UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POSTGRADO

LA SEGURIDAD EN EL COMERCIO ELECTRONICO COMO SOLUCION A UNA NUEVA FORMA DE LLEVAR ACABO TRANSACCIONES COMERCIALES

POR

ING. FRANCISCO CABRERA TAQUE

T E S I S

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA ADMINISTRACION CON ESPECIALIDAD EN RELACIONES INDUSTRIALES

CD. UNIVERSITARIA ENERO DEL 2002

LA SEGURIDAD EN EL COMERCIO ELECTRONICO COMO SOLUCION A UNA NUEVA FORMA DE LLEVAR ACABO TRANSACCIONES COMERCIALES

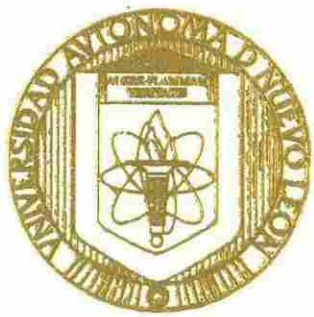
F. C. T.

2002

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POSTGRADO



LA SEGURIDAD EN EL COMERCIO ELECTRONICO COMO SOLUCION A UNA NUEVA FORMA DE LLEVAR ACABO TRANSACCIONES COMERCIALES

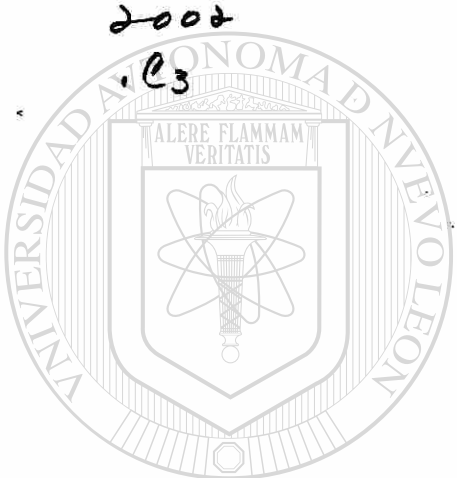
POR

ING. FRANCISCO CABRERA TAQUE

T E S I S

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA ADMINISTRACION CON ESPECIALIDAD EN RELACIONES INDUSTRIALES

CD. UNIVERSITARIA ENERO DEL 2002



UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECAINCA Y ELECTRICA

DIVISION DE ESTUDIOS DE POSGRADO

LA SEGURIDAD EN EL COMERCIO ELECTRONICO COMO SOLUCION A UNA NUEVA FORMA DE LLEVAR ACABO TRANSACCIONES COMERCIALES

POR

ING. FRANCISCO CABRERA TAQUE

TESIS

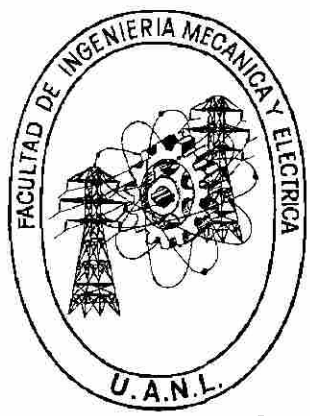
EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA ADMINISTRACION CON ESPECIALIDAD EN RELACIONES INDUSTRIALES

CD. UNIVERSITARIA, A ENERO DEL 2002

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECAINCA Y ELECTRICA

DIVISION DE ESTUDIOS DE POSGRADO



LA SEGURIDAD EN EL COMERCIO ELECTRONICO COMO SOLUCION A UNA NUEVA FORMA DE LLEVAR ACABO TRANSACCIONES COMERCIALES

POR

ING. FRANCISCO CABRERA TAQUE

TESIS

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA ADMINISTRACION CON ESPECIALIDAD EN RELACIONES INDUSTRIALES

CD. UNIVERSITARIA, A ENERO DEL 2002

UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE INGENIERIA MECANICA Y ELECTRICA
DIVISION DE ESTUDIOS DE POSGRADO

Los miembros del comité de tesis recomendamos que la tesis **"La seguridad en el comercio electrónico como solución a una nueva forma de llevar acabo transacciones comerciales",** realizada por el alumno **Ing. Francisco Cabrera Taque**, matricula 0814540 sea aceptada para su defensa como opción al Grado de Maestro en Ciencias de la Administración con Especialidad en Relaciones Industriales.

El comité de Tesis

Asesor
M.C. Roberto Villarreal Garza

Coasesor
M.C. Carlos B. Garza Treviño

Coasesor
Dr. Victoriano F. Alatorre González

Vo. Bo.
M.C. Roberto Villarreal Garza
División de Estudios de Postgrado

San Nicolás de Los Garza, N.L. Diciembre del 2001.

Todo y Nada

Le pedí fuerzas a Dios para poder llegar más lejos, y me hizo débil para que aprendiera humildemente la obediencia...

Le pedí salud para poder hacer grandes cosas, y me hizo frágil para que hiciera cosas mejores...

Le pedí riquezas para poder ser feliz, y me dio la pobreza para que pudiera ser sabio...

Le pedí poder para ser admirado por los hombres, y me dio la debilidad, para que pudiera sentir la necesidad de Dios...

Le pedí todas las cosas para gozar de la vida, y me fue dada la vida para disfrutar de todas las cosas...

No tengo nada de lo que pedí, pero sí todo lo que esperaba. Casi a pesar de mí mismo, mis silenciosas plegarias fueron escuchadas.

Simplemente... Gracias.

Dicen que a veces la palabras no bastan para realmente expresar lo que uno siente, por lo general, hay veces que uno quisiera decir muchas cosas y no encuentra uno la manera de cómo decirlas, y también cuando uno intenta acordarse de todos y cada uno de las personas que lo apoyaron a uno en las buenas y en las malas, los nombres nos faltan, y no es por que uno no se acuerde, sino que tal vez son tantas las personas que de una manera u otra siempre lo han alentado a uno a seguir adelante y no quedarse en el camino; entonces uno si las enumera nunca acabaría y muy probablemente dejaría al alguien omitido por error, por eso mejor tratando de evitar este detalle y no queriendo ofender a nadie, no voy a escribir los nombres de ustedes, simplemente voy a realizar un agradecimiento general a todos y cada una de las personas que a través de los años me han enseñado algo, algunas de ellas sin siquiera saberlo, por que, de alguna manera u otra todos tenemos algo que enseñarles a los demás.

Les deseo a todos lo mejor del mundo, desde muy dentro de mi persona a todos y cada uno de ustedes, les deseo lo mejor y que siempre sigamos tratando de ser mejores en lo que hacemos, y sin importar las cosas materiales y vanas de esta vida, esperemos que si en esta vida no lo lográramos que en la otra vida, las cosas serán mejores para todos y cada uno de nosotros.

Atentamente

Ing. Francisco Cabrera Taque.

Prologo

El desarrollo de la presente Tesis "La seguridad en el comercio electrónico como una solución a una nueva forma de llevar acabo transacciones comerciales" es para tratar de dar solución a una problemática de suma actualidad, en el cual se pretende dar un antecedente de solución para futuras generaciones que deseen tomar como modelo a seguir a seguir esta Tesis.

Se tomaron en consideración todas las normativas y reglamentos que existen actualmente en el mundo. Se tiene que considerar que la información que se maneja en esta tesis pudiera variar con respecto a la fecha en que se tome como referencia, dado que en este medio las normas y reglamentos varían con el tiempo, tratando de ser mas acorde a los tiempos que se estén viviendo.

Este proyecto es algo que me ha gustado desarrollar dado que para mi persona es fácil hablar de este tema, dado que diariamente en el desarrollo de mi vida cotidiana estoy involucrado en este tipo de procesos.

Tratando de siempre tomar de referencia lo que es de uso práctico y del bien común.

Ing. Francisco Cabrera Taque

Capítulo Pagina

Síntesis

Ante un nuevo milenio y a las fuertes presiones mundiales para lograr la globalización, el avance de la tecnología se presenta con un esquema integrado a los negocios conocido como comercio electrónico. Existe poca información sobre comercio electrónico debido a que el modelo se encuentra aún en gestación y en un periodo de evaluación. Las empresas que han apostado por este cambio se encuentran en el dilema de ver hacia atrás para analizar su situación actual y reconsiderar la estrategia para abordar esta nueva forma de hacer negocios.

Durante el presente trabajo se incluye una revisión del estado del arte de la actividad de comercio electrónico en el ciberespacio y sobre la seguridad al realizar transacciones electrónicas en Internet. El presente trabajo pretende presentar una base teórica sobre el comercio digital que permita tomar la decisión de ingresar a esta nueva forma de realizar negocios.

Cualquier proyecto de comercio electrónico debe partir de la definición de una estrategia de comercio digital que considere los cambios y requerimientos de negocio en los rubros de procesos, recursos humanos, aspectos legales, proceso de digitalización, aspectos económicos y culturales. La estrategia debe contener los objetivos, alcances, beneficios y oportunidades de la empresa en caso de incursionar en el comercio electrónico.

Adicional a lo anterior se debe realizar un análisis de riesgos que permita establecer los planes de prevención de riesgos, así como los planes de

contingencia que permitan mitigar el impacto en caso de ocurrencia de algún riesgo. De igual forma el proceso de selección de tecnologías como infraestructura de comunicaciones hardware y software requiere de un proceso de análisis de las tecnologías existentes, de su robustez y tendencias del mercado para determinar la tecnología adecuada a los procesos de negocio que sufrirán una conversión al nuevo modelo de negocios electrónicos.

En el proceso de selección de tecnologías es necesario realizar un estudio por separado de la seguridad del nuevo sistema para determinar las técnicas de criptografía, algoritmos y protocolos de comercio electrónico, ya que existen algoritmos que han sido descifrados o se han detectando vulnerabilidades. Para el caso de protocolos, adicional al análisis de seguridad de cada uno de ellos, es necesario identificar la aplicación que será realizada debido a que el protocolo SET se utiliza para realizar pagos electrónicos de forma segura y el protocolo SSL permite establecer conexiones seguras cliente-servidor para aplicaciones preferentemente del tipo negocio a persona.

La seguridad total de un sistema de comercio electrónico permitiría asegurar con toda certeza la eliminación de los riesgos y amenazas a los que se encuentra expuesto un sistema computacional. Existen dos grupos de amenazas que incluyen: las propias de un sistema distribuido conectado mediante una red; y los inherentes al comercio digital como son la privacidad, integridad y verificación de la identidad de la información. Es por lo anterior que, en ningún momento se pretende garantizar la seguridad total al incorporarse al comercio digital, más bien dar la idea de que el comercio electrónico es seguro si se utilizan las técnicas, mecanismos, algoritmos y protocolos adecuados.

Es importante establecer que la intención del presente trabajo es establecer una guía de referencia para realizar un proyecto de comercio electrónico.

CAPITULO 1

1 Introducción

1.1 Descripción del Problema

El problema al que me refiero, esta identificado en el Departamento de Mercadotecnia y Ventas el cual solicito a el área de Sistemas de la empresa en la cual yo presto mi servicio como asesor externo una solución confiable y segura para la misma, el nombre de esta empresa es DIRONA S.A. la cual a su vez es una compañía que forma parte del Grupo QUIMMCO.

DIRONA S.A. se encuentra situada al norte de la ciudad de Monterrey N.L., esta es un empresa del la rama metal mecánica y teniendo como sus principales líneas de producción la fabricación de ejes automotrices, entre algunos otros productos que maneja esta compañía se encuentran la producción de ejes del tipo Tandem, ejes motrices, ejes direccionales y frenos, los cuales son utilizados en la industria automotriz pesada, como son tractocamiones, camiones comerciales de carga y autobuses.

El problema se presento con la apertura del Comercio en México a través del Tratado de Libre Comercio y la necesidad actual de la empresa de Globalizar su mercado y aumentar su cartera de clientes a nivel nacional e internacional, además que en todo momento que se presentara alguna posible eventualidad

en alguna transacción comercial esta estuviera cubierta, por lo que se vio en la necesidad de desarrollar una forma de comercio, el cual pudiera llegar a cualquier punto ó rincón del planeta y el cual a su vez estuviera presente las 24 horas del día, los 365 días del año, y a su vez asegurarle con toda certeza al cliente que contara con la seguridad y atención que este tipo de negocio requiere, dado que siendo una transacción comercial de suma importancia deberá ser segura en todo momento, con lo cual se cubriría cualquier posible necesidad de algún cliente potencial.

1.2 Objetivo de la Tesis

El objetivo primordial de esta tesis es poder demostrar de una manera clara y contundente, que a través de un método científico como lo es la Administración de los Recursos Humanos y Tecnológicos, nuestra empresa tendrá de una manera constante y permanente un contacto mas directo con cualquier posible cliente, no solamente nacional sino también a su vez internacionalmente, con lo que se podrá se llegar a otros mercados que antes no se tenían contemplados, teniendo la confianza y respaldo de nuestros clientes que todas sus transacciones comerciales estarán seguras y siempre tendrá una respuesta inmediata a toda auditoria tanto del cliente como de la empresa.

1.3 Hipótesis

Con unas perfecta planeación y llevando un estudio adecuado de las necesidades que se pretenden cubrir de la empresa se llevara acabo el desarrollo e implementación de un Site de comercio electrónico para la empresa, con lo que se le dará un seguimiento mas adecuado a las necesidades del cliente el cual se estima tener a punto en un periodo de 6 meses, contado en todo momento con la supervisión y seguimiento adecuado por parte de la empresa.

1.4 Limites del Estudio

Esta investigación esta dirigida específicamente a la empresa DIRONA S.A. en las áreas de Mercadotecnia, Ventas y Sistemas por lo que contando con la colaboración del personal que labora en estos departamentos se lograra una perfecta integración del mismo.

Tanto el estudio, como el análisis de cada una de las diversas soluciones que se llevaran acabo para la correcta implementación del programa, serán en su medida una correcta inversión para que nuevas tecnologías sean puestas en operación. Teniendo en cuenta el corto tiempo en que se pretende poner en operaciones esta forma de negocios, nos enfocaremos en gran medida a plantear las mejores y más valiosas herramientas para una correcta operación.

1.5 Justificación del Trabajo

Estoy plenamente convencido que con la creación de este tipo de solución que se plantea se dará una muy variada y completa estrategia de negocios con lo cual se cubrirán todas y cada una de las posibles necesidades que pudieran surgir a nuestros clientes.

Además teniendo como antecedente que otras empresas muy importantes como son IBM, Suns, Banamex, Banorte, Cemex, entre otras de muy diversos giros comerciales han desarrollado una estrategia parecida, y han obtenido resultados favorables, se opta por este proyecto. Tomando en cuenta también que con esta investigación se pretende dejar un antecedente para cualquier otra empresa que quiera desarrollar un tipo de estrategia parecida busque la mejor solución a sus requerimientos.

1.6 Metodología

1.- llevare acabo una recolección de toda la información que se tiene del problema a través de entrevistas a cada uno de los departamentos involucrados y además entrevistando a los clientes.

2.- Realizare un estudio y aplicación de cada una de las leyes y normas que se tienen para el comercio electrónico, incluyendo los reglamentos, manuales y anexos que existen para este tipo de negocio. Con lo que en aspecto legal tratare de cubrir esta área.

3.- Realizando un adecuado estudio de cada una de las necesidades a cubrir en lo que se refiere a normativas, políticas y reglamentos internos de la empresa, para que en este aspecto la empresa quede en todo momento complacida con la información y seguimiento de cada uno de los objetivos de la misma.

4.- Llevare un control de cada una de las aplicaciones propuestas y evaluación de las mismas, para que en gran medida cada una de las estrategias sugeridas, tanto en aspecto informativo, manejo y seguridad de la misma sean correctamente utilizadas.

5.- Propondré el Estableciendo un programa de seguimiento y evaluación que permita en gran medida comprobar los resultados que se pretenden obtener con este estudio en el plazo señalado.

1.7 Revisión Bibliografica

La cantidad de libros utilizados de apoyo en la realización de la presente obra, y de los cuales se hace mención al final de esta obra en el capitulo correspondiente a la bibliografía, se pueden dividir en 4 grandes grupos: el

CAPITULO 2

2 Introducción al Comercio Electrónico

2.1 Origen del Comercio Electrónico

El origen del comercio electrónico se dio en los años 70's con la introducción de las transferencias electrónicas de fondos (Electronic Funds Transfer – EFT) entre los bancos para el mejor aprovechamiento de los recursos computaciones existentes en la época. Mediante redes privadas y seguras se optimizaron los pagos electrónicos. Se incluyeron servicios como puntos de venta (Points Of Sales – POS) en tiendas y almacenes para pagos con tarjetas de débito y pagos de la nómina a los empleados de las empresas utilizando cheques en sustitución de efectivo. [Kalakota 97]

El primer EFTPOS en línea y comercial fue utilizado en Francia en 1983. Con la introducción de computadoras personales económicas y técnicas de conmutación de paquetes se enlazaron terminales inteligentes a los sistemas computacionales de los bancos por primera vez.

La banca electrónica inició en los Estados Unidos debido a que los arreglos de compensación entre los bancos, los cuales eran numerosos y dispersos geográficamente, eran de extrema ineficiencia. Los usuarios corporativos empezaron a presionar para obtener mejoras. Los sistemas de compensación

basados en papel, dentro del Reino Unido, eran relativamente eficientes lo que significaba que la presión para el cambio por parte de los clientes corporativos era mucho menor que en los Estados Unidos. La centralización de la compensación en papel de la transferencia de crédito se inicio en 1960 en el Reino Unido. En diciembre de 1971 se abrió a los negocios el Banker's Automated Clearing System (BACS).

Los primeros cajeros automáticos (ATM - Automatic Teller Machine) fueron introducidos al público en el Reino Unido en 1969. Para 1985 existían 160,000 en bancos de todo el mundo. [Welch 99]

Para 1973 se desarrolló el sistema de pagos internacional coordinado por la Society for Worldwide Interbank Funds Transfer (SWIFT, www.swift.com). En 1977 se iniciaron las operaciones para pagos internacionales cuando tenían 239 bancos participantes en 15 países.

Durante finales de los 70's y principios de los 80's el comercio electrónico se dio entre empresas mediante tecnologías de mensajes electrónicos como el intercambio electrónico de datos (Electronic Data Interchange – EDI) [Botts 96], [Clarke 98], [Eniac 98] y el correo electrónico. Estas tecnologías de mensajes electrónicos impulsaron las mejoras en los procesos de negocios al reducir el intercambio de papeles e incrementar la automatización de las oficinas. Los negocios intercambian tradicionalmente a través de papel, por ejemplo cheques, ordenes de compra y documentos de embarque.

La estandarización que proponía el EDI permitió a las compañías enviar y recibir documentos de negocios entre los distintos proveedores en una forma electrónica. Pero el principal problema para la adopción del EDI es el alto costo de implantación, operación y mantenimiento de los equipos de cómputo y comunicaciones, ya que se requiere utilizar redes privadas como las VPN (Virtual Private Network) y equipo especializado para el procesamiento de la

información. Con lo cual los pequeños proveedores quedaban fuera del comercio con las grandes empresas que utilizaban el EDI. [Pulido 99]

A mediados de los 80's una nueva forma de tecnología de comercio electrónico se introdujo como una nueva forma de servicios en línea. Este intercambio de información incluyó la utilización de nuevas formas de interacción social como son los Chat rooms o el IRC (inter-relay chat), así como el intercambio de conocimiento mediante los grupos de noticias (newsgroups) y los programas de transferencias de archivos (File Transfer Protocol – FTP).

Esta interacción social formó un sentimiento de comunidad virtual conocida como ciberespacio o Social WEB. [Social_web 00] Durante los 80's y 90's el cambio fue hacia las transferencias electrónicas y el uso de tarjetas de débito como Visa Electrón y Switch.

A finales de los 80's y principios de los 90's el comercio electrónico se dio con las tecnologías de intercambio de mensajes electrónicos y formaron parte integral de los sistemas de flujo de trabajo (workflow) y de trabajo colaborativo (groupware) [CSCW 00] teniendo como el ejemplo más común el Lotus Notes [LOTUS_NOTES 00]. El groupware se enfocó principalmente en convertir los métodos existentes no electrónicos en una plataforma electrónica para mejorar los procesos de negocio.

En la segunda parte de los 90's, el advenimiento del World Wide Web (WWW) en el Internet, representó un cambio dramático en el comercio electrónico al proveer una solución tecnológica de fácil uso al problema de la publicación, administración y diseminación de la información y el conocimiento. El WWW permitió a los pequeños negocios competir en equidad tecnológica para realizar negocios de forma económica (economías de escala) con empresas multinacionales, las cuales poseen un gran capital económico. [ISPO_CEC 99], [CORNELLA 99]

Y es aquí donde el comercio digital tiene la gran oportunidad de posicionarse como un elemento estratégico para las organizaciones de hoy, permitiendo integrar los procesos de la propia empresa, entre las diversas empresas, e incluso llegando a los usuarios finales; con esto el comercio electrónico logra poner en práctica el concepto de globalización. [Machover 97]

2.2 Definición de Comercio Electrónico

Algunas actividades realizadas en un entorno de negocios son el establecimiento de comunicación electrónica con los clientes, proveedores, distribuidores, grupos de la industria e inclusive con los competidores.

Estas actividades tienen el objetivo de incrementar la eficiencia de la comunicación de negocios, expandir los mercados y mantener la viabilidad de largo plazo del negocio. [Kalakota 96]

Comúnmente el Comercio Electrónico es asociado con la compra y venta de información, productos o servicios a través de las redes de computadoras.

Pero el CE debe de ser asociado a los procesos de negocio de una organización mediante una re-ingeniería de procesos con el objetivo de reducir costos, obtener tiempos menores del ciclo de productos, respuestas más rápidas de los clientes y el mejoramiento de la calidad de servicio.

Así la utilización de los esfuerzos de re-ingeniería basados en las tecnologías de intercambio de mensajes electrónicos permiten reducir el uso de papel e incrementar la automatización, siendo estos últimos elementos clave para el cambio hacia el comercio electrónico. [Kalakota 96], [ISPO_CEC 99], [Riggins 98].

Dependiendo de las diversas perspectivas tenemos las siguientes definiciones:

- **Comunicaciones**: el CE es la entrega de información, productos o servicios, o pagos a través de líneas telefónicas, redes de computadoras o cualquier otro medio electrónico.
- **Procesos de negocios**: el CE es la aplicación de la tecnología hacia la automatización de transacciones de negocio y flujos de trabajo.
- **Servicio**: el CE es una herramienta que permite obtener el deseo de las organizaciones, clientes y administración de reducir los costos de servicio mientras se mejora la calidad de los bienes y se incrementa la velocidad de la entrega de servicios.
- **En línea**: el CE permite comprar y vender productos e información en Internet y otros servicios en línea.

Según [Kalakota 97] el comercio electrónico puede definirse como una "metodología moderna de negocios que permite a las organizaciones, comerciantes y clientes reducir costos mientras se mejora la calidad de los productos y servicios, así como incrementar la velocidad de entrega".

Con los antecedentes mencionados podemos determinar que el CE no es únicamente una simple tecnología o herramienta sino que es una combinación de tecnologías, aplicaciones, procesos y estrategias de negocios. [Keen 97]

Por lo anterior, la definición propia del autor utilizada en el presente trabajo de tesis es:

> "El comercio electrónico es una nueva forma de realizar negocios de forma electrónica para intercambiar información, bienes, servicios y capital mediante las tecnologías emergentes que lo hacen posible".

Los términos de comercio electrónico y comercio digital se utilizan de forma indistinta en el presente trabajo de tesis para denominar a los mismos conceptos.

2.3 Categorías de Comercio Electrónico

Según [Applegate 96] se pueden identificar tres clases de aplicaciones de comercio electrónico que son: el comercio electrónico negocio a consumidor (B2C - Business to Consumer), negocio a negocio (B2B - Business to Business) e intraorganizacional (B - Business).

Esta clasificación depende de los participantes y las actividades que realizan entre ellos para realizar un negocio de forma electrónica.

2.3.1 Comercio Electrónico Negocio a Consumidor (B2C)

Esta es el área del comercio electrónico donde se ha visto la mayor actividad en las últimas décadas, la cual va desde el uso de cajeros automáticos hasta las compras electrónicas a través de Internet. [Keen 97]

Se le denomina comercio electrónico negocio a consumidor cuando una empresa realiza las funciones de mercadeo, promoción, publicación de información y catálogos de productos o servicios y pago con tarjeta de crédito o débito.

El sistema está dirigido al usuario final o consumidor y el procedimiento normalmente se realiza mediante la navegación de páginas en Internet con algún programa que permita el intercambio de información de forma segura.

Desde la perspectiva del consumidor [Kalakota 97], el comercio electrónico facilita las siguientes transacciones:

- Interacción social mediante la comunicación desde o hacia los consumidores a través del correo electrónico, la videoconferencia y los grupos de noticias.
- Administración de las finanzas personales mediante aplicaciones electrónicas para administrar las inversiones, cuentas personales y el uso de herramientas de banca en su casa.
- Compra de productos, servicios o información permitiendo al consumidor encontrar información en línea de productos o servicios existentes o nuevos para realizar la compra en línea.

Esta forma de realizar comercio electrónico permite a una persona realizar transacciones electrónicas seguras con una empresa. Sitios como http://www.amazon.com han tenido un gran éxito al colocar un inmenso catálogo de libros y permitiendo a los visitantes realizar compras en línea de forma rápida y segura. De igual forma, www.cdnow.com, www.ebay.com, www.yahoo.com, www.mypoints.com, entre otros, han aprovechado las oportunidades de Internet como un nuevo canal de venta y distribución de productos y servicios.

Para una transacción de comercio electrónico entre una persona y una empresa es necesario verificar la identidad de las partes involucradas, garantizar la privacía e integridad de la información, es por ello que se utilizan mecanismos para codificar la información enviada por un usuario y evitar así riesgos y posibles ataques a la información. Normalmente se utilizan páginas codificadas con protocolos como el Socket Secure Layer (SSL) y el Secure Electronic Transaction (SET), los cuales se explican en capítulos posteriores.

Debido a las implicaciones anteriores, la seguridad es una de las principales preocupaciones de los usuarios del comercio electrónico persona a negocio, la confianza es un elemento tan importante que puede determinar el futuro y éxito

de la empresa. En algunos países, como México, aún no se encuentra arraigada la confianza para el uso de los sistemas de comercio digital.

2.3.2 Comercio Electrónico Negocio a Negocio (B2B)

El comercio digital negocio a negocio permite a dos empresas realizar transacciones seguras, las cuales intercambian información directamente de sus sistemas computacionales.

Anteriormente el intercambio de información se realizaba mediante el uso de redes privadas, pero en la actualidad esto es logrado mediante el uso de las Extranets, las cuales permiten ligar las estrategias de intranets e Internet en el nuevo concepto de comercio electrónico. Así las órdenes de compra o pedidos, formatos de entrega, facturación y cobranza pueden ser enlazados para optimizar tiempos y costos.

Adicionalmente esta nueva forma de trabajar permitirá integrar las cadenas de valor de ambas empresas. La administración de la relación con los clientes (CRM – Customer Relation Management) permite un acercamiento con el cliente generando una mejor atención al cliente, mejora en tiempos de respuesta de soporte tanto en el esquema de B2B como de B2C. Por otro lado las cadenas de suministros (Supply Chain) serán utilizadas como estrategias de valor agregado, reducción de tiempos que permitirán una ventaja competitiva.

Se espera que en los próximos años esta forma de comercio electrónico (B2B) sea el que domine el mercado y se estima que será aproximadamente el 80% de las transacciones electrónicas que se realicen como se verá mas adelante en el comparativo entre B2C y B2B.

Desde la perspectiva de las organizaciones el comercio digital negocio a negocio facilita las siguientes actividades del negocio:

- Administración de los suministros para reducir los tiempos y costos de procesamientos de compras.
- Administración del inventario para reducir los tiempos de orden, embarque y distribución. De igual forma se reducen y optimizan los niveles del inventario en sus máximos y mínimos adecuados.
- Administración de la distribución para facilitar el envío de documentación de embarque como son notas de carga, ordenes de compra y manifiestos de reclamo entre otros, permitiendo una mayor precisión en la información presentada.
- Administración de los canales de distribución para diseminar la información de forma rápida y segura acerca de especificaciones técnicas o de pago.
- Administración del pago para el envío o recepción de pagos electrónicos entre los proveedores o distribuidores incrementando la velocidad y reducción de errores al realizar los pagos de facturas.

Esta integración de las cadenas de suministro entre empresas para optimizar los procesos, reducir los costos y tiempos de entrega, requiere de un alto grado de seguridad y control en las acciones que se requieren realizar. La seguridad es un aspecto sumamente importante en el establecimiento de las relaciones entre empresas, debido a ello, se realizan inversiones cuantiosas para garantizar la privacía e integridad de la información, además de verificar la identidad de las entidades involucradas en una transacción electrónica.

Al garantizar la seguridad de la información, los sistemas inter organizacionales cambiarán la forma en que las empresas conducen sus relaciones de negocios o como utilizan el Internet para ganar una ventaja competitiva. [Riggins 98]

2.3.3 Comercio Electrónico Dentro del Negocio (B)

Por último tenemos al comercio electrónico dentro del negocio el cual permite visualizar a la empresa como pequeñas unidades de negocio o entidades trabajando bajo el concepto de comercio electrónico. El procesamiento de información y envío de mensajes debe ser realizado como transacciones electrónicas seguras realizadas día a día en una empresa. Esta forma de operar puede cambiar incluso la visión y misión que dieron origen a la empresa para dar como resultado un cambio radical de operación y estrategia. Desde la perspectiva de una empresa las facilidades para el comercio electrónico dentro del negocio son las siguientes:

- Comunicación en grupo que permite la comunicación rápida y eficiente entre los integrantes de la empresa mediante la utilización del correo electrónico, la videoconferencia, y los tableros de mensajes. El objetivo es la diseminación de la información para obtener mejores resultados con empleados más informados.
- Publicación electrónica para organizar, publicar, diseminar y transferir el conocimiento dentro de la organización como son: los manuales, especificaciones de productos, etc. Mejorando la toma de decisiones estratégicas, tácticas y operativas.
- Productividad de la fuerza de venta para mejorar el flujo de información entre el área de producción y de ventas y/o entre la organización y los clientes.

En una empresa que se encuentra en un proceso de optimización y mejora continua, la incorporación del comercio electrónico tiene un significado particular de resistencia al cambio debido a la automatización de los procedimientos de operación, es por ello que los mecanismos de seguridad sobre la confidencialidad e integración de la información electrónica deben ser

parte del proceso de incursión al mundo digital, evitando así riesgos de pérdida de información por ataques de los propios empleados de la empresa.

Existen riesgos e implicaciones adicionales, los cuales se explican a mayor detalle en el capítulo de análisis del riesgo.

2.4 Banca Electrónica

2.4.1 Introducción

Como se mencionó anteriormente, las aplicaciones bancarias fueron las primeras en iniciar el uso de la revolución tecnológica que representa el comercio electrónico. En la actualidad son las instituciones financieras las que realizan grandes inversiones de recursos para mantenerse a la vanguardia y es por ello que se dedica una sección especial para mostrar la participación en las tres categorías del comercio digital. Como ejemplos tenemos: www.banamex.com, www.visa.com.mx, www.prosa.com.mx, entre otros.

La banca electrónica no es actualmente restrictiva para las corporaciones multinacionales con requerimientos extensos de intercambio de información. Ya que también, las pequeñas empresas obtienen ventajas considerables al utilizar los servicios de la banca electrónica. Los proveedores de servicios de banca electrónica respondieron a las necesidades de las pequeñas empresas y usuarios finales al extender una gran variedad de los productos disponibles a través de acceso electrónico. Esto fue impulsado por el uso efectivo de las tecnologías emergentes para la entrega de servicios, incluyendo el Internet. Estos desarrollos así como la llegada de la moneda única europea (EURO) ha traído nuevos retos y oportunidades para los proveedores de servicios de banca electrónica. [EURO 00]

La variedad de servicios bancarios que pueden ser entregados a la casa u oficina de un cliente por la tecnología electrónica se han expandido considerablemente desde los primeros pasos que se tomaron hace 25 años aproximadamente. Los bancos utilizan ahora la tecnología para transmitir información, instrucciones y transacciones necesarias para conducir negocios de forma electrónica. La calidad, variedad y precio de los servicios electrónicos son una parte importante del posicionamiento competitivo de un banco en su entendimiento del cliente corporativo.

El consumidor final aprovecha las ventajas que ofrecen sistemas como el Banco en su casa o "Home Banking", el cual permite entre otros servicios: revisar estados de cuenta, consulta de saldos y transferencia entre cuentas. De igual forma el uso de cajeros automáticos ha permitido a los millones de usuarios la disponibilidad en cualquier momento de sus recursos monetarios.

El comercio electrónico de empresa a empresa en un banco se realiza al permitir a dos organizaciones realizar transferencias de fondos o pagos programados ya sea entre cuentas del mismo banco o entre diferentes bancos. En algunos países, como México, donde aún no se realiza de forma transparente.

A continuación se muestra una tabla que describe algunos ejemplos de operaciones bancarias, así como las entidades participantes, tecnología utilizada y seguridad requerida:

Categoría	Actividades	Entidades Participantes	Tecnología Electrónica utilizada	Seguridad Requerida
B2C	• Un cliente deposita fondos en una cuenta bancaria • Un cliente retira efectivo de una cuenta bancaria • Un cliente consulta un saldo	Cliente Banco	ATM (Automatic Teller Machine) Páginas en Internet	Codificación de número de tarjetas y números confidenciales (Algoritmo DES) Uso de páginas Web seguras (SSL)
B2B, B	• Un cliente paga un tercero	Cliente que paga El banco que paga El banco que recibe El receptor Cámara de compensaciones	EFTPOS (Electronic Funds Transfer Point of Sale) SWITCH Sistemas de pago o transferencia de fondos entre bancos	Redes privadas como VPN y VAN´s

TABLA 2.1: Relación de Entidades Participantes y Actividades.

Los requerimientos de seguridad varían para el comercio electrónico negocio a negocio o negocio a consumidor. Mientras que los usuarios requieren una cantidad menor de seguridad debido al alto costo que representa descifrar una transacción de una suma pequeña; para los bancos que realizan para transacciones entre empresas o inclusive entre bancos, es necesario el uso de redes privadas de costo elevado para realizar transacciones de grandes montos de capital.

Existe una relación directa entre los recursos y el esfuerzo requerido para romper un esquema de seguridad y la posible ganancia por el uso o venta de la información. La efectividad de los sistemas electrónicos bancarios fue inhibida por los cuatro factores siguientes:

1. La tecnología de comunicación se encontraba en su infancia y era inadecuada para la cobertura local y global, los bancos y clientes no se podían comunicar internacionalmente entre sus mismas organizaciones o entre otras.

2. La mayoría de las compañías y bancos tenían sistemas incompatibles, inclusive de distintas marcas en un mismo banco.
3. Los fabricantes de computadoras no habían desarrollado estándares de tecnología que permitieran el intercambio de datos directamente entre los sistemas computacionales.
4. El hardware y software de computadora era costoso en comparación con los ahorros en la eficiencia debido a la automatización de la organización.
5. La seguridad y el costo asociado a ésta, han sido factores limitantes para avanzar en la definición de una estrategia a corto, mediano y largo plazo del comercio electrónico.

Actualmente estos problemas se han resuelto o minimizado y es por ello que las principales instituciones bancarias de todo el mundo se encuentran ofreciendo o en vías de ofrecer nuevos servicios y productos financieros en formato digital.

Según las estadísticas, el 50% de las transacciones bancarias se realizan a través de cajeros automáticos, banca por teléfono y banca basada en computadora. [McChesney 97]

Existen 3 modelos principales de banca electrónica que han emergido: Banco por PC o cliente pesado, el cliente ligero sin control de estados y el cliente ligero con control de estados.

El primer modelo se realiza mediante la instalación de programas como Quicken o Money de Microsoft en la PC de forma local, con las consecuencias de administración y actualización de versiores. Se le denomina cliente pesado debido al requerimiento de espacio en disco duro que necesita el usuario para instalar las aplicaciones.

El segundo enfoque se realiza a través de un navegador de Internet pero sin almacenamiento de información. Y consiste en visitar una página en Internet que permite realizar ciertas operaciones o funciones predeterminadas por las instituciones financieras.

Por último, el tercer modelo y nuevo paradigma para la banca por Internet, permite almacenar información en el cliente. Este concepto de aplicación permite, por ejemplo, utilizar una página en Internet y almacenar información en la computadora cliente de forma permanente y para su uso sin la necesidad de estar conectado a Internet. [McChesney 97]

A continuación se presenta una introducción al modelo de banca electrónica mediante el uso de Internet orientado al consumidor o usuario final de los diversos servicios bancarios.

2.4.2 Banca por Internet

Otra de las funciones de las instituciones financieras es proveer sistemas de pago electrónico. Actualmente se ofrecen servicios de pago mediante terminales o POS (Points of Sale), las cuales permiten procesar las órdenes de pago en el establecimiento designado previamente, mediante autorizaciones en línea.

Adicional a lo anterior, tenemos que los bancos han encontrado a Internet como un canal de entrega eficiente y alternativo para los servicios financieros. Con el Internet los bancos pueden asegurar el mantenimiento de su identidad como institución financiera y continuar el proceso de diferenciación entre los bancos, al ofrecer servicios personalizados e información financiera a través de sus propias páginas WWW.

El uso de la banca por Internet puede ser considerado en 3 tipos de actividades: promoción, información de productos, servicios y transacciones bancarias. [Yan 97]

En todos los casos, la fidelidad del cliente tiene una fuerte componente de confianza en el sistema de cómputo basado en la privacía e integridad de la información, verificación de la identidad de la institución y en la administración de la información.

Las condiciones anteriores no pueden ser garantizadas, debido a las características propias de Internet, que desde su diseño inicial no consideraron la seguridad como un componente esencial. Es por ello que es necesario introducir mecanismos de seguridad apropiados para permitir la transmisión de información de forma segura.

2.5 Conclusiones

El intercambio electrónico de bienes, servicios, información o capital entre diversas personas o empresas requiere considerar en primera instancia cambios de procesos, tecnología, estrategia y recursos humanos que permitan una incursión con el menor riesgo en el mundo del comercio electrónico. Los aspectos de seguridad en sistemas distribuidos y el comercio electrónico requiere de ciertos mecanismos, técnicas, algoritmos y protocolos que permitan minimizar el riesgo de un posible ataque o fraude.

La metodología utilizada para la investigación de los conceptos fue la recopilación de información publicada en artículos, revistas y libros, así como la navegación en Internet de los sitios que actualmente ofrecen comercio electrónico. Posteriormente se organizó este cúmulo de conocimientos para dar forma al documento que hoy tiene usted en sus manos. Este conocimiento fue

apoyado por ideas presentadas a lo largo del documento y en ningún momento presenta una propuesta o juicio sobre el comercio electrónico y su seguridad.

El contenido del texto incluye en los siguientes capítulos, una introducción al comercio electrónico, los cambios y requerimientos necesarios para el comercio electrónico, la situación actual en el mundo y en México, análisis de riesgo, problemas y aspectos críticos de la seguridad, mecanismos, técnicas, algoritmos y protocolos para el comercio electrónico, descripción del proyecto realizado que soporta los conocimientos presentados y las conclusiones del presente trabajo de tesis.

CAPITULO 3

3 Cambios y Requerimientos para la Adopción del Comercio Electrónico

3.1 Introducción

Para tomar la decisión de ingresar al mundo del comercio electrónico es necesario identificar los cambios y requerimientos más importantes. Durante el análisis de riesgos de comercio digital se deben incluir las oportunidades y riesgos que presenta la adopción del comercio electrónico. Después de tomar la iniciativa para iniciar el proceso de incursión del comercio digital existen algunos elementos a considerar como son: los requerimientos y cambios de negocios definidos en la estrategia de negocios que contienen ajustes a los procesos, tecnología, estrategia y recursos humanos.

> Esta estrategia debe estar alineada a la estrategia de tecnología, la cual considera aspectos de seguridad, infraestructura de comunicaciones y capacidad de procesamiento entre otros rubros.

3.2 Cambios y Requerimientos de Negocio

La entrada a la competencia en un mundo globalizado requiere identificar los cambios mínimos para permitir la participación en el gran mercado.

Los procesos del negocio de una empresa bajo el enfoque de comercio electrónico requieren ser entendidos y documentados para expresarlos en términos de una visión de comercio digital. Comúnmente se comete el error de considerar como suficiente, un sitio WEB poderoso o con un diseño efectivo. Siendo lo más importante el modelo de negocios que lo genera y no solo un conjunto de ideas aisladas e incompletas.

El conjunto de procesos de una empresa requieren de una re-ingeniería que permita adaptarlos al nuevo esquema de operación. El modelo de negocios que dio origen a la empresa puede ya no funcionar, y por lo tanto es necesario identificar los procesos clave donde es necesario tomar acciones para convertirlos en actividades orientadas al comercio electrónico Se denomina la E–ingeniería a este proceso, el cual considera re-inventar la forma en que se realizan negocios, que va desde la distribución de bienes o servicios, la colaboración y trabajo dentro de la compañía hasta la negociación y trato con los proveedores.

El análisis del cambio en la relación con los clientes y trato con los proveedores debe de ser profundo, ya que el comercio electrónico puede generar problemas, por ejemplo, si no se cuenta con la capacidad de producir el volumen que está demandando el mercado o nuestro proveedor no puede satisfacer los requerimientos de insumos, esta situación puede traer consecuencias legales debido al incumplimiento por una decisión equivocada, en caso de que no exista la capacidad de comprar, producir o distribuir al cliente los productos, servicios o información que puedan solicitar desde cualquier parte del mundo.

Según el marco de referencia de aplicaciones de IBM [IBM1 00], existen tres procesos prioritarios en las organizaciones que son: la administración de la relación con el cliente, los procesos internos del negocio y la administración de la cadena de suministro.

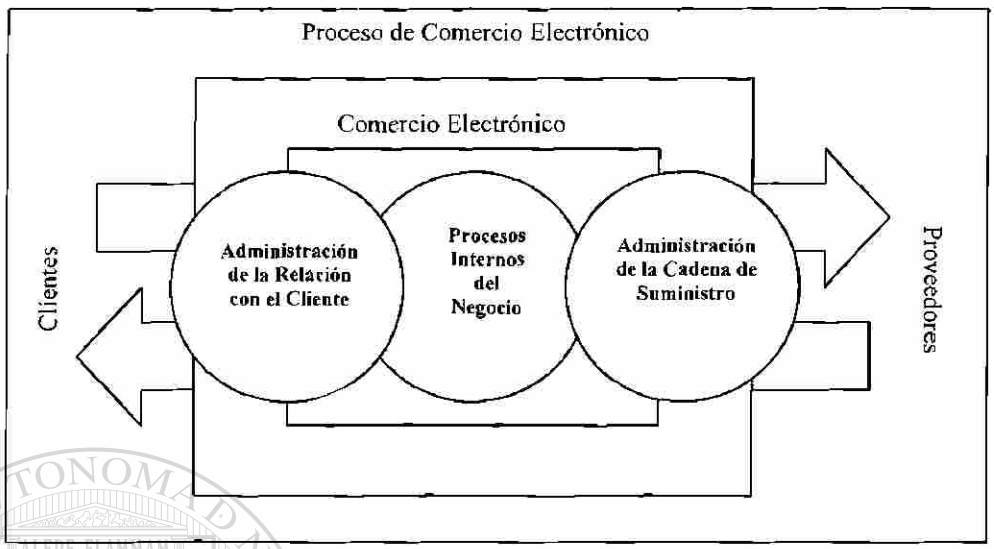


FIGURA 3.1: Procesos de e-Business IBM [IBM1 00]

Dentro de los cambios y requerimientos de negocio y basado en los procesos anteriormente mencionados, debemos considerar los siguientes aspectos:

3.2.1 Cambios y Requerimientos Orientados al Cliente

Anteriormente los cambios dentro de una empresa se encontraban orientados hacia los proveedores o a los procesos internos de operación y estrategia del negocio. En la actualidad el cliente es el principal actor para cualquier organización. Es de ahí que surjan conceptos como son: la personalización y la administración de la relación con el cliente o CRM (Customer Relationship Management).

En la actualidad la búsqueda de clientes es más exhaustiva que en el pasado debido al incremento y globalización de la competencia; en adición a lo anterior, el canal comunicación para la captación de clientes se ha convertido en un medio digital de publicidad y promoción que permite llegar a regiones lejanas y a mercados que antes no se consideraban como potenciales.

Después del proceso de atracción de los clientes, necesario tener una relación más estrecha para identificar sus requerimientos y necesidades y así poder proveer las soluciones solicitadas, lo cual implica la personalización de los servicios y productos para atender de forma casi única al cliente. Considerando este un esquema de retención de clientes. El cliente realiza sus compras de información, bienes o servicios en su propio espacio y tiempo, posiblemente sin la interacción con otra persona, más bien con una computadora o sistema que le permita encontrar los satisfactores a sus necesidades. [Hamm 99]

Es posible ahora que los usuarios busquen los precios más competitivos de los productos en un mundo global. Esto significa que la competencia de una empresa de bienes o servicios ahora son las empresas de todo el mundo. Así mismo un grupo de usuarios de distintas partes del mundo pueden unirse para comprar algún producto o servicio por un precio menor debido a la compra por volumen. El que un sistema por WEB recomiende al mejor postor o el mejor precio de venta, implica el requerimiento de nuevas reglas en la normatividad de la competencia entre empresas.

La relación de la empresa con los clientes es especialmente estrecha en el comercio electrónico negocio a persona. Debido a la globalización, los clientes tienen la capacidad de cambiar a otro proveedor de información, productos o servicios con solo presionar una tecla; es por ello que es necesario mejorar la administración de la relación con el cliente.

La personalización de los sitios en Internet y los sistemas de administración de la relación con el cliente (Customer Relationship Management – CRM) permiten a los usuarios almacenar una configuración definida por el usuario de acuerdo a sus necesidades y gustos; adicionalmente el contacto para el soporte técnico y atención a usuarios se vuelve más personalizado y disponible en todo momento y en todo lugar.

3.2.2 Re-ingeniería a la Organización

Las empresas pioneras en el cambio hacia el comercio digital han identificado que no es suficiente instalar sitios Web para clientes, empleados y proveedores. Para aprovechar al máximo la red es necesario re-inventar la forma en que conducen el negocio, la forma en que distribuyen los bienes, servicios o información, colaboración y administración del conocimiento dentro de la empresa y la relación con los proveedores.

Los proyectos de re-ingeniería pueden ser extremadamente complejos con cambios fundamentales de la tecnología, el negocio y la organización. Estos cambios según el autor:

> "Inclusive pueden cambiar el modelo y concepto del negocio que dieron origen a la empresa incluyendo su filosofía, misión y visión."

Por ejemplo, un banco en sus inicios realizaba las funciones de un almacén de objetos que representaban un valor como son el oro, la plata o los diamantes. En una segunda etapa los esfuerzos se canalizaban hacia almacenar y administrar el dinero, el cual es una representación intermedia de valor. Hacia el futuro vemos el cambio de un administrador y almacén de objetos hacia un servicio de valor agregado que únicamente representa cargos o abonos a números para representar electrónicamente transacciones. Esto será un proceso de eliminación de sucursales hacia una empresa virtual. Siendo así, un banco tendrá que adaptar sus procesos de recaudación y colocación de dinero, a servicios digitales de atención al cliente para el traslado de información.

Para iniciar la explotación de este tipo de negocios por Internet es necesario definir una estrategia de negocio que permita modificar el esquema actual de operación a nivel procesos, recursos humanos y tecnología. Es decir, hay que

alinear la estrategia de negocio a la nueva estrategia de comercio electrónico. Los procesos por si solos no fueron creados para competir en un mundo globalizado.

La introducción de un enfoque de comercio electrónico puede requerir de una re-ingeniería de procesos para modificar los procesos de compra de suministros, inventarios, operación básica y administración, producción, venta, promoción o distribución, e inclusive cambiar el concepto que dio origen a la empresa para transformar sus productos o servicios a un medio digital [Hamm 99]. En resumen, hay que modificar e integrar la cadena de valor de una organización

Es necesario definir las actividades o cambios de una organización con respecto a los proveedores, la empresa y la atención a clientes.

Dentro de las actividades o cambios a la organización con respecto a los proveedores tenemos:

- Análisis de los proveedores de insumos para determinar su capacidad de producción, distribución y entrega.
- En caso necesario, realizar una selección y sustitución de nuevos proveedores como plan de acción y contingencia.
- Realizar un análisis de la cadena de suministros

TABLA 3.1: Cambios o actividades de la empresa con respecto a los proveedores

Para el caso de la empresa se pueden realizar las siguientes acciones:

- Realizar un análisis de la capacidad de producción
- Cambiar los procedimientos y políticas de calidad
- Optimizar los procesos de producción con los conceptos de calidad, Just in Time, workflow, etc.
- Adaptar los procesos de comercio electrónico con los sistemas transaccionales y de toma de decisiones actuales
- Incluir esquemas de administración del conocimiento (KM) los cuales permiten aumentar la productividad de los empleados, mediante la compartición, adquisición y diseminación del conocimiento de los procesos del negocio
- Analizar los procesos de logística, inventarios y distribución de los productos
- En caso necesario, realizar una selección y sustitución de servicios de entrega de productos
- Realizar una estrategia de comercio electrónico para identificar oportunidades, riesgos e impactos al incursionar en el comercio electrónico
- Establecer planes de acción y contingencia de acuerdo a la estrategia de comercio electrónico

TABLA 3.2: Cambios o Actividades de la Empresa.

Para el caso de la atención a clientes se pueden realizar las siguientes acciones:

- Establecer nuevas políticas de atención a clientes
- Definir nuevos esquemas para dar soporte a los clientes

TABLA 3.3: Cambios o Actividades para la Atención a Clientes.

Además considero necesario:

"Para minimizar el impacto en la incursión en el comercio electrónico, realizar una definición de una estrategia de comercio electrónico, que identifique las oportunidades y riesgos"

3.2.3 Oportunidades, Beneficios y Riesgos

En el nuevo esquema electrónico de comercio se identifican nuevas oportunidades para los negocios y beneficios para los clientes como son los siguientes [ISPO_CEC 99]:

Oportunidades para los proveedores	Beneficios para los clientes
Presencia global	Opciones y selección global
Mayor competitividad	Calidad de servicio
Fabricación en masa	Productos y servicios personalizados
Reducción o eliminación de cadenas de suministro	Respuesta rápida a las necesidades
Ahorro sustancial de costos	Reducción sustancial de precios
Nuevas oportunidades de negocio	Nuevos productos o servicios

TABLA 3.4: Beneficios y oportunidades del comercio electrónico.

El comercio electrónico no es la panacea y existen múltiples problemas y riesgos que se presentan al incursionar en un proyecto de este tipo. Es por ello que en el capítulo 3 se hablará de la situación en México del comercio electrónico y en el 4 de análisis de riesgos al incursionar en un proyecto de comercio electrónico.

3.3 Recursos Humanos

3.3.1 Procuración de Recursos Humanos Especializados

Por otra parte, la nueva empresa basada en comercio electrónico requiere la contratación de recursos humanos altamente especializados en temas de comercio electrónico con conocimientos que van desde administración, mercadotecnia, negocios y finanzas, hasta tecnología, seguridad y matemáticas.

Es difícil encontrar un individuo que concentre tal conjunto de conocimientos y por ello se necesitará crear un staff dedicado, con el objetivo de definir e implementar una estrategia de comercio electrónico. Debido a los altos requerimientos de personal especializado es necesario contar con apoyo externo de empresas de consultoría, debido a que el comercio electrónico forma parte de las Tecnologías de Información emergentes y el conocimiento de procesos de negocio, y no existe un número tan alto de personas con la experiencia y el conocimiento requerido.

Otro problema con los recursos humanos es la reducción de plazas de trabajo o cambio de las funciones de los actuales empleados debido a la re-ingeniería de procesos y actividades o nuevos procedimientos de operación. En general en un cambio al enfoque de comercio electrónico existirá una resistencia al cambio, la cual debe de ser considerada en el análisis de riesgos.

3.3.2 Construcción de Comunidades Globales

El Internet trajo consigo cambios en la forma en que las personas interactúan. Aunque se considera que la computadora aísla a las personas, esto es parcialmente cierto, ya que debido al uso de Internet las personas mediante

el uso del correo electrónico, básicamente mantienen contacto y comunicación con un número mayor de usuarios. A pesar de ello la interacción física ha disminuido para ser reemplazada por el contacto a través del ciberespacio. [Social_web 00]

Los portales [Saha 99] son puntos de reunión que ofrecen de forma gratuita servicios como correo electrónico sin costo, búsquedas de información y programas de tráfico que permiten conducir a los usuarios a otros sitios en Internet mediante ligas. Actualmente, el comercio electrónico aprovecha la gran cantidad de usuarios que pertenecen a una comunidad virtual para ofrecer productos y servicios, ya que representan una fuente inmensa de posibles consumidores y estas vecindades son incubadoras que a su vez son utilizadas por empresas de comercio electrónico para realizar negocios.

Por ejemplo, FortuneCity un sitio en Internet (www.fortunecity.com) tiene aproximadamente 150,000 miembros registrados, America Online Inc. (www.aol.com) tiene aproximadamente 16 millones de suscriptores. [Gross 99]

Estos sitios basan su esquema de operación en la retención de los clientes y un factor de suma importancia es la confianza tanto en la difusión de su información personal con fines comerciales como en la garantía de seguridad al realizar compras por Internet.

3.4 Aspectos Legales

Actualmente, la legislación no ha avanzado al ritmo que lo ha hecho la tecnología o los esquemas de negocios.

Desafortunadamente para aquellos cuyo negocio se basa en el Internet o el comercio electrónico, el número de conflictos legales es mayor en reacción a este nuevo medio de negocios.

Los jueces y abogados intentan evadir el cambio del status quo sobre el comercio electrónico, pero las presiones por tratar asuntos como son: los contratos electrónicos, privacía, derechos de propiedad, patentes, derechos de autor, difamación, fraudes, crímenes computacionales, censura e imposición de impuestos, han hecho imperativo que los profesionales de sistemas, se concienticen de la evolución de las leyes sobre el Internet que afectarán el medio del cual están encargados de administrar. Una comunidad de sistemas de información bien informada es mucho más capaz de tomar los retos legales y políticos que implique el desarrollo del comercio electrónico.

Uno de los aspectos legales más críticos que amenaza el crecimiento del Internet como un medio de comercio es la exposición de los negocios de Internet, por ejemplo, al largo brazo de la jurisdicción de las cortes en los 50 estados diferentes de los Estados Unidos. Cada autoridad puede ejercer la autoridad a entidades (personas o corporaciones) en cualquier parte si puede demostrar jurisdicción. Esto en un contexto mundial es más complicado y requiere de tratados especiales entre los diversos países. Las diferencias en leyes criminales son mayores entre diversos países.

Existen restricciones de exportación de software o hardware que implemente sistemas de seguridad desde los Estados Unidos de América hacia el resto del mundo y esto dificulta la difusión y uso del comercio electrónico en todo el mundo. Esta restricción no limita a los sistemas de seguridad utilizados para ciertos usos como los sistemas financieros, entre otros. El Internet no conoce de límites o territorios, un sitio Web puede ser visitado de cualquier parte del mundo. Cuando se realiza una transacción electrónica, se plantea la pregunta de donde se realiza el negocio ¿En el estado o país de los clientes, en donde se procesan las ordenes o donde se almacena y embarca el producto? En caso de algún problema o amenaza, ¿qué leyes se utilizarán en el juicio?. [Alberts 98]

La legislación de los países debe contener acuerdos internacionales que protejan y promuevan el uso del comercio electrónico. Para ello, adicional a las leyes se requiere contar con las denominadas "Autoridades Certificadoras" las cuales se encargan de la expedición y administración de los certificados digitales los cuales como veremos más adelante, permiten verificar la identidad de una persona física o moral para posteriormente expedir un certificado que lo demuestre.

Otro problema que se presenta son los derechos de propiedad intelectual debido a la facilidad de realizar copias de la información digitalizada que representa un bien o servicio como también se verá más adelante.

3.5 Proceso de Digitalización

El comercio electrónico requiere la conversión de la información, bienes ó servicios a representaciones digitales. Aunque existen casos en la actualidad para los cuales no es posible la digitalización debido a restricciones de carácter físico o económico. Por ejemplo, los alimentos no pueden ser representados de forma digital con la tecnología actual, no siendo el objetivo del comercio digital. Para casos como éste, el comercio electrónico realiza transformaciones en los procedimientos de compra, producción o venta, mediante la automatización y mejora en los procesos de la cadena de suministros.

Pero para elementos como el dinero, información, bienes y servicios que pueden ser representados y transmitidos en un formato electrónico la situación cambia y el reto pasa de un esquema físico a esquemas económicos, legales, y tecnológicos.

El Internet es un medio ideal para el comercio electrónico de los bienes, servicios o información en formato electrónico ya que pueden ser mostrados,

vendidos y entregados a través del mismo medio a los diversos clientes. Es simplemente un nuevo canal de distribución que puede ser aprovechado para aumentar la eficiencia, reducir los tiempos de entrega y disminuir los costos del bien o servicio en cuestión.

La digitalización tiene ventajas significativas debido a que no existe empacado, inventarios y costos de entrega y se elimina el riesgo sobre el manejo de inventarios. Esto permite agregar nuevos productos a un costo mínimo. Y es posible registrar las ventas en tiempo real.

Al eliminar el empacado y la distribución se reduce el tiempo de alcanzar al mercado y esto lleva a la globalización de las ventas y expandir el mercado a cualquier punto del mundo. También se crea una conexión directa y más rápida con los clientes.

En el ambiente de comercio electrónico existen componentes del mercado que pueden ser remplazados con representaciones o sustitutos digitales. Algunos casos de los siguientes grupos pueden ser sujetos a un proceso de digitalización: [Steinauer 97]:

Elemento	Representación o sustitución digital
Dinero	Dinero Digital
Bienes	Objetos Digitales
Socios de Comercio	Agentes Digitales, Computadoras
Mecanismos físicos de transacción	Aplicaciones Electrónicas de intercambio de datos (EDI), Redes
Canales físicos de distribución y entrega	Entregas electrónicas

TABLA 3.5: Representación o Sustitución Digital de Diversos Elementos.

A continuación se presentarán algunos ejemplos de procesos de digitalización y la problemática que se puede presentar:

3.5.1 Dinero

Un elemento principal que hay que considerar en el comercio electrónico es la digitalización del dinero. Actualmente el uso de tarjetas de débito o crédito han reducido el uso de efectivo representado por monedas o billetes. Para iniciar es necesario definir el uso y significado del dinero, así como algunas de sus propiedades. El dinero es un acuerdo entre una comunidad para utilizar algo como un medio de intercambio. Así mismo el dinero puede definirse como información acerca de la forma en que intercambiamos energía. [Rheingold 99]

Algunas propiedades del dinero como actualmente se utiliza son: [Gleick 96]:

- El dinero es sucio debido a su manejo por múltiples personas
- El dinero es pesado y difícil de manejar debido al material con que se encuentra hecho
- El dinero es costoso debido a su costo de administración y creación. Por ejemplo los costos asociados a la impresión, manejo, almacenamiento seguro, destrucción, recolección y distribución. De igual forma los costos asociados a la falsificación del dinero

Como alternativas al uso de tarjetas de crédito o débito por parte de las instituciones bancarias, se han presentado algunas soluciones para la digitalización del dinero como son Bitbux, E-Cash, Netchex, CyberCash, Netbills, Mondex y DigiCash, permitiendo el uso de billeteras o monederos electrónicos que almacenan información que representa dinero. El uso de cheques electrónicos sustituye a los tradicionales cheques de papel especial, los cuales pueden ser falsificados o reproducidos. Estas soluciones plantean el uso de tarjetas inteligentes que contienen un chip el cual es capaz de almacenar de 2 a 4 KB de información de forma segura. Aunque su uso se ha visto restringido debido a los requerimientos de tecnología especial.

3.5.2 Bienes

Ejemplos de digitalización de bienes:

- Un libro, revista o periódico puede ser considerado como información bajo la perspectiva del contenido y/o del bien material y esto varía según la persona. Al considerar un proceso de digitalización es necesario tomar en cuenta los derechos de autor debido a la facilidad de propagación o copiado de la información, y por lo tanto es necesario utilizar algún medio que proteja la propiedad intelectual

- De igual forma una canción o la música en general puede ser representada en forma digital en contra parte a la representación analógica de los cassettes. En los últimos años mediante las técnicas de compresión el audio ha sido representado en formato digital, utilizando 4 MB en promedio para almacenar una canción de música. Actualmente en Internet es posible encontrar una gran variedad y cantidad de canciones de los artistas más populares. Se vuelve a presentar el problema de la propiedad intelectual ya que el espacio requerido y la capacidad de procesamiento para este formato han sido cubiertos por la tecnología actual

- Como ejemplo, tenemos al formato MP3 [Ponce 99] el cual es un formato para compresión de audio digital desarrollado por el Motion Picture Experts Group motivado por el crecimiento explosivo de Internet. El MP3 se ha hecho popular como formato de archivos de música tanto de forma legal como ilegal (Copias no autorizadas sin derechos de autor).

- El vídeo no es la excepción y mediante el uso de DVD (Digital Versatile Disk) es posible almacenar una película traducida a 5 idiomas, en un disco compacto del tamaño de los CD-ROM comunes. La capacidad actual del DVD es de 17.2 GB por disco y se espera un incremento significativo en los próximos años.

- Los procesos de digitalización de documentos oficiales como una factura son aspectos que limitan el desarrollo del comercio electrónico, es el caso de México donde la factura electrónica es una tarea inconclusa. [AMECE1 99]

3.5.3 Servicios

Ejemplos de digitalización de servicios:

- Las pólizas de seguros o los boletos de avión son reemplazados por documentos electrónicos eliminando así la utilización de papel. De igual forma, existen agentes virtuales que permiten ofrecer consultas y asesoría en línea para determinar la mejor opción basada en la conveniencia del cliente, de forma rápida e independiente de un espacio físico.

- Servicios como la educación no están al margen de la digitalización. Existen grandes esfuerzos en el mundo y en México para ofrecer educación digital de calidad a un mayor número de estudiantes. En el caso de México, el Tecnológico de Monterrey a través de la Universidad Virtual ofrece cursos de profesional y programas de postgrado bajo el concepto de educación a distancia. El apoyo en herramientas como el Internet y Lotus Notes han permitido establecer una comunidad virtual con el objetivo de cambiar el paradigma de enseñanza por el de aprendizaje. Este nuevo modelo se encuentra en constante evolución y actualmente

se ofrecen maestrías en línea evitando el desplazamiento hacia los centros de enseñanza. [RUV 99]

- Los siguientes sitios en Internet permiten obtener servicios en línea: www.aa.com, www.mexicana.com, www.sabre.com.mx, www.inlinea.com, www.autorate.com, www.paytrust.com y www.jngrace.com.

3.5.4 Información

Ejemplos de digitalización de información:

Desde su origen el software ha sido información digitalizada aunque debido a la falta de tecnologías que permitan la protección de la propiedad intelectual, su distribución se ha realizado a través de los medios tradicionales mediante los discos flexibles y compactos. Se espera en el corto plazo la distribución en forma electrónica evitando así los tiempos de entrega y la reducción de costos.

No todos los casos de digitalización son la panacea. Es necesario avanzar en áreas complementarias ya que existen algunas desventajas. Se requieren mecanismos que protejan la propiedad intelectual de la información, bienes o servicios que han sido cambiados a un formato electrónico. La opción más común es proteger la información o el producto digital mediante candados y autentificaciones de uso, ya que sin ellas existe una gran facilidad para copiar el producto.

En otros casos la tecnología debe madurar para permitir por ejemplo, una mayor compresión de la información y facilitar su distribución a través de la infraestructura de comunicaciones actual y de los años venideros. Más adelante cubriremos el impacto del riesgo y/o las desventajas de la tecnología y los procesos de digitalización.

3.6 Aspectos Económicos

Al considerar la incursión en el comercio digital se requiere realizar estudios económicos sobre el impacto que tendrá el desarrollo de un proyecto de comercio electrónico. Aspectos como costos en consultoría, infraestructura de comunicaciones, plataforma y aplicaciones. De igual forma los cambios en el negocio derivados por la optimización de procesos, aumento de ventas o requerimientos mayores de distribución o insumos.

Es necesario planear las inversiones y la toma de decisiones basadas en estudios de costo beneficio, evaluación de proyectos para determinar el retorno de la inversión, entre otras variables económicas. Con el objetivo de aprovechar las oportunidades y estar preparado para minimizar los riesgos.

El modelo ROI de análisis financiero considera la tasa de retorno sobre la inversión y se calcula mediante la siguiente fórmula:

$$ROI = \frac{\text{Utilidades (Varios Años)}}{\text{Inversión}}$$

Donde el valor del dinero para los rubros anteriores representa un valor distinto en el tiempo. Valores mayores y positivos representan oportunidades de negocio.

Estas medidas no son validas para las empresas de comercio electrónico denominadas "Internet Startup" ya que el ROI será seguramente un valor negativo en los primeros años y es por ello que se utilizan otras medidas como son la apreciación de las acciones.

Debido al alto riesgo que representa la seguridad en el comercio electrónico se requiere un estudio sobre el impacto económico en caso de alguna intrusión

a los sistemas. La seguridad se encuentra en relación con la inversión, una mayor seguridad requerirá una mayor inversión por lo tanto se tiene que hacer la pregunta si vale la pena el gasto, mediante un análisis de riesgos y costo beneficio. De igual forma el esfuerzo para romper la seguridad va en relación directa con la posible ganancia a obtener.

Por lo anterior es necesario ampliar en temas económico financieros que están fuera del alcance del documento de tesis.

3.7 Requerimientos Tecnológicos

La implementación de un sistema de comercio electrónico requiere de la tecnología que permita soportar los procesos de negocio establecidos por los planes de acción derivados de una estrategia de comercio electrónico.

El comercio electrónico requiere de una infraestructura tecnológica de comunicaciones, equipo de cómputo y aplicaciones que permitan el intercambio de información entre personas, empresas, entidades gubernamentales y financieras. Gracias al Internet y al WWW, el costo de iniciar el cambio hacia un modelo de comercio electrónico se reduce de manera drástica, debido a la utilización de la red pública de Internet y el aumento en la capacidad de procesamiento a un bajo costo. Es por ello que el comercio digital no sería posible si no existieran los adelantos tecnológicos que hoy se tienen.

Estos cambios tecnológicos pueden representar algunos problemas como son: la seguridad de las transacciones, y la implantación y administración de plataformas que permitan realizar transacciones de forma segura; es decir en general la administración segura de la información.

La seguridad requiere de equipo y software adicional al de una Intranet para minimizar el riesgo de un ataque. Internet es una gran red pública de

computadoras y por ello es necesario incrementar la seguridad y para ello se requiere personal especializado como se mencionó anteriormente.

Según la arquitectura tecnológica de IBM [IBM2 00] se presentan los siguientes elementos:

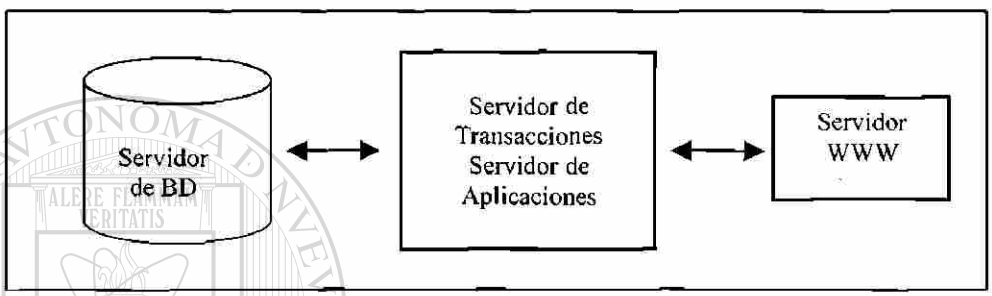


FIGURA 3.2: Arquitectura Tecnológica de IBM. [IBM2 00]

Los componentes de la arquitectura tecnológica se pueden agrupar en infraestructura de comunicaciones, hardware y software.

3.7.1 Infraestructura de Comunicaciones

El comercio electrónico requiere una infraestructura de comunicaciones que permita el intercambio de información en todo el mundo. El uso de una red de computadoras como lo es Internet sin fronteras o límites permite el desarrollo de las aplicaciones del comercio electrónico.

Como se mencionó anteriormente, el crecimiento en el uso de Internet no tiene precedente. El uso de la radio tomó 38 años para llegar a 50 millones de usuarios, la televisión tomó 13 años y únicamente 4 años para el Internet. [USDC 99]

Se requiere una gran infraestructura de comunicaciones para el intercambio de información entre un número creciente de usuarios de Internet es por ello que actualmente iniciativas como Internet II permitirán un aumento en el ancho de banda de hasta 2 GB/s y continua incrementándose debido al desarrollo de estándares como SONET [SONET 00] y SDH [SDH 00].

El uso de la fibra óptica y el aumento en su capacidad para transmitir información seguirá impulsando las comunicaciones a bajo costo.

El uso de redes privadas VPN (Virtual Private Network) y redes de valor agregado (Value Added Network) permiten realizar de forma más segura transacciones de comercio electrónico pero a costos más elevados. Es por ello que Internet y en el futuro Internet II [InternetII_A 00], [InternetII_B 00] será la opción más económica y viable para realizar comercio digital. Bajo este esquema de red pública y de menor costo la seguridad será el principal elemento tecnológico a resolver, ya que, como se ha mencionado, es un medio no seguro. Es por ello que la selección de mecanismos y técnicas de protección de la información será el principal asunto tecnológico a considerar.

La instalación de un esquema de seguridad para incorporarse al mundo de Internet requiere de equipo especializado en la protección de la información.

3.7.2 Hardware

El hardware y el software han vivido una carrera tecnológica debido al aumento en los requerimientos por parte de las aplicaciones y sistemas operativos. En respuesta a ella, el hardware aumenta el poder de procesamiento, continuando así una persecución interminable. Por ejemplo, la ley de Moore [Moore 00] nos dice que la capacidad de los procesadores será duplicada cada 18 o 24 meses con relación a su predecesor.

Para realizar comercio electrónico es necesario que las empresas realicen actualizaciones a la plataforma tecnológica existente. Este escalamiento o remplazo permite soportar los nuevos requerimientos de procesamiento debido a los altos volúmenes de transacciones de una empresa de gran tamaño. Para ello se hace uso de servidores que permitan ejecutar aplicaciones las 24 horas del día y los siete días de la semana (misión crítica); tolerancia a fallas y más del 99% del tiempo operando (alta disponibilidad); capacidad de crecimiento del sistema según las necesidades del negocio (escalabilidad) y una gran capacidad de almacenamiento. El comercio electrónico es posible gracias al crecimiento del poder de procesamiento de las computadoras de escritorio que ejecutan las aplicaciones y a los servidores que proveen el acceso a las bases de datos y aplicaciones.

Ha existido un aumento significativo en los últimos años en la capacidad de procesamiento. Por ejemplo, una computadora con procesador Pentium tiene la capacidad de procesar aproximadamente 400 millones de instrucciones por segundo (MIPS) y se esperan 100,000 MIPS para el 2012 [USDC 99], [USGWGEC 98]. Este aumento viene acompañado de la reducción en los costos de las computadoras.

Con el aumento de la capacidad de procesamiento los requerimientos son cubiertos mediante la tecnología de agrupar servidores, esta tecnología se denomina clusters y permite realizar división del trabajo entre varios servidores y así atender una mayor demanda de procesamiento de transacciones.

Adicionalmente se utiliza la arquitectura de tres capas que permiten administrar la carga de los servidores: un servidor de aplicaciones se comunica con un servidor de transacciones que administra los accesos al servidor de base de datos. Los resultados en rendimiento obtenidos con un diseño distribuido permite ejecutar aplicaciones de comercio electrónico de gran escala.

Es necesario establecer iniciativas que permitan aumentar la seguridad del comercio electrónico por medio del hardware. Por ejemplo, la inclusión de números de identificación en los procesadores. Específicamente Intel anunció que añadiría un número serial y único en los procesadores Intel Pentium III [Pentium_III 00]. Esta capacidad sería aprovechada por las aplicaciones de comercio electrónico y los sistemas operativos para verificar la identidad de los participantes. Aunque esto ha generado un rechazo debido a la falta de privacidad y falta de mecanismos que garanticen el anonimato al realizar compras ante las diversas entidades participantes.

3.7.3 Software

Las aplicaciones para comercio electrónico se encuentran basadas en la tecnología de Internet, para el caso especifico del comercio electrónico entre empresas, son denominadas Extranets. El desarrollo de las Extranets provee una liga entre la Intranet de la empresa y las estrategias de Internet. [Riggins 98]

En la actualidad, las aplicaciones Web deben de ser construidas siguiendo un estándar compatible a un servidor de aplicaciones, el cual permite modelar componentes con las funciones y datos de toda una organización, lo que representa la lógica del negocio. Actualmente una gran cantidad del desarrollo de aplicaciones para el comercio electrónico se realiza en el lenguaje de programación Java, el cual es multiplataformas y orientado a objetos. La tecnología utilizada en los servidores de aplicación en su mayoría esta basada en servicios desarrollados en el lenguaje Java. Entre las tecnologías utilizadas tenemos los Servlets (applets corriendo en el servidor) [Servlets 00], Java Server Pages (Generación de páginas dinámicas) [JSP 00], los Enterprise Java Beans (EJB) [EJB 00] que permiten modelar un proceso del negocio y sus reglas en un componente, y el acceso a bases de datos a través del JDBC (Java Database Connectivity) [JDBC 00].

Entre los sistemas operativos más utilizados para el comercio electrónico se encuentran el Windows de Microsoft para el lado del cliente y el UNIX para los servidores de bases de datos, transacciones y aplicaciones, debido a su estabilidad y a las características del equipo que utilizan.

Los manejadores de bases de datos relacionales u orientado a objetos como Oracle, Sybase, Informix o DB2 permiten el acceso a grandes cantidades de información y de procesamiento de transacciones. Bajo los nuevos esquemas de diseño de aplicaciones de comercio electrónico, el uso de un servidor de transacciones es recomendable para mejorar el rendimiento de las aplicaciones.

Adicional a lo anterior, el eXtensible Markup Language (XML) [XML 00] es una un nueva tecnología para aplicaciones WEB que se prevé sustituya el HyperText Markup Language (HTML) [HTML 00] en los próximos años. XML es el estándar del World Wide Web Consortium (W3C) completado en 1998 que permite crear etiquetas personalizadas y auto descriptibles, a diferencia del HTML. El anexo A presenta una breve introducción al XML. Las tecnologías anteriormente presentadas no contemplan la seguridad como un componente intrínseco. Cabe mencionar que las aplicaciones de comercio electrónico requieren de la implementación de rutinas de seguridad que incorporen algoritmos, técnicas y mecanismos, los cuales permitan realizar comercio electrónico de forma segura.

El desarrollo de componentes de seguridad debe ser revisado a detalle para evitar puertas falsas por parte de los proveedores o programadores de los componentes, poniendo en riesgo la seguridad de las organizaciones. Lo anterior será cubierto con más detalle en los próximos capítulos.

3.7.4 Tecnologías Actuales

A continuación se presentan algunos ejemplos de las tecnologías que actualmente se utilizan para realizar la

implantación de un proyecto de comercio electrónico. Adicionalmente se incluyen referencias URL (sitios en Internet) donde se puede encontrar más información al respecto. Los rubros considerados son Hardware y Software:

Hardware - Servidores	
DIGITAL AlphaServer Series ES, GS y SC	http://www.digital.com/alphaserver/es_series.html http://www.digital.com/alphaserver/gs_series.html http://www.digital.com/alphaserver/sc/index.html
HP 9000 Clase I, k, v y hyperplex	http://www.unixsolutions.hp.com/products/servers/lclass/ http://www.unixsolutions.hp.com/products/servers/kclass/ http://www.unixsolutions.hp.com/products/servers/vclass/ http://www.unixsolutions.hp.com/products/servers/hyperplex.html
SUN HPC10000 y HPC6500	http://www.sun.com/servers/hpc/products/hpc10000.html http://www.sun.com/servers/hpc/products/hpc6500.html
IBM RS6000 44P 270 y SP	http://www.rs6000.ibm.com/hardware/workgroups/44p_270.html http://www.rs6000.ibm.com/hardware/largescale/SP/
Software - Servidores de Aplicaciones	
BEA Weblogic IBM Websphere	http://www.beasys.com/products/weblogic/ http://www-4.ibm.com/software/webservers/appserv/
Software - Servidores de Transacciones	
BEA Tuxedo	http://www.beasys.com/products/tuxedo/
Software - Bases de Datos	
Oracle 8i	http://www.oracle.com/database/oracle8i/index.html
Sybase	http://www.sybase.com/products/databaseservers/ase/index.html
Informix	http://www.informix.com/ids2000/

TABLA 3.6: Tecnologías actuales. Hardware y Software

3.8 Aspectos Culturales

3.8.1 Regionalización y Globalización

Ante un mundo globalizado es requerido unificar los formatos de fecha, la fecha misma y la moneda utilizada en la realización de transacciones electrónicas.

El idioma comúnmente utilizado para el intercambio de información, turismo, compra y venta de productos o servicios es el inglés. Para lograr la masificación del uso de Internet y del comercio electrónico es necesario que los sistemas sean adaptativos permitiendo de forma transparente la presentación de la información en el idioma del usuario o cliente. Eliminando así la necesidad de aprender un idioma puente o intermedio para obtener los bienes, servicios o información requerido.

El lenguaje ha sido un factor limitante para el intercambio de productos y servicios, con el comercio electrónico es posible establecer un sitio multilenguajes que permita la comunicación sin la necesidad de conocer cada uno de las diversas lenguas y características propias.

Durante una transacción es necesario estandarizar y unificar los formatos de fechas y la utilización de una fecha única que permita registrar las operaciones con independencia de la ubicación del proveedor de bienes o servicios y de la entidad financiera que procese el pago.

3.8.2 Moneda

Como una representación intermedia o una forma de pago (equivalencia), la moneda requiere una transformación debido al contenido de poder o pertenencia que representa, ya que ahora únicamente se utilizara un número almacenado en algún sistema donde se aplicarán transacciones de cargo o abono.

Existen algunos problemas debido a que esta nueva forma de dinero electrónico no es tangible y hay un sentimiento de pérdida de poder.

3.9 Conclusiones

El esquema de requerimientos y cambios depende del origen de la empresa que desea incursionar en el mundo del Comercio electrónico.

Para una organización tradicional los cambios de negocio implican un rediseño de sus procesos para ser adaptados al nuevo modelo de transacciones electrónicas y esto sugiere una incursión lenta de la alineación de las tecnologías de información con la estrategia de negocio.

Por otra parte una empresa de las denominadas Internet Startup [Startups WWW], tiene un inicio vertiginoso, por lo cual los modelos de negocios no se encuentran bien fundamentados y únicamente depende de un conjunto de ideas que derivan en planes de acción. Es por ello que en muchos casos tienen que ver hacia atrás para revisar los planes de negocio y validar las estrategias previamente definidas.

Estos cambios varían en cada país debido a las grandes diferencias en lo económico, social, económico, cultural y tecnológico. Es por ello que a continuación se presenta la situación actual del comercio electrónico en el Mundo y el caso específico de México.

CAPITULO 4

4 Situación Actual del Comercio Electrónico en el Mundo y en México

4.1 Situación Actual del Comercio Electrónico en el Mundo

El comercio electrónico ha crecido en el mundo debido a la penetración que han tenido las computadoras en los hogares, el trabajo y la escuela. Actualmente, el uso de la computadora y de Internet representa una herramienta común y se espera que al igual que la televisión, tenga un mayor impacto en las actividades cotidianas de la vida de los seres humanos.

De igual forma se han incrementado los proveedores de servicios de Internet permitiendo a un costo relativamente bajo el acceso al Internet.

El número de usuarios que actualmente utilizan Internet es de aproximadamente 200 millones en todo el mundo. La siguiente figura muestra el número de usuarios de Internet en el presente y la proyección hacia el futuro:

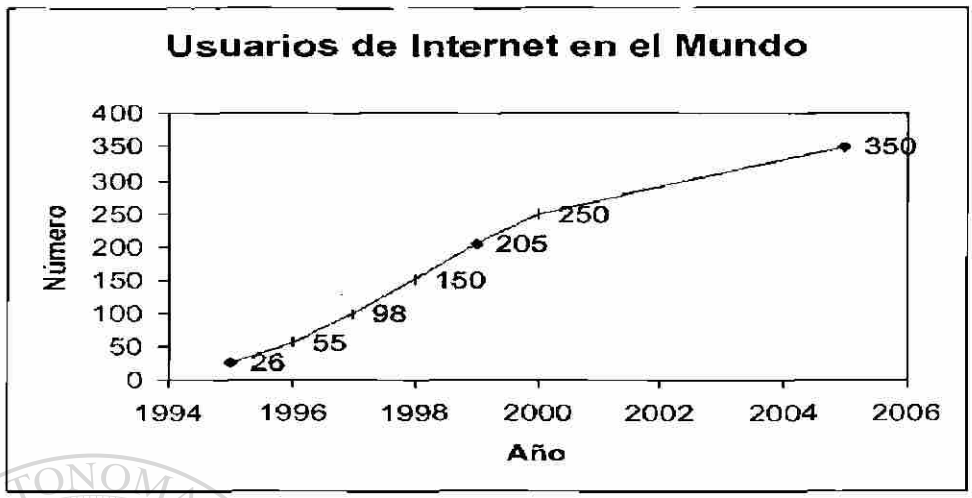


FIGURA 4.1: Número de Personas que Utilizan Internet en el Mundo

En la actualidad el costo de las computadoras y de Internet representa un elevando costo si se considera el alto nivel de pobreza en el mundo. Pero esta situación puede cambiar debido a la reducción de los costos de estas tecnologías permitiendo a los estratos más bajos incursionar en el uso de las nuevas tecnologías.

El comercio electrónico, según la clasificación presentada con anterioridad, muestra tres tipos de comercio electrónico denominados Persona a Negocio, Negocio a Negocio y dentro del Negocio. Los dos primeros son los mas importantes ya que el tercero puede ser incluido en el comercio electrónico. Como se muestra en la siguiente figura el crecimiento del comercio electrónico personal a negocio aumenta de forma lineal pero el comercio digital de B2B aumenta de forma exponencial y es ahí donde se tendrá un mayor auge y se espera que se realicen las mayores inversiones.

La figura muestra las cifras para los Estados Unidos ya que actualmente EU tiene una cuarta parte de los usuarios de Internet en el mundo, aunque se espera que Europa cierre la brecha existente con los Estados Unidos. Para ello se han establecido metas de instalar la infraestructura de comunicaciones necesaria en los años venideros.

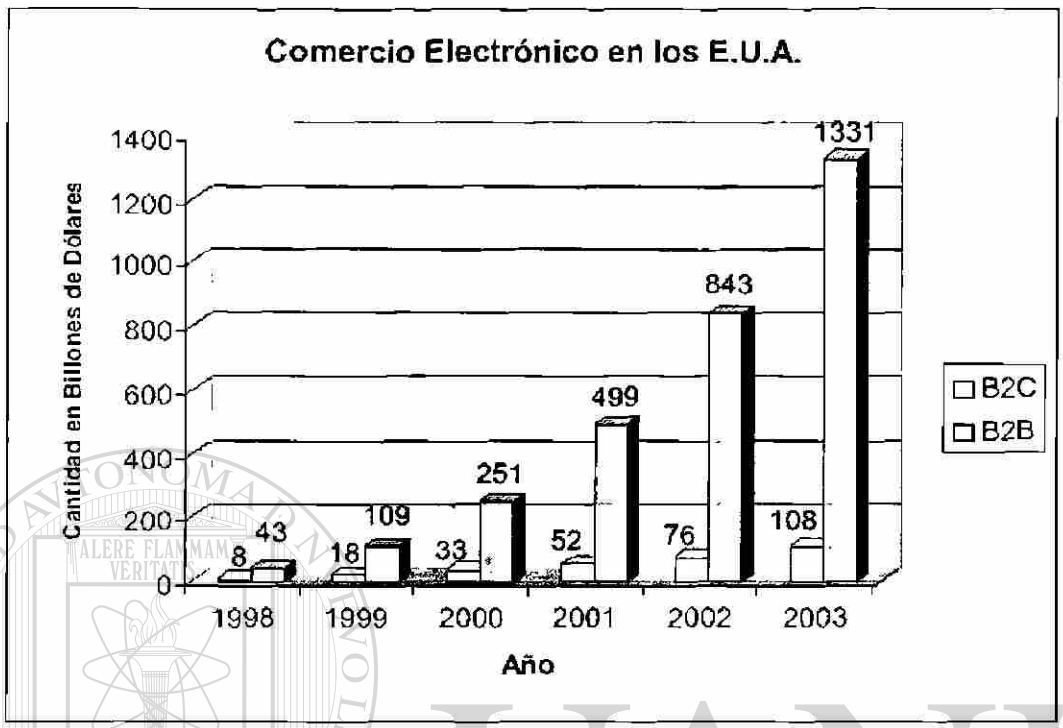


FIGURA 4.2: Cantidad en Dinero del Comercio Electrónico B2C y B2B en los E.U.A. [NUA2 00]

Existe actualmente un esfuerzo en los Estados Unidos de América denominado Internet II que representa la supercarretera de la información en donde un grupo de universidades y empresas de los Estados Unidos se han unido con el objetivo de contar con una infraestructura de alta velocidad para el intercambio de información y el comercio electrónico.

La misión de Internet II es:

"Facilitar y coordinar el desarrollo, implementación, operación y transferencia de tecnología de aplicaciones y servicios de red avanzados, para impulsar el liderazgo de los E.E.U.U. en investigación y la educación avanzada, y acelerar la disponibilidad de nuevos servicios y aplicaciones en el Internet"

Las metas de Internet II son [InternetII_A 00]:

- Permitir una nueva generación de aplicaciones
- Impulsar una capacidad de liderazgo en la investigación y educación
- Transferir nuevas capacidades a la red global de producción de Internet

Existe una gran diversidad de sitios en Internet que permiten realizar intercambios de productos, servicios o información, tanto bajo los esquemas de comercio electrónico negocio a persona o negocio a negocio. Entre los cuales están los siguientes:

La empresa www.amazon.com se dedica principalmente a la venta de libros en Internet. Con un catálogo de más de 3 millones de libros. Mediante su innovador servicio de compra con un solo click, permite a millones de usuarios obtener los libros requeridos desde su hogar, oficina o escuela. Ha sido uno de los éxitos más grandes del comercio electrónico negocio a persona.

Bajo un concepto diferente, www.priceline.com, permite mediante una forma revolucionaria de vender productos, establecer el precio de los productos o servicios deseados esperando que algún proveedor de servicios o empresa acepte el precio ofrecido.

Beneficios tangibles sobre todo en el ahorro de precios pueden ser obtenidos en www.mercata.com, el cual es una empresa de venta al menudeo que permite a grandes grupos de consumidores agruparse para alcanzar una compra eficiente, teniendo como resultado un precio menor para todos. Mercata ofrece productos de precio flexible (PowerBuys) y artículos de precio fijo (Group Values) en las áreas de electrodomésticos, salud, jardinería, regalos y artículos deportivos.

De forma similar, la red de demanda Accompany (www.accompany.com) conecta a las comunidades y a los proveedores de productos en un ciclo de compra en tiempo real para hacer corresponder a la demanda con la oferta. También realiza funciones para obtener precios por volumen de los proveedores. Existen esquemas como el de www.mypoints.com, el cual permite obtener puntos con el simple hecho de visitar páginas, comprar productos o leer mails. Modelos de negocio a negocio pueden ser encontrados en www.ariba.com y en www.b2bexplorer.com, los cuales mediante el concepto de digital marketplace permiten enlazar a compradores y proveedores en un mismo entorno. Todos estos ejemplos demuestran la gran variedad de servicios ofrecidos por Internet para la compra de productos, servicios o información, permitiendo la competencia en un mundo globalizado sin límites físicos.

4.2 Situación Actual del Comercio Electrónico en México

En México la situación económica, política, legal y social no permite el desarrollo de Internet y el Comercio Electrónico como en los Estados Unidos. Como se mencionó anteriormente, aún no existen condiciones suficientes para impulsar la economía de Internet, la falta de legislación apropiada, el cumplimiento de la misma, un alto grado de pobreza extrema en la que viven los mexicanos, entre otros factores, han impedido la incursión del comercio electrónico a los estratos sociales más bajos.

Sin embargo, estas barreras están en proceso de romperse y el futuro en México se visualiza prometedor, las estadísticas de crecimiento mencionadas posteriormente en este mismo capítulo permiten a los emprendedores de la nueva economía realizar planes de inversión.

Para entender la situación actual del comercio electrónico en México es necesario primero mencionar el número de usuarios y la base instalada de PC por sector.

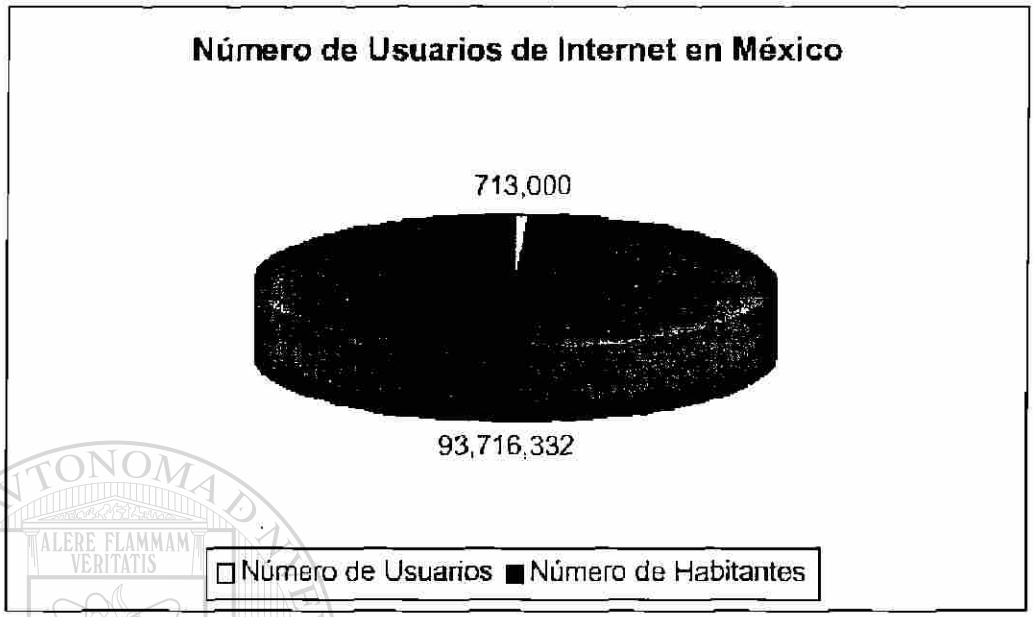


FIGURA. 4.3: Número estimado de usuarios de Internet en México (IDC Diciembre 1998) [NUA3 00]

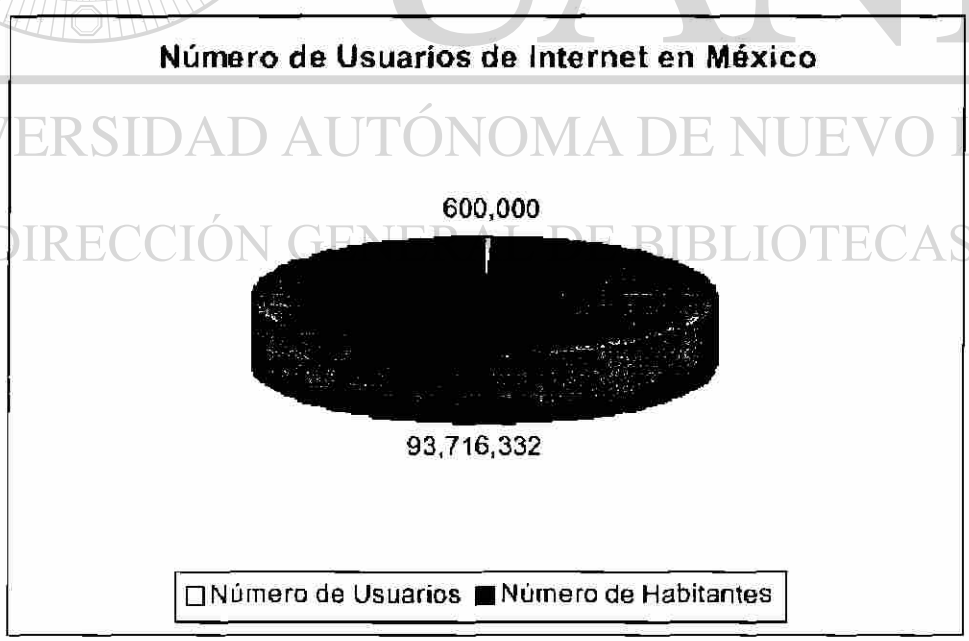


FIGURA 4.4: Número estimado de Usuarios de Internet en México (IABIN Abril 99) [NUA3 00]

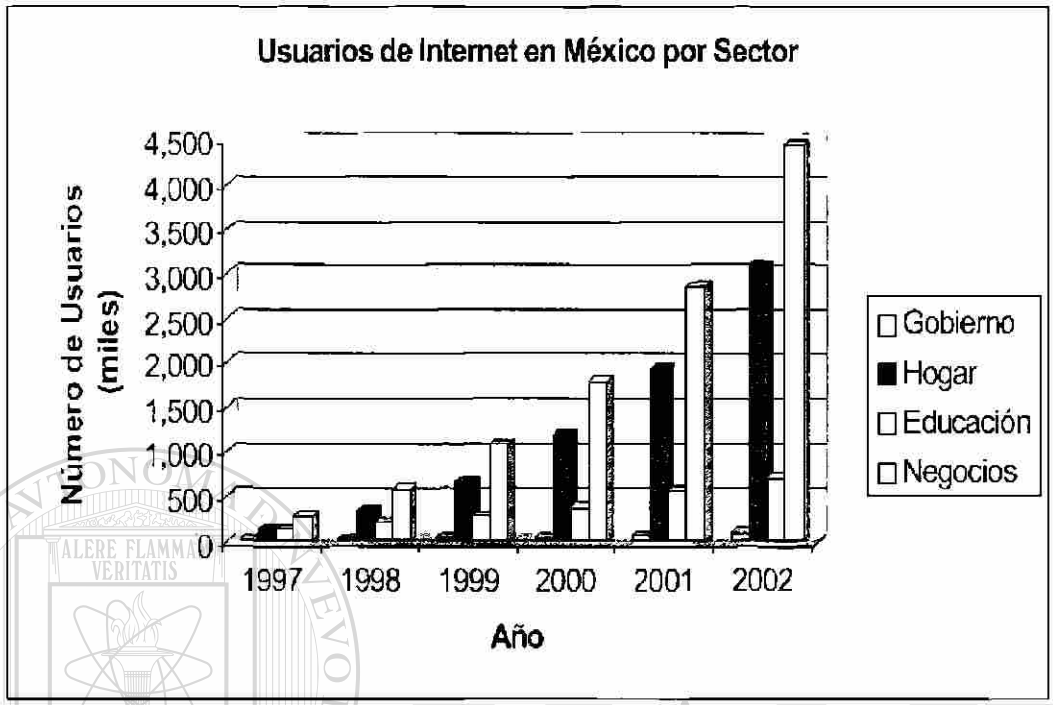


FIGURA 4.5: Proyección de usuarios de Internet en México por sector. [Garres 98]

	1997	1998	1999	2000	2001	2002
Hogar	140,878	337,575	675,719	1,190,388	1,945,255	3,108,502
Gobierno	13,855	24,509	29,237	41,674	71,955	99,461
Educación	141,814	210,251	280,483	376,540	567,745	709,966
Negocios	299,137	596,790	1,092,905	1,796,483	2,859,144	4,466,562
Total	**595,684**	**1,169,125**	**2,078,344**	**3,405,085**	**5,444,099**	**8,364,491**

TABLA 4.1: Proyección de Usuarios de Internet en México por sector. [Garres 98]

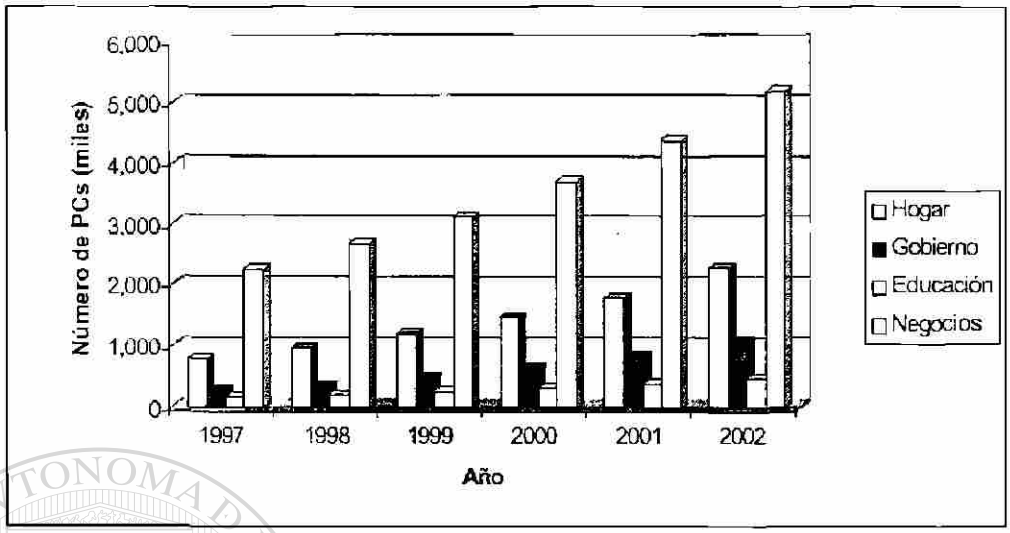


FIGURA 4.6: Base instalada y proyección de PCs en México por sector [Garres 98]

	1997	1998	1999	2000	2001	2002
Hogar	786,068	983,247	1,218,163	1,488,603	1,814,467	2,311,417
Gobierno	263,331	360,563	484,707	649,609	856,178	1,087,726
Educación	175,554	212,096	255,109	309,338	372,251	453,219
Negocios	2,286,127	2,686,007	3,144,201	3,739,204	4,402,127	5,212,019
Total	**3,511,080**	**4,241,912**	**5,102,180**	**6,186,753**	**7,445,023**	**9,064,381**

TABLA 4.2: Base instalada y proyección de de PC's en México

Las estadísticas anteriores muestran un comportamiento creciente en el número de computadoras en los diversos sectores haciendo un especial énfasis en el hogar. Este crecimiento permitirá tener a un número mayor de mexicanos conectados a la red, con lo cual se espera un desarrollo similar en el comercio electrónico en México tanto en sitios nacionales como internacionales.

País	Fecha	Número de Habitantes	Fuente
México	1997	93,716,332	INEGI

TABLA 4.3: Número estimado de habitantes en México [INEGI1 00]

Aproximadamente el 3.75% de los mexicanos en 1997 tienen acceso a Internet lo cual se encuentra muy por debajo del 25% aproximadamente de los norteamericanos.

Es por ello que se deben ampliar las iniciativas para impulsar las condiciones necesarias que permitan un mayor número de usuarios de Internet.

4.3 Antecedentes de Internet II en México

Siguiendo el desarrollo mundial de redes de datos de mayor capacidad y velocidad para utilizarlas en aplicaciones de alta tecnología, y en un esfuerzo conjunto, el Gobierno Mexicano, la Comunidad Universitaria y la Sociedad Mexicana en general, tomaron la iniciativa de desarrollar una red de alta velocidad y unirse a la red internacional denominada Internet II, con el fin de dotar a la Comunidad Científica y Universitaria de México de una red de telecomunicaciones que le permita crear una nueva generación de investigadores, dotándolos de mejores herramientas que les permitan desarrollar aplicaciones científicas y educativas de alta tecnología en el ámbito mundial. [CUDI_MX1 99]

Entre los actuales miembros de CUDI están [CUDI_MX2 99]:

En su carácter de Asociados Académicos:

- Instituto Politécnico Nacional (IPN), Instituto Tecnológico de Estudios Superiores de Monterrey(ITESM), Universidad Autónoma de Nuevo León (UANL), Universidad Autónoma Metropolitana (UAM), Universidad de Guadalajara (U. de G.), Universidad de Las Américas - Puebla (UDLA-P) y Universidad Nacional Autónoma de México (UNAM)

Los miembros actuales en su carácter de Asociados Institucionales:

- Consejo Nacional de Ciencia y Tecnología (CONACYT) y Teléfonos de México, S. A. de C. V. (TELMEX)

Como Afiliados se encuentran:

- Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE), Universidad Anáhuac del Sur (UAS), Universidad Autónoma de Tamaulipas (UAT), Universidad de Colima (UCol), Universidad Iberoamericana (UIA), Instituto Tecnológico Autónomo de México (ITAM), Universidad Autónoma de Coahuila (UAC), Universidad Autónoma de Chihuahua (UACH), Universidad Tecnológica de México (UNITEC) y Universidad del Valle de México (UVM)

4.4 Ejemplos de Sitios en México

México aunque a un paso menos acelerado ha incursionado con una gran diversidad de sitios en Internet que permiten realizar intercambios de productos, servicios o información, tanto bajo los esquemas de comercio electrónico negocio a persona o negocio a negocio. Entre los cuales están los siguientes:

Existen dentro de la industria financiera como www.bancomer.com www.bital.com.mx o www.banamex.com.mx. Este último permite realizar operaciones bajo el enfoque de negocio a persona o negocio a negocio.

El portal financiero de BANAMEX fue el primero en su tipo. Actualmente ofrece 3 tipos de servicios de comercio electrónico: Bancanet, Banamex Plaza y EDI. Adicionalmente permite a los usuarios tener una cuenta de correo

electrónico y pone a su disposición información bursátil, del tipo de cambio y sobre los productos y servicios que ofrece el corporativo.

Mediante Bancanet Banamex permite realizar el servicio de banca por Internet, entre las operaciones permitidas están la consulta de saldos, estados de cuenta, manejo de chequeras, pagos, trasferencias entre cuentas, inversiones, etc.

BANAMEX a través de su servicio EDI Financiero permite realizar transacciones de comercio electrónico a través de EDI (Electronic Data Interchange). Este servicio permite realizar de forma programada y automática el pago a los proveedores de forma segura. [BNX_EDI 99]

Banamex Plaza funciona como un centro comercial permitiendo realizar compras en línea con distintos proveedores que a través del sitio dan a conocer sus productos. De igual forma, www.visa.com.mx, quien desarrolló el protocolo de SET para realizar pagos electrónicos de forma segura, el cual se detalla más adelante, menciona que muchas instituciones financieras en el mundo están ya ofreciendo este servicio a sus clientes. En el caso de México, Banamex, Bancomer, Banorte, BBV y Citibank han anunciado públicamente que están trabajando para habilitar este servicio. [VISA_MX 99]

La empresa PROSA (Promoción y Operación, S.A. de C.V., www.prosa.com.mx) es la única empresa en México especializada en el Switch de transacciones electrónicas de medios de pago. Se encuentra formada entre otros bancos por Serfin, Banorte, Citibank, Bital, INVERLAT, BBV, etc.

Actualmente PROSA permite realizar comercio electrónico seguro a través de PROCOMM utilizando como tecnología base a SET (Secure Electronic Transaction) y Secure Socket Layer (SSL).

Existen empresas como www.decompras.com.mx y www.deremate.com.mx que permiten realizar compras en línea o subastas de diversos productos promocionados a un precio menor y en ocasiones sin costo de envío. Adicionalmente utiliza el concepto de cupones de descuento los cuales son recibidos por correo electrónico.

En el caso de servicios tenemos a www.yoyomedia.com, empresa que ofrece programas de lealtad de puntos y mercadotecnia directa por Internet.

Entre las formas de obtener puntos están: la lectura de correo electrónico, visitas a páginas, para posteriormente cambiarlos por productos o con otros programas de puntos como Banamex.

Estos sitios permiten comprobar la diversidad de sitios de comercio digital ofrecidos en México.

4.5 Aspectos Legales en México

Sobre los aspectos legales ya se ha comentado con anterioridad y ahora es necesario profundizar en cuanto a los aspectos legales en el caso específico de México referente al comercio electrónico, ya que no existe un marco legal suficiente.

El día 17 de mayo de 1999, fue publicado en el Diario Oficial de la Federación un decreto que reforma diversas disposiciones en materia penal. En dicho decreto, se modifica entre otros el Titulo Noveno "Revelación de secretos y acceso ilícito a sistemas y equipos de información" en su Capítulo II "Acceso ilícito a sistemas y equipos de informática".

El artículo 211 de forma general se refiere a actividades o actos que sin autorización o con autorización, indebidamente copien, modifiquen, destruyan o

provoquen pérdida de información, de archivos, sistemas o equipos informáticos.

Al que sin autorización conozca o copia información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad.

Según [Marín 99] es preocupante para los técnicos y profesionales del campo informático saber de estas nuevas regulaciones pues lo que expresan, aparentemente es un conocimiento parcial del modo informático de operar.

Los profesionales de la informática que realizan labores de construcción y mantenimiento deben de seguir lineamientos que permitan garantizar la confiabilidad de los programas. En caso de ocurrir un error en la ejecución del software es necesario determinar la responsabilidad de los integrantes del equipo, ya que la pérdida de información ocasiona pérdida en las ganancias de las empresas. Aun cuando se considere que los humanos no estamos exentos de errores.

Adicional, a la responsabilidad mencionada anteriormente, se requiere determinar si existe mala fe o dolo en los errores de los sistemas, en cuyo caso las penas deben de ser mayores y se debe castigar con mayor severidad.

La propuesta según [Marín 99] es incorporar el concepto de "intencionalidad", así como los atenuantes comentados como son el grado de importancia de la acción sancionada y la reposición o reconstrucción de la información dañada. No solo el fraude debe incluirse en una legislación integral para el comercio electrónico, es necesario considerar conceptos de propiedad intelectual, aceptación de firmas digitales en sustitución de las comunes, el establecimiento de las autoridades certificadoras, definiendo sus roles, funciones y responsabilidades.

El Banco de México y la AMECE (Asociación Mexicana de Estándares de Comercio Electrónico) se encuentran trabajando para definir el marco legal, económico, de infraestructura y estándares requeridos para el desarrollo del comercio electrónico en México. Es necesario incluir a las instituciones financieras y educativas en la definición de los nuevos procedimientos ya que no es únicamente un asunto de negocios, sino también económico, político, social y científico.

El Grupo de Trabajo Multisectorial para impulsar la legislación del Comercio Electrónico (GILCE) [AMECE2 99] integrado por la Asociación Nacional del Notariado Mexicano (ANNM), la Asociación Mexicana de Estándares para el Comercio Electrónico (AMECE, www.amece.com.mx), la Asociación Mexicana de Tecnologías de Información (AMITI), Asociación de Banqueros de México (ABM), tiene el objetivo de ayudar a la definición de los requerimientos nacionales en materia de Comercio Electrónico, incluyendo reformas a los códigos civiles del Distrito Federal, Código de Comercio y del Código Federal de Procedimientos Civiles.

CAPITULO 5

5 Análisis de Riesgo

5.1 Introducción

Existen preguntas cruciales al realizar transacciones por Internet como son: ¿Que pueden perder al hacer uso de Internet los clientes, comerciantes y bancos?, ¿En quien deben confiar? Y ¿Quién toma el riesgo?. [Camp 97]

Ante estas preguntas, es necesario establecer una estrategia de comercio electrónico que permita identificar las oportunidades y los posibles riesgos a los que se enfrentarán las empresas.

Este ejercicio para identificar las amenazas, costos y beneficios permitirá tomar la decisión de entrar o no al comercio electrónico. Es por ello que a continuación se presenta un procedimiento para evaluar los riesgos y establecer un plan para su administración.

En cualquier proyecto de implantación o desarrollo de sistemas es necesario realizar un plan de administración de riesgos.

El plan generalmente incluye actividades como la identificación y cuantificación de riesgos, la realización de un plan de acción para minimizar los riesgos y planes de contingencia para mitigar el impacto en caso de que ocurran los riesgos. Normalmente la administración de los riesgos se realiza antes, durante y después del proceso de implantación o desarrollo de sistemas.

Un proyecto de implantación o desarrollo de comercio electrónico tanto en el ámbito tecnológico o de negocios, requiere un análisis de los posibles riesgos. Se deben incluir aspectos de negocios, tecnológicos, recursos humanos, sociales y económicos.

A continuación se presentan los lineamientos [PMBOK1 WWW] y descripción de algunos posibles riesgos en un plan general de administración de riesgos para un proyecto de negocios electrónicos.

No se detallan e incluyen todos los riesgos por restricciones del alcance del presente trabajo y se hace especial énfasis en aspectos tecnológicos y relacionados a la seguridad computacional, requerida para realizar comercio electrónico entre dos entidades productivas a través de Internet.

El análisis de riesgo del comercio electrónico comienza con la inclusión de un análisis previo y con alcance limitado, el cual debe determinar los riesgos económicos y de negocio en caso de no incursionar en el comercio electrónico.

Este marco conceptual define una estrategia para el comercio digital de una organización, la cual debe estar alineada a la estrategia del negocio.

Los resultados presentados en este estudio permitirán apoyar la toma de decisiones sobre la definición y ejecución de planes de acción para el cambio a este nuevo modelo de negocios.

Cabe mencionar que el objetivo de este estudio esta enfocado al análisis de riesgos del comercio electrónico y no al riesgo asociado al proyecto de desarrollo o implantación de un sistema de comercio digital.

Existen cuatro fases durante un proceso de administración de riesgos, las cuales se detallan y ejemplifican a continuación:

5.2 Metodología de Análisis del Riesgo

La fase de identificación del riesgo propone como primer paso el conocimiento y alcance del proyecto a realizar.

Esto se logra mediante una revisión de la documentación que dio origen al proyecto como la solicitud de una propuesta (RFP - Request For Proposal) y mediante reuniones con los principales participantes en el proyecto pertenecientes a las diversas áreas del negocio y de la tecnología.

El resultado de este análisis es un documento que describe el proyecto, su alcance y los elementos o condiciones de su origen.

Determinar el alcance de un proyecto y las causas que le dieron origen puede ser un buen principio para el análisis del riesgo.

Posteriormente se realiza un análisis de riesgos con los usuarios y personal de sistemas para determinar los posibles riesgos del proyecto. El documento final será una matriz de riesgos como se muestra a continuación:

Identificación de Riesgos				
Id	Descripción del Riesgo	Causas	Probabilidad de Ocurrencia	
			B2C	B2B E
1	• Pérdida de la confidencialidad e integridad de la información	• Transmisión de información por medios no seguros • Penetración en el esquema de seguridad de la empresa • Incorrecta selección de mecanismos, técnicas, algoritmos o protocolos de encripción • Falta de infraestructura de almacenamiento y distribución de llaves públicas	Alto	Medio
2	• Incapacidad para atender órdenes de compra de los clientes	• Falta de capacidad de producción • Problemas en la obtención de insumos • Medios de distribución insuficientes	Alto	Medio
3	• Falta de ventas o distribución por Internet	• Resistencia al cambio y rechazo por parte de los clientes a la compra por Internet	Medio	Medio
4	• Falta de actualización y escalabilidad de la infraestructura, plataforma y aplicación	• Incorrecta selección de la infraestructura, plataforma y herramientas de desarrollo • Selección de tecnologías propietarias o con bajo nivel de soporte	Bajo	Medio
5	• Fracaso de la estrategia de comercio electrónico	• Falta de persona con experiencia, conocimiento y visión en el área de comercio electrónico bajo el enfoque de negocios, tecnología, legal, impuestos, mercadotecnia, etc.	Bajo	Medio
6	• Problemas financieros	• Incompleto análisis financiero y económico al no considerar variables financieras y económicas como el flujo de caja, inversiones, costos, ROI, análisis costo/beneficio, etc.	Bajo	Bajo
7	• Pérdida de competitividad y posible salida del mercado	• Falta de análisis sobre la competencia de la empresa • Incorrecta estrategia de mercadotecnia y publicidad	Medio	Bajo

TABLA 5.1: Matriz de Identificación de Riesgos

Después de realizar la identificación de riesgos con las causas asociadas y determinar la probabilidad de ocurrencia es necesario cuantificar el impacto del riesgo al negocio en caso de que este se presentara.

La cuantificación de un riesgo en el comercio electrónico depende de la pérdida que pueda ocasionar.

Por ejemplo, se puede permitir cuantificar como riesgo de bajo impacto la pérdida independiente o individual de una compra bajo el esquema de micro

pagos durante la visita a un sitio en Internet, pero no aplicaría la misma cuantificación a una transacción bancaria de montos extremadamente grandes.

Recordemos que para que exista un impulso o un potencial riesgo de romper la seguridad o penetrar un sistema debe existir una jugosa ganancia, el esfuerzo es directamente proporcional a la ganancia o beneficio a obtener, sin descuidar el hecho de que existen personas que únicamente realizan los intentos por fama, amor o ego para demostrar su conocimiento.

El riesgo asociado se basa en la cantidad que una empresa esta dispuesta a perder con relación a la posible ganancia, aunque esto puede ser considerado como una apuesta, no lo es, ya que se basa en un estudio de costo/beneficio que determinará la posible pérdida con el estimado de beneficios o ganancias a obtener.

Es necesario identificar el costo que tendrá la ocurrencia del riesgo con base a las variables de tiempo, calidad, recursos y dinero. Identificando las oportunidades a seguir y a las amenazas a responder o las oportunidades a ignorar y las amenazas a aceptar. A continuación se presenta el complemento a la matriz de riesgos presentada en la sección anterior:

Identificación de Riesgos			
Id	*Consecuencias de ocurrir el riesgo*	*Impacto en el Negocio*	
		B2C	*B2B-B*
1	• Pérdida de la confianza por parte de los usuarios para la compra vía Internet • Mala imagen en el mercado y pérdida de competitividad	Medio	Alto
2	• Pérdida de la oportunidad de venta e insatisfacción del cliente	Medio	Bajo
3	• Problemas financieros y de capacidad de expansión	Bajo	Bajo
4	• Saturación de la capacidad del sistema, necesidad inversiones grandes para el reemplazo de la tecnología	Bajo	Alto
5	• Problemas legales, de impuestos y de negocio	Medio	Alto
6	• Liquidez y posible quiebra	Alto	Alto
7	• Reducción de la participación del mercado y posible quiebra	Medio	Medio

TABLA 5.2: Matriz de Cuantificación de Riesgos

Durante el proceso de administración de riesgos es necesario desarrollar planes de respuesta a los riesgos.

Uno de estos planes se concentra en la prevención de la ocurrencia de los riesgos. Algunas actividades permiten minimizar la posibilidad de aparición del riesgo.

De igual forma, es necesario realizar un plan de contingencias para minimizar el impacto de los riesgos riesgo cuando estos se presenten.

Para iniciar la planificación de actividades para minimizar la ocurrencia y el impacto es necesario establecer prioridades a cada uno de estos riesgos de acuerdo a la siguiente figura:

FIGURA 5.1: Criterios de Valores para Analizar el Riesgo---

Para nuestro ejemplo de comercio electrónico tenemos las siguientes figuras:

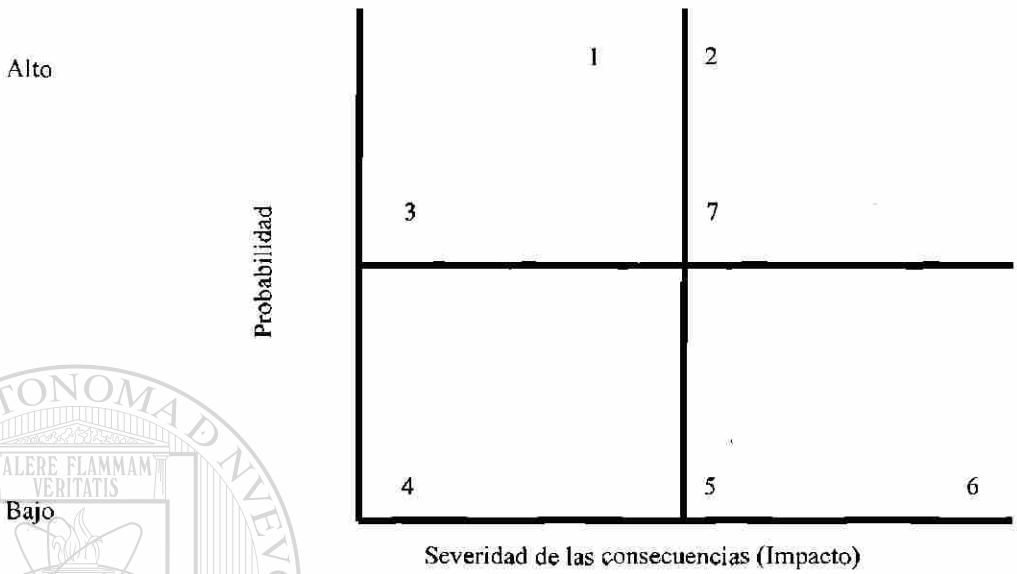


FIGURA 5.2: Valores del Riesgo para B2C

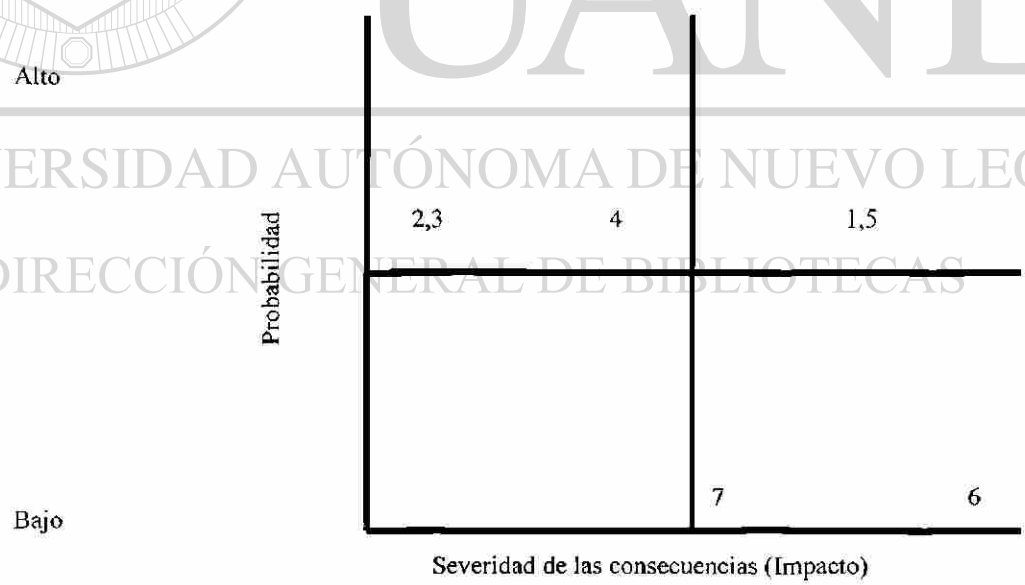


FIGURA 5.3: Valores del Riesgo para B2B-B

Después de realizar la planeación y análisis preliminar, es necesario revisar la documentación obtenida con las áreas involucradas de la empresa al nivel de usuario y de sistemas.

Es necesario establecer periodos regulares y establecidos para revisar el status de los riesgos y en caso de algún cambio tomar acciones para minimizar su ocurrencia, o realizar las actividades establecidas en el plan de contingencias en el menor tiempo posible y evitar así mayores consecuencias. Después de las revisiones es necesario realizar cambios o ajustes a los planes de administración de riesgos, con ello es posible que no exista algún impedimento para continuar la operación o el proyecto.

5.3 Conclusiones

El análisis previo pretende ser un ejercicio que cada una de las empresas debe realizar para definir el plan de administración de riesgos, de ninguna manera se considera como un ejemplo representativo o completo. De igual forma, el análisis de riesgos debe ser parte de la estrategia de comercio electrónico.

El plan de administración de riesgos contenido en las matrices debe de ser revisado continuamente, ya que los riesgos y las condiciones varían constantemente.

Los riesgos para el B2C y el B2B-B son diferentes y por tanto debe existir un plan general que los incluya por separado. Entre las diferencias se encuentran: la tecnología utilizada, nivel de seguridad requerido e integración con otros sistemas internos y externos.

De las figuras anteriores podemos determinar para nuestro ejemplo que los riesgos que deben de ser seguidos más de cerca son: la seguridad en la

información (Id 1) y el fracaso de la estrategia de comercio electrónico de la empresa (Id 2); de ahí la necesidad de contar con personal capacitado y experimentado para el desarrollo de la estrategia de negocios y tecnológica.

La decisión de incursionar en un esquema de comercio electrónico debe estar soportada por la estrategia ya que las decisiones que se tomen pueden cambiar el destino de la empresa, tanto en sentido positivo como en el negativo.

CAPITULO 6

6 Problemas de Seguridad en un Sistema Distribuido

6.1 Introducción

Los problemas de seguridad en el comercio electrónico tienen su origen en los sistemas distribuidos, ya que sus características no hacen seguro el acceso a la información. Adicionalmente, el comercio electrónico tiene requerimientos especiales para mantener en forma segura la información. Estos serán analizados a detalle en los próximos capítulos.

Para entender las posibles situaciones de riesgo en la seguridad es necesario conocer algunos conceptos como son los siguientes:

En primer término tenemos que la seguridad computacional trata sobre los procedimientos administrativos y la protección tecnológica aplicados al hardware, software y datos para asegurar en contra de accesos no autorizados ya sean de forma accidental o deliberada para la diseminación de los datos en los sistemas computacionales. [Hsiao 79]

Así mismo, la privacidad computacional concierne a los requerimientos morales y legales para proteger los datos de acceso no autorizado y su

diseminación. Los asuntos involucrados con la privacidad computacional son por lo tanto, decisiones políticas relativas a las personas que tienen acceso a determinada información o el derecho a diseminar cierta información.

> La motivación de la seguridad y la privacidad puede ser encontrada en el deseo de mantener en secreto los asuntos militares, aplicaciones industriales o la compartición de información en las sociedades modernas. La relación entre los asuntos de privacidad y las medidas de seguridad deben estar mostradas en medidas legislativas de seguridad que afectan todos los aspectos de la seguridad computacional. [Hsiao 79]

Debido a las consideraciones de las implicaciones sociales, la legislación determina el tipo de información que es recolectada y por quien, el tipo de acceso y la diseminación, los derechos de autor, las penalidades y los asuntos de licenciamiento. [Hsiao 79]

6.2 Sistema Distribuido

Un sistema distribuido, como lo es Internet, es una colección de computadoras autónomas enlazadas por una red con software diseñado para producir una facilidad computacional integrada. [Coulouris 94]

La aplicación de los sistemas distribuidos va desde aplicaciones bancarias, empresariales, multimedia hasta su utilización para el procesamiento paralelo teniendo a su disposición miles de procesadores a través de Internet para lograr un objetivo común.

Las características clave de los sistemas distribuidos son: el soporte a la compartición de recursos, la apertura, concurrencia, escalabilidad, tolerancia a fallas y transparencia.

En un sistema distribuido existen diversas amenazas y formas de solucionarlas o minimizarlas. [Oppliger 95], [Yahya 97]

- Los canales de comunicación deben ser seguros en contra de escuchas (eavesdropping) e intromisiones (tampering) al contenido del mensaje.
- Los servidores deben ser capaces de verificar la identidad de sus clientes.
- Los clientes deben ser capaces de verificar la autenticidad de los servidores.
- La identidad del origen del mensaje debe ser verificable después de que el mensaje haya sido enviado a un tercero, esto es análogo al uso de firmas en los documentos convencionales.

Los métodos disponibles para alcanzar los objetivos mencionados anteriormente están basados en el uso de criptografía para proteger a los mensajes mediante un servicio de distribución de llaves para permitir a un par de procesos establecer un canal de comunicación seguro.

Utilizando llaves para la encripción de los mensajes junto con un servicio de autentificación que permita a los clientes, servidores y otras entidades de comunicación proveer al otro evidencia convincente de su identidad. [Chew 97]

Como ejemplo de un servicio de distribución de llaves y servicios de autentificación tenemos al Kerberos, el cual realiza funciones tanto de autentificación como de distribución de llaves.

Las entidades involucradas en un proceso de autentificación son: la aplicación cliente, la aplicación servidor y el servidor de autentificación Kerberos o el centro de distribución de llaves.

Una debilidad del Kerberos es que el mensaje inicial de la aplicación no es encriptado hacia el servidor de autentificación y esto permite a un intruso escuchar y recolectar los tickets enviados [Chew 97].

Aunque esta vulnerabilidad es difícil de explotar debido a la composición del ticket y la dificultad de suplantar la identidad de un proceso o usuario.

El uso de Kerberos es inapropiado para Internet debido al extenso uso de mensajes entre procesos requeridos para la autentificación. [Chew 97]

Bajo el enfoque de seguridad un sistema distribuido puede verse en dos vertientes:

- La primera es que los sistemas distribuidos son inseguros
- Y la segunda es que los sistemas distribuidos pueden poner en riesgo a los otros sistemas distribuidos mediante el uso del paralelismo y distribución de cargas de trabajo.

Por ejemplo distributed.net [DISTRIBUTED_NET 99] tiene como misión:

"El desarrollar software abierto, fácilmente portable, altamente adaptable, así como redes y demás infraestructura necesaria para soportar el software. Conduciendo y soportando activamente la investigación del computo distribuido de todos tipos".

"Nosotros desplegamos nuestro software para formar una computadora distribuida globalmente e inmensa para resolver problemas de gran escala y proveer un conjunto accesible de poder computacional para proyectos que así lo requieran". [DISTRIBUTED_NET 99]

Las amenazas de seguridad pueden ser descritas en la siguiente taxonomía según:

Amenaza	Descripción
Física	Robo de componentes y sistemas
Debilidades de losSistemas	Aprovechamiento de las debilidades o huecos de seguridad de los sistemas operativos u otros programas los cuales se explotan para obtener acceso no autorizado a los sistemas
Programas malignos	Un perpetrador inserta programas malignos o malévolos (Ej. virus) en un sistema con la intensión de causar daño o destrucción de la información manejada por un Sistema
Accesos legítimos	Usurpación legítima de la identidad de un usuario mediante la adquisición de derechos de acceso a través de trampas de passwords o descifrado de passwords para tener acceso a los recursos de los sistemas
Basados en comunicaciones	Las redes de comunicación dan oportunidad para el acceso ilegal a información como el eavesdropping (escuchar indiscretamente), IP spoofing (sustitución de la fuente origen de paquetes), etc.

TABLA 6.1: Tipos Básicos de Amenazas. [Jayaram 98]

La administración de la seguridad computacional requiere de dos enfoques como son los accesos físicos y los lógicos. Es por ello que presentamos brevemente una descripción de los riesgos que se pueden presentar, de igual forma se menciona la seguridad operacional.

Las acciones de prevención y respuesta a problemas de seguridad deben estar consideradas desde aspectos físicos, operacionales y lógicos para ello es necesario establecer los lineamientos, normas y procedimientos para la contabilidad, niveles de control, tipos de controles (en términos de clasificación de datos y configuración del sistema, flujos de información e inventarios) y reglas.

En cuanto a la seguridad física, ésta considera los aspectos relacionados con la seguridad en las instalaciones, control de acceso de personal y el manejo del equipo físico, incluyendo software, hardware y comunicaciones, prevención y recuperación de pérdida debido a desastres naturales, interferencia electromagnética y electrónica y entrada maliciosa y destrucción, entre otros.

Deben existir medidas de prevención y de recuperación debido a amenazas tanto internas como externas, las cuales son parte de la seguridad operacional. Para estas amenazas e intrusiones, las causas, efectos y significados deben de ser estudiados.

Aspectos más complejos de la seguridad operacional incluyen el análisis de riesgos mencionado anteriormente, la evaluación y el aseguramiento. Conociendo los riesgos involucrados, la seguridad operacional puede ser expresada en términos de indicadores cuantitativos, factores de costo y opciones.

En cuanto a la seguridad lógica mediante la identificación y autentificación apropiada, un usuario puede ganar acceso a un sistema computacional.

La identificación y autentificación pueden ser obtenidas de la siguiente forma:

- a través de algo que el usuario conozca (como un password simple o complejo, passwords de una vez, handshaking a través de una sesión de preguntas o respuestas o a través de una invocación dinámica de un programa)
- a través de algo que el usuario porte (llaves, tarjetas de banda magnética o badges)
- a través de características físicas o biológicas del usuario (voz, huellas dactilares o la geometría de la mano, o la cara).

6.3 Aspectos Críticos de la Seguridad en el Comercio Electrónico a través de Internet

Cada día un número mayor de personas utilizan Internet para intercambiar información, bienes y servicios de forma segura.

Uno de los principales riesgos al incorporar la tecnología de Internet al comercio electrónico es la falta de seguridad para intercambiar información entre dos entidades, mediante un medio no seguro como lo es Internet, ya que desde su origen la seguridad no fue considerada como un punto relevante en su diseño. [Russ 97], [Sheperd 96], [Deswarte 97]

El riesgo de utilizar Internet como medio para realizar transacciones electrónicas seguras es minimizado si se utilizan los mecanismos, técnicas y algoritmos adecuados.

Es por ello, que es necesario realizar un análisis profundo y continuo sobre los algoritmos y protocolos utilizados en el desarrollo de proyectos de comercio electrónico.

En los capítulos subsecuentes se presentan los conceptos necesarios para entender los mecanismos, técnicas, algoritmos y protocolos para el desarrollo de un proyecto de comercio electrónico.

CAPITULO 7

7 Mecanismos de Seguridad del Comercio Electrónico

7.1 Introducción

Para minimizar el riesgo al realizar comercio electrónico entre dos entidades es necesario considerar cuatro aspectos básicos de la seguridad. El primero es la autentificación [Chew 97], [Baldwin 97], [Lu 92] que determina la identidad de las entidades participantes. El segundo es la confidencialidad [Baldwin 97], [Carter 98] que asegura la privacidad de la información.

Mediante la integridad [Baldwin 97] se garantiza el mensaje evitando la modificación de información. Y por último con la no - repudiación [Chew 97] se logra evitar el desconocimiento de envío y recepción de un mensaje. Ahora analicemos con mayor detalle los mecanismos y técnicas que garantizan estos cuatro aspectos.

7.1.1 Autentificación

La autentificación es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información; estas entidades pueden ser personas, procesos o computadoras.

Existen varias formas de autentificación como son:

- Autentificación basada en claves o passwords
- Autentificación basada en direcciones
- Autentificación criptográfica

La verificación de la identidad mediante claves o passwords se realiza mediante la compartición de una contraseña (password), el cual se envía a una entidad para validar el conocimiento del mismo. Cuando se utiliza el método basado en direcciones se asume la identidad de la fuente inferida de la dirección de red contenida en los paquetes que se envían.

Estos dos métodos presentan debilidades ya que es posible escuchar la información enviada o la pretensión de ser otra persona. Los protocolos de autentificación criptográfica son más seguros que los anteriores.

La idea básica es que se prueba la identidad al realizar una operación criptográfica en una información proporcionada por alguna o ambas entidades participantes.

Desde otra perspectiva existen 3 formas de lograr la autentificación [SecurityDynamics WP] como se ha mencionado:

- Lo que es uno
- Lo que se conoce
- Lo que se tiene

Como ejemplos de estas formas de autentificación tenemos: las huellas digitales, la retina y la voz (lo que es uno: biometría). Por el lado están los passwords (lo que se conoce, siendo lo más utilizado en la actualidad) y por último un disco, una llave o un certificado digital (lo que se tiene). [Chew 97]

La autentificación fuerte [Lobel 99] asegura que una organización permita únicamente a los usuarios autorizados el acceso a los recursos corporativos.

Esta autentificación se logra mediante el uso de al menos dos de las tres formas de autentificarse mencionadas anteriormente y es común la utilización de la autentificación biométrica.

La autentificación biométrica permite la identificación de una persona basada en sus atributos físicos. Básicamente se utilizan la huella digital, el reconocimiento de voz, la retina (el patrón Vessel de sangre), la dinámica de la firma (velocidad, dirección y presión) y el reconocimiento del iris, entre otras.

Estas tecnologías que permiten identificar a una persona deben cumplir ciertas características mencionadas a continuación para un sistema biométrico efectivo:

- La *precisión* es la característica más crítica de un sistema de verificación e identificación biométrica. El sistema debe separar con toda precisión a las personas autenticas de los impostores. Se debe considerar dentro de l precisión la tasa de rechazo errónea. Esta es generalmente un porcentaje en la cual las personas auténticas son rechazadas como no identificadas por el sistema biométrico.
- Algunas veces es denominado error del Tipo I. Un rechazo de este tipo puede traer efectos negativos como frustración o impedimento para realizar operaciones. Por ejemplo una persona auténtica no puede realiza una operación bancaria debido a que el sistema no la reconoce
- La *tasa de aceptación errónea* es un porcentaje en el cual un impostor es aceptado como autentico por el sistema biométrico. Es conocido como error del tipo II y es el error más importante.
- Debe existir un balance entre estas dos medidas y es ajustado mediante un dispositivo de sensibilidad que contienen la mayoría de los sistemas biométricos
- Otra característica de los sistemas biométricos es la *velocidad* la cual es la capacidad de procesamiento de datos y generalmente es de 5 segundos para el proceso completo de verificación de la identida

TABLA 7.1: Características de un Sistema Biométrico para Autentificación

La aceptación de los dispositivos por parte de los usuarios también debe ser considerada para la selección del sistema biométrico. [Krause 99]

Debido a la disminución de los costos de los equipos biométricos, cada vez se utilizan más con el consecuente aumento de la seguridad otorgada por este método de autentificación.

Las funciones de verificación biométrica pueden ser incorporados por ejemplo: a los cajeros automáticos, terminales punto de venta y computadoras personales. [Stockel 95]

Cada método mencionado anteriormente tiene un nivel distinto de autentificación como se muestra en la siguiente figura, y este corresponde al valor de la información que esta siendo protegida. [SecurityDynamics WP]

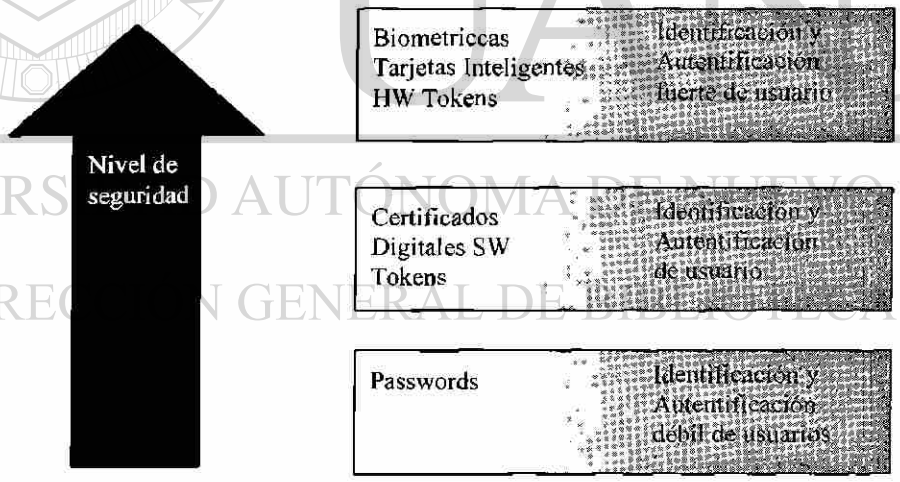


FIGURA 7.1: Niveles de Seguridad

Es importante mencionar el uso de certificados digitales [Kapidzic 95], [Winslett 99] los cuales hacen la función de una credencial de identificación de una persona.

Estos certificados son emitidos por una autoridad certificadora la cual verifica la identidad mediante un soporte documental de la persona o entidad interesada. [Hsu 98]

La autoridad certificadora deber ser una tercero confiable cuyo rol sea [Carter 98], [Kapidzic 95]:

> "Ser el responsable de la generación y distribución de las llaves, y garantizar la autenticidad de las llaves."

Este rol en los sistemas criptográficos de llave pública es muy importante ya que es difícil validar la autenticidad de una llave pública y esto es logrado mediante la certificación de la llave por alguna entidad registrada como autoridad certificadora. [Carter 98], [Chen 95]

Es posible que en un sistema de criptografía asimétrico, la llave pública sea interceptada y enviada otra llave pública del intruso para capturar y descifrar los mensajes. Esto es un ataque activo donde la llave pública es modificada o cambiada para después escuchar los mensajes y descifrarlos.

Adicionalmente al problema de la seguridad de las llaves o certificados, la administración de las llaves es un problema debido a la necesidad de accesarlas en cualquier momento y lugar.

En ocasiones es difícil la replicación de las llaves y llevar un control de versiones ya que algunos certificados tienen caducidad y es necesario regenerarlos.

Por otro lado si un certificado es revocado entonces es necesario notificar a las autorizadas certificadoras.

Las firmas digitales tienen la función de autentificación y verificación de la integridad de la información. Como se vera más adelante, esto es logrado mediante el uso de la criptografía pública.

Si la identificación y autentificación utilizan las firmas digitales, entonces se requiere de certificados. Estos pueden ser otorgados por una organización o un tercero de confianza.

La infraestructura comercial de llaves publicas esta emergiendo en conjunto con la comunidad de Internet. Los usuarios pueden obtener certificados con varios niveles de aseguramiento.

Por ejemplo los certificados de nivel 1 verifican la dirección de correo electrónico. El nivel 2 verifica el nombre de usuario, su dirección, número de seguro social y otra información contra una base de datos del buró de crédito. El nivel 3 está disponible para compañías.

Este nivel provee identificación por fotografía adicional a los elementos del nivel 2. Una vez obtenido el certificado digital entonces puede ser cargado a una aplicación de correo electrónico o aun navegador de Internet (Web Browser).

Muchos de los servidores y navegadores de Internet incorporan el uso de certificados digitales. Mediante SSL 3.0 se pueden autentificar tanto el cliente como el servidor.

Los certificados utilizados están basados en el estándar de X.509 el cual describe al poseedor del certificado y el periodo de validez entre otra información. [Krause 99]

Los protocolos de autentificación son la base de la seguridad en muchos de los sistemas distribuidos y es por tanto esencial asegurar que esos protocolos funcionen correctamente.

Desafortunadamente, su diseño ha sido extremadamente propenso a errores. A pesar de que los protocolos de autentificación típicamente tienen pocos mensajes, la composición de cada mensaje puede ser sutil y las interacciones entre mensajes pueden ser complejas.

Los diseñadores de protocolos comúnmente comprenden o interpretan erróneamente las técnicas existentes, copiando las ventajas de los protocolos existentes de forma inapropiada.

Como resultado de ello, muchos de los protocolos encontrados en la literatura contienen defectos de seguridad o redundancia. Para complicar esto, los protocolos utilizan diferentes criptosistemas. [BURROWS 90]

7.1.2 Confidencialidad

La confidencialidad es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipular dicha información. Un servicio de confidencialidad es designado para evitar la disponibilidad del tráfico de un mensaje a entidades o usuarios no autorizados. Los usuarios pueden ser una persona, un proceso, un programa, etc.

Esta característica de la información debe asegurar que ninguna entidad no autorizada entienda la información. Para lograr esto se utilizan las técnicas de encripción o codificación de datos, mediante las cuales se codifica un mensaje de tal forma que no pueda ser entendido por el ser humano o descifrado por un equipo computacional.

El nivel o grado de confidencialidad debe estar en relación con la importancia de la información. Debe existir un balance entre el esfuerzo requerido para obtener la información decodificada y la ganancia que se obtendría con ello.

La confidencialidad debe incluir el tiempo de diseminación de la información por ejemplo, el presupuesto anual de una empresa tendría una vigencia de un año. [Krause 99]

7.1.3 Integridad

La integridad de la información corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales.

Las firmas digitales codifican un mensaje de tal forma que mediante una función hash (la cual es similar a un Checksum) calcula un resumen único (message digest) del mensaje original.

Esta función solo es de una vía, esto es que no existe reversión del procedimiento de cálculo, con lo cual no es posible determinar el mensaje original a partir del digest. Una buena función hash debe detectar el más mínimo cambio en el mensaje original.

La validación de la integridad del mensaje se da al aplicar al mensaje original la misma función hash y comparar el resultado con el resumen (message digest) recibido.

El objetivo de verificar la integridad es debido a la preocupación para mantener la información sin modificación o modificada por usuarios autorizados.

Los servicios de no-repudiación ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información.

Esta característica garantiza que la persona o entidad que envía un mensaje no pueda rechazar el envio o recepción de un mensaje. Es necesario este mecanismo debido al proceso de comercio electrónico de envío y recepción de información para garantizar la realización de las transacciones para ambas entidades participantes.

Existen dos lados de la no-repudiación, un lado es relevante para el emisor, conocido como no-repudiación de origen, para asegurar que el emisor no pueda negar el envío del mensaje.

El otro lado es del receptor, conocido como no-repudiación del receptor, para asegurar que el receptor no pueda negar la recepción del mensaje. [Yan 97]

Mediante las técnicas de autentificación se garantiza la no-repudiación debido a la utilización de la llave privada de cada entidad.

Aquí se presenta un conflicto debido a la falta de privacidad al validar al emisor y receptor. El seguimiento de una información o mensaje desde su origen hasta su destino es requerido para garantizar la seguridad y para cuestiones de auditoria y aspectos legales.

El problema es el uso indiscriminado, ya sea en total ausencia o permitiendo acceso en cualquier punto a toda la información.

Es necesario identificar la información que debe conocer cada una de las entidades participantes en el proceso de comercio electrónico y con ello permitir la privacidad de forma fraccionada a las partes autorizadas para su uso.

7.2 Conclusiones

La combinación de la autentificación, confidencialidad, integridad y no-repudiación como mecanismos de seguridad, descritos anteriormente, permite garantizar con un cierto grado de confiabilidad la seguridad en una transacción electrónica.

Para minimizar los riesgos del comercio electrónico en Internet es necesario conocer algunos conceptos, técnicas y algoritmos que permitan implementar un sistema de seguridad.

El siguiente capítulo explica las técnicas utilizadas por la criptografía, las cuales permiten aumentar el grado de confianza en las aplicaciones de comercio electrónico.

CAPITULO 8

8 Técnicas de Seguridad

8.1 Introducción

Para entender la seguridad en el comercio electrónico es necesario conocer y entender los siguientes básicos:

La Criptología (del griego criptos = oculto y logos = tratado, ciencia) es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias:

- Criptografía
- Criptoanálisis

La Criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial.

El Criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original.

Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su Criptoanálisis correspondiente. [Fúster 98]

La Criptografía como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Como tal, permaneció durante siglos vinculada muy estrechamente a los círculos militares diplomáticos, puesto que eran los únicos que en principio tenían auténtica necesidad de ella.

En la actualidad la situación ha cambiado drásticamente: el desarrollo de las comunicaciones electrónicas, unido al uso masivo y generalizado de las computadoras, hace posible la transmisión y almacenamiento de grandes flujos de información confidencial que es necesario proteger.

Con la introducción del comercio electrónico y sus requerimientos de proteger la información, cuando la Criptografía pasa de ser una exigencia de minorías a convertirse en una necesidad real del hombre común, que ve en esta falta de protección de sus datos privados una amenaza para su propia intimidad.

El esquema fundamental de un proceso criptográfico (cifrado/descifrado) puede resumirse como se muestra en la siguiente figura [Fúster 98]:

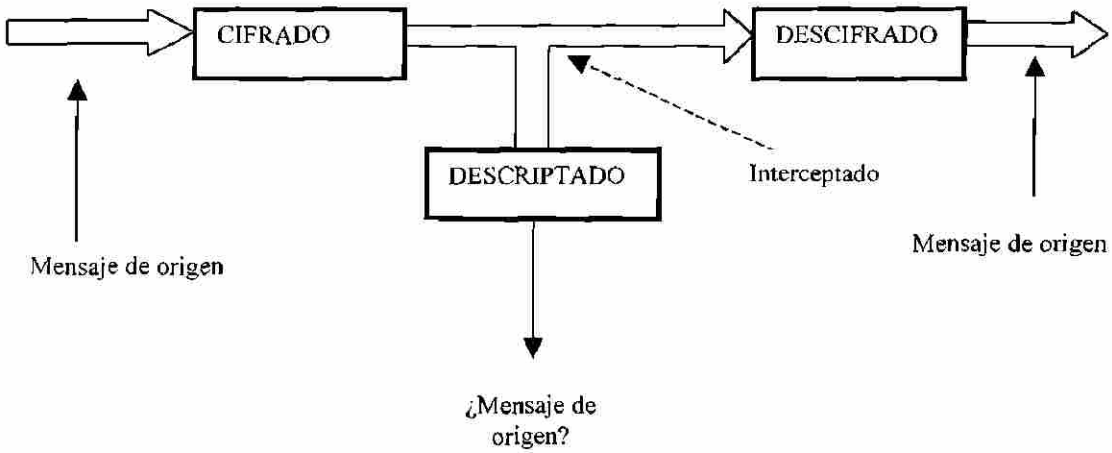


FIGURA 8.1: Proceso general de cifrado/descifrado

A y B son, respectivamente, el emisor y receptor de un determinado mensaje. El emisor A transforma el mensaje original (texto claro o plano), mediante un procedimiento de cifrado controlado por una clave, en un mensaje cifrado (criptograma) que se envía por un canal público.

En recepción B, con conocimiento de la clave transforma ese criptograma en el texto original, recuperando así la información original. Un buen sistema criptográfico será por tanto, aquel que ofrezca un cifrado sencillo pero un descifrado (procedimiento de criptoanálisis) imposible o, en su defecto, muy difícil.

La finalidad de la criptografía es mantener la confidencialidad del mensaje y que la información contenida en el criptograma permanezca secreta. Adicionalmente se garantiza la integridad del mensaje para que este no sea modificado, y la identidad del remitente o destinatario.

Anteriormente la seguridad de la Criptografía clásica era probable pero en la actualidad los procedimientos de la Criptografía moderna han de tener una seguridad matemáticamente demostrable. [Anderson 99]

Los principios básicos utilizados en los primeros criptosistemas fueron la sustitución y permutación de la secuencia de caracteres. Pero esto ha cambiado y actualmente se utilizan algoritmos matemáticos más complejos.

El tipo particular de transformación aplicada al texto claro o las características de las claves o llaves utilizadas marcan la diferencia entre los diversos métodos criptográficos. Teniendo así la siguiente clasificación.

8.2 Métodos Simétricos o Criptografía de Llave Secreta

Este esquema de encripción es llamado simétrico [Rajsbaum 99], [Fúster 98] debido al uso de la misma llave para encriptar y desencriptar un mensaje.

Esto es que el emisor y el receptor tienen una llave secreta compartida conocida por ambos.

El algoritmo más conocido es el DES (Data Encryption Standard) [RSA 99], [DES_FIPS_ 46-1 88]. Inventado por IBM y adoptado como un estándar por el gobierno de los EUA a finales de los 70's. DES es rápido, seguro y confiable. Aunque actualmente la fortaleza de DES con una llave de 56 bits de longitud se ha puesto en tela de juicio, debido al potencial existente de los sistemas distribuidos los cuales trabajan colaborativamente para romper el algoritmo, logrando un tiempo menor a 3 meses para desencriptar el mensaje. Con esto se han propuesto variantes como el Triple – DES. [DES_FIPS_46-3 99]

Debido a estos logros de ruptura del algoritmo DES, se iniciaron esfuerzos para diseñar algoritmos más seguros y libres de las restricciones de exportación. La National Institute of Standards and Technology (NIST) lanzo la convocatoria Advanced Encryption Standard Development Effort [AES 99] con la idea de seleccionar el algoritmo que sustituirá al DES.

El hecho de que el emisor y receptor requieran conocer la llave secreta nos lleva al problema del envío de la llave para poder desencriptar el mensaje enviado por un emisor.

La utilización de medios como el teléfono, fax o correo electrónico son lentos y sujetos de ataques, es por eso que se utilizan algoritmos de llave pública o asimétricos para el envío de la llave y posteriormente se utilizan los algoritmos de llave simétrica como el DES.

8.3 Métodos Asimétricos o Criptografía de Llave Pública

Este esquema de criptografía es el opuesto a la criptografía simétrica, puesto que utilizamos una llave para encriptar y otra diferente para desencriptar.

Anticipadamente se deben crear dos llaves, las cuales están matemáticamente relacionadas de tal forma que cualquier mensaje o texto encriptado con una de las llaves solamente pueda ser desencriptado con la otra y viceversa.

Una de las llaves debe ser designada para ser privada o secreta y la otra para ser pública y dada a conocer a todas las personas interesadas en enviar algún mensaje encriptado. Basado en la premisa de que no es posible derivar la llave secreta a partir de la pública o al revés.

Una de las desventajas de este esquema de encripción es el problema de la lentitud del cálculo ya que un algoritmo asimétrico tarda de 10 a 1000 veces más tiempo de computo que los algoritmos simétricos.

Es de ahí que surja la combinación de ambos métodos. Utilizando los algoritmos asimétricos para enviar la llave única y secreta de los algoritmos simétricos.

Otro conflicto que se genera con los esquemas de criptografía asimétricos es la distribución de las llaves públicas, ya que un impostor puede enviar llaves publicas asumiendo o suplantando la identidad de otra persona y con esto el problema de la autentificación se vuelve a presentar. [Mcclure 98], [PKI 99]

Si el problema de distribución y confianza del origen de la llave público es resuelto, entonces se puede asegurar la identidad del emisor debido a la encripción del mensaje con la llave privada y desencripción con la llave pública correcta. Las autoridades certificadoras realizan el procedimiento de crear los certificados digitales, la administración y envío.

8.4 Firma Digital

El Digital Signature Standard [NIST 92] propuesto por el NIST especifica el Digital Signature Algorithm (DSA) apropiado para las aplicaciones que requieren una firma digital en lugar de escrita. La firma digital DSA es un par de números largos representados en una computadora como cadenas de dígitos binarios. La firma digital es calculada utilizando un conjunto de reglas y un conjunto de parámetros permitiendo la identificación del originador y la integridad de la información.

El DSA incluye la generación de la firma y su verificación. La generación utiliza una llave privada para generar la firma y la verificación de la firma hace uso de la llave pública correspondiente. [Sirbu 97]

Una función hash es utilizada para el proceso de generación de la firma para obtener una versión condensada de los datos y esto es denominado message digest. En el próximo capítulo se explica el funcionamiento del algoritmo MD5, el cual es utilizado para la generación de firmas digitales.

Por lo anterior, una firma digital es un código que es agregado a un mensaje, que puede ser verificado por el receptor para autentificar al creador del mensaje.

Es importante verificar en un sistema de autentificación dos condiciones:

- La firma de un documento de tal forma que la falsificación sea imposible.
- La verificación de que la firma fue realizada por aquel a quien representa.

El temor a los riesgos de seguridad ha creado una demanda de características construidas directamente en los sistemas de comercio electrónico. Los mecanismos y técnicas de seguridad existentes pueden ser combinados para minimizar un gran rango de las amenazas del comercio electrónico. [Baldwin 97]

CAPITULO 9

9 Algoritmos y Protocolos para el Comercio Electrónico

9.1 Introducción

Los algoritmos son procedimientos que detallan un conjunto definido de instrucciones simples que al ser ejecutadas pueden resolver un problema específico. Es importante determinar la cantidad de recursos de tiempo y espacio que requieren los algoritmos para ejecutarse [Weiss 92].

Este análisis de la complejidad de los algoritmos tiene una relación directa con la seguridad que proveen y es otro elemento a considerar en el criptoanálisis. Dado al avance de la tecnología y las ciencias computacionales, algunos algoritmos que antes se creían seguros, ahora ya no lo son y con esto ha quedado al descubierto la vulnerabilidad de los demás algoritmos. Este es el caso específico del algoritmo DES. [DES_CHAL_III 99]

Para resolver estos problemas se están desarrollando algoritmos más seguros, los cuales únicamente puedan ser descifrados mediante la búsqueda exhaustiva o fuerza bruta en un tiempo mayor a la validez de la información que se desea proteger y que inclusive las máquinas actuales y de los próximos años no puedan romper en los períodos necesarios.

Por otra parte, un protocolo es un conjunto de reglas, convenciones o estándares que utilizan dos o más dispositivos para comunicarse.

A continuación se presentan los algoritmos RSA de criptografía de llave pública, DES de criptografía privada DES y MD5 para firmas digitales, de igual forma se presentan los protocolos SET para transacciones electrónicas y el protocolo SSL para comunicación cliente servidor de forma segura bajo el estándar WWW.

9.2. Algoritmo RSA

9.2.1. Introducción

El RSA es el criptosistema de llave pública más popular basado en el modelo de Diffie-Hellman, el cual ofrece encripción y firmas digitales (autenticación). Ron Rivest, Adl Shamir y Leonard Adleman desarrollaron el RSA en 1977, de ahí su nombre formado por la primera letra del apellido de sus inventores. [RSA 99]

La longitud de la llave es variable, la más popular es de 512 bits, pero en la actualidad la llave de 1024 bits es comúnmente utilizada por el Pretty Good Privacy (PGP). [PGP 00].

[YAMAMOTO 96] De igual forma el tamaño de bloques de datos RSA es variable, pero el bloque de texto plano (sin encriptar) debe ser menor que la longitud de la llave. El tamaño del texto cifrado es de la misma longitud que la llave.

RSA es considerablemente más lento que el DES. Es utilizado normalmente para realizar funciones que el DES no puede realizar como la distribución de llaves. El PGP utiliza el algoritmo RSA para distribuir la llave de sesión secreta al destinatario.

9.2.2. Algoritmo RSA

Para generar el par de llaves: privada y pública [Fúster 98].

1. Se eligen dos números primos muy grandes p y q (por ejemplo de 256 bits de longitud)	Seleccionar p,q
2. Hacer n = p * q y guardar en secreto p, q. Es prácticamente imposible obtener los factores de una n tan grande. Se llama modulo a n.	$n = p * q$
3. Para generar la llave pública, escoja un número e, tal que $1 \leq e \leq \phi(n)$, o sea menor a n que sea primo relativo a $\phi(n) = (p-1)(q-1)$. Lo que significa que e y theta(n) no tienen factores en común excepto al 1. Por tanto	$\phi(n) = (p-1)(q-1)$
4. Sea la llave pública {e, n}. E es el exponente publico.	{e, n}
5. Para generar la llave privada, Calcular d que es el inverso multiplicativo (mediante el algoritmo de Euclides extendido) de e mod $\phi(n)$. De otra forma encontrar otro número d tal que (ed-1) SEA DIVISIBLE por (p-1)(q-1).	$e\,d \equiv 1 \pmod{\phi(n)}$
6. La llave privada es {d, n} D es el exponente privado.	{d, n}
Es necesario mantener secretos los números p,q y $\phi(n)$	

TABLA 9.1: Algoritmo RSA

Para encriptar un mensaje m < n para una persona B, únicamente se utiliza la llave pública de B para generar el texto encriptado:

$$c = m^e \bmod n \qquad (9.1.2\text{-a})$$

Unicamente la persona B puede desencriptar el texto cifrado c ya que solo B tiene la llave privada {d, n}:

$$m = c^d \bmod n \qquad (9.1.2\text{-b})$$

Para firmar el mensaje es necesario hacer:

$$s = m^d \bmod n \qquad (9.1.2\text{-c})$$

Para verificar la firma de B se requiere hacer:

$$m = s^e_B \bmod n \qquad (9.1.2\text{-d})$$

donde e es la llave pública de B.

9.2.3. Seguridad del RSA

Algunos ejemplos de ataques serían:

1. El algoritmos RSA se basa en el principio de la dificultad de factorizar un número grande n=p*q donde p y q son números primos grandes.
2. Dada la llave pública {e, n}, es difícil encontrar d el cual es el inverso multiplicativo de e, dado que p y q son desconocidos.
3. Existe un grado alto de dificultad para obtener la llave privada d a partir de la publica (n, e). De cualquier manera si se puede factorizar n en p y q se puede obtener la llave privada d. La seguridad de RSA se basa en el supuesto de la dificultad de la factorización.

Según [RSA 99] existen pocas interpretaciones posibles para romper el algoritmo RSA.

La más peligrosa sería para un atacante el descubrir la llave privada que corresponde a una llave pública dada. Esto permitiría al atacante tanto leer los mensajes encriptados con la llave publica y falsificar las firmas. La manera obvia para realizar este ataque es factorizar el modulo publico n en dos factores primos p y q. A partir de p, q y e, el exponente publico, un atacante puede fácilmente obtener d, el exponente privado. La parte difícil es factorizar n; la seguridad de RSA depende de la dificultad de factorizar. De hecho, la tarea de recuperar la llave privada es equivalente a la tarea de factorizar el modulo; se puede utilizar d para factorizar n, de igual forma el uso de la factorización de n para encontrar d. Las optimizaciones en HW no debilitan el RSA siempre y cuando se utilicen longitudes adecuadas de la llave.

Otra forma de romper el RSA es encontrar una técnica para calcular las raíces e mod n. Dado que $c = m^e \bmod n$, la raíz e de c mod n es el mensaje m. Este ataque permite la recuperación de mensajes encriptados y la falsificación de firmas sin conocer la llave privada. Este ataque es conocido por ser el equivalente de la factorización. No existen métodos actualmente conocidos para romper el algoritmo de esta forma. Pero en casos especiales cuando múltiples mensajes relacionados son encriptados con el mismo exponente pequeño, puede ser posible la recuperación de mensajes.

Estos ataques mencionados son la única forma conocida durante la investigación para romper el algoritmo RSA. Existen métodos para recuperar únicamente mensajes únicos dada una misma llave o recuperaciones parciales de mensajes.

9.3. Algoritmo DES.

9.3.1. Introducción

El algoritmo DES es un acrónimo para Data Encryption Standard y el nombre del Federal Information Processing Standard (FIPS) 46-1 [DES_FIPS_46-1 88], [Mathew DES], [Fúster 98] el cual describe el algoritmo de encripción de datos (DEA – Data Encryption Algorithm). El DEA se encuentra también definido en el estándar ANSI X9.21. Originalmente desarrollado por IBM y conocido como Lucifer, la NSA y la National Bureau of Standards (NBS, ahora el National Institute of Standards and Technology, NIST) jugaron un rol sustancial en las etapas finales del desarrollo.

El DEA, comúnmente llamado DES, ha sido estudiado extensivamente desde su publicación y es el algoritmo simétrico más conocido y utilizado del mundo.

El DEA tiene un tamaño de bloque de 64 bits y utiliza llaves de 56 bits durante la ejecución (8 bits de paridad son eliminados de la llave completa de 64 bits). El DEA es un criptosistema simétrico, específicamente un cifrador Feistel de 16 rondas y fue diseñado originalmente para su implementación en hardware. Cuando es utilizado para comunicación, tanto el emisor como el receptor deben conocer la misma llave secreta, la cual puede ser utilizada para encriptar y desencriptar el mensaje o para generar y verificar un código de autentificación de mensajes (Message authentication code – MAC). El DEA puede ser utilizado para encripción por un único usuario como el almacenamiento de archivos encriptados en el disco duro. Pero en un ambiente multiusuario, la distribución de llaves de forma segura puede ser difícil y la criptografía de llave pública provee una solución ideal a este problema.

El National Institute of Standards and Technology (NIST) ha certificado el DES (FIPS 46- 1) cada cinco años, la última vez fue en 1993 pero no será certificado otra vez. Esto debido a la vulnerabilidad del algoritmo utilizando una llave de 56 bits. Es por ello que el NIST ha iniciado un esfuerzo para desarrollar el Advanced Encryption Standard (AES) [AES 99]. Para especificar un algoritmo de cifrado de bloques simétrico, el cual reemplazará al algoritmo DES.

9.3.2. Algoritmo DES

El algoritmo DES [Fúster 98], [Mathew DES] trabaja alternativamente sobre las dos mitades del bloque a cifrar. En primer lugar se hace una permutación inicial fija y, por tanto, sin valor criptográfico. Después se divide el bloque en dos mitades, la derecha y la izquierda. A continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar módulo 2 la parte izquierda con una transformación g(k1) de la parte derecha, mediante una clave k1. Después se intercambian las partes derecha e izquierda. En la siguiente figura [Fúster 98] se presenta el esquema. En la vuelta número 16 se

omite el intercambio, pero se termina el algoritmo con una permutación final que es la inversa de la inicial.

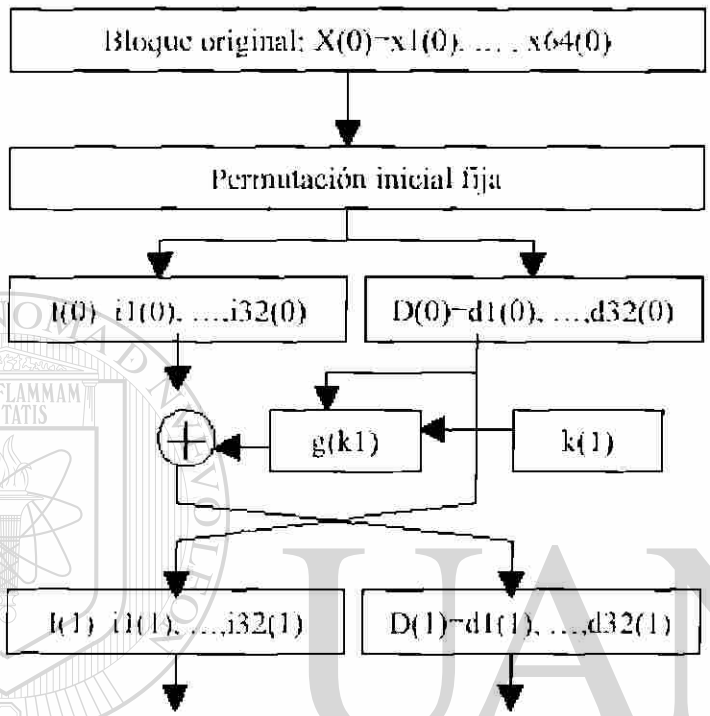


FIGURA. 9.1: Funcionamiento del algoritmo DES.

Para descifrar el algoritmo DES basta con repetir la operación modular, que es una involución; es decir, su aplicación repetida dos veces conduce a los datos originales. En la figura siguiente [Fúster 98] se puede ver el funcionamiento de la involución. No es preciso invertir la transformación g(k1) sino repetirla. Esto permite que dicha transformación sea una función de un solo sentido, empleando operaciones no lineales.

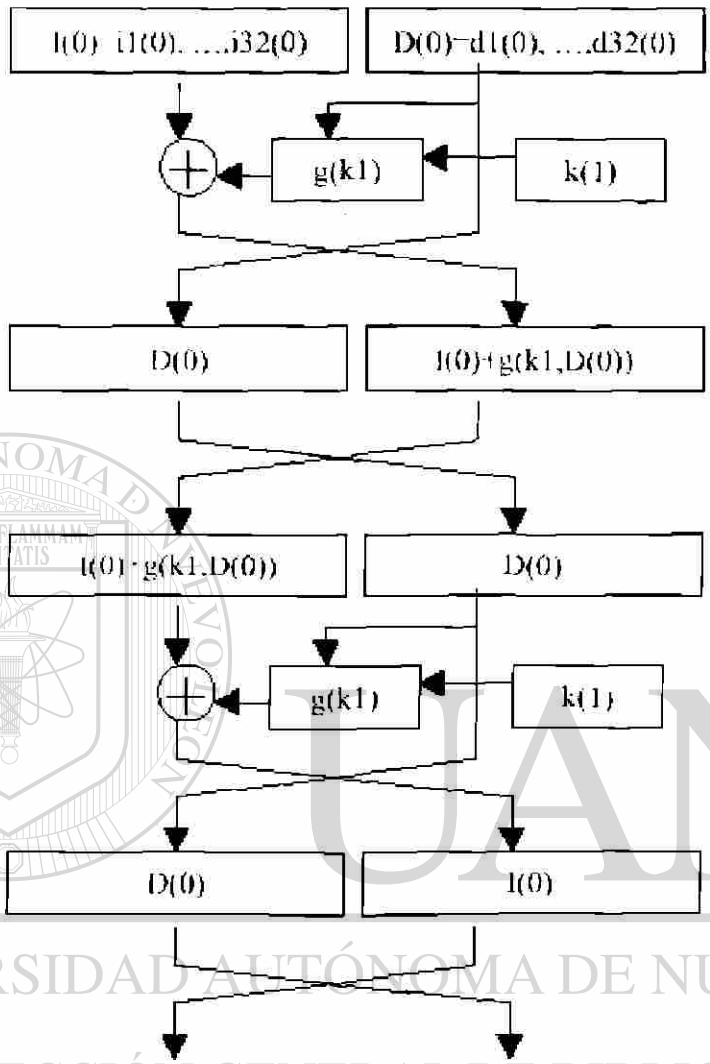


FIGURA. 9.2: Involución en el DES.

Es necesario describir las manipulaciones realizadas en el algoritmo DES. La transformación g(k1) es un conjunto de operaciones que se combinan según se muestra en la siguiente figura [Fúster 98].

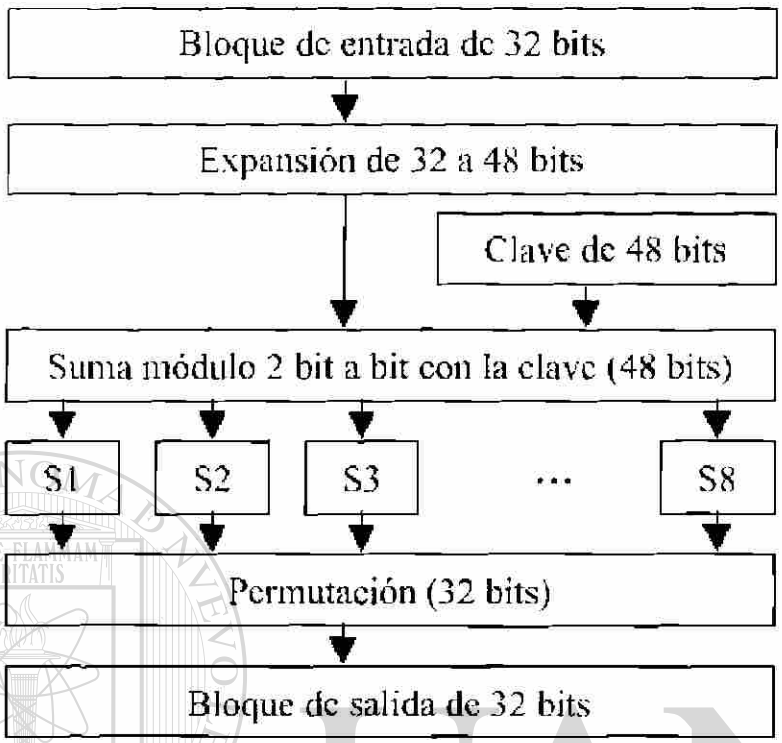


FIGURA. 9.3: Estructura de la transformación g del algoritmo DES.

El algoritmo DES puede ser utilizado para la encripción en varios modos definidos oficialmente [DES_FIPS_81 80] y estos modos tienen una variedad de propiedades:

- El modo Electronic CodeBook (ECB) encripta simplemente bloques de 64 bits de texto plano, uno tras de otro, utilizando la misma llave DES de 56 bits.
- En el modo Cipher Block Chaining (CBC) cada bloque de 64 bits de texto plano se aplica la función OR exclusivo con los bloques previos antes de ser encriptado con la llave DES, con esto la encripción de cada bloque depende de los bloques previos dependiendo del contexto completo del mensaje. Este modo ayuda la protección en contra de ciertos ataques pero no de búsqueda exhaustiva o criptoanálisis diferencial.

- El modo Cipher FeedBack (CFB) permite utilizar el DES con longitudes de bloque menores a 64 bits.
- El modo OFB permite al DES ser utilizado como un flujo de cifrado.

9.3.3. Seguridad del DES

No se han descubierto ataques fáciles al DES, a pesar de los esfuerzos de los investigadores en varios años. El método obvio de ataque es la búsqueda exhaustiva de fuerza bruta para el dominio de llaves, este proceso toma 255 pasos en promedio. Alguna vez se planteó la posibilidad de construir una computadora de propósito especifico capaz de romper el DES por búsqueda exhaustiva en un tiempo razonable. Posteriormente Hellman mostró un cambio en el manejo de memoria que permite mejorar la búsqueda exhaustiva si la cantidad de memoria era abundante. Estas ideas pusieron en tela de juicio la seguridad del algoritmo DES. Los estimados según Wiener son de 35 minutos para realizar la búsqueda exhaustiva con una computadora de un millón de dólares.

El primer ataque al DES que es mejor que la búsqueda exhaustiva en términos de requerimientos computacionales fue la anunciada por Biham y Shamir utilizando una técnica llamada criptoanálisis diferencial. Este ataque requiere la encripción de 247 textos planos escogidos por el atacante. Este ataque no es práctico debido a los requerimientos excesivos de datos y la dificultad en montar un ataque de los textos planos escogidos. Biham y Shamir consideraron seguro al algoritmo DES.

Más recientemente Matsui desarrollo otro ataque conocido como criptoanálisis linear. De acuerdo a este método una llave DES puede ser recuperada por el análisis de 243 textos planos conocidos. Este ataque también resultó impráctico debido al tiempo y poder computacional requerido.

Recientemente se realizó un reto para lograr romper el algoritmo, el objetivo se cumplió en 56 horas mediante el uso del computo distribuido, se puede encontrar más información y detalle en [DISTRIBUTED_NET 99] y en [RSA 99].

El conceso de la comunidad acerca del DES es que todavía no es inseguro, pero pronto lo será, ya que las llaves de 56 bits se están convirtiendo vulnerables a la búsqueda exhaustiva. A partir de noviembre de 1998, el DES no es permitido en el uso del gobierno de los Estados Unidos de Norteamérica. El Triple-DES será utilizado mientras el AES se encuentra listo para ser utilizado como se mencionó anteriormente.

Recomendaciones y consideraciones para utilizar el algoritmo DES.

- Se deben cambiar las llaves DES con frecuencia para prevenir ataques que requieran un análisis sostenido de los datos. En un ambiente de comunicación se debe encontrar una manera segura de comunicar la llave DES entre el emisor y el receptor. Utilizando el RSA o alguna técnica de llave publica para la administración de llaves, resuelve estos dos problemas: el primero es que se genere una llave por cada sesión y la administración segura de la llave DES al encriptarla con la llave publica RSA del receptor.

- Para mayor seguridad se recomienda utilizar la triple encripción con el CBC.
- Las llaves DES pueden ser probadas para que no sean llaves débiles de la siguiente forma.
  1. Existen 4 llaves débiles k para las cuales $E_k(E_k(m))=m$
  2. Existen 12 llaves semi débiles que vienen en pares k1 y k2 tales que $E_{k1}(E_{k2}(m))=m$
  3. Es mejor seleccionar la llave de forma aleatoria de entre 2^{52}

9.4. Algoritmo MD5

9.4.1. Introducción

El algoritmo MD5 o Message Digest toma como entrada un mensaje de longitud arbitraria y regresa como salida una "huella digital" de 128 bits del mensaje (Llamado message-digest, resumen o compendio del mensaje). Se estima que es imposible obtener dos mensajes que produzcan el mismo message-digest. También es imposible producir un mensaje que arroje un message-digest predefinido. Este algoritmo es útil como firma digital de mensajes que serán compactados y encriptados mediante un criptosistema de llave pública.

El MD5 fue desarrollado por Rivest en 1991. Se encuentra optimizado para máquinas de 32 bits. La descripción completa de los algoritmos se puede localizar en [RFC1321 92]. Es básicamente igual a su predecesor MD4 [RFC1320 92] pero con protecciones y un poco más lento pero más seguro. El algoritmo consiste en cuatro rondas distintas. El tamaño del resumen del mensaje así como los requerimientos de padding son iguales que el MD4.

9.4.2. Algoritmo MD5

Empezamos suponiendo que tenemos un mensaje de b-bits como entrada y que se desea encontrar su message-digest. Aquí b es un entero no-negativo arbitrario que puede ser cero y no necesariamente tiene que ser un múltiplo de 8, la longitud también puede ser arbitrariamente grande. El mensaje puede ser representado de la siguiente forma:

m_0 m_1 ... m_{b-1}	(9.3.2-a)

Los siguientes 5 pasos son realizados para calcular el message-digest del mensaje.

Paso 1. Agregado de bits de relleno

El mensaje es "padded" (extendido) para que su longitud en bits sea casi un múltiplo de 512 bits de longitud (congruente a 448, módulo 512). Los 64 bits restantes serán cubiertos con el tamaño del mensaje (expresado en 64 bits).

Paso 2. Agregado de la longitud

Una representación en 64 bits de la longitud b del mensaje es agregada al final del mensaje resultante en el paso previo. Si la longitud del mensaje requiere más de 2^{64} bits entonces se toman únicamente los 64 bits menos significativos.

Como resultado de este paso se obtiene un mensaje de longitud exactamente en múltiplos de 512 bits.

Equivalentemente, este mensaje tiene la longitud exacta de 16 palabras de (32-bits). Sea M[0 ... N-1] que denotan las palabras del mensaje resultante, donde N es un múltiplo de 16.

Paso 3. Inicialización del buffer MD

Un buffer de cuatro palabras (A, B, C, D) es utilizado para calcular el message-digest, donde cada palabra es un registro de 32 bits. Los registros son inicializados a los siguientes valores en hexadecimal con los bytes menos significativos primero.

Palabra A:	01	23	45	67
Palabra B:	89	ab	cd	ef
Palabra C:	fe	dc	ba	98
Palabra D:	76	54	32	10

Paso 4. Procesamiento del mensaje en bloques de 16 palabras

Primero se definen cuatro funciones auxiliares (F,G, H,I) que toman como entrada 3 palabras de 32 bits y producen una palabra de 2 bits.

F(X,Y,Z)=XY not(X) Z

G(X,Y,Z)=XZ Y not(Z)

H(X,Y,Z)=X xor Y xor Z

I(X,Y,Z)=Y xor (X not(Z))

Se define una tabla T[i] de 64 elementos T[1..64] con base a la parte entera de 4294967296 por abs(sin(i)), donde i esta dado en radianes.

Después se ejecuta el siguiente proceso a cada bloque de 16 palabras.

For i = 0 to N/16-1 do /* Copiar el bloque i en X */
For j = 0 to 15 do
Set X[j] to M[i*16+j].
end /* del ciclo en j */
AA = A ; BB = B; CC = C; DD = D
Round 1
Round 2
Round 3
Round 4
Ejecutar las sig. sumas. (Incrementar c/u de los 4 reg. por el valor anterior al inicio del bloque/
A = A + AA
B = B + BB
C = C + CC
D = D + DD
End /* del ciclo en i */

Round 1. Sea [abcd k s i] la siguiente operación a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 0 7 1]	[DABC 1 12 2]	[CDAB 2 17 3]	[BCDA 3 22 4]
[ABCD 4 7 5]	[DABC 5 12 6]	[CDAB 6 17 7]	[BCDA 7 22 8]
[ABCD 8 7 9]	[DABC 9 12 10]	[CDAB 10 17 11]	[BCDA 11 22 12]
[ABCD 12 7 13]	[DABC 13 12 14]	[CDAB 14 17 15]	[BCDA 15 22 16]
Round 2. Sea [abcd k s i] la siguiente operación a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 1 5 17]	[DABC 6 9 18]	[CDAB 11 14 19]	[BCDA 0 20 20]
[ABCD 5 5 21]	[DABC 10 9 22]	[CDAB 15 14 23]	[BCDA 4 20 24]
[ABCD 9 5 25]	[DABC 14 9 26]	[CDAB 3 14 27]	[BCDA 8 20 28]
[ABCD 13 5 29]	[DABC 2 9 30]	[CDAB 7 14 31]	[BCDA 12 20 32]
Round 3. Sea [abcd k s t] la siguiente operación a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 5 4 33]	[DABC 8 11 34]	[CDAB 11 16 35]	[BCDA 14 23 36]
[ABCD 1 4 37]	[DABC 4 11 38]	[CDAB 7 16 39]	[BCDA 10 23 40]
[ABCD 13 4 41]	[DABC 0 11 42]	[CDAB 3 16 43]	[BCDA 6 23 44]
[ABCD 9 4 45]	[DABC 12 11 46]	[CDAB 15 16 47]	[BCDA 2 23 48]
Round 4. Sea [abcd k s t] la siguiente operación a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s) /* Realizar las siguientes 16 operaciones */			
[ABCD 0 6 49]	[DABC 7 10 50]	[CDAB 14 15 51]	[BCDA 5 21 52]
[ABCD 12 6 53]	[DABC 3 10 54]	[CDAB 10 15 55]	[BCDA 1 21 56]
[ABCD 8 6 57]	[DABC 15 10 58]	[CDAB 6 15 59]	[BCDA 13 21 60]
[ABCD 4 6 61]	[DABC 11 10 62]	[CDAB 2 15 63]	[BCDA 9 21 64]

FIGURA. 9.4: Procedimiento para el cálculo del algoritmo RSA

Paso 5. Salida

El message-digest producido como salida es A, B, C y D. Esto es empezando con el menos significativo como A y el más significativo como D.

9.4.3. Seguridad del MD5

El único ataque conocido es la búsqueda exhaustiva, aunque se han detectado pseudo colisiones para el MD5.

9.5. Protocolo Secure Socket Layer (SSL) Versión 3.0

9.5.1. Introducción

El SSL es un protocolo de seguridad que provee privacidad en las comunicaciones a través de Internet. El protocolo permite a las aplicaciones cliente/servidor comunicarse de tal forma, de acuerdo al diseño, para prevenir la escucha (eavesdropping), intromisiones (tampering) o falsificación de mensajes (message forgery) evitando así la creación ilegal de mensajes, como si fueran oficiales.

Las metas del protocolo SSL V3.0 [SSL 96] en orden de prioridad son:

- Seguridad criptográfica: SSL debe ser utilizado para establecer una conexión segura entre dos entidades.
- Interoperabilidad: Las diversas aplicaciones SSL V3.0 deber ser capaces de intercambiar con éxito los parámetros criptográficos sin conocer el código de la otra aplicación.
- Extensibilidad: SSL busca proveer un marco de trabajo en el cual se puedan incluir nuevos métodos de encripción sin la necesidad de crear un nuevo protocolo y evitar la necesidad de implementar una nueva y completa librería de seguridad.
- Eficiencia relativa: Las operaciones criptográficas tienden a utilizar intensivamente el CPU sobre todo en operaciones de llave pública. Por esta razón el protocolo SSL ha incorporado un esquema opcional de cache para sesiones con el objeto de reducir el número de conexiones que deben ser establecidas a partir de cero.

La meta principal del protocolo SSL es proveer privacidad y confiabilidad entre dos aplicaciones que se encuentran comunicando. El protocolo esta compuesto de dos capas. En el nivel más bajo, encima de algún protocolo confiable de transporte (ej. TCP) se encuentra el protocolo de registro SSL (SSL Record Protocol). Este es utilizado para la encapsulación de varios protocolos de más alto nivel. Uno de esos protocolos encapsulados, el protocolo de iniciación de SSL (Handshake Protocol), permite al servidor y cliente la autentificación mutua, así como la negociación del algoritmo de encripción y las llaves criptográficas antes de que el protocolo de aplicación transmita o reciba el primer byte de datos. Otra ventaja del SSL es la independencia del protocolo de aplicación y se puede utilizar un protocolo de mas alto nivel de forma transparente.

El protocolo SSL provee seguridad en la conexión con 3 propiedades básicas:

- La conexión es privada. Se utiliza encripción después de haber realizado el proceso de iniciación y haber negociado una llave secreta. La criptografía simétrica es utilizada para la encripción de datos. Ejemplo: DES, RC4.
- La identidad de las entidades puede ser autentificada utilizando la criptografía asimétrica o de llave publica. Ejemplo: RSA, DSS.
- La conexión es confiable. El transporte de mensajes incluye una verificación de la integridad de los mensajes utilizando un código de autentificación de mensaje (MAC – Message Authentication Code) basado en una llave. Para los cálculos MAC son utilizadas funciones hash seguras (ej. SHA, MD5).

Las cuatro operaciones criptográficas utilizadas son: el firmado digital, encripción cifrada en flujo, encripción cifrada en bloque y encripción de llave pública.

- En el firmado digital, funciones hash de una vía son utilizadas como entrada para el algoritmo de firmado. En el caso de firmado de RSA una estructura de 36 bytes de dos funciones hash (una SHA y otra MD5) es firmada (encriptada con la llave privada). En DSS, los 20 bytes del hash SHA son ejecutados directamente a través del algoritmo de firmado digital sin un hashing adicional.
- En la encripción cifrada en flujo, el texto plano es pasado por una función Or exclusiva con la misma cantidad de salida generada por un generador pseudo aleatorio de números seguro.
- En la encripción cifrada en bloques, cada bloque de texto plano se encripta usualmente en bloques de 64 bits.
- En la encripción de llave pública, funciones de una vía con trampas (trapdoors - rutinas que permiten ingresar al sistema sin que la identidad sea autentificada) secretas, son utilizadas para encriptar los datos de salida. Los cuales pueden ser únicamente desencriptados con la llave privada y viceversa.

9.5.2. Protocolo SSL

El protocolo SSL es un protocolo de capas. En cada una, los mensajes pueden incluir campos para longitud, descripción y contenido. SSL toma los mensajes para ser transmitidos, fragmenta los datos en bloques manejables, opcionalmente compacta los datos, aplica el MAC, encripta y transmite el resultado. Los datos recibidos son desencriptados, verificados, descomprimidos y ensamblados de nueva cuenta para ser entregados a los clientes de más alto nivel.

la iniciación es completada, las dos entidades tiene secretos compartidos los cuales son utilizados para encriptar registros y calcular los MAC en sus contenidos. El MAC es calculado antes de la encripción.

Protocolos Adicionales

Es posible modificar la estrategia de cifrado mediante el cambio de especificaciones de cifrado como son las llaves o el algoritmo utilizado. De igual forma existe un protocolo de alerta que permite anunciar la descripción y severidad de diversos mensajes como los errores o la finalización de la conexión para evitar el ataque por truncamiento.

Protocolo de iniciación (handshake)

Los parámetros criptográficos del estado de sesión son producidos por el protocolo de iniciación, que opera en la parte superior de la capa de registro. Cuando un cliente y servidor SSL inician por primera vez la comunicación, existe un acuerdo sobre la versión del protocolo, la selección de algoritmos criptográficos, la autentificación mutua y las técnicas de encripción de llave pública para generar los secretos compartidos.

Protocolo de datos de la aplicación

En el protocolo de datos de aplicación, los mensajes de datos de aplicación son llevados por la capa de registro y son fragmentados, compactados y encriptados según el estado de conexión actual. Los mensajes son tratados como datos transparentes a la capa de registro.

Criptografía

El intercambio de llaves, autentificación, encripción y algoritmos MAC son determinados por el servidor.

- Cálculos de criptografía asimétrica. Los algoritmos asimétricos son utilizados en el protocolo de iniciación para autentificar a las partes y para generar las llaves y secretos compartidos. Se utilizan los siguientes algoritmos: Diffie Hellman, RSA, Fortezza.
- Cálculos de criptografía simétrica. Esta técnica es utilizada para encriptar y verificar la integridad de los registros SSL y es especificada por el CipherSpec actual. Un ejemplo típico es encriptar los datos con el DES y generar los códigos de autentificación con el MD5. Antes de que la encripción segura y la verificación de integridad puedan ser realizadas en los registros, el cliente y el servidor requieren generar información secreta y compartida solo conocida por ellos. Este valor es de 48 bytes y es denominado el secreto maestro. El cual se utiliza para generar llaves y secretos para cálculos de encripción y MAC.

Los elementos mencionados previamente son parte del protocolo SSL y pueden ser representados de forma gráfica aunque parcialmente, como se muestra en el diagrama del apéndice A.

9.5.3. Análisis del protocolo SSL

El protocolo SSL requiere para su implementación seguir las siguientes recomendaciones:

- Las restricciones de exportación de US limitan las llaves RSA para encripción a 512 bits pero no establece límites en la longitud de las

llaves RSA para las operaciones de firma. Los certificados deber de ser mayores a 512 bits de longitud, dado que las llaves RSA de 512 bits no son seguras para operaciones que requieran gran seguridad. Por tanto las llaves deben de ser cambiadas diariamente o cada 500 transacciones, por ejemplo.

- SSL requiere un generador de números pseudo aleatorios criptográficamente seguro (pseudorandom number generator PRNG). Los PRNG basados en operaciones hash seguras como el MD5 y SHA son aceptables pero no proveen mayor seguridad que el tamaño del estado del generador de números aleatorios. Por ejemplo los PRNG basados en MD5 usualmente proveen 128 bits de estado.
- Las implementaciones son responsables de verificar la integridad de los certificados y debe generalmente soportar mensajes de revocación de certificados. Los certificados deben ser verificados siempre para asegurar el firmado apropiado por una autoridad certificadora confiable (CA).

De acuerdo al análisis [Wagner 96] el protocolo SSL presenta imperfecciones menores que pueden ser fácilmente corregidas sin modificar la estructura básica del protocolo. En general el protocolo SSL 3.0 provee una seguridad excelente contra la escucha y los ataques pasivos. Aunque se han revelado algunos ataques pasivos, por lo que es necesario modificar la especificación para detectar ataques como cambio del algoritmo de cifrado y el engaño de algoritmo de intercambio de llaves. Otro problema mayor es la comunicación entre SSL 3.0 y 2.0 o la intrusión para hacer creer que la otra parte utiliza la versión 2.0 del protocolo, ya esta versión tiene un gran número de problemas de seguridad que pueden ser aprovechadas. El protocolo SSL de iniciación tiene varias vulnerabilidades. Una imperfección en el protocolo no necesariamente produce una implementación vulnerable. No obstante es

necesario que la especificación prevenga explícitamente de una ataque o permita la prevención directa.

El estudio [Mitchell 97] utiliza una herramienta de análisis denominada Murφ para analizar el protocolo de inicialización de la especificación SSL 3.0. El enfoque de trabajo fue utilizar modelos escalables los cuales permiten ir incrementado las variables o condiciones y por ello el nivel de seguridad. Al ser aplicado al SSL 3.0 la herramienta no detecto problemas o riesgos de la seguridad del protocolo.

9.6. Protocolo SET

9.6.1. Introducción

Debido a las predicciones sobre el incremento de la industria del comercio electrónico, las instituciones financieras o los emisores de tarjetas de crédito o débito requieren establecer medios seguros para ofrecer a sus clientes la conveniencia y seguridad de los pagos en línea. [Brands 95] El protocolo Secure Electronic Transaction (SET) [SET 99], [Varadharajan 96] fue desarrollado en 1995 en conjunto por Visa y Martercard como un método para transacciones seguras de pago con tarjeta a través de redes abiertas. SET es publicado como una especificación abierta para la industria.

Adicionalmente a las dos empresas mencionadas se tuvo asistencia en el desarrollo de la especificación por parte de GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa y VeriSign. [Visa 97]

El protocolo SET permite satisfacer la demanda del mercado para el procesamiento de transacciones en línea, con una relación costo – beneficio aceptable y de forma segura.

Los sistemas de pagos y las instituciones financieras deben proveer servicios para transmisión confidencial, autentificación de entidades involucradas, aseguramiento de la integridad de instrucciones de pago en las ordenes de compra de bienes y servicios y autentificar la identidad del poseedor de la tarjeta de crédito o débito y el comerciante o proveedor.

Para cumplir los requerimientos mencionados anteriormente, el protocolo SET utiliza la criptografía para provee confidencialidad a la información, asegurar la integridad de los pagos y autentificar tanto al comerciante como al poseedor de la tarjeta.

Con base a lo anterior, SET define los algoritmos y protocolos necesarios para ofrecer los servicios requeridos de seguridad. La especificación denota las siguientes características:

- Confidencialidad de la información. SET utiliza la encripción de mensajes para asegurar la confidencialidad de la información.
- Integridad de los datos. SET provee las firmas digitales que aseguran la integridad de la información de pago.
- Autentificación de la cuenta del poseedor de la tarjeta. SET utiliza las firmas digitales y los certificados del poseedor de la tarjeta para asegurar la autentificación de la cuenta del poseedor de la tarjeta.
- Autentificación del comerciante. SET provee el uso de firmas digitales y certificados del comerciante para asegurar la autentificación del comerciante.
- Inter operabilidad. SET utiliza protocolos y formatos de mensaje previamente definidos para asegurar la interoperabilidad.
- El alcance de la especificación incluye la aplicación de los algoritmos criptográficos (como el RSA y DES), los formatos de mensajes de certificados, compra, autorización, captura y de los objetos en cuestión, así como los mensajes entre los participantes.

9.6.2 Protocolo SET

SET utiliza la criptografía de llave privada y de llave pública para asegurar la confidencialidad. La integridad y autentificación son aseguradas mediante el uso de firmas digitales.

Combinada con los message digest, la encripción utilizando la llave privada permite a los usuarios firmar digitalmente los mensajes. Un message digest es un valor generado por un mensaje que es único a ese mensaje. SET utiliza un par de llaves públicas y privadas para la encripción y decripción de los mensajes y otro par para la creación y verificación de las firmas digitales.

Para garantizar la autentificación es necesario una tercero de confianza para autentificar la llave pública y es denominada Autoridad Certificadora (AC) como se mencionó en la sección 8.1.1.

El diagrama del Apéndice A muestra un esquema parcial del proceso de encripción.

9.6.3. Análisis del protocolo SET

No se encontró evidencia de análisis de la seguridad del protocolo que muestren problemas. Sin embargo los comentarios son con relación a la eficiencia del algoritmo o al marcado uso a los pagos electrónicos sin proporcionar un marco completo del flujo de las operaciones del comercio electrónico.

9.7. X.509

9.7.1. Introducción

La recomendación o norma internacional X.509 [X.509 93] define un marco para ofrecer servicios de autentificación por el directorio a sus usuarios. Describe dos niveles de autentificación: simple mediante el uso de una contraseña como verificación de una identidad pretendida y fuerte, que implica credenciales formadas usando técnicas criptográficas.

Esta norma fue elaborada para facilitar la interconexión de sistemas de procesamiento de información con el fin de proporcionar servicios de directorios. El conjunto de todos estos sistemas, junto con la información contenida por el directorio pueden ser considerados como un todo integrado, llamado directorio. La información contenida por el directorio, denominada colectivamente base de información de directorio (DIB), se utiliza típicamente para facilitar la comunicación entre, con o sobre objetos tales como entidades de aplicación OSI, personas, terminales y listas de distribución.

Adicionalmente la norma define un marco para el suministro de servicios de autentificación por el directorio a sus usuarios. Estos usuarios incluyen el propio directorio, así como otras aplicaciones y servicios. El directorio puede emplearse para satisfacer las necesidades de autentificación y otros servicios de seguridad. Es el lugar natural para obtener la información de autentificación de cada una de las demás partes.

El método de autenticación fuerte especificado en esta especificación de directorio se basa en los criptosistemas de claves públicas. Es una gran ventaja de esos sistemas el que los certificados de usuario pueden estar contenidos en el directorio como atributos, y ser comunicados libremente dentro del sistema del directorio y obtenidos por los usuarios del directorio del mismo modo que

otra información de directorio. Se supone que los certificados de usuario están formados por medios «fuera de línea», y que son introducidos en el directorio por su creador. La generación certificados de usuario la efectúa cierta autoridad de certificación «fuera de línea» que está completamente separada de los DSA en el directorio. En particular, no se imponen requisitos especiales a los suministradores del directorio para almacenar o comunicar certificados de usuario en una manera segura.

El marco de autentificación fuerte no obliga a utilizar un criptosistema en particular. Se pretende que el marco sea aplicable a cualquier criptosistema de llave pública adecuado, y soportará por consiguiente cambios en los métodos usados como un resultado de futuros avances en criptografía, técnicas matemáticas o capacidades de computación. Sin embargo, dos usuarios que desean autentificar tienen que soportar el mismo algoritmos criptográfico para que la autentificación se realice de forma correcta.

El procedimiento para obtener una llave pública de un usuario es el siguiente: Para que un usuario confíe en el procedimiento de autentificación, tiene que obtener la llave pública del otro usuario desde una fuente en la cual confía. Dicha fuente, llamada autoridad decertificación (CA), usa el algoritmo de llave pública para certificar la clave pública, produciendo un certificado. El certificado, cuya forma se especifica en esta cláusula, tiene las siguientes propiedades:

- Cualquier usuario con acceso a la llave pública de la autoridad de certificación puede extraer la llave pública que fue certificada.
- Ninguna parte que no sea la autoridad de certificación puede modificar el certificado sin que esto sea detectado (los certificados son infalsificables).

Como los certificados son infalsificables, pueden publicarse insertándolos en el directorio, sin que éste tenga que tomar disposiciones especiales para protegerlos.

Una autoridad de certificación produce el certificado de un usuario firmando una colección de informaciones, incluidos el nombre distinguido y la llave pública del usuario, así como un identificador único opcional con información adicional sobre el usuario. No se especifica aquí la forma exacta del contenido del identificador único, que se deja a la autoridad de certificación y podría ser, por ejemplo, un identificador de objeto, un certificado, una fecha u otra forma de certificación sobre la validez del nombre distinguido.

El siguiente tipo de datos ASN.1 puede usarse para representar certificados:

```
Certificate ::=          SIGNED { SEQUENCE {
version                  [0] Version DEFAULT v1,
serialNumber                     CertificateSerialNumber,
signature                        AlgorithmIdentifier,
issuer                   Name,
validity                 Validity,
subject                  Name,
subjectPublicKeyInfo     SubjectPublicKeyInfo,
issuerUniqueIdentifier   [1] IMPLICIT UniqueIdentifier OPTIONAL,
subjectUniqueIdentifier  [2] IMPLICIT UniqueIdentifier OPTIONAL
```

9.8. Resumen y Conclusiones de los Algoritmos y Protocolos para el Comercio Electrónico

La siguiente tabla muestra los mecanismos proporcionados por los algoritmos y protocolos de comercio electrónico:

	RSA	DES	MD5	SSL	SET	X.509
Autentificación	X		X	X	X	X
Confidencialidad	X	X		X	X	
Integridad			X	X	X	
No - Repudiación	X			X	X	X

TABLA 9.2: Resumen de algoritmos y protocolos

La autentificación y no-repudiación pueden ser verificados únicamente cuando la creación, almacenamiento y distribución de llaves sean confiables, solo así la identidad puede ser garantizada, como se mencionó anteriormente, la participación de una autoridad certificadora permitirá facilitar el proceso de autentificación.

No solo los algoritmos de encripción y las técnicas criptográficas requieren una revisión sobre la seguridad que proveen. Los protocolos de autentificación y de comercio electrónico también así lo requieren.

Debido a la demanda de acceso seguro para realizar compras por parte de los consumidores, los protocolos de comercio electrónico requieren de métodos formales para verificar su diseño e implementación. Es por ello que actualmente hay estudios como el [Bolignano 97] que realizan propuestas para verificar estos protocolos y así evitar amenazas a la seguridad en su utilización para el comercio electrónico.

Finalmente, la selección de los algoritmos y protocolos de comercio electrónico depende del proyecto que se requiera implementar. Para proyectos de comercio electrónico entre Persona a negocio se recomienda el uso de SSL versión 3, pero para un proyecto de negocio a negocio, el protocolo SET y el lenguaje XML son una opción que cada vez se utiliza más.

Con relación a los algoritmos, el RSA sigue siendo seguro por lo tanto se recomienda continuar con su uso. Para el caso del algoritmo DES, la situación es diferente, ya que aunque se recomienda utilizar el Triple DES, es necesario dar seguimiento al avance del es fuerzo para sustituir el algoritmo DES por parte de la NIST, ya que se encuentra en las rondas finales para liberar la especificación del nuevo algoritmo de encripción simétrica o llave privada.

El uso de firmas digitales se recomienda utilizar el MD5 ya que su seguridad es suficiente para la mayoría de los proyectos.

A continuación se presentan los proyectos que se realizaron como soporte a la base teórica, los algoritmos utilizados fueron el DES, RSA y MD5 para realizar una implementación simple del procedimiento de transferencia de información segura del protocolo SET.

CAPITULO 10

10 Proyecto de Comercio Electrónico Desarrollado

10.1 Proyecto de desarrollo de un Site de Comercio Electrónico de una Empresa Maquiladora de Ejes y Frenos para Camiones

10.1.1 Antecedentes

Con el progreso de la humanidad, el hombre a buscado la manera de hacer mas fácil la forma en que realiza su vida cotidiana, y con el desarrollo de nuevas técnicas y procedimientos de realizar las cosas lo a logrado, por este motivo desarrolla día a día nuevas herramientas, formas y procedimientos, las cuales las a llevado e implementado para con ello tratar de llevar una vida mas vida practica. Una de estas técnicas que actualmente esta teniendo un enorme auge es la de realizar transacciones comerciales con las empresas de una manera mas rápida y segura, dado que la complejidad y aunado a esto la confianza que se tiene actualmente de este tipo de procedimientos por su seguridad y eficacia, las empresas están llevando acabo inversiones en este punto para poder desarrollar sus herramientas propias para realizar dichos negocios.

Una de estas Empresa en la cual se me permitió participar de manera plena en el desarrollo e implementación de un Site del tipo comercial fue la Empresa DIRONA S.A. de C.V., en la cual tratando de competir de manera mas plena y de la manera mas eficiente, visualizo como objetivo a corto plazo el poner a funcionar un departamento que se encargara de este proyecto, en el cual se llevo acabo la tarea de buscar una manera segura, rápida y eficiente de llevar acabo las mismas. Dado que actualmente nuestro país esta sufriendo una acelerado crecimiento en su factor tecnológico y aunado a esto la competencia mas amplia de no solo en el ramo nacional, sino también en plano internacional se creo esta herramienta que trataremos de explicar más detalladamente más adelante.

DIRONA S.A. de C.V., para dar solución a este problema se creo la división llamada SUDISA, la cual se encuentra ubicada en la ciudad de Guadalajara Jalisco, y dicha división tiene como objetivo: llevar acabo el total control y manejo de todas las ventas, manejo y seguimiento de las transacciones comerciales realizadas por la empresa a través del E-commerce.

10.1.2 Descripción del proyecto

Para la realización de este objetivo se trato de visualizar todos y cada unos de los puntos requeridos por parte de la empresa y sus clientes directos e indirectos. Se crea un portal de negocios, en el cual cualquier persona que cubra con cierto perfil para ser considerado cliente de negocios, en el cual se llevara acabo la consulta, la verificación de precios, cantidad de material en existencia, la solicitud en línea del mismo y su compre, y el seguimiento correspondiente a dicha nota de compra. El portal de transacciones comerciales permitió desarrollar un agente virtual de ventas, el cual muestra sugerencias sobre las diferentes piezas que se manufacturan en la empresa así como su existencia física y su tiempo de entrega. Esto se logro mediante la inclusión de un motor de PROLOG desarrollado en el lenguaje JAVA. Este motor permite realizar inferencias sobre una pequeña base de datos la cual lleva la relación y

orden de los inventarios reales y a su vez tratar de llevar un completo orden de la producción de la empresa. La interfaz gráfica permite capturar el modelo, tipo, el destino, el costo y el tipo de pago de las notas de venta. El proyecto fue delimitado para aceptar un rango mínimo de valores y opciones de ventas, además de tener una base de conocimientos muy limitada, esto con el objeto de presentar un programa ligero para ser utilizado en un ambiente como Internet, y dado que algunos clientes no cuentan todavía con una infraestructura más poderosa para realizar sus transacciones por este medio más rápido.

10.2 Tecnologías a utilizar

El tipo de herramientas a utilizar para la realización de este proyecto, es envase al tipo de aplicaciones de uso común actualmente en la industria de las telecomunicaciones e informática y normas y reglamentos que rigen este tipos de negocios, actualmente en nuestro país y a nivel mundial. Para lo cual se considero la normativa del tipo de trafico (o flujo) de datos que circulan a través de Internet actualmente, además tomando en cuenta el echo de que aun en estos días, algunas empresas se niegan a estar invirtiendo constantemente en nuevos equipos y materiales de telecomunicaciones, se trato de utilizar un sistema complejo el cual permitiera en pocos segundos el llevar acabo cierto tipo de operaciones en el menor tiempo posible. Para lo cual se utilizaron las herramientas como son Java el cual permite el desarrollo de aplicaciones cliente - servidor que se ejecutan en un navegador de Internet. Adicionalmente se utilizó una implementación de CORBA denominada Orbacus CORBA, permitiendo así el diseño de una aplicación distribuida para el procesamiento de transacciones, también se utilizo la Herramienta de seguridad de logi.crypto, las cuales son una implementación de los principales algoritmos de seguridad como son: DES, RSA, MD5, etc. Estas librerías permitieron realizar la implementación del esquema de seguridad según el protocolo SET., Lenguaje C++ por ser un complemento de para la puesta en marcha de dichas herramientas, Xml por ser un lenguaje de programación de paginas electrónicas

de alta complejidad, Remote Method Invocation (RMI) de Java el cual sirve para manejar y manipular bases de datos en tiempo real no importando la ubicación del usuario que la manipule, de los navegadores de Internet Nestcape y Explorer sus librerías de seguridad en su condigo fuente, así como el plug-in de VRML (Cosmoplayer) por ser un medio complejo y de baja cantidad de requerimientos para manipulación de base de daos lo cual es muy satisfactorio ya dado que la gran mayoría de los usuarios en la actualidad no cuentan con la infraestructura tan actualizada en sus sistemas de comunicaciones.

Considerando el flujo de capital que se lleva acabo en este tipo de giros comerciales, se tienen que utilizar las mejores herramientas tanto humanas como del tipo electrónico.

Teniendo como antecedente lo anterior, también se procedió a la implantación de un sistema de control de flujo de usuarios para interactuar con los servidores en los que se colocaría la información, se colocaron candados de protección llamados Proxy´s que funcionan como escudos y filtran la información que pasa por ellos.

10.3 Proceso de Operación

El proceso de manejo de este Site por parte de los usuarios o clientes a manejar nuestra información vital, se manejo de la siguiente manera:

Dar de alta un cada uno de los usuarios, para esto se le asigno un Login y un Password único de identificación, el cual no puede ser alterado ni modificado en linea, para mayor seguridad y confianza de parte de un cliente.

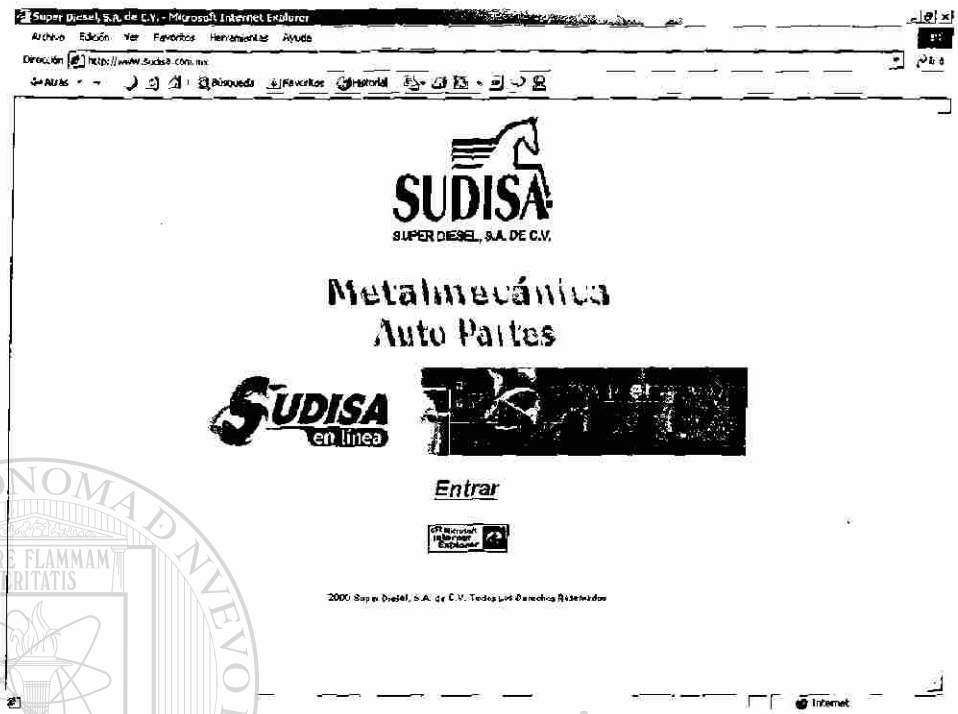


FIGURA 10.1: Pagina de presentación de nuestro proyecto.

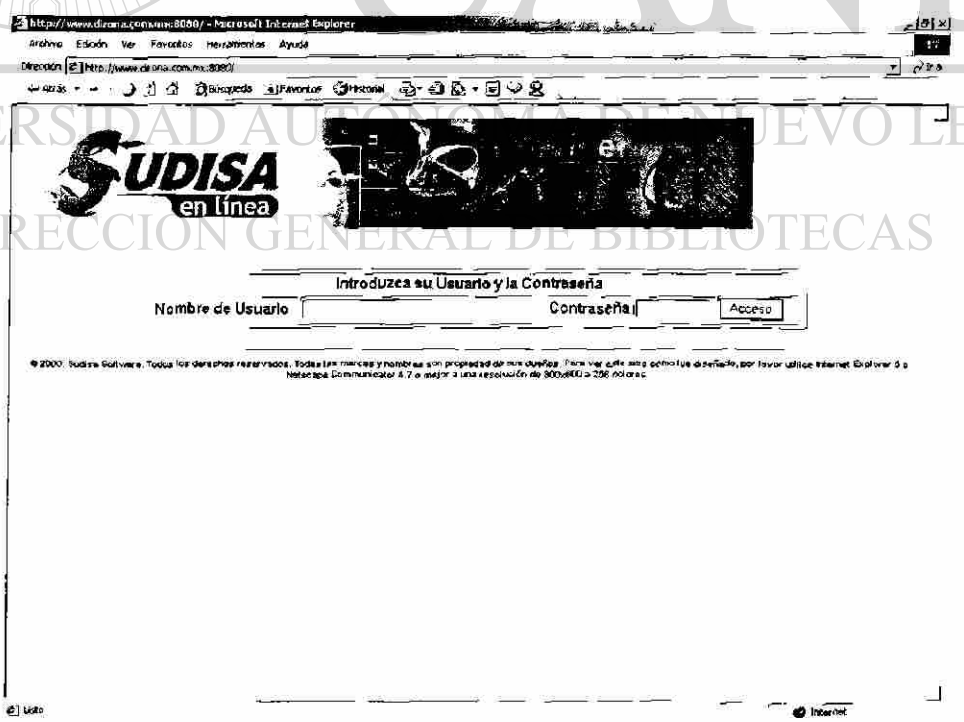


FIGURA 10.2: Pagina de identificación de Usuarios.

En dado caso de que el usuario no sea reconocido por el sistema, el usuario es ubicado en un sistema básico de consulta simple de datos.

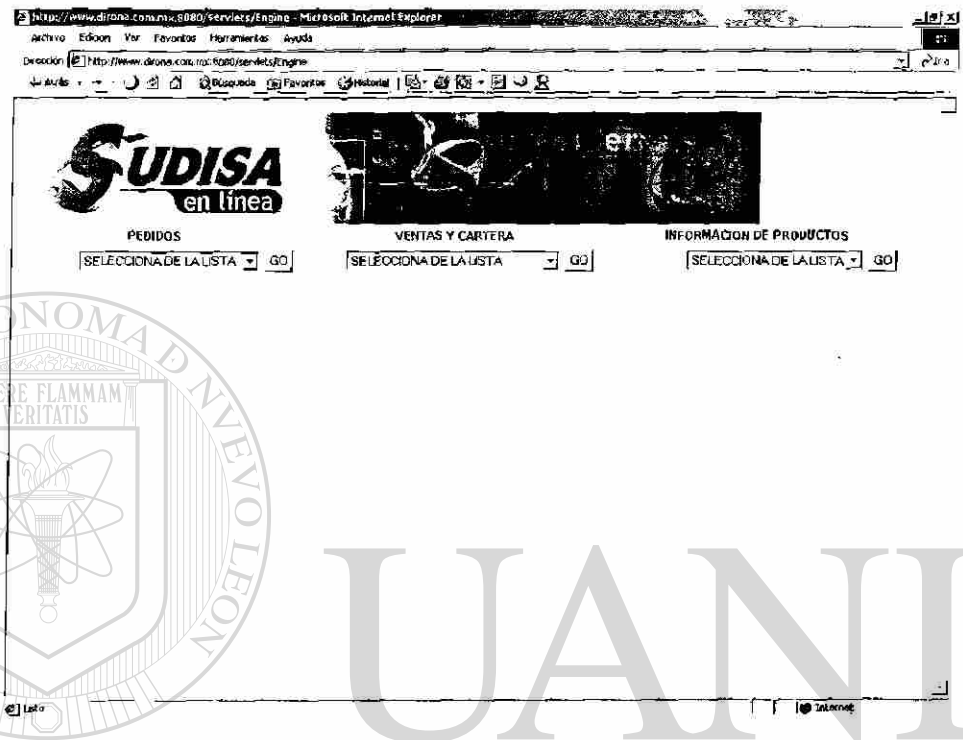


FIGURA 10.3: Despliegue de pagina de consulta simple.

Si del caso contrario su identificación es adecuada en el sistema, se le despliega la misma pantalla, pero mostrando un pequeño cambio el cual consiste en dar una bienvenida.

En la siguiente serie de figura se muestran los primeros 3 menús con operaciones básicas de consulta de pedidos, captura del mismo, manejo de estados de cuenta, y existencias de los mismos entre otras cosas.

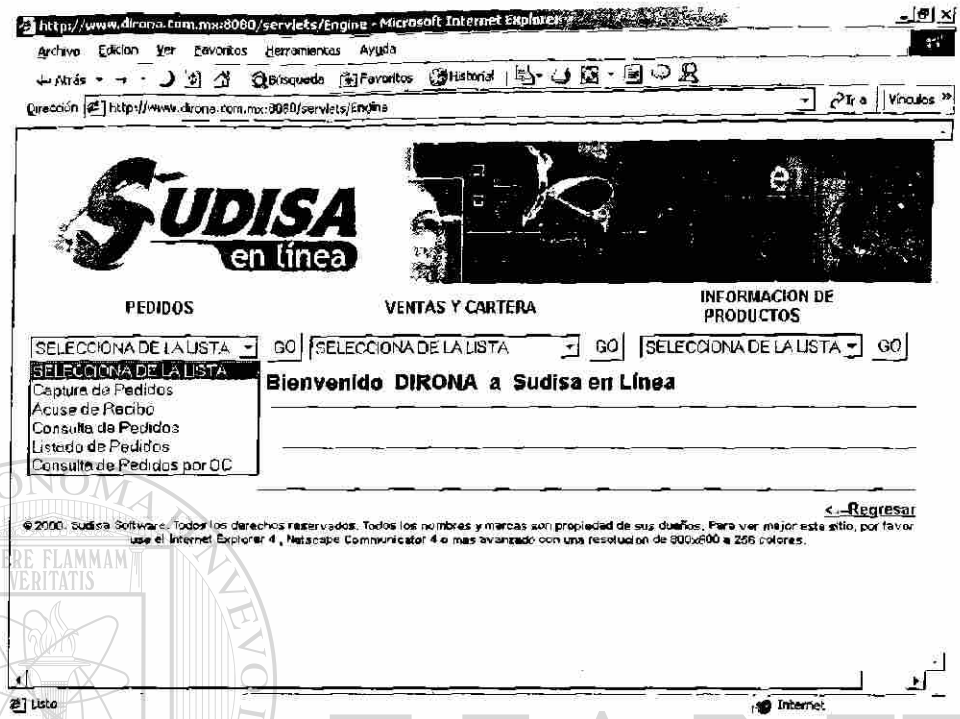


FIGURA 10.4: Despliegue del primer menú.

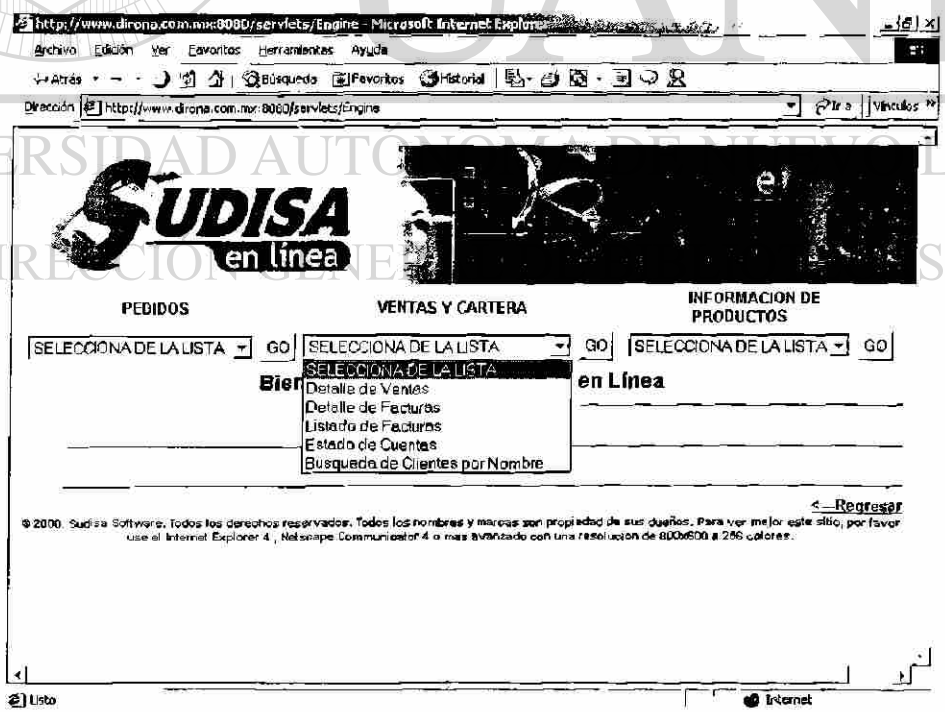


FIGURA 10.5: Despliegue del segundo menú.

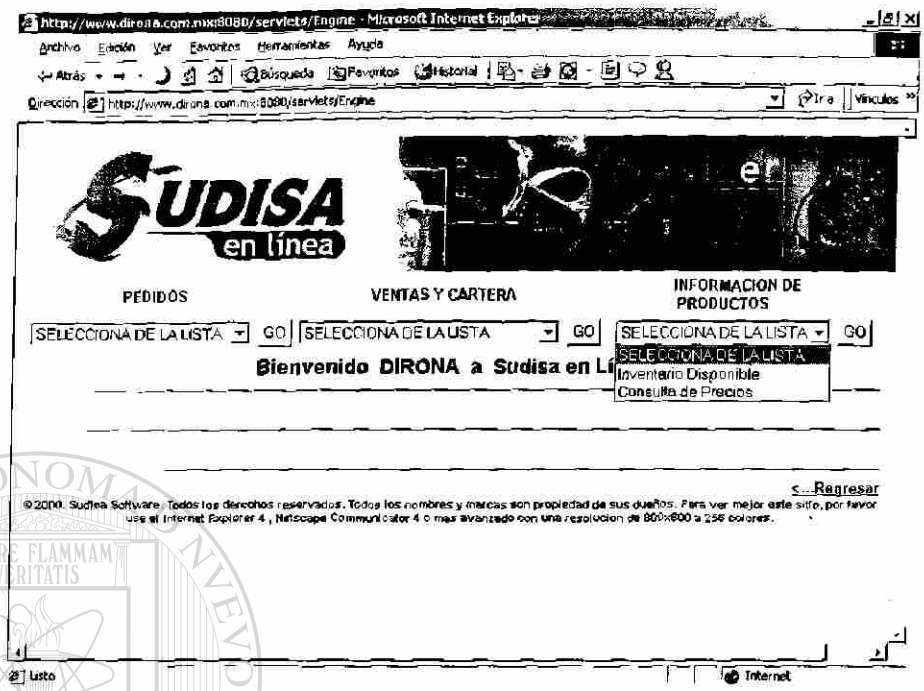


FIGURA 10.6: Despliegue del tercer menú.

En la pantalla siguiente se muestra la forma de llenado de una forma para la captura y levantamiento de una orden de pedido de piezas.

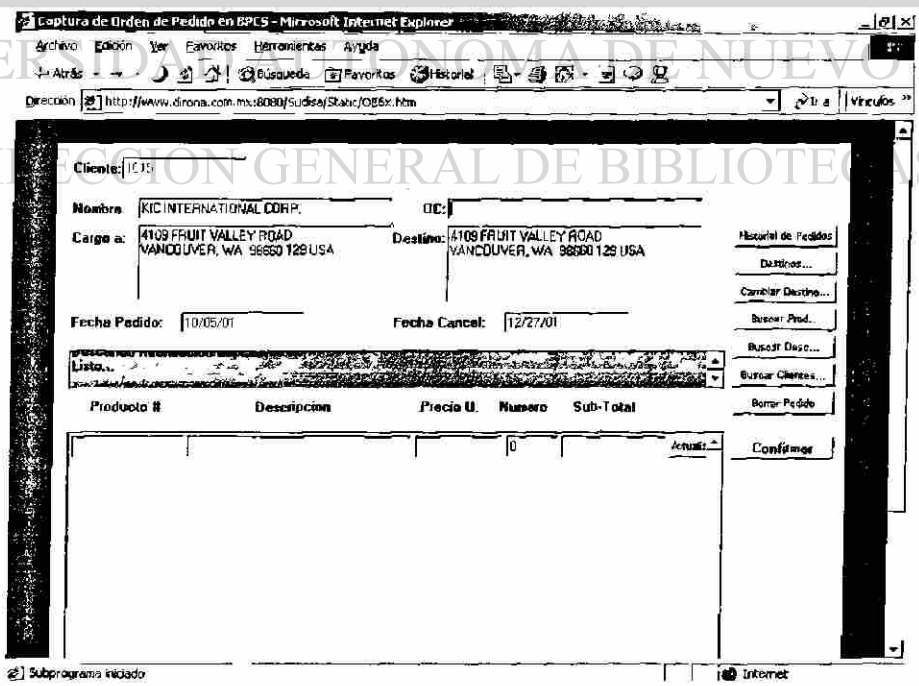


FIGURA 10.7: Despliegue la forma de solicitud de pedido.

En la que se puede apreciar como datos primarios en nombre del cliente, su dirección fiscal del mismo y el lugar donde se proceda a depositar la carga, además de anexar información referente a la fecha de solicitud del mismo y fecha máxima para la cancelación del mismo, y en la parte inferior una descripción detallada de cada una de las piezas a adquirir por parte del cliente, a la derecha se puede apreciar una serie de botones que dan paso a cada una de las operaciones de llenado de la forma descrita.

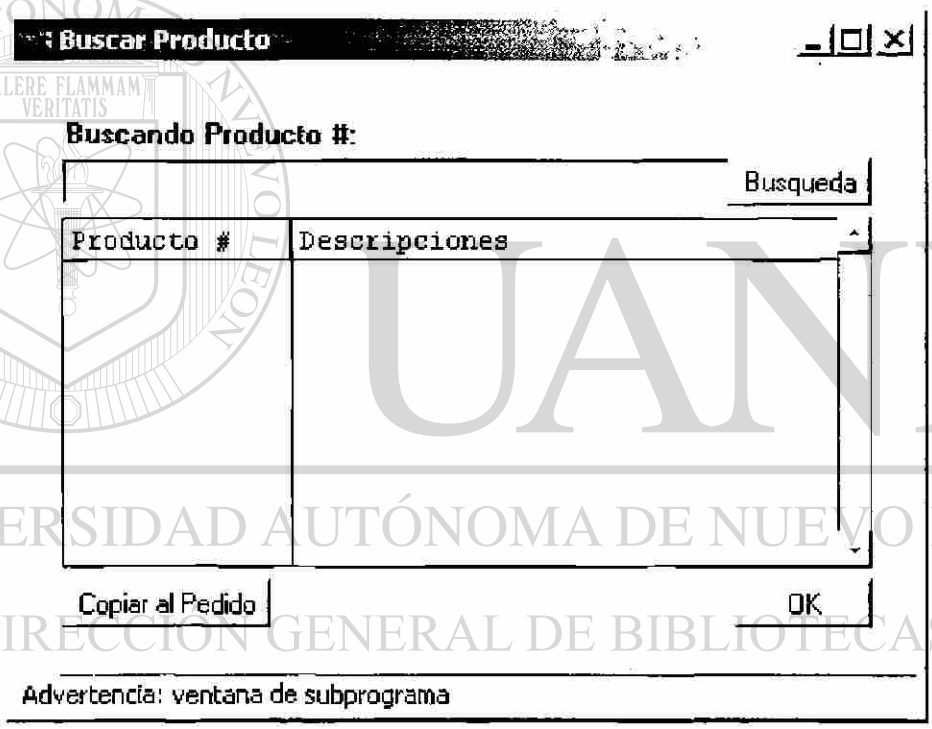


FIGURA 10.8 Menú búsqueda de productos.

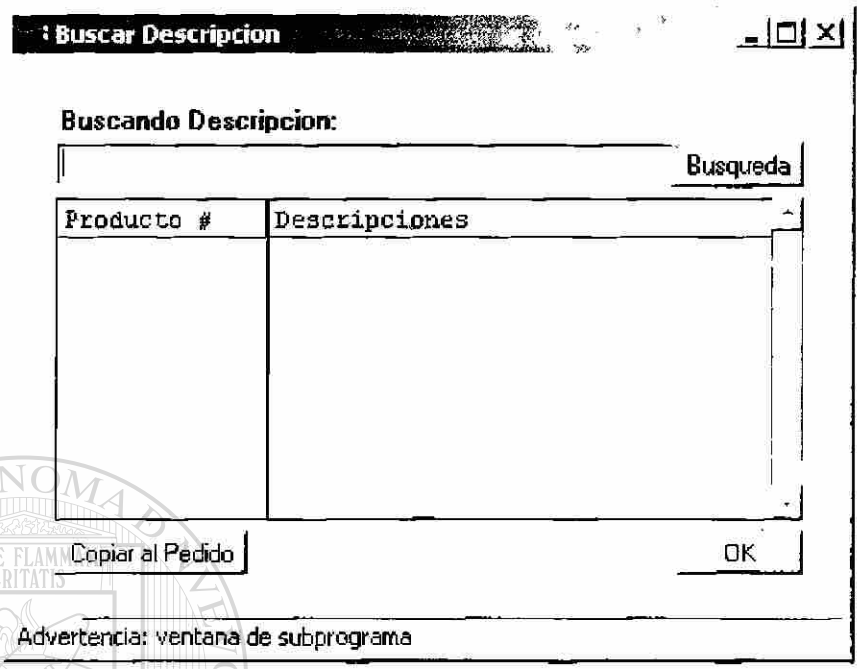


FIGURA 10.9 Menú búsqueda de articulo por numero de parte.

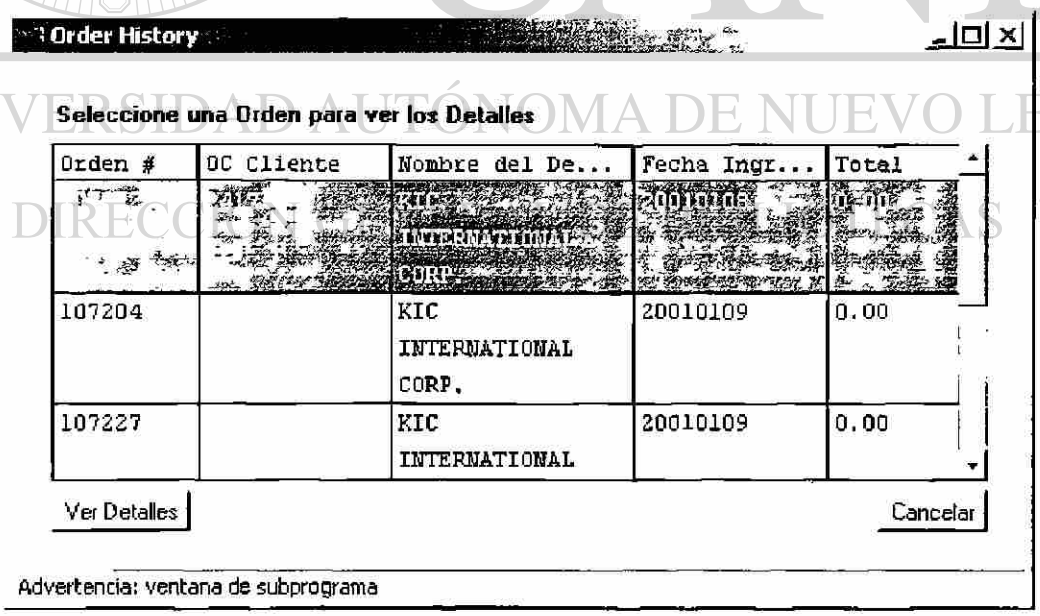


FIGURA 10.10 Menú detallando cada uno de los pedidos del cliente.

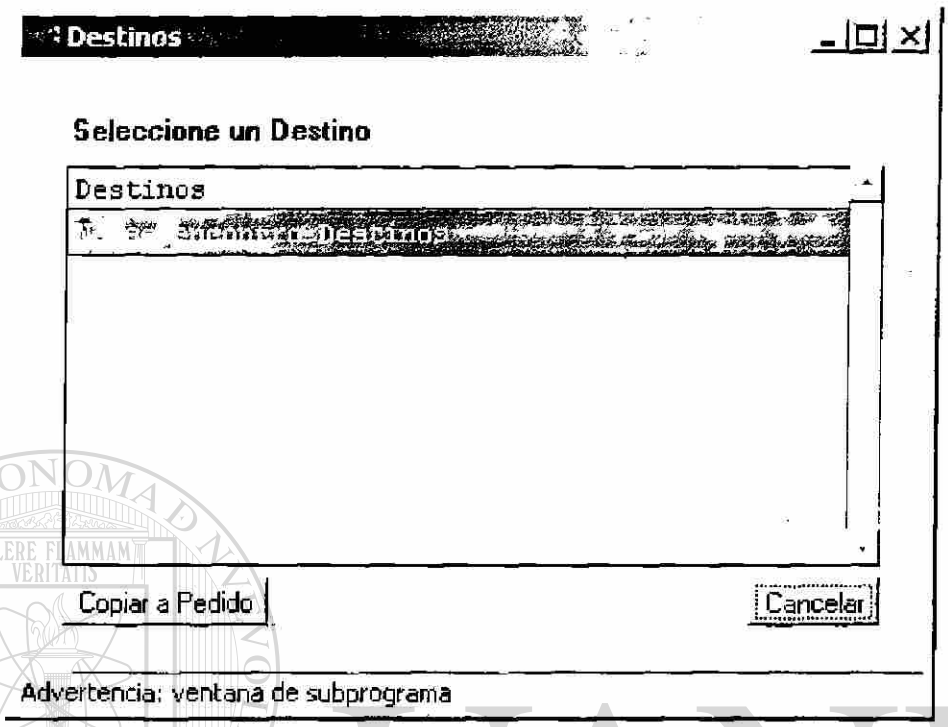


FIGURA 10.11 Menú de verificación de destino.

FIGURA 10.12: Menú de modificación del destino.

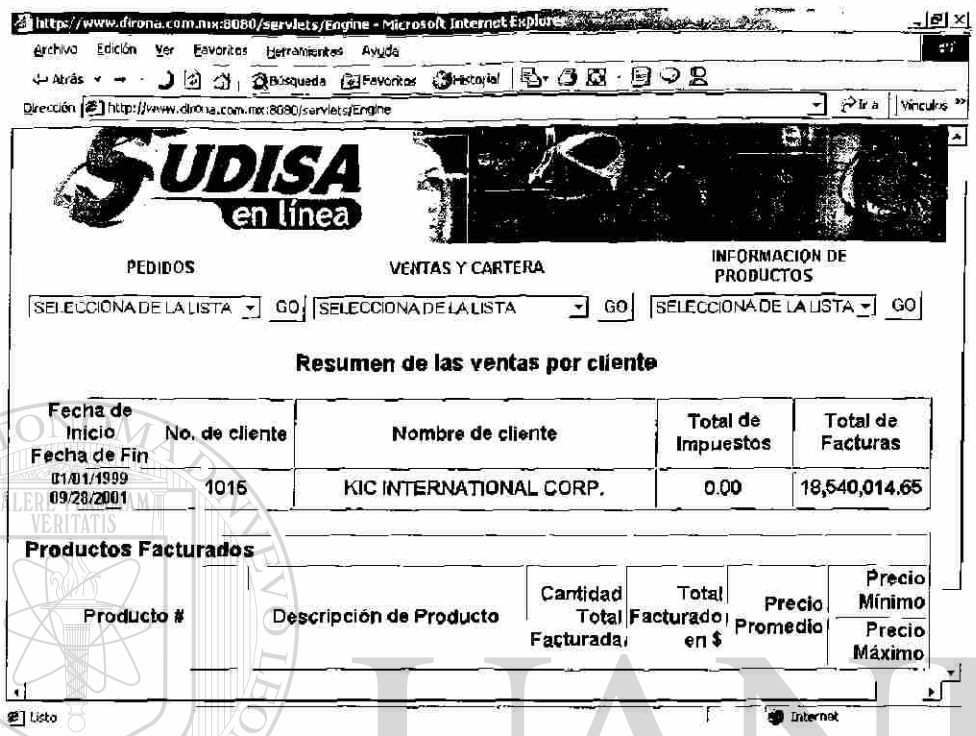


FIGURA 10.13: Resumen de ventas realizadas.

10.4 Conclusiones

La puesta en marcha de este tipo de proyectos deja muchas buenas expectativas a todos las personas que quieren poder cubrir más ampliamente las inquietudes, su poder de crecimiento y bajos costos de operación dado que siempre se puede mantener un contacto directo entre el proveedor y su cliente.

Para las personas que deseen o quieran desarrollar un campo de trabajo, este nueva forma de trabajo es altamente satisfactorio, dado que su potencial de crecimiento es muy elevado.

Como nota final se tienen que considerar los siguientes puntos para una correcta puesta en marcha de un proyecto parecido.

Problema Detectado	Solución o trabajo a futuro
Autentificación mutua entre el cliente y el servidor	Utilización de encripción asimétrica, lo cual a su vez generó el siguiente problema
Administración y distribución de las llaves públicas utilizadas para autentificar	Es necesario realizar una investigación para dar solución a este problema y se deja como un trabajo a futuro la distribución, almacenamiento y administración de llaves públicas o certificados. Lo anterior quedó fuera del alcance de este proyecto
Excesivo el tiempo de envío del servidor al cliente de la librería de CORBA	Las librerías de CORBA deben de ser incluidas en los navegadores. Aunque se encuentran algunas versiones incompletas del estándar en el Netscape
Falta de análisis de los algoritmos utilizados en la implementación y específicamente en las librerías utilizadas para evitar problemas de seguridad como puertas traseras o caballos de Troya.	Es necesario incluir en la metodología de desarrollo de sistemas de comercio electrónico una etapa durante la cual se realice un análisis de las librerías de seguridad que serán utilizadas en el proyecto

TABLA 10.1 Problemas y Soluciones a Futuro.

CAPÍTULO 11

11 Conclusiones y Recomendaciones

11.1 Conclusiones

El trabajo de investigación realizado en el desarrollo de la tesis permitió identificar los cambios y requerimientos necesarios para incursionar en el comercio electrónico, el cual tendrá un gran crecimiento en el número de usuarios del Internet, que es actualmente de más de 200 millones en todo el mundo. Queda claro el potencial para el intercambio de productos, servicios o información por medio de este nuevo medio de venta y distribución.

Existe una gran cantidad y diversidad de sitios en Internet que ofrecen productos, servicios o información bajo el esquema de negocio a persona y negocio a negocio.

Actualmente en México se requiere avanzar en temas y aspectos legales, económicos, sociales y políticos para aprovechar la ventaja competitiva que ofrece el comercio electrónico, con la consecuente reducción de costos de operación. La generación de nuevos productos y servicios, y la necesidad de recursos humanos especializados. Debido al retraso en México del comercio digital, existen múltiples oportunidades que pueden ser aprovechadas por emprendedores, así como la generación de proyectos de investigación y vinculación del área académica y empresarial. Derivado de los anterior, es

posible crear las empresas denominadas "Internet Startups", las cuales presentan un gran riesgo pero también una gran oportunidad.

La tecnología se encuentra lista para enfrentar los requerimientos de infraestructura de comunicaciones, hardware, software y seguridad que requieren las aplicaciones de transacciones electrónicas. A pesar de ello es necesario realizar un análisis de riesgo que permita identificar y cuantificar los riesgos al realizar un proyecto de comercio electrónico.

Durante el desarrollo del proyecto de implementación del protocolo SET, el cual se basó en el esquema básico de seguridad presentado en el Apéndice A permitió detectar algunos problemas como fueron: la administración y distribución de llaves, validación de la seguridad en las librerías de código, el uso e implementación de algoritmos más seguros, entre otros.

El uso de certificados por parte de las empresas debe de ser extendido a los usuarios finales, así como la creación de autoridades certificadores y la legislación correspondiente. Por otra parte es necesario definir nuevos protocolos de comercio electrónico que complementen la capacidad de pagos electrónicos del SET. Para ello el uso del XML debe permitir un mayor intercambio de información de forma transparente entre las empresas.

La hipótesis presentada en la tesis fue que es posible minimizar los riesgos de la seguridad del comercio electrónico a través de Internet siempre y cuando se utilicen los mecanismos, técnicas, algoritmos y protocolos adecuados, los cuales deben de ser analizados de forma continua, ya que pueden ser atacados en cualquier momento poniendo al descubierto su vulnerabilidad.

Por tanto, la correcta selección e implementación de los mecanismos, técnicas, algoritmos y protocolos para el comercio electrónico permite garantizar

con un alto porcentaje la seguridad en las transacciones electrónicas a través de Internet.

Por lo anterior, la realización de un proyecto de comercio electrónico presenta retos que van desde la base teórica del comercio electrónico y la estrategia hasta la selección de los mecanismos, técnicas, algoritmos y protocolos de comercio digital. La investigación y el desarrollo de la clínica empresarial logró cumplir el objetivo de presentar una confrontación de la teoría con un proyecto real, el cual identificó la complejidad de los proyectos de comercio electrónico.

Finalmente en el Apéndice A se incluyó una guía del documento que pretende unificar los conceptos presentados en este documento de forma gráfica, permitiendo identificar los temas relevantes para el desarrollo de un proyecto de comercio electrónico tanto para el modelo de negocio a persona como el modelo de negocio a negocio, el cual incluye el modelo de intra-negocio.

11.2 Recomendaciones

El desarrollo del presente trabajo de tesis sobre el comercio electrónico y la seguridad inherente a cualquier sistema distribuido, deja algunas incógnitas que deberán ser aclaradas y detalladas en diversos trabajos en un futuro.

Es necesario desarrollar proyectos de comercio electrónico utilizando el estándar XML y SSL, con el objetivo de evaluar de forma práctica las ventajas y desventajas de ambas tecnologías, además de identificar situaciones o problemas distintos a los presentados en esta tesis en la implementación de un proyecto de comercio electrónico.

Un proyecto que involucra ambas tecnologías es un "digital marketplace", el cual permite a un grupo de empresas realizar las operaciones de compra y venta mediante el apoyo de un sistema capaz de extender dichas operaciones a un tercero.

Adicionalmente es necesario desarrollar una guía de seguridad que permita definir un procedimiento de verificación de la autentificación, confidencialidad, integridad y no - repudiación.

Además de incluir un estudio profundo sobre la seguridad bajo el enfoque matemático. Es importante incluir lineamientos base para la definición de una estrategia de comercio digital y profundizar en los aspectos económicos, de negocios, sociales y legales requeridos para una incursión en esta nueva forma de realizar negocios de forma electrónica.

BIBLIOGRAFIA

1. Advanced Encryption Standard [AES 99], NIST, http://csrc.nist.gov/encryption/aes/, Año de Consulta 2001

2. Alberts Robert J. [Alberts 98], Townsend Anthony M., Whitman Michael E., The Threat of Long-Arm Jurisdiction to Electronic Commerce, Communications of the ACM, Diciembre 1998, Vol 41. No 12.

3. Comité Editorial AMECE [AMECE1 99], La Factura Electrónica: un documento que las empresas ya están esperando, http://www.amece.com.mx/f_bole22.html, Noviembre 2000

4. GILCE [AMECE2 99] y la legislación del Comercio Electrónico, http://www.amece.com.mx/f_bole24.html, Diciembre 2000

5. Anderson Ross J. [Anderson 99], Why Cryptosystems Fail, Communications of the ACM, Noviembre 2000 Vol. 37 No. 11, pg. 32-40

6. Applegate [Applegate 96], L.M., Holsapple, C.W., Kalakota, R., Radermacher, F.J., y Whinston, A.B., Electronic commerce: building blocks of new business oportunity. J. Organiz. Comput. Electr. Comm. 6. 1 (1997), pg. 1-10

7. Baldwin Robert W. [Baldwin 97], Chang C. Victor, Locking the e-safe, IEEE, Febrero 1997, pg. 40-46.

8. Banamex [Bnx_edi 99], EDI, http://www.banamex.com/portal/banamex/bdigital/edi.htm, Año de Consulta 2001

9. Bolignano Dominique [Bolignano 97], Dyade GIE, Towards the Formal Verification of Electronic Commerce Protocols, IEEE, 1997, pg. 133-146.

10. [Bosak 99] Bosak Jon, Bray Tim, XML and the Second-Generation WEB, Scientific American, Mayo 1998.

11. BOTTS Steve [Botts 96], The Internet as a Key Element of your EDI Strategy, Premenos Corp., 1996,, http://www.commerce.net/events/conference/1996/edi/index.htm

12. Brands Stefan [Brands 95], Electronic Cash on the Internet, IEEE, 1997, pg. 64-84

13. [Burrows 90] BURROWS MICHAEL, ABADI MARTIN, ROGER NEEDHAM, A Logic of Authentication, ACM Transactions on Computer Systems, Vol 8, No. 1, Febrero 1999, Páginas 18-36.

14. Camp L. Jean [Camp 97], Sirbu Marvin, Critical Issues in Internet Commerce, IEEE Communications Magazine, Mayo 1998, pg. 58-62.

15. [Carter 98] Carter Glyn, A matter of trust, IEEE , 1999

16. [Clarke 98] CLARKE, Roger, Electronic Data Intechange (EDI): An Introduction, Xmax Consultancy Pty Ltd, Australian National University, Diciembre 1999, http://www.anu.edu.au/people/Roger.Clarke/EC/EDIIntro.html

17. CORNELLA [Cornella 99], Alfonso, Ciclo de Vida y Cadena de Valor en Información, EXTRA!-NET, El impacto de la información online en las organizaciones, Mensaje 162, ESADE Barcelona, 1999. http://www.extra-net.net/articulos/en961009.htm

18. Courouris G. [Coulouris 94], Dollimore J., Kindberg T., Distributed Systems: Concepts and Design, Addison – Wesley, Febrero 1996.

19. http://orgwis.gmd.de/focus.html#SWB, http://www.dml.cs.ucf.edu/cybrary/fyi_cscw.html, Año de Consulta 2001

20. Cudi – Corporación Universitaria para el Desarrollo de Internet, Antecedentes, WWW, http://www.internet2.edu.mx/antece.htm, Año de Consulta 1999

21. Cudi [CUDI_MX2 99]– Corporación Universitaria para el Desarrollo de Internet, Miembros, WWW, http://www.cudi.edu.mx/membre.htm, Año de Consulta 2001

22. Chew Suan-Suan, Kok-Leong Ng, Chye-Lin Chee, Iauth: An Authentication System for Internet Applications, IEEE, 1997, pg. 654-659

23. http://www.nist.gov/ [DES_FIPS_46-1 88] Fecha de Publicación 22 de enero de 1988

24. http://csrc.ncsl.nist.gov/cryptval/des/fr990115.htm, Publicación 15 de enero de 2000

25. DES Modes of Operation [DES_FIPS_81 80], Publicación en diciembre 2 de 1980

26. DES Challenge [DES_CHAL_III 99] III http://www.rsa.com/rsalabs/des3/des3_qa.html, Año de Consulta 1999.

27. Deswarte Yves [Deswarte 97], Internet Security Despite Untrustworthy Agents and Components, IEEE, 1997, pg. 218 –219

28. Distributed net [DISTRIBUTED_NET 99], http://distributed.net, Año de Consulta 2001

29. DTD [DTD 00], http://www.w3.org/XML/1998/06/xmlspec-report/ 19980910.htm, Año de Consulta 2000

30. Enterprise Java Beans (EJB) [EJB 00] , Año de Consulta 2000, http://java.sun.com/products/ejb/index.html, http://java.sun.com/products/ejb/newspec.html, http://java.sun.com/products/ejb/docs.html,

31. ENIAC Page [Eniac 98], Qué es EDI?, 1998, http://www.eniac.com/edihtm.htm

32. EURO PAPERS [EURO 00], http://europa.eu.int/euro/html/rubrique-defaut5.html?rubrique=133&lang=5, Año de Consulta 2000

33. Fúster Amparo [Fúster 98], Martínez Dolores de la Guía, Hernández Luis, Montoya Fausto, Muñoz Jaime, Técnicas Criptográficas de protección de datos, Alfaomega, 1998

34. Garcés Rosas José [Garcés 98], Moreno Ledezma Gabriel, La Oferta de Servicios Internet en México, Tendencias Generales 1997-2002, Select - IDC, 1998.

35. XML Reality Check [Gartner 99], GartnerGroup, Conference presentation, 1999

36. Gleick James, The End of Cash, http://www.around.com/money.html,[Gross 99] Gross Neil, Building Global Communities, Business Week, Marzo 22 1999, pg. EB22– EB23.

37. Hamm Steve [Hamm 99], Stepanek Marcia et al., Electronic Business a Survival Guide, Business Week, Marzo 22 2000, pg. EB6 – EB27.

38. [Hsiao 79] Hsiao David K. [Hsiao 79], Kerr Douglas S., Madnick Stuart E., Computer Security, Academic Press ACM Monograph Series, 1989

39. Hsu Yung-Kao [Hsu 98], Seymour Stephen P., AN INTRANET SECURITY FRAMEWORK BASED ON SHORT-LIVED CERTIFICATES, IEEE, Marzo – Abril 1998.

40. HTML [HTML 00], Año de Consulta 2000 http://www.w3.org/TR/html4/, http://www.ietf.org/rfc/rfc1866.txt,

41. IBM Application Framework for e-business [IBM1 00], Año de Consulta 2000, http://www-4.ibm.com/software/ebusiness/AppServices.html

42. Arquitectura Tecnológica (IBM) [IBM2 00], Año de Consulta 2000, http://www-4.ibm.com/software/ebusiness/e-comServices.html, http://www-4.ibm.com/software/ebusiness/paper-arch_overview.html.

43. INEGI [INEGI1 00], Estructura Poblacional de México, WWW, http://www.inegi.gob.mx/poblacion/espanol/estrupob/pob_01.html, Año de Consulta 2000

44. Mission de Internet 2 [InternetII_A 00], WWW, Año de Consulta 2000 http://www.internet2.edu/html/mission.html#,

45. http://www.internet2.org [InternetII_B 00], Año de Consulta 2000

46. Comisión Europea [Ispo_cec 99], Electronic Commerce - An Introduction, Julio 1999, http://www.ispo.cec.be/ecommerce/answers/introduction.html

47. Jayaram N.D. [Jayaram 98], Morse P L R, NETWORK SECURITY - A TAXONOMIC VIEW, IEEE, Año de Consulta 1998

48. Java Database Connectivity (JDBC) [JDBC 00], Año de Consulta 2000, http://java.sun.com/products/jdbc/index.html, http://java.sun.com/products/jdbc/datasheet.html, http://java.sun.com/products/jdbc/features.html, http://java.sun.com/products/jdk/1.3/docs/guide/jdbc/index.html

49. Java Server Pages (JSP) [JSP 00], Año de Consulta 2000, http://java.sun.com/products/jsp/index.html

50. Kalakota Ravi [Kalakota 96], B. Whinston Andrew, FRONTIERS OF ELECTRONIC COMMERCE, 1996.

51. Kalakota Ravi[Kalakota 97], B. Whinston Andrew, ELECTRONIC COMMERCE A Manager's Guide, 1998

52. Kapidzic Nada, Davidson Alan, A Certificate Management System: Structure, Functions and Protocols, IEEE, 1995, pg. 153-160.

53. G.W. Keen Peter [Keen 97], Balance Craigg, ON – LINE PROFITS A MANAGER'S GUIDE TO ELECTRONIC COMMERCE. Harvard Business School Press Boston, Massachusetts, 1997.

54. Krause Micki [Krause 99], Tipton Harold F., Handbook of Information Security Management, 1999, editorial Auerbach.

55. Lobel Mark [Lobel 99], The Case for Strong User Authentication, Security Dynamics, http://www.securid.com/products/whitepapers/casestrong-wp.html, Año de Consulta 1999

56. LOTUS NOTES [LOTUS_NOTES 00], Año de Consulta 2000 http://www.lotus.com/home.nsf/welcome/notes, http://www.lotus.com/home.nsf/welcome/domino, http://www.lotus.com/products/r5web.nsf/webfamilypi/Family+of+Servers?opendocument, http://www.lotus.com/home.nsf/welcome/learnspace,

57. Lu W.P. [Lu 92], Sundareshan M.K., Enhanced Protocols for Hierarchical Encryption Key Management for Secure Communication in Internet Environments, IEEE Transactions on Communications, Vol 40 No 4, Abril 1992, pg. 658 – 660

58. Machover Carl [Machover 97], Internet Business Opportunities, IEEE, 1997, pg. 138-143.

59. Marín Erasmo [Marín 99], Comentarios a la Modificación del Artículo 211 del Capítulo II del Código Penal "Acceso Ilícito a Sistemas y Equipos de Informática", Revista Soluciones Avanzadas, Volumen 7, No. 71, Julio 1999, pg. 23-24.

60. Fischer Mathew [Mathew 00], How to implement the Data Encryption Standard, Eurocrypt informations, http://www.satswiss.com/twinpics/des-how-to.html, Año de Consulta 2001

61. McClure Stuart [Mcclure 98], PKI tames network security. (developing a public key infrastructure), InfoWorld, Septiembre 14 1998 v20 n37 pg65.

62. McChesney Michael C. [mcchesney 97], Banking in cyberspace: an investment in itself, IEEE SPECTRUM, Febrero 1997, pg. 54-49.

63. Mitchell John C. [Mitchell 97], Shmatikov Vitaly, Stern Ulrich, Finite-State Analysis of SSL 3.0 and Related Protocols, Stanford University, Agosto 1997.

64. http://www.intel.com/intel/museum/25anniv/hof/moore.htm, Año de consulta 2000

65. NIST [Nist 92], The Digital Signature Standard, Communications of the ACM, Julio 1999 Vol. 35, No. 7, pg. 36 – 40

66. [NUA1 00] Nua Internet Surveys, How Many Online, WWW, http://www.nua.ie/surveys/analysis/graphs_charts/comparisons/how_many_online.html., Año de Consulta 2000

67. Nua Internet Surveys [NUA2 00], Ecommerce US, WWW, http://www.nua.ie/surveys/analysis/graphs_charts/comparisons/ecommerce_us.html, Año de Consulta 2000

68. Nua Internet Surveys [NUA3 00], América Latina, WWW, http://www.nua.ie/surveys/how_many_online/s_america.html, Año de Consulta 2000

69. Oppliger Rol f[Oppliger 95], Internet security enters the Middle Ages, IEEE, Octubre 1998, pg. 100-101

70. http://www.intel.com/PentiumIII/ [Pentium_III 00], Año de Consulta 2000

71. Pretyy Good Privacy [PGP 00], Año de Consulta 2000, http://www.pgpi.org, http://www.pgpi.org/doc/pgpintro/,

72. Understanding Public Key Infrastructure (PKI) The Key Management Problem [PKI 99], Security Dynamics, Año de Consulta 1999, http://www securid.com/products/whitepapers/pki/index.html

73. Project Management Institute [PMBOK1 99], A Guide to the Project Management Body of Knowledge, 1996, PMI Publishing Division, WWW, Año de Consulta 1999, http://www.pmi.org/publictn/pmboktoc.htm

74. Ponce Bob [Ponce 99], The Impact of MP3 and the Future of Digial Enterteinment Products, IEEE Communications Magazine, Septiembre 1999.

75. Pulido Karla [Pulido 99], EDI y XML en el comercio electrónico entre empresas, Trabajo de Tesis, ITESM - CCM, 1999.

76. Rajsbaum Sergio [Ra0jsbaum 99], Panorama General de Criptografía y seguridad, Parte II, Soluciones Avanzadas, Año 7 #71, Julio 99, pg. 38-48

77. RDF [RDF 00], Año de Consulta 2000, http://www.w3.org/RDF/

78. R. Rivest [RFC1320 92], RFC 1320, The MD4 Message-Digest Algorithm, http://andrew2.andrew.cmu.edu/rfc/rfc1320.html, Abril 1992.

79. R. Rivest [RFC1321 92], RFC 1321, The MD5 Message-Digest Algorithm, http://andrew2.andrew.cmu.edu/rfc/rfc1321.html, Abril 1992.

80. Rheingold Howard [Rheingold 99], The Internet and the Future of Money, Tomorrow Column, http://www.transaction.net/press/tomorrow.html, Año de Consulta 1997

81. Riggins Frederick J. [Riggins 98], Rhee Hyeun-Suk (Sue), Toward a unified view of Electronic Commerce, Communications of the ACM, Octubre 1998 Vol. 41 No. 10, pg. 88 – 95.

82. RSA Laboratories [RSA 99] , FAQ About Today's Cryptography v4.0 http://www.rsa.com, Año de Consulta 1999

83. Russ Mundy [Russ 97], Chair, Panel On Security Of The Internet Infraestructure, IEEE,1997, pg. 72

84. Universidad Virtual [RUV 99], ITESM, http://www.ruv.itesm.mx, Año de Consulta 2000

85. Saha Avi [Saha 99], Application Framwork for e-business:Portals, IBM Software Strategy, November 1999, http://www-4.ibm.com/software/developer/library/portals/index.html

86. SDH Pocket Guide [SDH 00], Año de Consulta http://www.wg.com/techlibrary/articles/sdh_guide1.html

87. The Role of Strong Authentication in Securing Business Over the Internet [securitydynamics WP], Whitepaper Security Dynamics.

88. Java Servlets [Servlets 00], Año de consulta 2000, http://java.sun.com/products/servlet/index.html, http://java.sun.com/products/servlet/2.2/, http://java.sun.com/products/servlet/2.2/javadoc/index.html.

89. SET [SET 99], Año de Consulta 1999, http://www.setco.org/, http://www.setco.org/set_specifications.html

90. Sheperd Simon J [Sheperd 96], LESSONS LEARNED FROM SECURITY WEAKNESSES IN THE NETSCAPE WORLD WIDE WEB BROWSER, IEEE, 1996

91. Sirbu Marvin A. [Sirbu 97], Credits and debits on the Internet, IEEE SPECTRUM, Febrero 1997, pg. 23-29.

92. Social Web Research Program [Social_web 00], http://orgwis.gmd.de/projects/SocialWeb/, Año de Consulta 00

93. SONET Telecommunications Standard Primer [SONET 00], http://www.tek.com/Measurement/App_Notes/SONET/, Año de Consulta 2000

94. Freier Alan O. [SSL 96], Karlton Philip, Kocher Paul C., The SSL Protocol Version 3.0, Internet Draft, Netscape Communications Corporation, Marzo 1999

95. Internet Startups [Startups 00], http://www.internetnews.com/bus-news/article/0,1087,3_314701,00.html, Año de Consulta 2000

96. Steinauer Dennis D. [Steinnauer 97], Wakid Shukri A., Rasberry Stanley, Trust and Traceability in Electronic Commerce, Standard View Vol 5. No 3, Septiembr 1997, pg. 118-124.

97. Stockel Anna [Stockel 95], Securing Data and Financial Transactions, IEEE, 1998, pg. 397- 401.

98. Tidwell Doug [Tidwell 99], Tutorial: Introduction to XML, XML developerWorks Team, Julio 1999, http://www.ibm.com/developerWorks

99. Recomendación UIT – T X.509 [X.509 93], diciembre de 1993. Servicios de Directorio. Autenticación.

100. Margherio, ET. AL. [USDC 99], The emerging digital economy, U.S. Department of Commerce, Año de consulta 1999

101. U.S Government Working Group on Electronic Commerce [USGWGEC 98], First Annual Report, Noviembre 1999

102. Varadharajan Vijay [Varadharajan 96], Mu Yi, On the Design of Secure Electronic Payment Schemes for Internet, IEEE, 1996, pg. 78-87.

103. SET Secure Electronic Transaction Specification Book 1: Business Description, Visa – Mastercard [Visa 97], Mayo 31 de 1999.

104. Visa México [Visa_mx 99], http://www.visa.com.mx/s3_tec_com3.html, Año de Consulta 2001

105. Wagner David [Wagner 96], Schneier Bruce, Analysis of the SSL 3.0 protocol, The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, Noviembre 1996, pp. 29-40. http://www.counterpane.com/ssl.html

106. Weiss Mark Allen [Weiss 92], Data Structures and Algorithm Analysis, Benajamin Cummings, 1998

107. Welch Brian [Welch 99], Electronic banking and treasury security, CRC Press NatWest, 1999

108. Winslett Marianne [Winslett 99], Ching Neil, Jones Vicki, Slepchin Igor, Assuring Security and Privacy for Digital Library Transactions on the Web: Client and Server Security Policies, IEEE, pg. 140-151, Año de Consulta 1999

109. Xlink [XLINK 00], Año de consulta 2000, http://www.w3.org/TR/xlink/

110. Recomendación W3 XML [XML 00], Año de Consulta 2000, http://www.w3.org/XML/, http://www.w3.org/TR/1998/REC-xml-19980210

111. XSL [XSL 00], Año de Consulta 2000, http://www.w3.org/Style/XSL/Overview.html, http://www.w3.org/TR/xsl/, http://www.w3.org/TR/xslt,

112. Yahya Y. Al-Salqan [Yahya 97], Future Trends In Internet Security,IEEE,1997, pg. 216- 217.

113. YAMAMOTO Kazuhiko [Yamamoto 96], An Integration of PGP and MIME, IEEE, 1996, pg. 17-24.

114. Yan Gloria [Yan 97], C. Paradi Joseph And Suneel Bhargava, BANKING ON THE INTERNET AND ITS APPLICATION, IEEE, 1997, pg. 275-284

Listado de Tablas de Referencia

Listado de Figuras de Referencia

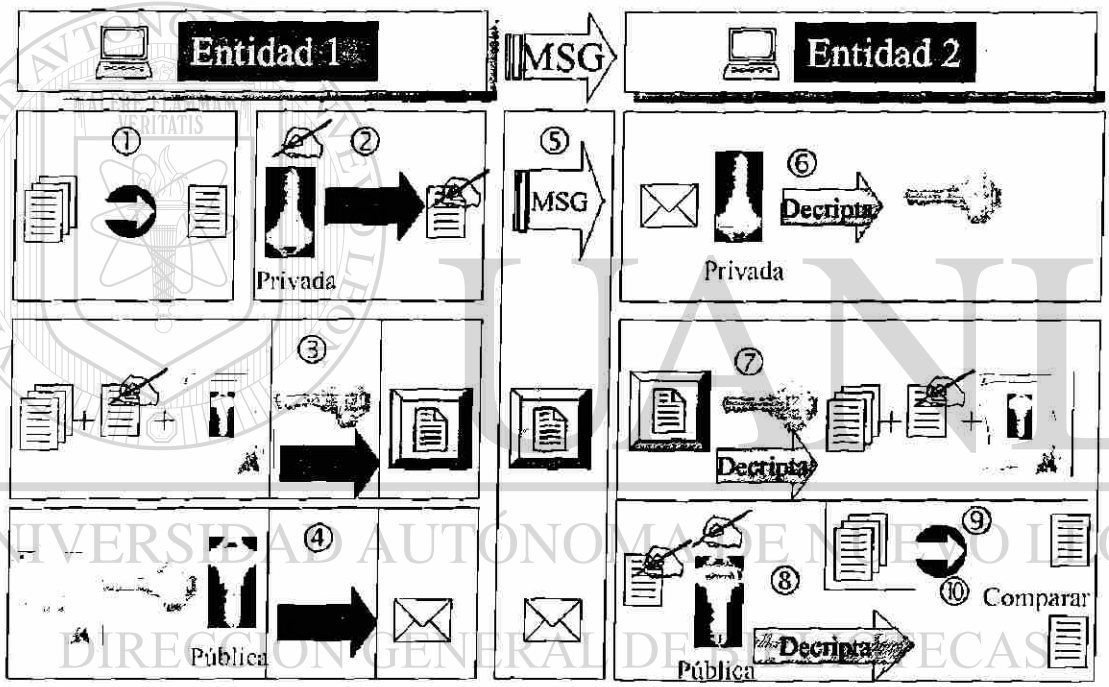
APENDICE A

DIAGRAMA DEL PROTOCOLO SET

GUIA DE REFERENCIA

DIAGRAMA DEL PROTOCOLO SSL

DIAGRAMA DEL PROTOCOLO SET



1. Crear el Message Digest
2. Crear la firma digital
3. Generar una llave simétrica aleatoria
4. Encriptar la llave simétrica
5. Envío de mensaje
6. Desencriptar la llave simétrica
7. Desencriptar la información
8. Desencriptar el Message Digest
9. Crear el Message Digest
10. Comparar los Message Digest

GUIA DE REFERENCIA

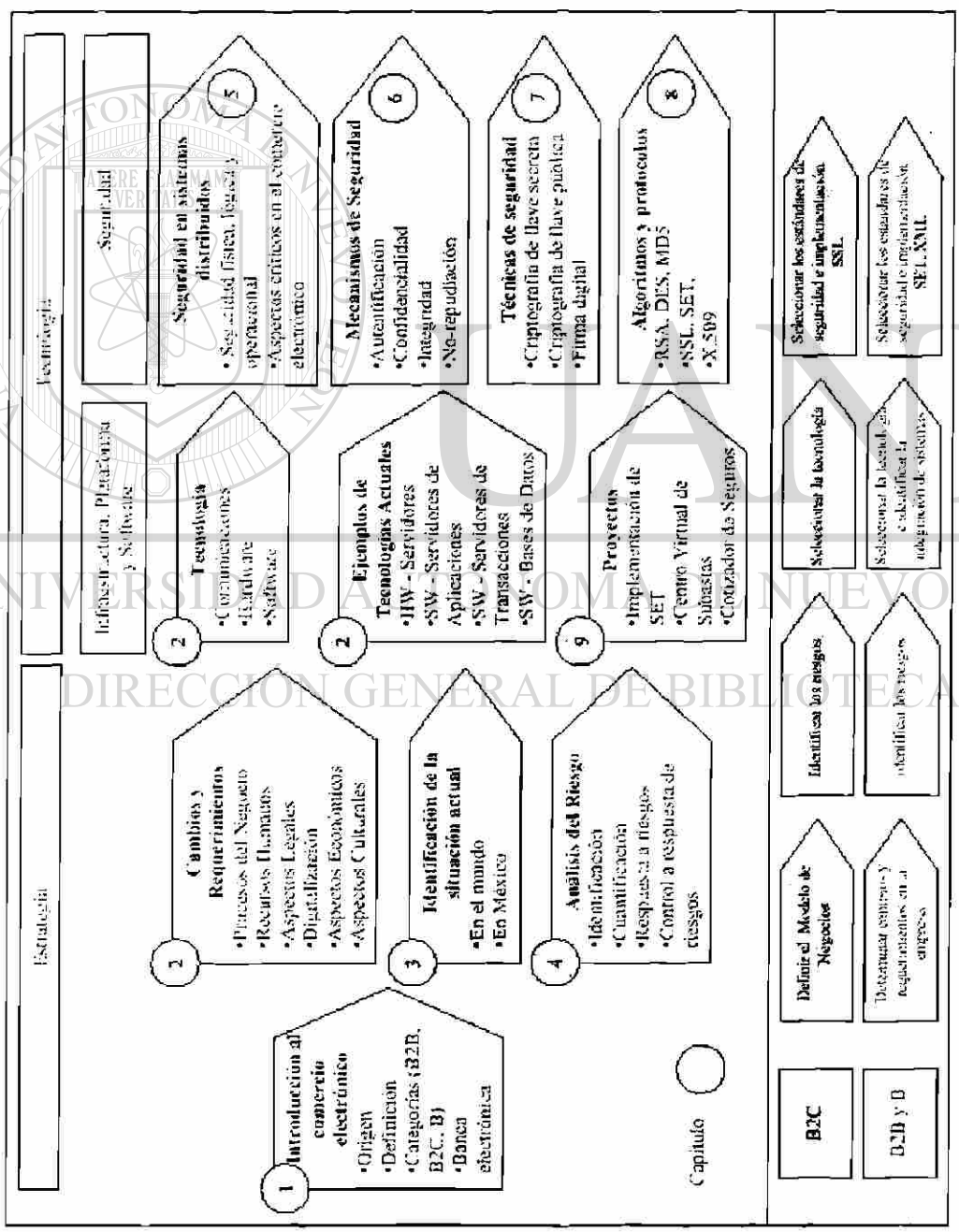
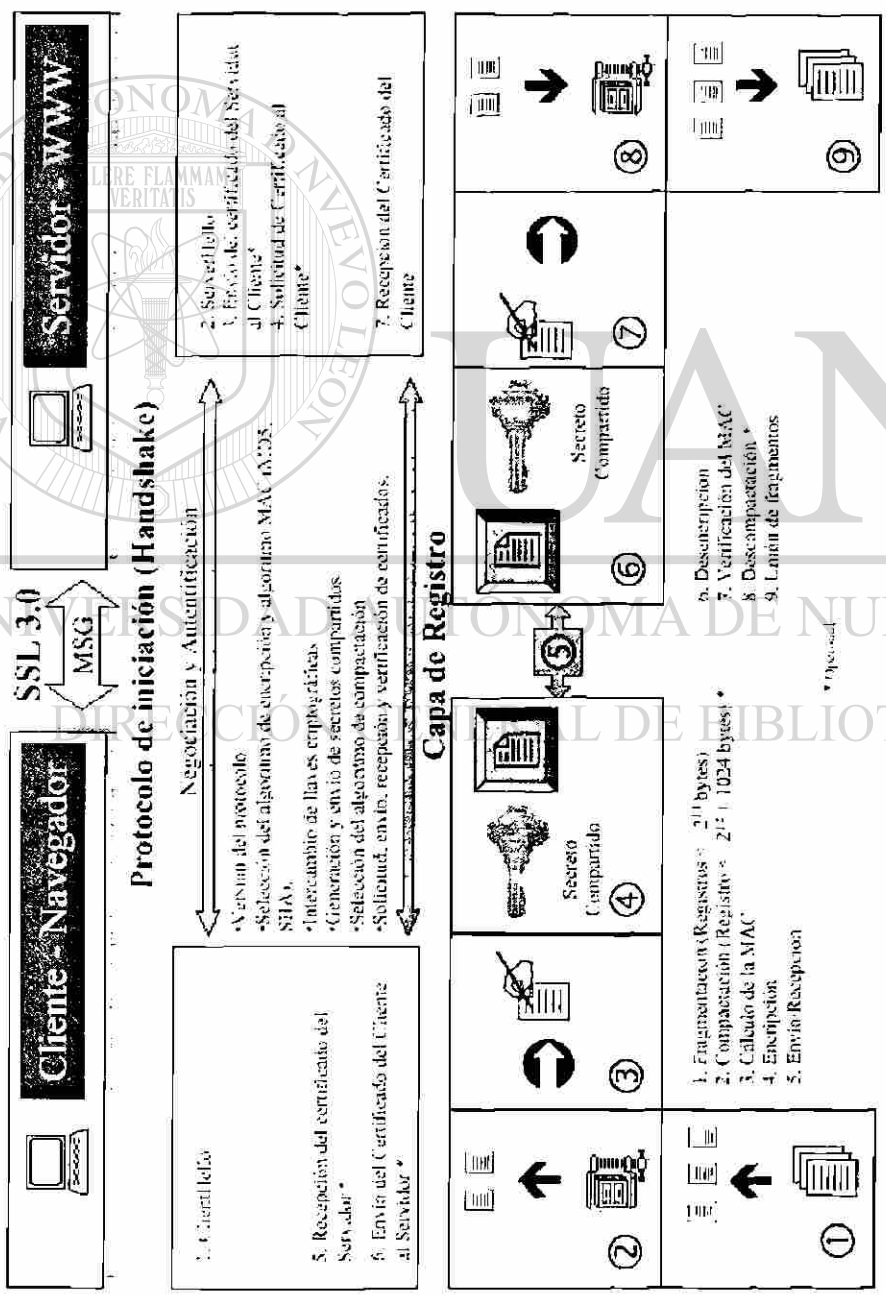


DIAGRAMA DEL PROTOCOLO SSL



APENDICE B

ANEXO A. Introducción al XML

ANEXO A. Introducción al XML

El eXtensible Markup Language (XML) [XML 00] es una nueva tecnología para aplicaciones WEB que se prevé sustituya el HyperText Markup Language (HTML) en los próximos años. XML es el estándar del World Wide Web Consortium (W3C) completado en 1998 que permite crear etiquetas personalizadas y auto descriptibles, a diferencia del HTML. [HTML 00]

La respuesta entusiasta hacia el XML es impulsada debido a la esperanza de resolver uno de los problemas más grandes del WEB y es el la gran cantidad de información disponible y la dificultad para encontrar de forma precisa la información requerida. Estos problemas se deben a la naturaleza del HTML, lenguaje principal de WEB. A pesar de ser el lenguaje más exitoso de publicación electrónico, este es superficial y únicamente expresa como se debe ver el texto, imágenes y botones en una página. La utilización de etiquetas enmarcadas los símbolos (<,>) muestran como se debe ver la información en el browser.

En 1986 surgió un estándar de la International Standards Organization (ISO) llamado Standard Generalized Markup Language (SGML), el cual es un metalenguaje que ha probado su utilidad en aplicaciones de publicación. Por cierto el HTML fue definido utilizando el SGML. El único problema con el SGML es, que es demasiado general.

A partir del SGML el grupo de W3C se dio a la tarea de eliminar los problemas del SGML y desarrollo el XML, el cual consiste en una serie de reglas para crear un metalenguaje a partir de la nada. Estas reglas aseguran que un solo programa compacto llamado parser pueda procesar estos nuevos lenguajes.

A diferencia de la mayoría de los formatos de datos, el XML también hace sentido al ser humano, debido a que consiste en texto ordinario. El poder de XML radica: que las etiquetas siempre vienen en pares como los paréntesis y que pueden ser anidados, uno dentro de otro en múltiples niveles. Esta regla de anidamiento automáticamente obliga a una cierta simplicidad en cada documento XML, el cual toma la estructura conocida como árbol y con ello, las relaciones no son ambiguas Por último otra fortaleza del XML es la utilización del sistema de codificación de caracteres llamado Unicode. Permitiendo así la generación de texto en la mayoría de los lenguajes en el mundo.

Estas características han permitido generar etiquetas específicas para cada industria haciendo más fácil y precisa la búsqueda de información. Como parte del proyecto XML se ha creado un estándar complementario para los metadatos. El Resource Description Framework (RDF) [RDF WWW]el cual hace para los datos WEB lo que las tarjetas de un catálogo en una librería, hace por los libros. Con esto la recuperación de información será más rápida y precisa.

Otra estándar XML denominado Xlink [XLINK 00] permitirá escoger dentro de una lista de múltiples direcciones para realizar las funciones de ligas o hypertexto en el HTML. A diferencia presenta la ventaja de tener ligas indirectas almacenadas en una base de datos. El proceso de actualización se realiza en la base de datos.

Las caracteristicas anteriores permitirán un procesamiento eficiente, búsquedas más precisas y enlaces más flexibles, con lo cual se revolucionará la

estructura del WEB, haciendo posible nuevas formas de acceso a la información.

Al definir un nuevo lenguaje XML los diseñadores deben acordar por lo menos tres cosas: las etiquetas que serán permitidas, el esquema de anidamiento y como se deben procesar las etiquetas. Los dos primeros dos, el vocabulario y la estructura son típicamente codificados en un Document Type Definition (DTD) [DTD 00], aunque su uso no es imperativo. Aunque su uso hace más fácil la escritura de software.

En cuanto al estilo el XML permite "escribir una vez y publicar en cualquier parte". El XML permite etiquetar el contenido y aplicar reglas para dar formato mediante plantillas (Stylesheets) utilizando el eXtensible StyleSheet Languaje (XSL) [XSL 00].

Con esta nueva forma de incluir el formato y contenido se puede realizar el intercambio de documentos estandarizados como actualmente se realiza en el mundo de los negocios mediante el uso de ordenes de compra, facturas, recibos, etc. Los documentos funcionan ya que no es necesario conocer los procedimientos internos de las partes involucradas y únicamente se expone la información necesaria. Con ello los negocios en línea podrán utilizar esta nueva forma de intercambiar documentos. [Bosak 99]

Las aplicaciones XML proveen ventajas debido a la habilidad para el intercambio de datos. Las diversas organizaciones o las diferentes partes de una organización difícilmente estandarizan un conjunto de herramientas, y por lo tanto, la comunicación entre dos grupos toma una gran cantidad de tiempo. XML hace fácil el envío de datos estructurados a través del WEB sin pérdida de información en la transferencia. [Tidwell 99]

XML simplifica las transacciones negocio a negocio en el WEB y el intercambio de información entre negocios (B2B) se realiza mediante el seguimiento a las reglas de un documento definido en el DTD.

La importancia de XML viene de sus implicaciones y aplicación potencial para el comercio electrónico basado en el WWW, la administración del contenido de una organización, búsqueda de información, descripciones técnicas, integración de aplicaciones y comunicación entre aplicaciones y entre servidores. [Gartner 99]

El XML y el Internet han reducido las barreras del comercio electrónico con relación al costo y a la complejidad. El XML no reemplaza el EDI (Electronic Data Interchange) sino por el contrario lo extienda permitiendo a las pequeñas y medianas compañías realizar comercio electrónico. El EDI es una tecnología probada por más de 20 años con más de 300,000 empresas en todo el mundo, pero tiene la desventaja de utilizar pequeños mensajes con códigos que representan valores completos y el alto costo de implementación. Es ahí donde el XML combina los metadatos con datos permitiendo la fácil lectura de mensajes para el ser humano y las computadoras.

El uso de XML para aplicaciones de comercio electrónico requiere la inclusión de un esquema de seguridad que permita garantizar la autentificación, confidencialidad, integridad y no-repudiación. Esto puede complementarse con el uso del protocolo SSL y el uso de certificados en los navegadores de Internet que estarán disponibles en poco tiempo.

GLOSARIO

AES	Advanced Encription Standard (encriptación Avanzada del tipo estandar)
ATM	Automatic Teller Machine. (Cajero Automático)
B Business.	Categoría de comercio electrónico que considera a los procesos Internos del negocio
B2B Business to Business.	Categoría de comercio electrónico que considera el comercio electrónico entre empresas
B2C Business to Consumer.	Categoría de comercio electrónico que considera el comercio electrónico entre una empresa y un consumidor final
BACS	Banker's Automated Clearing System (Sistema Bancario Automatizados)
CD ROM	Compact Disk Read Only Memory (disco compacto)
Certificado Digital	Archivo que contiene información sobre la identidad de una persona, empresa o sistema
Ciberespacio	Conjunto de seres humanos interconectados a través de computadoras y redes de telecomunicaciones sin importar la geografía física
Clientes	Máquinas o computadoras que realizan la función de solicitar información a un servidor bajo la relación cliente/servidor

Clusters	Grupo de terminales o computadoras conectadas a una unidad de control en común o servidor que comparten la carga de trabajo y brindan apoyo en caso de que algún nodo falle
CORBA	Common Object Request Broker Architecture (Arquitectura y especificación para la creación, distribución y administración de programas u objetos distribuidos en una red)
CRM	Customer Relation Management (Término de la industria de tecnologías de información para las metodologías, software y capacidades en Internet que ayudan en la forma en que se relacionan las empresas con sus clientes)
Checksum	Conteo de número de bits en una unidad de transmisión utilizada para verificar que el número de bits recibidos sea el mismo que el número de bits enviados
DES	Data Encription Standard (Estándar de encripción de criptografía de llave privada)
DSS	Digital Signature Standard
DVD	Digital Versatile Disk (Tecnología de discos ópticos que remplazarán al CDROM)
Eavesdropping	Escuchas
EDI	Electronic Data Interchange (Intercambio electronico de Datos)
EFT	Electronic Funds Transfer (fundamentos de Transferencia Electronica)
EFTPOS	Electronic Funds Transfer Point Of Sales Enterprise Java Beans (Arquitectura desarrollada por SUN para la administración de componentes desarrollados en el lenguaje de programación JAVA)

Extranet	Red privada que utiliza los protocolos de Internet y los sistemas de telecomunicaciones públicos para compartir de forma segura, información de negocios y operaciones entre diversas empresas
FTP	File Transfer Protocol (Protocolo de transferencia de archivos entre computadoras a través de Internet)
Groupware	Programas que ayudan a las personas a trabajar de forma colaborativa y de forma colectiva sin importar su ubicación física Hash Función unaria que es utilizada para mapear un argumento a un resultado de un tamaño predeterminado.
HTML	HyperText Markup Language (Conjunto de símbolos y marcas que permiten consultar información en el WWW a través de un navegador como Netscape o Internet Explorer Internet Sistema de computadoras conectadas en red pública en todo el mundo Internet II Proyecto de universidades y empresas de EU para el desarrollo de redes y aplicaciones avanzadas para la enseñanza e investigación)
Intranet	Red privada basada en las tecnologías y protocolos de Internet IRC
Java	Lenguaje de programación diseñado para ambientes distribuidos en Internet
Java Server Pages	Tecnología utilizada para el control del contenido y apariencia de páginas WWW
JDBC	Especificación de Interface de programación de aplicaciones para conectar al lenguaje de programación Java con base de datos
Kerberos	Método seguro para la autentificación de solicitudes a servicios

KM	Knowledge Management (Tecnología de Información para la administración del conocimiento que permite adquirir, almacenar y transferir el conocimiento entre personas mediante el uso de un sistema)
Llave privada	Llave mantenida en secreto y otorgada por una autoridad certificadora que permite junto con la llave pública realizar operaciones de encripción y decripción
Llave pública	Llave otorgada por una autoridad certificadora la cual se distribuye a la personas que requieran enviar un mensaje, que permite junto con la llave privada realizar operaciones de encripción y decripción
MAC	Message Authentication Code (mensaje Automatizado)
Message forgery	Falsificación de mensajes
MIPS	Míllions of instructions per second (Unidad para definir la capacidad de procesamiento de una computadora)
MP3	MPEG-1 Audio Layer-3 (Formato para la compresión de secuencias de sonido y audio)
Newsgroups	Grupos de noticias (Discusión de temas específicos a través de comentarios escritos a un servidor de Internet centra)l
NIST	National Institute of Standards and Technology
PGP	Pretty Good Privacy (Programa utilizado para encriptar y decriptar información generalmente correo electrónico)
Portales	Sitio WEB de inicio y punto de entrada hacia otros sitios en Internet
POS	Point Of Sales (puntos de venta)
RFP	Request For Proposal (Búsqueda avanzadas)

RMI	Remote Method Invocation (Librerías de programación en Java para ejecutar métodos en un equipo remoto)
SDH	Synchronus Digital Hierarchy (Estándar para transmisión síncrona de datos)
Servlets	Tecnología Java que permite ejecutar programas en un servidor
SET	Secure Electronic Transaction (tranzaciones electronicas de alta seguridad)
SONET	Estándar para transmisión de datos sincronos en medios ópticos
SSL	Socket Secure Layer
SWIFT	Society for Worldwide Interbank FundsTransfer Tampering Intromisiones (Sociedad reguladora)
VAN	Value Added Network (Red de compartición de servicios de banda ancha)
VPN	Virtual Private Network (Red privada de datos que utiliza la infraestructura de las redes publicas de datos de forma segura mediante procedimientos de seguridad)
VRML	Virtual Reality Modeling Language (Lenguaje para la descripción de imágenes en 3 dimensiones e interacciones con el usuario)
WWW	World Wide Web
XML	Extensible Markup Language (Lenguaje que permite integrar además de formato a las páginas WWW, un significado y descripción de la información contenida en el documento)

AUTOBIOGRAFIA

Candidato para el Grado de Master en Ciencias de la Administración con especialidad en Relaciones Industriales.

Tema de Tesis: "La Seguridad en el Comercio Electrónico como Solución a una nueva forma de llevar acabo Transacciones Comerciales de las Empresas"

Nació en la ciudad de Poza Rica de Hgo. Veracruz, el 27 de Julio de 1976, Hijo del Sr. Francisco Cabrera Martínez y de Sra. Maria de la luz Taque Cabrera, Hermano de Sr. Ernesto C. Cabrera Taque, Srita. Gloria Cabrera Taque y Jorge Cabrera Taque.

Egresado de la Facultad de Ingeniería Mecánica y Eléctrica de Universidad Autónoma de Nuevo León, Obteniendo el grado de Ingeniero en Electrónica y Comunicaciones, en Diciembre de 1998.

Contando también con el Titulo de Técnico en Electromecánica, del C.B.T.i.s. No. 78, de la Ciudad de Poza Rica de Hgo. Veracruz, egresado en Junio de 1994.

Contando con la Experiencia Profesional en el área de la investigación, implementación y desarrollo de nuevas Tecnologías, y en las áreas de la

Informática y las Telecomunicaciones, Habiendo participado en el desarrollo e implementación del Site de Comercio de la Compañía Dirona S.A. de C.V., además de Participar y colaborar en el Departamento de Electrónica y Comunicaciones de la Facultad de Ingeniería Mecánica y Eléctrica de la Universidad Autónoma de Nuevo León.