eudora, facilitando mucho la tarea en el entorno Windows, y PGP Disk , un programa diseñado específicamente para la protección de discos duros.

Pretty Good Privacy Fone: Es un programa con las características del PGP tradicional, que permite hacer llamadas telefónicas normales vía modem, comprimiendo encriptando la voz, para luego digitalizarla sin que terceras personas puedan acceder a las mismas y llegue segura al receptor. Se utiliza para este intercambio de claves el algoritmo de clave pública DH.

International Data Encription Algorithm (IDEA): Este programa de encriptación algorítmica de Ascom Systec Ltd. de Suiza, utiliza el mismo sistema de seguridad de Pretty Good Privacy (PGP). Su implementación es simple y puede ser utilizado en todo el mundo.

Ha sido registrado con normas ISO/IEC y UNI/EDIFACT (lo que posibilita la implementación de aplicaciones EDI).

Authosign-AEA Technology: AEA Technology desarrolla un conjunto de herramientas informáticas destinadas a confirmar la integridad de los documentos que se envían mediante correo electrónico como encriptación, firma digital, etc.

Dentro de las instituciones más destacadas que brindan servicios de secure server, para llevar adelante las actividades de comercio electrónico, podemos mencionar las siguientes:

Verisign es una de las más prestigiosas compañías líderes, que provee la infraestructura de llaves públicas (PKI) y soluciones para certificados digitales usados por empresas, sitios Web y consumidores, para llevar adelante las comunicaciones y transacciones seguras en Internet y redes privadas en todo el mundo.

La compañía Terisa Systems trabaja en la creación de productos para seguridad en la WWW, que son muy fáciles de utilizar pero a la vez garantiza que la compra - venta a través de tarjetas de crédito sea segura, de igual forma para el uso de firmas digitales en contratos mercantiles, con el empleo de claves criptográficas como el RSA.

Secude, es un programa de seguridad que autentiza y proteje las comunicaciones privadas realizadas por e-mail, brinda la infraestructura para la utilización de firmas electrónicas, encriptación, redes de autenticación, contratos digitales, aplicaciones EDI y distribución de softwares por la Red. Para su desarrollo emplea claves simétricas y asimétricas con algoritmos RSA.

La corporación IBM, ha desarrollado productos y servicios para la protección de las actividades de negocios realizados electrónicamente como antivirus, criptografía y contrafuegos, implementando así un mayor grado de seguridad al empresario.

Data Fellows desarrolló un programa denominado F-Secure Commerce para encriptar y autentificar cualquier clase de documento, utilizando métodos de encriptación que incluyen DES, 3DES, IDEA, Blowfish y RSA, con aplicación sobre las versiones de Windows 3.1; NT y 95.

La corporación Internet Security Systems (ISS), es la pionera en proveer sistemas adaptables a la gestión de seguridad y protección de programas, tales como contrafuegos, autenticación y encriptación. La ISS aporta con varias herramientas seguras para las

actividades de comercio electrónico como: Real Secure, Internet Scanner y System Security Scanner.

Visa conocida mundialmente por la emisión de "dinero plástico" o tarjetas de crédito, ha incorporado al mundo de los negocios, el uso de herramientas de pago seguras, mediante la aplicación de SET, facilitando así a clientes y vendedores las transacciones on line.

El Sistema Mondex emplea la tarjeta de crédito para pagos digitales, opera a nivel mundial a través de bancos e instituciones financieras como una subsidiaria de Master Card Internacional.

La corporación Cybercash, posee sus oficinas centrales en Reston, Estados Unidos, reconocida mundialmente por proveer soluciones de pago seguras para el comercio electrónico, asi como un sistema de pago y facturación interactivo a través de la WWW, entre empresas y consumidores.