EL COMERCIO ELECTRÓNICO Y LA SEGURIDAD DE SUS TRANSACCIONES

I.S.C. Patricia Leonor García Corral*
M. C. Francisco J. Alvarez Rodríguez*

I. INTRODUCCIÓN

La diseminación generalizada de las tecnologías de información tanto en los lugares de trabajo como en los mismos hogares aunada al incremento en el uso de *Internet* y otras redes de computadoras, ha creado una nueva forma de conducir el comercio y el mercado.

Se están sobrepasando las estructuras organizativas antiguas y erradicando las barreras entre divisiones de empresas, así como las existentes entre las empresas y sus proveedores y clientes.

El comercio electrónico es un medio para hacer posible y soportar tales cambios; permite que las empresas sean más eficientes y flexibles en sus operaciones internas, trabajar más estrechamente con sus proveedores y dar mejor respuesta a las necesidades de sus clientes.

El impacto del comercio electrónico se dejará sentir tanto en las empresas como en la sociedad en general y tal vez su implantación va a cambiar el modo de vida como en su momento lo hicieron el automóvil o el teléfono.

Sin embargo, en el mundo anónimo del *Internet*, los clientes y los vendedores deben enfrentarse a un nuevo conjunto de amenazas como son: accesos no autorizados, alteración de datos, monitoreo por personas ajenas y negación de servicios. Todos estos peligros pueden tener como principales consecuencias: fraudes, interrupción de servicios, pérdida de ventas, robo de información confidencial y la pérdida de confianza de los clientes.

Una de las soluciones planteadas para enfrentar estos problemas depende del tipo de comercio electrónico que se trate, de empresa a empresa o de cliente a empresa. En el caso de comercio entre empresas, la alternativa es el uso de *IED (Intercambio Electrónico de Datos)* en donde las partes interesadas ya han establecido una relación contractual e intercambian mensajes sobre una red segura. Esta relación exige el acuerdo de los participantes en la definición y orden de los campos, ya que la integración de la información a la aplicación específica de cada socio será de forma automática y sin manipulación humana, por esto se requiere la información en un formato estándar.

Pero es en el caso del comercio entre cliente y empresa donde las amenazas que se mencionaron causan más estragos, debido a que las comunicaciones se llevan a cabo sobre la red mundial más amplia e insegura del mundo: *Internet*, y casi todos los negocios se realizan entre "desconocidos" lo cual suma un riesgo muy grande a la transacción.

Por lo antes mencionado, este artículo tiene como objetivo el mostrar aspectos generales de lo que es el comercio electrónico, los protocolos de seguridad más comunes y estandarizados para el manejo de información confidencial, y las empresas certificadoras de servidores seguros para esta actividad .

Se plantea el uso de estos certificados digitales como solución a los problemas de seguridad y se justifican los esfuerzos que se están llevando a cabo en lo que respecta a mejoramiento de la misma, para hacer que el comercio electrónico sea una alternativa confiable para hacer negocios.

II. ¿QUÉ ES EL COMERCIO ELECTRONICO?

Se puede definir al comercio electrónico como: *Cualquier tipo de transacción comercial en que las partes interactúan virtualmente (a través de medios electrónicos) en lugar de realizar contactos directos.* Sin embargo, esta definición es muy amplia, ya que abarca desde los cajeros automáticos hasta las transacciones comerciales hechas en *Internet*, y no capta el espíritu actual del comercio electrónico.

En este sentido, el comercio electrónico (basado en *Internet*) abarca

* Desarrolla sistemas bajo tecnología WEB, Egresada de la U.A.A.
** Profesor Investigador, Depto. de Sistemas Electrónicos, U.A.A, fjalvar@correo.uaa.mx

una amplia gama de actividades, incluidos el acceso a información comercial, el intercambio de bienes y servicios por medios digitales, el suministro en línea de contenidos digitales, las transferencias electrónicas de fondos, el comercio electrónico de valores, el contacto en línea con los fabricantes, la contratación pública, la mercadotecnia, los servicios posventa directos al consumidor, la certificación de identidades y transacciones y, en general, todo lo relacionado a *Internet* con implicaciones económicas y comerciales. Corresponde igualmente a productos y servicios (de información o servicios financieros y jurídicos), y tanto a actividades tradicionales como la educación, como en nuevas actividades (centros comerciales virtuales).

Se puede decir, entonces, que el comercio electrónico consiste en efectuar todas las operaciones inherentes al comercio convencional como comprar, vender, solicitar productos o servicios, etc., a través de un medio electrónico. Es una herramienta que ha impactado las actividades económicas en su conjunto, en particular las relaciones y transacciones más frecuentes, vinculando los distintos sectores de la industria y los servicios.

El comercio electrónico no es un sueño futurista, ya que está ocurriendo ahora, con algunas actuaciones satisfactorias y bien implantadas. Tiene lugar en todo el mundo, y aunque los Estados Unidos, Japón y Europa están liderando el camino, el comercio electrónico es esencialmente global, tanto en concepto como en ejecución.

Se tienen registrados diversos estudios interesantes en relación al uso del comercio electrónico, en particular hay uno que contempló 386 entrevistas [Andersen Consulting, 1998] de las cuales se obtuvieron resultados que indican que la mayoría de los directivos encuentra grandes ventajas con este tipo de comercio. El 82% opina que en sus empresas se hará un uso más amplio de éste en pocos años. A pesar de esto, sólo en un 39% de los casos el comercio electrónico es parte significativa de la forma actual de operar en estas compañías; el otro factor que puede afectar el desarrollo de esto es que más de la mitad de los entrevistados cree que la mejor actitud "ahora" consiste en "esperar y ver cómo evoluciona" en sus respectivos mercados.

Otros datos interesantes del estudio son que el comercio electrónico aporta una mayor velocidad en las transacciones (73%), que mejora la gestión de la información (69%) y el servicio al cliente(68%), además de facilitar el acceso a los mercados globales (63%); sin embargo, las limitaciones de estos beneficios radica en la diferencia de acceso a la tecnología, que es evidente entre países desarrollados y no desarrollados.

La realidad del comercio electrónico se concreta en dos escenarios del futuro: el dejarse guiar por la política de "esperar y ver" que se resume en una amenaza para la competitividad, pérdida de cuota de mercado y de puestos de trabajo o aprovechar la ventaja competitiva del comercio electrónico, provocando de esta forma el aumento de la competitividad, la creación de nuevas empresas y el crecimiento del empleo.

Para aquellas empresas que exploten completamente su potencial, el comercio electrónico ofrece la posibilidad de cambios que modifiquen radicalmente las expectativas de los clientes y redefinan el mercado o creen mercados nuevos.

III. TIPOS DE COMERCIO ELECTRONICO

Entre los distintos tipos de comercio electrónico que se realizan se destacan los siguientes tres niveles [Saltó, 1999]:

- ***Empresa - Consumidor***: El medio de acceso que se utiliza es *Internet*. Se refiere al comercio desarrollado hacia el consumidor final. La empresa ofrece la gama de productos con intención de venta, que se responde por las intenciones de compra y quedando el trámite de pago de forma electrónica, aunque la entrega de la gran mayoría de los productos necesariamente es física. Los beneficios de este tipo de comercio son muy grandes; el cliente no tiene que moverse de su casa, su capacidad de elección es mayor, no necesita trasladarse a los lugares de compra para buscar distintas opciones y elegir las más convenientes, además de la facilidad de compra con el simple número de la tarjeta de crédito y esperar la entrega de los productos adquiridos en su propio domicilio.

  Por otro lado, los riesgos existentes en esta forma de comercio se deben a la carencia de costumbre por parte del consumidor y la falta de una cultura económica que posibilite la masificación. También es posible que el tiempo de espera del producto por falta de planeación logística del proveedor se haga muy espaciada de la fecha de compra. A pesar de lo anterior, sus perspectivas de desarrollo son alentadoras.

- ***Empresa – Empresa***: En este caso, los mecanismos deben ser más precisos y seguros. El medio utilizado es el *Intercambio Electrónico de Datos (IED)*, mediante el cual se transmite información estructu-

rada de computadora a computadora con el fin de que el emisor y el receptor cuenten con información uniforme y la puedan procesar sin necesidad de papel ni capturas reiterativas. Se da principalmente para satisfacer la demanda de insumos, materias primas, transporte, almacenaje y otros servicios de uso productivo.

Existen una multitud de transacciones que se pueden hacer mediante *IDE* con base en estándares previamente acordados entre ambas partes y que funcionan en el mundo. *IDE* se integra a los sistemas de cómputo independientemente de las plataformas técnicas y permiten el resurtido y la producción, además del pago en estrecho contacto con las instituciones financieras, la fecha, el lugar de entrega, etc. El *Intercambio de Datos Electrónico* es una forma de simplificación de las relaciones comerciales que reduce sustancialmente los costos, disminuye errores humanos en recaptura, el gasto en papel, permite la recepción puntual de los productos y la producción precisa sin mantener grandes inventarios.

- ***Instancias gubernamentales***: Utilizan como medio de comunicación *Internet* por los particulares requerimientos de las licitaciones y registro de participantes, además del pago de bienes y servicios que proporciona el gobierno, las compras gubernamentales, el pago y el trámite de asuntos relacionados con los impuestos, etcétera.

Las empresas que participan del Comercio Electrónico se pueden agrupar en tres mecanismos básicos [Saltó, 1999]:

- ***Catálogos Electrónicos:*** son una especie de escaparates virtuales. Una empresa que está interesada en comercializar bienes o servicios, monta los mismos en un medio electrónico, que sea accesible a la comunidad a la que desea llegar.

- ***Subastas:*** Se sigue el principio del intercambio de valores bursátiles. Se establecen las condiciones de compra de un producto y se lo lleva el mejor postor. Representan un mecanismo de mercado que aprovecha las oportunidades de los medios de electrónicos de comunicación entre proveedores y clientes. Es un sistema de mercado en tiempo real.

- ***Licitaciones:*** Éstas tienen que ver con actividades de adquisición de productos o servicios por parte del gobierno, pero aprovechando los medios electrónicos para la agilización de procesos.

IV. SEGURIDAD EN EL MANEJO DE LA INFORMACION

El objetivo de la seguridad en computadoras es prevenir que los invasores logren objetivos a través de accesos no autorizados o el uso no autorizado de computadoras y redes.

Existen tres categorías de seguridad: confidencialidad, integridad y disponibilidad. La **confidencialidad** requiere que la información sea accesible sólo a aquellos autorizados para esto; la **integridad** requiere que la información permanezca sin alteraciones por accidentes o intentos maliciosos, y la **disponibilidad** significa que los sistemas de cómputo permanezcan trabajando sin degradación de acceso y proveyendo recursos a los usuarios autorizados cuando se requiera. [Howard, 1997]

Los recursos que se quieren proteger son los procesos (programas en ejecución), los archivos (colecciones de registros o datos) y los datos en tránsito (paquetes de datos que se transmiten a través de una red).

En nuestro caso de estudio (comercio electrónico), el elemento que ha llegado a crear más desconfianza, es la seguridad en el manejo de información confidencial (transmisión y almacenaje) de las transacciones que se realizan electrónicamente, aclarando que es un aspecto en el que se ha avanzado mucho en los últimos años y que será más confiable conforme se extienda esta forma de comercio.

Actualmente, los clientes y las empresas deben enfrentar algunas amenazas cuando hacen negocios a través Internet y las más comunes son [Netscape, 1999]:

- **Accesos sin autorización**: Alguien hace un acceso o un mal uso de un sistema de cómputo para interceptar información y robar datos delicados.

- **Alteración de datos**: En el contenido de una transacción comercial se modifican datos como: nombre, número de tarjeta de crédito, monto de la transacción, etc. y éstos son alterados durante su transmisión.

- **Acciones de repudio**: Una de las partes interesadas en la actividad comercial niega que la transacción ocurrió o que fue autorizada.

- **Acciones de monitoreo**: Se da al romper mecanismos de seguridad en las redes de computadoras (sin autorización) y monitorear la información confidencial que está siendo transmitida.

- **Negación de servicios**: Un usuario sin permisos o privilegios suficien-

tes apaga servidores o niega el acceso a los visitantes.

Las amenazas mencionadas representan un obstáculo para el desarrollo del comercio electrónico en algunos países, y como se puede ver, gran parte de estos problemas tienen que ver con el manejo de información confidencial en las transacciones. Por esto se han dedicado esfuerzos en el planteamiento de nuevas soluciones que permitan eliminar los efectos de estos problemas y así, tanto empresas como clientes puedan concentrarse en obtener los mayores beneficios que este tipo de comercio les ofrece.

V. PROTOCOLOS DE SEGURIDAD.

Un número considerable de diferentes protocolos de seguridad se han introducido con el fin de establecer "canales seguros" de comunicación sobre redes abiertas como lo es *Internet*, para que de esta forma, las partes interesadas en realizar una transacción en la que se maneje información confidencial puedan "ser inmunes" a los ataques de terceros.

Cada uno de los protocolos que resume la *tabla 1* tiene una aplicación específica y actualmente sólo *SET (Secure Electronic Transactions)* y *SSL (Secure Sockets Layer & Transport Layer Security)* son los que se han implantado para efectos de proporcionar esquemas de seguridad para las partes interesadas en realizar comercio electrónico.

Técnicamente, no hay similitudes entre *SET* y *SSL*, exceptuando que ambos hacen uso de la criptografía de llave pública de *RSA* Data Security Inc. (empresa dedicada a la construcción, diseño de soluciones de seguridad para las tecnologías de información, telecomunicaciones,

Protocolo	Acciones que realiza
CDPC (Cellular Digital Packet Data)	Este es un estándar diseñado que permite a los clientes el envío de datos de computadora sobre las existentes redes celulares.
DNSSEC (Domain Name System Security Extensions)	Es un protocolo para la distribución segura de servicios de nombres como *hostname* y direcciones IP.
DOCSIS (Data Over Cable Service Interface Specification)	Este estandariza el cable módem para la transmisión segura de datos con protección hacia la negación y robo de servicios, así como la protección de la privacidad de los clientes.
IEEE 802.11	Es un protocolo estándar para la seguridad de redes de área local del tipo inalámbricas.
IPSec (IP Security Protocol)	Es un estándar para los servicios de autenticación basada en servicios de: criptografía, integridad y confidencialidad en la capa de datagramas de IP.
PPTP (Point-to-Point Tunneling Protocol)	Este estándar es usado para crear comunicaciones entre redes virtuales privadas a través de *Internet* bajo la tecnología de protocolos en "Conductos"; trabaja en la capa de datagramas de IP.
SET (Secure Electronic Transactions)	Estandariza las transacciones seguras con tarjetas de crédito a través de *Internet*.
S/MIME (Secure MIME)	Garantiza la transmisión segura, almacenaje, autenticación y retransmisión de información secreta en la capa de aplicaciones.
SSH (Secure Shell)	Este protocolo permite a los usuarios accesos remotos seguros de computadora a computadora a través de una red.
SSL & TLS (Secure Sockets Layer & Transport Layer Security)	Habilita un "canal seguro" entre dos aplicaciones para la transmisión segura de datos y la autenticación mutua.

Tabla 1. Protocolos de Seguridad [RSA, 1999]

servicios financieros e industrias del entretenimiento). Pero aún así, *RSA* les permite alcanzar distintos objetivos de seguridad.

VI. SSL (SECURE SOCKETS LAYER)

El protocolo *SSL* fue desarrollado por *Netscape Communications Corporation* para proporcionar seguridad y privacidad sobre *Internet*. El protocolo proporciona encriptación de datos, autentificación del servidor, integridad de mensajes y autentificación opcional de clientes para conexiones TCP/IP. *SSL* está disponible en la mayoría de los navegadores y servidores *WEB*, y al instalar un certificado digital habilita las capacidades del protocolo.

SSL es una aplicación independiente, permitiendo que otros protocolos como HTTP y Telnet sean montados sobre él de manera transparente.

El protocolo *SSL* es insertado entre el protocolo TCP y al protocolo de aplicación. *SSL* opera en 2 fases. En la segunda fase los datos son encriptados usando un algoritmo y llaves escogidas en la primer fase. Actualmente *Netscape* usa el algoritmo *RC4* que es un algoritmo de encriptación inventado por *RSA* Data Security Inc. para la encriptación de datos. De cualquier forma, *SSL* soporta un rango de otros algoritmos de encriptación incluyendo *DES* (Data Encryption System desarrollado por el gobierno de los Estados Unidos).

SSL está disponible en dos versiones: la de 40 bits y la de 138 bits; esto se refiere a la longitud de la llave de sesión encriptada, la cual es generada para cada transacción. Entre más larga sea la llave es más difícil romper el código de encriptación.

La mayoría de los navegadores soportan sesiones *SSL* de 40 bits; y los más recientes navegadores, permiten a los usuarios transacciones en sesiones encriptadas de 128 bits.

VII. SET (SECURE ELECTRONIC TRANSACTIONS)

El protocolo *SET* (Secure Electronic Transactions) es un conjunto de normas de seguridad, encriptadas, que constituyen una forma estándar para la realización de transacciones de pago a través de Internet.

El protocolo *SET* autentifica a los titulares de las tarjetas de crédito, los comerciantes y los bancos. Garantiza la confidencialidad de la información de pago y asegura que los mensajes no serán manipulados.

Este protocolo fue desarrollado en 1996 por *Visa, Master Card* y empresas como *IBM, Microsoft, Netscape, RSA, Verisign,* entre otras para:

- Proteger el sistema de tarjetas de crédito utilizadas en *Internet*.
- Generar en la mente del consumidor una opinión de confianza respecto al nuevo concepto de Internet como mercado.
- Descubrir y aplicar nuevas transacciones financieras seguras para este nuevo canal.

La especificación *SET* está dividida en 3 libros [SETCO, 1999]:

- La descripción del negocio, que da una vista general del proceso.
- La guía del programador, que describe los mensajes, campos y el apropiado perfil del procesamiento.
- La definición formal del protocolo que proporciona la más rigurosa descripción de los mensajes y campos de *SET*.

Si se encuentra alguna discrepancia entre la definición formal del protocolo y los otros libros, la definición formal del protocolo debe ser seguida.

La implantación del protocolo *SET* aporta una serie de beneficios de carácter inmediato:

- Autentifica los titulares de las tarjetas de crédito, los comerciantes y los bancos que intervienen en las operaciones comerciales por *Internet*.
- Garantiza la máxima confidencialidad de la información del pago.
- Asegura que los mensajes financieros no serán manipulados dentro del circuito del proceso del pago.
- Proporciona interoperabilidad entre distintas plataformas de hardware y software.

Evitando con esto:

- El pago de compras con tarjetas de crédito no autorizadas.
- El robo de información financiera del comprador.

Las instituciones financieras tales como: *American Express Company, JCB Company Limited, MasterCard International, Nippon Shinpan Company Limited, PBS International A/S/Dankort* y *Visa International*, emiten certificados *SET* para vendedores y para posee-

dores de tarjetas de crédito [SETCO, 1999].

VIII. LOS CERTIFICADOS DIGITALES Y LAS AUTORIDADES CERTIFICADORAS

Los **certificados digitales** son una clase de archivos electrónicos que actúan como un tipo de pasaporte en línea. Son proporcionados por una autoridad certificadora confiable, la cual verifica la identidad del poseedor del certificado. [Netscape, 1999]

Los certificados digitales hacen dos cosas:

- Autentifican que el poseedor (personas, sitios web e incluso recursos de la red) es verdaderamente quien dice ser.
- Protegen los datos intercambiados en línea de robos y alteraciones.

Las **autoridades certificadoras** son los equivalentes digitales de las oficinas de pasaportes. Emiten certificados y validan la identidad y autoridad de los poseedores. [Netscape, 1999]

Una empresa que quiere comenzar a vender en *Internet* necesita, entre otras cosas, instalar y configurar un servidor seguro. Como consecuencia de este proceso, la empresa obtendrá su par exclusivo de claves (pública y privada), que empleará para cifrar sus comunicaciones seguras.

Una vez generadas sus claves, el servidor necesita ser certificado como servidor seguro, es decir, se requiere que una tercera parte fiable verifique la implementación que ese servidor concreto hace del protocolo de seguridad, y avale digitalmente la autenticidad de la relación entre ese servidor seguro (con sus claves) y la empresa que lo posee. Las terceras partes encargadas de otorgar certificados digitales se conocen como autoridades de certificación. Una de las más aceptadas a nivel mundial es *Verisign*.

También los clientes necesitan certificados para intercambiar información cifrada y autentificada con los servidores seguros. Los navegadores de Internet traen incorporadas de serie las llaves públicas raíz (o certificados) de las principales autoridades certificadoras. De esta forma, cuando un usuario visita un servidor seguro acreditado por *Verisign*, el navegador puede iniciar con él un intercambio cifrado, pues dispone de las claves necesarias y reconoce a *Verisign* como una autoridad de certificación válida.

No obstante, los navegadores proporcionan al usuario control absoluto para decidir qué certificados considera fiables y cuáles no; es decir, para retirar alguno de los existentes, actualizarlo o añadir alguno nuevo.

Además de incorporar claves públicas de autoridades de certificación, se puede solicitar e incorporar al navegador, certificados de cliente (o usuario), de mayor o menor nivel, para que se acredite al usuario ante determinados servidores que requieren su identificación, algo que será imperativo si se implanta *SET*. *Verisign* permite obtener uno de estos certificados, de mayor o menor nivel (estos últimos suelen ser además gratuitos).

Los certificados digitales tienen fecha de caducidad, por lo que si se utiliza una versión antigua de un programa navegador, es probable que los certificados que incorpore estén ya caducados. En este caso, se deben incorporar nuevos certificados o actualizar el navegador completo.

IX. CONCLUSIONES

El comercio electrónico es tecnología para el cambio. Las empresas que lo miren como un "añadido" a su forma habitual de hacer negocios, obtendrán 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.

En la medida que el sistema comercial electrónico se robustezca será más seguro este mundo virtual, se reducirán los tiempos de entrega, los canales de distribución serán más eficaces, se ampliará la capacidad de satisfacer los pedidos con precisión y el proceso de producción será más eficiente al abrir cauces a la automati-zación de los procesos; todo esto fundado en la eficiencia tecnológica.

Mucha gente se muestra escéptica a la proliferación del comercio electrónico en México, esto debido a los efectos que causan las devaluaciones en las tasas de interés. Esto se refiere a que si el contar con una tarjeta de crédito convencional para comprar en *Internet* es cada vez más difícil, se va a restringir el poder de compra a un sector más reducido. Sin embargo, podemos ver las estrategias que empresas similares han adoptado ante este problema como son pago con depósito en cuenta, pago al entregar, o entrega y pago en bodega. Lo anterior tiene sus inconvenientes pero son soluciones sólo temporales para la entrada de mejores opciones de pago.

Hacer un comercio electrónico seguro se dará en la medida que las propias empresas y personas que lo administran evolucionen sus propios procesos y modifiquen esa cultura del papel en la que está basada nuestra cultura, más que propiamente por la inseguridad de las transacciones comerciales.

En este momento especialistas y organismos como el Comité EDI México, el Banco de México, la AMECE, la UNCITRAL, entre otros, están trabajando en todos los temas para resolver problemas jurídicos y validar las tecnologías más adecuadas que permitirán el desarrollo de un comercio electrónico seguro en nuestro país.

Por lo anterior, se puede comentar que los esfuerzos a todos los niveles nacionales e internacionales por lograr salvar problemas de seguridad y estandarización de procesos, deberán aunarse a cambios de actitudes y cultura hacia esta nueva forma de hacer negocios, ya que la tecnología por sí sola, no es suficiente .

X. BIBLIOGRAFÍA

[Abbott, 1999] Abbott Shawn. The debate for secure e-commerce. Performance Computing. Febrero de 1999. Vol 17. No.2 USA

[Andersen Consulting, 1998] Andersen Consulting. Antonio Mena, socio responsable de ecommerce. El reto del comercio electrónico: Europa en la encrucijada. http://www.marketingycomercio/numero6/6comercioel.htm

[Benítez, 1997] Benítez Campoy. Comercio Electrónico en Internet: el futuro ya está aquí. http://www.kriptopolis.com

[Campero, 1999] Campero Daniel. Intercambio Electrónico de Datos. Boletín 18. Junio 1999.

[Forester, 1999] Forester. Revista Fortune. Febrero de 1999. USA

[Howard, 1997] Howard John D. Un análisis de incidentes de seguridad en Internet 1988 –1995. Pittsburgh, Pennsylvania Abril 7, 1997. CERT®.

[Maña, 1999] José A. Mañas. Secure Electronic Transactions

[Netscape, 1999] Sitio Netscape http://home.netscape.com/security/
Sección sobre seguridad en Internet. Referente a generalidades sobre el protocolo SSL y su funcionamiento.

[RSA, 1999] RSA Data Security. http://www.rsa.com/
Sitio de la empresa RSA que se dedica a la construcción, diseño de soluciones de seguridad para las tecnologías de información, telecomunicaciones, servicios financieros e industrias del entretenimiento. Contiene información sobre los productos de la empresa, los estándares, infamación sobre los protocolos de seguridad entre otros.

[Salido, 1999] Javier Salido. ¿Es seguro el comercio por Internet.
http://cvirtual.racsa.co.cr/seguridad.html
Un artículo que compara una transacción normal contra una transacción electrónica presentando los problemas de ambas. Incluye una sección que habla sobre certificados de identidad

[Saltó, 1999] Saltó Antonio. Aspectos de Comercio Electrónico. Boletín 17. Mayo 1999.

[Serrano, 1999] Serrano Manuel. ¿Cómo serán las tiendas del futuro?. Boletín 20, Agosto 1999, Revista Código 84, AECOC, España.

[SETCO, 1999] SET home http://www.setco.org/
Contiene información referente al protocolo SET como certificados SET, instituciones bancarias que trabajan bajo este esquema de seguridad, publicaciones, soporte técnico, etc.

[Verisign ,1999] Verisign Inc. http://www.verisign.com/
Sitio de la empresa Verisign, principal proveedor de certificados digitales en el mundo.