UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
" CUAUTITLÁN "

REDES DE COMPUTADORAS.
INTERCAMBIO ELECTRONICO DE DATOS (E.D.I.) EN INTERNET:
ANALSIS DE TENDENCIAS

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE:

LICENCIADA EN INFORMATICA

P R E S E N T A:

MILDRED KARINA ORTIZ ALVAREZ

ASESOR:
L.I. CARLOS PINEDA MUÑOZ.

Cuautitlán Izcalli, Edo. de México, 1997.

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

UNIVERSIDAD NACIONAL AVPNMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS SUPERIORES-CUAUTITLAN

DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JAIME KELLER TORRES
DIRECTOR DE LA FES-CUAUTITLAN
P R E S E N T E .

AT'N: ING. RAFAEL RODRIGUEZ CEBALLOS
Jefe del Departamento de Exámenes
Profesionales de la FES-C.

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Redes de Computadoras. Intercambio Electrónico de Datos (E.D.I.) en Internet: Análisis de Tendencias

que presenta la **pasante:** Mildred Karina Ortiz Alvarez

con número de cuenta: 9011135-4 **para obtener el Título de:**

Licenciada en Informática.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO.

A T E N T A M E N T E .
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Edo. de México, a 13 **de** Octubre **de 19**97.

MODULO:	PROFESOR:	FIRMA:
I	Lic. Carlos Pineda Muñoz	
II	Ing. Miguel Alvarez Pasaye	
III	Ing. Moisés Hernández Duarte	

DEP/VOBOSEM

A la Piedra Angular de mi vida, quien día con día y a lo largo de mi carrera me mostró su poder y amor y me enseñó que el principio de la sabiduría es el temor de Jehova.

Jehova, Dios de los Ejércitos

A la mujer que me dio el ser, que me mostró el camino de rectitud y horadez, atenta de mis logros y aliento de mis fracasos, la cual siempre me dio su apoyo incondicional y desinteresado, su amor y cariño. A mi mejor amiga.

Mi Madre, Ernestina.

A un gran hombre que fue ejemplo de rectitud, honradez y fortaleza quien siempre buscó lo mejor para mí y a quien debo mucho de lo que soy.

Mi Padre, Luis.

A una gran mujer que me enseñó a esforzarme cada día, a dar lo mejor de mí y siempre tuvo una palabra de aliento para animarme a seguir adelante y nunca desmayar.

Mi Abuelita, Esther.

A Mi Tío Roberto

Quien siempre me ha apoyado incondicionalmente durante mi vida y me ha brindado su amor y cariño desinteresado.

A Don Jesús

Que con sus consejos y apoyo desinteresado ha contribuido a que yo llegue a la meta final de mis estudios profesionales.

A Mis Hermanas: Magda, Judith, Esther, Ruth y Tayde

Por que siempre me muestran su amor a través de sus consejos, me han enseñado a ser una buena estudiante, a esforzarme por lograr lo que quiero y que a pesar de nuestras diferencias, siempre cuento con ellas.

A Mis Sobrinitos: Alex y Lalito

Por su amor y su cariño, por que cuando me he encontrado abrumada y triste ustedes han sido la alegria que borra mis tristezas y mi fatiga.

A René

Que siempre con su amor, cariño y comprensión me ha ayudado a culminar una de mis grandes metas.

A la Universidad Nacional Autónoma, la Máxima Casa de Estudios, y a la Facultad de Estudios Superiores Cuautitlán

Por brindarme la oportunidad de pertenecer a ellas, de formarme profesionalmente, adquiriendo los conocimientos necesarios para poner en alto el nombre de las instituciones a las que represento.

A Todos Mis Maestro

Por haberme transmitido sus conocimientos y experiencias, poniendo el mejor de sus esfuerzos en cada una de sus enseñanzas.

Al Lic. Carlos Pineda Muñoz

Por haber puesto el máximo empeño para que este trabajo se realizara lo mejor posible.

A los integrantes de la División EDI de GCC: Jesús, Gil, Elsa, Jorge, Carlos, Alberto, Adriana, Maricarmen, Claudia y Lucero

Por su amistad, su comprensión y la gran ayuda que me brindaron para realizar este trabajo. Gracias Muchachos.

Al Dr. Ariel Waller

Gracias maestro por todo el apoyo incondicional que siempre me ha dado, por enseñarme que todo lo que deseamos lograr en esta vida tiene un gran esfuerzo, por ser ejemplo de fortaleza, integridad y profesionalismo.

A los miembros del Coro Miguel C. Meza, Especialmente a las Contraltos

Por apoyarme con sus oraciones y consejos.

A Todos Aquellos
Que con su ayuda y apoyo contribuyeron a la terminación de mis estudios profesionales
José de Jesús Ramos Ojeda
Alfredo Ortiz
Federico Vargas
Victor J. Núñez Vega
Victor Manuel Núñez

INTRODUCCION

La revolución computacional ha transformado la manera de trabajar de las personas. Este escenario ha dado como resultado lo que muchos denominan "Comercio Electrónico" (EC), el cual, está modificando la forma de hacer las transacciones comerciales de compra-venta de productos y servicios. Al mencionar el Comercio Electrónico, se tiene que hacer referencia al Intercambio Electrónico de Datos (E.D.I., Electronic Data Interchange) el cual, es parte inherente del EC.

EDI es la automatización del intercambio de transacciones de negocios tales como: ordenes de compra, facturas, pagos, etc. entre una compañía y sus proveedores, clientes, bancos, u otros socios comerciales a través de enlaces de comunicaciones públicas o privadas.

Actualmente la mayor parte de las empresas utilizan las redes de Valor Agregado (VANs) para la realización del EDI, pero debido al alto costo de estas (600 USD anuales aprox..) algunas de ellas han buscado otra forma de intercambiar sus transacciones comerciales a través de una red que resulte más económica y que permita tener las mismas alternativas que una VAN proporciona; por lo tanto, optaron por la tecnología de redes bajo el protocolo TCP/IP la cual, es usada transmitir mensajes por Internet.

La tecnología Internet ha creado un canal adicional por el cual los mensajes EDI pueden llegar hasta sus socios comerciales con una autenticación, integridad en los datos, y confidencialidad en el intercambio de éstos.

Debido a las grandes ventajas que ofrece EDI por Internet muchas empresas especializadas en la creación y venta de software para hacer EDI, como Premenos Corp., Harbinger, Elcom Systems, entre otros, han desarrollado diferentes opciones para realizar el Intercambio Electrónico de datos (EDI) a través de Internet.
Las opciones que algunas empresas utilizan para el Intercambio Electrónico de Datos por Internet son: Encriptación de Datos, Páginas Electrónicas y las tan afamadas Páginas Web.

El presente trabajo hace referencia a cada una de las 3 tendencias, existentes hoy en día, para realizar el Intercambio Electrónico de Datos en Internet, las posibles áreas en donde éstas se pueden aplicar, un análisis de estas tendencias con el fin de visualizar cuál de ellas ofrece más beneficios para las empresas, así como, cuál va en ascenso y cuál no.

En el capítulo I, se tratan tópicos generales acerca de EDI e Internet con el fin de poder sensibilizar en un mayor grado, la relación existente entre uno y otro; además de contar con las bases necesarias para entender esta relación. Algunos de estos tópicos son: el origen de EDI e Internet, su funcionamiento, Qué son, etc. El capítulo 2 describe dos de las tres tendencias para la realización del Intercambio Electrónico de Datos en Internet: Enciptamiento de Datos y las Formas Electrónicas; identificando algunos conceptos esenciales para poder comprender estos temas como son qué es el encriptamiento, algoritmos de encriptamiento, qué son las formas electrónicas, sus principales características, etc. Por su parte el capítulo 3 explica el funcionamiento de las Páginas Web, que son la tercera tendencia para la realización del Intercambio Electrónico; además muestra como ejemplo de esta tendencia, un software llamado OM-Transact que utiliza el Web para intercambiar transacciones comerciales, así como algunos conceptos esenciales relacionados con este tópico. Por último el capítulo 4 muestra algunos casos en donde se han aplicado cada una de las tendencias mencionadas anteriormente, con el propósito de ebozar el panorama general de cada una de ellas.

OBJETIVOS

GENERAL

Investigar en que consisten las diferentes opciones para la realización del Intercambio Electrónico de Datos (EDI) por Internet.

PARTICULARES

1. Proponer las posibles áreas de aplicación de cada opción con base a sus características.
2. Precisar las ventajas y desventajas de cada una de las opciones para la ejecución del Intercambio Electrónico de Datos a través de Internet.
3. Dar una perspectiva de qué tendencia va en incremento y cual no.

HIPÓTESIS

"La utilización del Intercambio Electrónico de Datos (EDI) por Internet en alguna de sus modalidades, resultará benéfico para las organizaciones en diversos aspectos tales como: costos, operabilidad, utilización de estándares y tecnología de punta, entre otros."

INDICE

CAPITULO

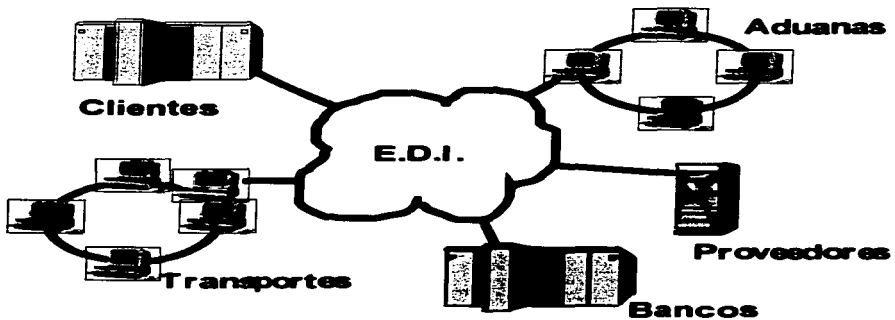
1

INTERCAMBIO ELECTRONICO DE DATOS (E.D.I) E INTERNET

1.1. CONCEPTOS

EDI (Electronic Data Interchange)

- El Intercambio Electrónico de Datos (EDI) es comúnmente definido como la transferencia -aplicación a aplicación - de documentos de negocios entre computadoras. Muchas empresas eligen EDI por considerarlo un método rápido, barato, y seguro para enviar o recibir ordenes de compra, facturas, avisos de embarque así como otros documentos comerciales usados frecuentemente.
- Intercambio de información de negocios aplicación a aplicación entre una compañía y sus socios comerciales.
- Intercambio de datos o formas estándares para negocios computadora a computadora.



INTERNET

- Es la unión de muchas redes bajo un estándar de comunicación llamado TCP/IP (Transmission Control Protocol / Internet Protocol).
- Es el inter-trabajo de redes corporativas, gubernamentales y de educación existentes, las cuales utilizan estándares de telecomunicaciones en común. No es una nueva red física, sin embargo nuevas facilidades pueden ser accedidas.
- Red global de redes de ordenadores cuya finalidad es el permitir el intercambio libre de información entre todos sus usuarios.

Una característica de Internet es que está basada en los intereses mutuos de los usuarios para comunicarse en una forma efectiva a través de una vía electrónica, mensajes y archivos. Las comunicaciones de Internet pueden ser:

- Interpersonal (persona a persona).
- Correo electrónico (e-mail), ó,
- Proceso a proceso como: EDI.

Una vez visualizadas las diferentes conceptualizaciones que les han dado a los dos principales temas de este trabajo EDI e INTERNET y antes de conocer la mecánica de su funcionamiento, así como la relación existente entre ellos, se expondrá una breve reseña histórica de éstos.

1.2. ORIGENES

Es importante el conocimiento de los orígenes de EDI e Internet para poder entender la evolución que han tenido, estar en posibilidades de comprender la relación existente entre ellos y lo más importante, el porque Internet es una gran herramienta para el comercio electrónico.

EDI

En los años 60's las compañías tenían requerimientos internos de procesamiento de datos,

en los cuales, sólo se introducían los datos a las computadoras para la generación de reportes.

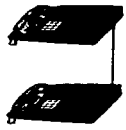
En los 70's cambió el esquema, ya que en las organizaciones surgió la necesidad de compartir información interna entre los departamentos que las conformaban.

En la década de los 80's se generó la necesidad de compartir información tanto interna como externa entre las compañías.

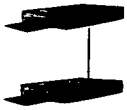
De 1960 y 1980, se utilizaron diversos medios para transmitir información entre empresas, destacándose el correo, el teléfono, recientemente el FAX, y los servicios de mensajería.

Los problemas principales que tenían con estos medios de comunicación eran los siguientes

- Correo.- El período de entrega de la información es de 4 a 7 días.
- Teléfono.- Presenta muchos errores de recaptura.
- FAX.- Hay que recapturar la información y a veces es ilegible.
- Mensajería.- Sus costos son altos.



De Teléfono a Teléfono (voz y captura)



De Fax a Fax (papeles y captura)

Computadora a Computadora (no hay papeles ni captura)

Tratando de dar solución a estos problemas, en 1960, algunas empresas, crearon formas propias para intercambiar información, diseñando formatos e interfaces de comunicación

propios, obligando de esta manera, a sus proveedores a la participación en este nuevo proyecto. Un ejemplo claro, de este panorama es K-Mart, la cual, desarrolló su propio sistema de compras para enviar órdenes de compras electrónicas a sus proveedores, los cuales a su vez, por el deseo de venderle a K-Mart, se vieron forzados a adoptar este sistema. Pero un nuevo problema surgió cuando varias empresas que tenían su propio sistema intentaban intercambiar electrónicamente sus documentos comerciales, ya que era necesario instalar diferentes sistemas para poderse comunicar con cada una de las compañías que habían diseñado su propio software. En este marco fue como surgió el Intercambio Electrónico de Datos (EDI: Electronic Data Interchange), cuyo objetivo es el de transmitir datos de manera electrónica que puedan ser procesados por una computadora, utilizando formatos estándar.

Con esta nueva forma de intercambiar información las empresas adquirían grandes ventajas como:

- Un medio rápido
- Generación de menos errores
- No-necesidad de recapturar la información
- Utilización de vía de comunicación barata
- Menor costo de intercambio cuando la alternativa de tiempo real era utilizada.
- Flexibilidad al utilizar campos de longitud variable.
- Flexibilidad en su utilización - Puede ser utilizado para intercambio en tiempo real o en intercambio de información fuera de línea por cinta o disco flexible.

Históricamente, los siguientes eventos fueron significativos en la formación de EDI:

1) La formalización de estándares para el intercambio electrónico de datos entre empresas ferrocarrileras, navieras, aéreas y automotrices. Cambio de nombre al Comité Coordinador de Datos de Transportación por el de Asociación para el intercambio electrónico de datos (1968).
2) El desarrollo y publicación del primer conjunto de estándares (1974 - 1975).
3) La definición de la tecnología para el proceso de transmisión EDI (1976 - 1977).
4) La participación de ANSI y el desarrollo del standard X.12 (1978).
5) La formación del Comité, para la revisión del diccionario de datos EDI (1985 - 1988).

6) La coordinación Intercontinental de los estándares EDI (1984).
7) Primera publicación de estándares EDIFACT.

Como se pudo apreciar en lo expuesto anteriormente la década de los 80's fue la más fructífera para el EDI, en ella se generaron los primeros estándares que cubrían a todas las industrias; así como también los subconjuntos de los que ya existían, para aplicaciones de ramas industriales. Algunos de ésto son:

ASOCIACION	APLICACION
ANSI (American National Standards Institute) X.12	Todas las industrias
CIDX (Chemical Industry Data eXchange)	Química
AIAG (Automotive Industry Action Group)	Automóviles
VICS (Voluntary Interindustry Communication Standards)	Ventas al por menor
TALC (Textil / Apparel Linkage Council)	Textiles

Con el paso del tiempo el EDI ha adquirido mayor fama entre las empresas, tanto a nivel nacional como internacional debido a las ventajas feacientes derivadas de él.

En México, se conoció EDI, por medio de las llamadas empresa transnacionales, las cuales, tomando como ejemplo a sus antecesoras, han obligado a sus proveedores a realizar transacciones comerciales a través de EDI, lo cual ha hecho que más personas se interesen por saber lo que es EDI, lo que implica implantar EDI y sobre todo de las ventajas tan grandes que les trae el uso de éste; no sólo en el hecho de poder venderle a cierto cliente, sino que al tener EDI pueden establecer comunicación con sus propios proveedores y en el caso de empresas grandes con sus filiales.

Algunas empresa establecidas en México que están haciendo uso de EDI para sus transacciones comerciales son:

- Vitro Corporativo
- Volkswagen
- Comercial Mexicana
- Chrysler
- Gigante
- Ford
- Ferrocarriles Nacionales de México
- Nissan
- Grupo Cifra
- Nadro
- Mazón Hermanos
- Wyeth
- Price Club
- Coca-Cola
- Liverpool
- Sears, entre otros.

Internet

En 1969, la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos de América, en su afán de evitar que otros países como la exunión Soviética se infiltraran en su información militar, decidió patrocinar una investigación enfocada en la construcción de redes de intercambio de información, que dividían a esta, en paquetes con el domicilio, destino, los cuales de forma independiente y aleatoria se movían por diferentes redes y sistemas y al llegar a su destino, sufrían un ensamblaje. De esta manera, surgió ARPANET (Advanced Research Proyect Agency Network) la cual prometía mantener la integridad de la comunicación en el caso de una emergencia en Estados Unidos de América.

ARPANET fue concebida bajo el prototipo de que en el momento menos pensado cualquier parte de la red pudiese desaparecer y el resto de ésta debe seguir trabajando como si nada hubiera pasado; además la información que viajara por ella nunca debía usar la misma ruta dos veces.

Con el tiempo, esta red tuvo mucha demanda por los investigadores pertenecientes a ella, debido a la posibilidad de envío de información a sus colegas los cuales estaban geográficamente muy distantes. Este fue el motivo por el que en 1975 la Agencia de Comunicaciones de la Defensa delos Estados Unidos de América dividió a ARPANET en dos redes:

- ARPANET destinada al uso de la comunidad científica
- MILNET para uso de requerimientos militares.

Sin embargo, a pesar de esta división, la información que circulaba en estas redes podía ser compartida por medio de una interconexión llamada DARPA Internet (Defense Advanced Research Proyect Agency), comúnmente conocida como Internet.

El hecho que ARPANET estuviera limitada a unos cuantos, dio origen a la creación de algunas redes proveedoras de servicios de información de investigación y académica. Estas redes no eran parte de Internet, pero con el tiempo se hicieron conexiones a ésta con el fin de facilitar el intercambio de información.

En 1986, la Fundación Nacional de Ciencias (NSF) ayudó a la expansión de Internet, al crear algunos centros de supercómputo a los cuales estaban conectados investigadores de los Estados Unidos. Algunos de estos centros eran:

- Supercomputadora Nacional de Cornell, Universidad de Cornell, Cornell, Nueva York.
- Centro Nacional de Supercómputo, John Von Neuman, Princeton, Nueva Jersey.
- Centro Nacional para Aplicaciones de Supercómputo (NCSA), Universidad de Illinois, Champaign, Illinois.
- Centro de Supercómputo de Pittsburgh, Pittsburgh, Pensilvania.
- Centro de supercómputo de San Diego, Universidad de California, San Diego California.
- División de Cómputo Científico del Centro Nacional de Investigaciones Atmosféricas, Boulder, Colorado.

Como consecuencia a la gran demanda, de esta red, la NSF trató de utilizar la red ARPANET para la comunicación de los centros, pero por problemas burocráticos ésto no fue posible; por lo que decidió construir su propia red cimentada en la tecnología IP de ARPANET. Esta red conectaba a los centros mediante enlaces telefónicos de 56,000 bits por segundo (56Kbps) y se le llamó NSFNET.

A través del tiempo, la NSFNET se convirtió en la piedra angular de Internet debido a las redes de alta velocidad que se conectaban supercomputadoras de la NSF. Las líneas de transmisión de esta red estaban constituidas por teléfonos, fibras ópticas y un enlace por satélite; a su vez, son supercarreteras que llevan tráfico a distancias largas y a velocidades grandes. Los datos viajan a redes de nivel medio, que direccionan éstos mediante sus propios sistemas. En última instancia, los datos llegan a los usuarios finales, quienes se conectan a la red a través de proveedores de servicios, los cuales a su vez, se conectan por área local.

La NSFNET continúa creciendo, más de 80 países tienen servidores y redes que se conectan a esta red.

Los mayores costos para mantener la NSFNET son proporcionados por la Fundación Nacional de Ciencias, universidades, laboratorios estadounidenses y corporaciones de alta tecnología; pero últimamente, a raíz de la derogación de las reglas que prohibían aplicaciones comerciales en la NSFNET de Internet, las compañías comerciales empezaron a incursionar en investigaciones, conexiones y nuevas aplicaciones de Internet, ya que lo ven como un vehículo para desarrollar sus negocios, mercadeo directo, ventas de productos y soporte a clientes.

Poco a poco la NSFNET representa una porción más pequeña en Internet; ésto se debe a que redes comerciales privadas y regionales se conectan a Internet directamente, sin que la información use el segmento de sistema NSFNET.

Las ventajas que muchos comerciantes le ven a Internet son:

- Reducción de gastos excesivos
- Servicio las 24 hrs. del día

- Revisiones veloces a los catálogos de información.

El proyecto más ambiciosos destinado a usar Internet para negocios con fines de lucro es CommerceNet, consorcio de 40 compañías de Silicon Valley, al cual el gobierno de los EUA asignó 6 millones de dólares para su desarrollo.

1.3 Cómo Trabajan

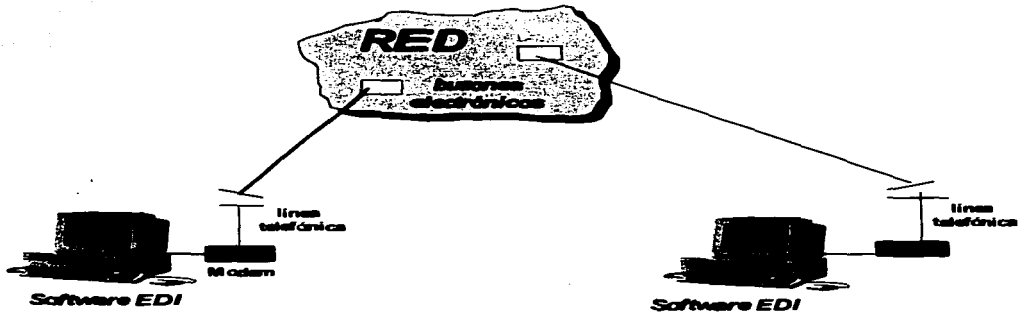
EDI

EDI empieza con un acuerdo comercial entre 2 socios comerciales. se realizan decisiones de común acuerdo a cerca de los estándares a ser usados, la información a intercambiar, la red a través de la cual viajará ésta y cuándo será enviada.

Uno de los socios comerciales crea un documento, por ejemplo una factura en su aplicación de negocios. El traductor EDI automáticamente formatea la factura de acuerdo a los estándares EDI. El traductor crea y empaqueta el documento en una envoltura electrónica que lleva el identificador de su socio comercial.

La parte de las comunicaciones puede ser parte del software traductor o una aplicación separada. El software de comunicaciones marca el número telefónico del nodo de la red. El paquete que contiene el documento es transmitido a la VAN. Esta lee el identificador que trae el paquete y los pone en el buzón correcto.
El módem del socio comercial que recibe la información, llama a la red, y obtiene el paquete almacenado en el buzón. El traductor EDI abre el paquete y traduce los datos del formato estándar a un formato leíble por su aplicación. El sistema de cuentas por pagar del socio comercial receptor crea un cheque de la factura electrónica.

La clave para un EDI eficiente es introducir los datos una vez. El sistema EDI hace el resto del trabajo. Los datos se mueven sin ninguna intervención de la aplicación del socio emisor a la del socio receptor y sin ningún proceso adicional que alente el proceso.



INTERNET

Internet es una red de conmutación de paquetes; no cuenta con una parte de la red dedicada a sus actividades. Lo que se desea enviar, se divide en paquetes, los cuales se mezclan con los mensajes de otras personas, se ponen en un conducto, se transfieren a otro lugar y todos son clasificados nuevamente. Pero, ¿cómo realiza Internet cada uno de estos procesos, los cuales permiten que la información llegue a diferentes lugares del mundo?.

Las diversas partes de Internet están conectadas por un conjunto de computadoras que se conocen como enrutadores, los cuales interconectan las redes. Estas redes así como las líneas telefónicas son el medio a través del cual la información va de un lugar a otro. Los enrutadores determinan la dirección de los "paquetes de información". No todo enrutador cuenta con una conexión a cada uno de los otros enrutadores de la red, sino que, cada uno es fijado en el destino de los paquetes y éste decide a dónde enviarla, es decir, elige cuál es el enlace más apropiado para enviarlos. Esta decisión la realiza, con base en algunas reglas que definen la operación de Internet. Estas reglas son conocidas como protocolos.

Los principales protocolos que rigen el funcionamiento de Internet son: IP y TCP.
TCP (Transmission Control Protocol) es el que se encarga de dividir la información en paquetes así como de enumerar cada uno de éstos para que el receptor pueda verificar la información y ponerla en el orden adecuado.

IP (Internet Protocol) añade al principio de los paquetes sus respectivos domicilios destino. Los domicilios de Internet o mejor conocidos como Direcciones IP están constituida por un número de 32 bits, al que se representa más como cuatro cifras separadas por puntos entre cada una de ellas (.) como: 132.123.12.130. Cada parte que conforma una dirección IP se le llama octeto. Los primeros números del domicilio indican a los enrutadores la red a la que se pertenece. Los últimos números señalan la computadora o equipo anfitrión que debe recibir el paquete. Cada computadora tiene un domicilio único

Una vez que cada paquete tiene su dirección, la red los puede transmitir.
Cuando los paquetes llegan a su destino, el TCP reúne los sobres, extrae la información de ellos y la pone en el orden adecuado. Si algún paquete se pierde en la transmisión, el receptor solicita su retransmisión al emisor. Al ya tener toda la información en el orden adecuado, TCP, la pasa a la aplicación del programa que esté utilizando sus servicios.

1.4 Estándares EDI

La definición de los estándares EDI es:

- Un conjunto de reglas, acordadas, aceptadas, y adquiridas voluntariamente, mediante las cuales los datos son estructurados en formatos de mensaje para intercambio de información operativa o de negocios.

Los estándares para EDI son desarrollados y mantenidos por 2 cuerpos de estándares acreditados; uno creado por los Estados Unidos de Norteamérica y otro establecido por las Naciones Unidas. Estos grupos definieron un lenguaje común para el Intercambio Electrónico de Datos.

1.4.1 ANS X12

En 1979, el Instituto Nacional de Estándares americanos (ANSI) creó un comité conocido como el Comité de Estándares Acreditados X12 (ASC X12) para desarrollar estándares nacionales para la mayoría de los documentos de los diferentes negocios. El primer estándar Nacional Americano de EDI fue publicado en 1983.
El estándar X12 de EDI de formato de documentos es un conjunto de transacciones.

1.4.2 UN/EDIFACT

El cuerpo internacional de estándares, Intercambio Electrónico de Datos para la Administración, Comercio y Transporte (UN/EDIFACT) fue establecido por las Naciones Unidas en 1985.

Los estándares internacionales para el EDI ocurren bajo la conducción de las Naciones Unidas (UN).

Los estándares son desarrollados y mantenidos regionalmente por los consejos de UN/EDIFACT representados en África, Asia, Australia, Nueva Zelanda, Europa Oriental y Occidental, así como en Latinoamérica.

Dos veces al año los representantes de estos consejos se reúnen para recomendar estándares para publicaciones de las Naciones Unidas. El ASC X12 es el representante de UN/EDIFACT en los Estados Unidos de Norteamérica.

1.5 EDI por Internet

El uso de EDI ha existido por más de una década y cada día millones de dólares en transacciones son intercambiadas vía EDI. Hasta hace algunos años, la mayoría de los negocios estadounidenses continuaban llevando a cabo negocios utilizando los anticuados sistemas de papel, pero a que se debía ésto, si las ventajas que representaba el uso del EDI, eran muy claras.

Para muchos clientes, el principal problema era o es el costo. El costo del software EDI y la red de comunicaciones han desalentado a muchas empresas y para aquellas quienes

desean implementar EDI, los factores de costo algunas veces limitan la expansión para incluir nuevas aplicaciones y socios comerciales. El elemento más caro asociado con EDI es la red de comunicaciones.

Las redes VAN causan gastos por la transmisión de datos, tiempo de conexión, mantenimiento y soporte. Estos cargos van en aumento. Un gran número de pequeñas empresas y sus socios comerciales gastan millones de dólares por los servicios de una VAN.

El desempeño actual del EDI por redes propias es también un problema, desde que la disponibilidad de la información depende de la velocidad de los modems y de los procesos desatendidos mediados por VANs. Los altos costos y la baja rapidez de los servicios de una VAN son directamente el resultado de la tecnología de las redes propias sobre las cuales ellos están basados.

El surgimiento de Internet como un medio para el comercio electrónico sugiere una solución potencial a las limitaciones de las redes propietarias. Una robusta colección de múltiples redes públicas y privadas interconectadas a través del mundo ofrece una gama muy amplia de posibilidades para la transmisión de transacciones comerciales, ya que éstas pueden ser enviadas a varios socios comerciales en diferentes puntos del globo terráqueo al mismo tiempo y con un bajo costo.

La fuerza de Internet es clara cuando uno considera que fue diseñado originalmente para resistir un ataque nuclear, bajo un protocolo de comunicaciones abiertas como lo es TCP/IP. Internet utiliza muchos caminos alternativos para lograr un alto grado de flexibilidad.

La red Internet ofrece algunas ventajas como un medio para el comercio electrónico:

- Es globalmente muy accesible
- Ofrece una renta mensual baja
- El volumen de información y el tiempo por día son independientes del precio de transmisión de datos.
- Su robustez debido a múltiples caminos alternativos, gateways, e interconexiones.
- Tiene un gran ancho de banda para la transmisión de datos.
- Es una plataforma independiente.

A pesar de las grandes ventajas que ofrece Internet para el comercio electrónico, existen algunos problemas inherentes a él:

- Falta de seguridad
- Incapacidad para confirmar la integridad de los mensajes.
- Vulnerabilidad a la intercepción y fabricación de mensajes.
- Dificultades en la obtención confiable de la autenticidad de los mensajes.

Para solucionar estos problemas las empresas dedicadas al desarrollo de software EDI, han creado programas que garantizan la seguridad de los datos en el Intercambio Electrónico de datos.

CAPITULO

2

ENCRIPTAMIENTO Y FORMAS ELECTRONICAS

2.1 ENCRIPTAMIENTO. CONCEPTO

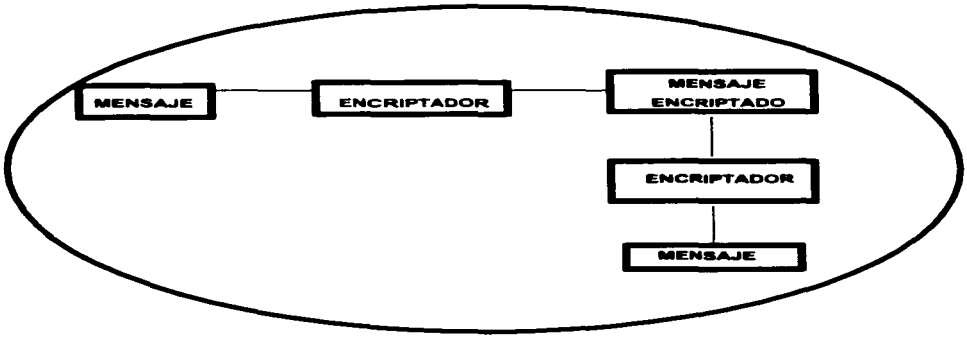
- Proceso de tomar información que existe de manera legible y convertirla en una forma que otros no puedan entender.
- Proceso de transformar un archivo texto en un archivo cifrado[1].

2.1.1 Conceptos Básicos

AUTENTIFICACION

- Evaluar si el autor del mensaje es quien dice ser.
- Verificar la integridad del mensaje.

CRIPTOSISTEMA



1. Electronic Data Interchange.ASC X12 Standards. Draft version 3 release 6, 1995.

CLAVE PUBLICA

Puede ser hallada por cualquiera, no se esconde.

CLAVE PRIVADA

Sólo la conoce un cierto grupo o persona

LLAVE DE ENCRIPTAMIENTO

Parámetro que determina la transformación de archivo plano a archivo cifrado o viceversa.

DATO LLAVE

Llave utilizada para encriptar y desencriptar o autentificar datos.

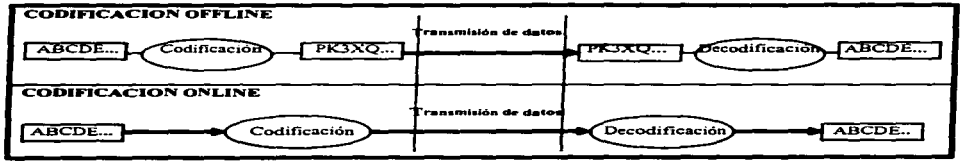
2.1.2 Técnicas de Encriptamiento

2.1.2.1 OffLine

En la técnica offline los datos son codificados antes de la transmisión y descodificados después de la transmisión. el algoritmo de encriptamiento puede ser de cualquier grado de complejidad. Como ejemplo de esta, se tiene al PGP (Pretty Good Privacy).

2.1.2.2 OnLine

La encriptación o codificación online se lleva a cabo durante la transmisión, es decir, tanto el encriptamiento como el desencriptamiento de los datos son realizados en el momento de la transmisión. Un ejemplo de esta técnica es el SSL (Secure Transport Layer).



2.1.3 Estándares Para el Encriptamiento

2.1.3.1 AUTACK

Un AUTACK es una autentificación y acuse de recibo UN/EDIFACT que se aplica a las transacciónes EDI y transmite información importante y segura, tal como datos integros y autentificados.

2.1.3.2 DES

DES es un cifrador de bloque para encripción definido y respaldado por el Gobierno de los EUA en 1977 como estándar oficial. Originalmente fue desarrollado por IBM para ser implementarlo en hardware; es el cifrador más conocido y el que tiene un uso más extenso en todo el mundo. Este algoritmo es un criptosistema simétrico, que es utilizado para comunicación (El emisor y el receptor deben conocer la misma clave secreta, para poder encriptar y desencriptar el mensaje). Puede ser usado para almacenar archivos en un disco duro en forma encriptada.
Si este cifrador se utiliza en un ambiente multiusuarios la distribución de la clave resulta difícil, por lo que se recomienda criptografía de llave pública. Tiene una longitud de bloque de 64 bits y una llave de 56 bits durante el encriptamiento. Es un Feistel cipher de 16 rondas.

2.1.3.3 MD5

MD5 es un algoritmo de mensajes sintetizados desarrollado por Rivest en 1991. Implicado en aplicaciones de firma digital en donde un mensaje grande tiene que ser comprimido de una manera segura antes de ser firmado con la llave privada. El algoritmo toma un mensaje de una longitud arbitraria y produce un mensaje comprimido de 128 bits. La mecánica de encriptamiento es la siguiente:

El mensaje es comprimido para asegurarse que su longitud en bits mas 448 es divisible entre 512. Una representación binaria de 64 bits de la longitud original del mensaje es concatenada al mensaje. El mensaje es procesado en bloques de 512 bits en una estructura repetitiva Damgard/Merkle y cada bloque es procesado en 4 distintas rondas o iteraciones. Cuenta con un cinturón de seguridad **RC2.**

2.1.3.4 RC2

RC2 es un encriptador de bloque con llave de longitud variable diseñado por Rivest para RSA Data Security. RC2 viene de "Ron's Code (Código de Ron)" o "Rivest's Cipher (Cifrador de Rivest)". Es tan rápido como DES y está diseñado como un drop-in (auto-remplazo) para

DES. Este puede tener más o menos seguridad que DES contra búsquedas exhaustivas, utilizando el tamaño apropiado de llave. Tiene una longitud de bloque de 64 bits y es 2 ó 3 veces más rápido que DES en software. El algoritmo es confidencial y propiedad de RSA Data Security. RC2 puede ser utilizado de la misma forma que el DES.

Tiene un estatus especial, ya que su proceso de aprobación de exportación es tan simple y rápido como el proceso de exportación criptográfica. Debido a lo anteriomente expuesto, los tamaños de la llave se manejan de acuerdo al fin que se le quiera dar, así se tiene:

- Llave de 40 bits para lo relacionado a la exportación de algún producto.
- Llave de 56 bits es permitida para subsidiarios y oficinas en el extranjero de las compañías de los EUA.

Una cadena adicional de entre 40-80 bits, llamada salt, puede ser usada para frustar a los atacantes quienes tratan de generar una larga tabla de posibles encriptaciones. La cadena salt es adicionada a la llave de encriptación y esta llave alargada es usada para encriptar el mensaje. por lo que no es encriptada con el mensaje.

2.1.3.5 RC4

RC4 es un encriptador de flujo de caracteres con llave de longitud variable con operaciones orientadas a bytes, diseñado por Rivest para RSA Data Security. El algoritmo está basado en el uso de una permutación aleatoria. Trabaja de la misma forma que el RC2, pero con la diferencia de que RC4 es un cifrador de flujo de caracteres.

Por el hecho de que este algoritmo es confidencial, ha sido revisado por analistas independientes bajo las condiciones de no divulgar su estructura, ni su funcionamiento.

2.1.3.6 RSA

RSA es un criptosistema de llave pública para la encriptación y autentificación. Fue inventado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman. Trabaja de la siguiente manera: toma dos números arbitrarios, p y q, para encontrar su producto $n = pq$; n es llamado "módulo". Escoge un número ,e, menor que n y un número primo relativo a $(p-1)(q-1)$, lo cual significa que e y $(p-1)(q-1)$ no tienen factores comunes excepto 1. Encuentra otro número d, tal que $(ed-1)$ es divisible entre $(p-1)(q-1)$. Los valores e y d son llamados exponentes público y privado respectivamente. La llave pública es el par (n,e); la llave privada es (n,d). Los factores p y q pueden conservarse con la llave privada o destruirse.

A continuación se explica cómo el RSA puede usarse tanto para encriptar como para autentificar.

Encriptación RSA: Suponiendo que Erika desea mandar un mensaje *m* a Alejandro. Erika crea el texto cifrado o encriptado (ciphertext) *c* por medio de una exponenciación: $c = m^e \bmod n$, donde *e* y *n* son la llave pública de Alejandro. Ella manda *c* a Alejandro. Para desencriptar, Alejandro utiliza la exponenciación: $m = c^d \bmod n$: la relación entre *e* y *d* asegura que Alejandro recuperó correctamente *m*. Como Alejandro es el único que conoce *d*, él es el único que puede desencriptar *m*.

Autentificación RSA: Suponiendo que Erika desea mandar un mensaje *m* a Alejandro de tal manera que él esté seguro de que el mensaje es auténtico y que es enviado por Erika. Erika crea una firma digital *s* exponenciando: $s = m^d \bmod n$, donde *d* y *n* son la llave privada de Erika. Ella manda *m* y *s* a Alejandro. Para verificar la firma, Alejandro realiza una exponenciación y checa que el mensaje *m* ha sido recuperado: $m = s^e \bmod n$, donde *e* y *n* son la llave pública de Erika.

Cualquiera puede enviar y encriptar mensajes o verificar la firma del mensaje, usando las llaves públicas, pero sólo alguien que posea la llave privada puede descifrar o firmar un mensaje.

2.1.3.7 S/MIME

S/MIME es una especificación para la seguridad de mensajes electrónicos. En 1995, algunos vendedores de software se reunieron y crearon S/MIME para resolver un importante problema, la intercepción de e-mail. Datos sensiblemente protegidos en una preocupación real, especialmente en un mundo que rápidamente crece en las conexiones de red. La meta de S/MIME es hacer fácil el aseguramiento de los mensajes de aquellos que se dedican a leer correos sin permiso.

S/MIME son las siglas de Secure/Multi-purpose Internet Mail Extensions. Esta especificación fue diseñada para ser fácilmente integrada en productos de e-mail y mensajes.
S/MIME construye seguridad en la parte superior del protocolo estándar de la industria de acuerdo a un conjunto de estándares criptográficos (PKCS). El hecho de que S/MIME fue creado utilizando otros estándares es importante para algunas cosas que están siendo

implementadas. Por su enfoque S/MIME está siendo utilizado para software EDI, productos en Internet y servicios en línea de comercio electrónico.

2.1.3.8 S-HTTP

S-HTTP (Secure Hypertext Transfer Protocol) es una extensión del HTTP (Hypertext Transfer Protocol) que provee servicios de seguridad. Originalmente fue desarrollado por Enterprise Integration Technnologies, posteriormente, Terisa Systems continuó desarrollo de éste. HTTP es el protocolo que forma la base del World Wide Web, permitiendo el intercambio de documentos multimedia en el Web. S-HTTP es diseñado para proveer confidencialidad, autenticidad, integridad y no-repudiación mientras soporta múltiples mecanismos de administración de llaves y algoritmos criptográficos a través de la opción de negociación entre las partes involucradas en cada transacción.

S-HTTP puede usar cualquiera de los cuatro métodos para intercambiar llaves de datos encriptados. Los posibles métodos son RSA, out-band, in-band y los Kerberos. Si RSA es usado, las llaves de los datos encriptados son intercambiados por el criptosistema de llave pública RSA. Out-band se refiere a un acuerdo de llaves externo, mientras que in-band se refiere a la llave transportada en un mensaje protegido por S-HTTP en otra sesión. En el método de los Kerberos, la llave es obtenida del servidor de Kerberos. Los algoritmos criptográficos soportados por S-HTTP incluyen DES, triple-DES, DESX, IDEA, RC2 y CDMF.

2.1.3.9 SSL

El protocolo handshake SSL (Secure Socket Layer) fue desarrollado por Netscape Communication Corp. para proveer seguridad y privacidad a través de Internet. El protocolo soporta la autentificación del cliente y del servidor. Este es una aplicación independiente, que permite protocolos como: HTTP, FTP y Telnet para ser estratificados por encima de éste transparentemente.

El protocolo SSL está capacitado para tratar con llaves de encripción así como también autentificar el servidor antes que los datos sean intercambiados por el nivel superior (aplicación).

SSL mantiene la seguridad e integridad del canal de transmisión, a través de la utilización del encriptamiento, autentificación y códigos de autentificación de mensajes.

SSL consta de dos fases:

1ª Fase.- El servidor en respuesta a la petición del cliente envía su certificado y sus preferencias de encriptadores; entonces, el cliente genera una llave maestra, la cual, éste encripta con la llave pública del servidor y transmite la llave maestra encriptada a el servidor. El servidor recupera la llave maestra y autentifica él mismo al cliente para poderle enviar un mensaje encriptado con la llave maestra. Subsecuentemente los datos son encriptados con las llaves derivadas de la llave maestra.

2ª Fase (opcional).- El servidor envía un reto al cliente. El cliente autentifica al servidor para retornar su firma electrónica en el reto, así como también su llave pública certificada.

Una variedad de algoritmos de encriptamiento son soportados por SSL. Durante el proceso de "handshacking", el criptosistema de llave pública RSA es usado. Después del intercambio de llaves los encriptadores que se pueden utilizar son: RC2, RC4, IDEA, DES, DES-triple y MD5 (Algoritmo de Mensajes Sintetizados). La certificación de la llave pública sigue la sintaxis del X.509.

2.1.3.10 X.509

La autenticación de directorio en X.509 puede ser llevada a cabo usando las técnicas de llave secreta o de llave pública; la última está basada en las certificaciones de llave pública. El estándar no especifica un algoritmo criptográfico en particular, sin embargo un informe anexo de el estándar describe el algoritmo RSA.

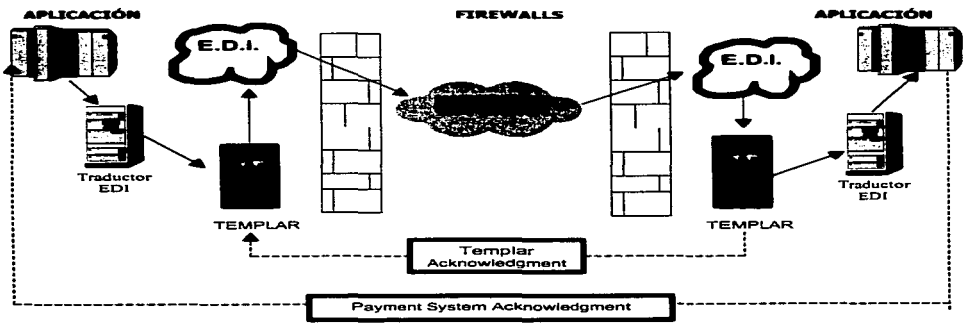
Una certificación X.509 consiste de los siguientes campos:

- Versión
- Número de serie
- Firma de identificación del algoritmo.
- Nombre del emisor
- Período de validación
- Nombre del usuario receptor
- Información de la llave pública
- Identificador único del emisor (sólo versión 2 y 3).
- Identificador único del receptor (sólo versión 2 y 3).
- Extensiones (sólo versión 3).
- Firma en los campos

Esta certificación es firmada por el emisor para autenticar la ligadura entre el nombre del receptor y la llave pública del receptor.
El estándar X.509 es soportado por varios protocolos incluyendo PEM, PKCS, S-HTTP y SSL.

2.1.45 Templar, Software para el Encriptamiento de mensajes EDI

Templar es un software creado por Premenos Corp., que permite la transmisión segura y confiable de documentos EDI a través de una red abierta tal como, Internet. Utiliza el protocolo TCP/IP en un formato MIME para la seguridad del e-mail a través del mecanismo de transporte de correo SMTP.
Templar reside entre el software traductor EDI y el sistema de transporte de datos. Al finalizar cada intercambio, Templar aplica las políticas de seguridad que los socios comerciales acordaron. Templar también rastrea los mensajes en el nivel del intercambio EDI y provee una bitácora de auditoría que informa los procesos de éste. La siguiente figura muestra como un documento se mueve de una aplicación a través de una red abierta a otra aplicación.

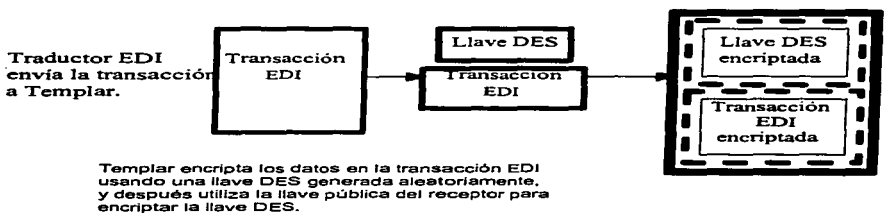


Seguridad de Templar

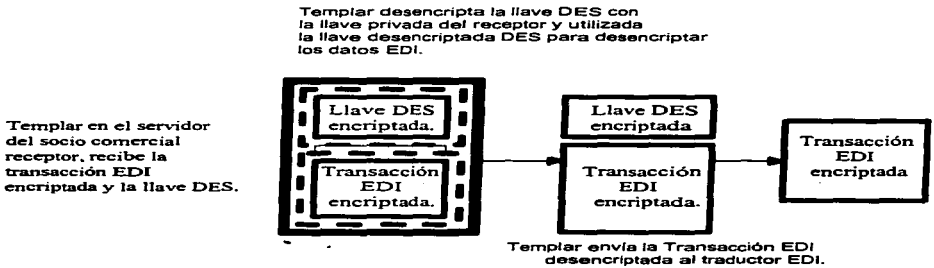
Templar provee las siguientes características de seguridad:

Encripción y Desencripción para la confidencialidad de las transacciones
Para encriptación y desencriptación, Templar combina la criptografía de llave única (llave simétrica) con la criptografía de llave pública/privada (llave asimétrica). También usa el Estándar de Encriptación de Datos (DES), RC2 y RC4 para los estándares de sus llaves únicas; para los estándares de sus llaves públicas/privadas utiliza el criptosistema RSA.

Cuando el traductor EDI manda a Templar una transacción EDI destinada a un socio comercial que espera ser encriptada, Templar primero encripta los datos en el intercambio con una llave aleatoria DES, RC2 o RC4. Después encripta la llave DES con la llave pública del receptor. A continuación, encapsula la transacción EDI y la llave DES, RC2 o RC4 ambos encriptados en una envoltura S/MIME y envía el paquete a través de la red abierta en un mensaje con formato S/MIME. A continuación se muestra el proceso en forma gráfica:



Para desencriptar una transacción EDI, Templar primero utiliza la llave privada del receptor con el fin de desencriptar la llave DES, RC2 o RC4. Después utiliza la llave DES, RC2 o RC4 desencriptada para desencriptar los datos EDI y poder enviar la transacción desencriptada al traductor EDI. En el siguiente esquema se muestra este proceso más claramente.



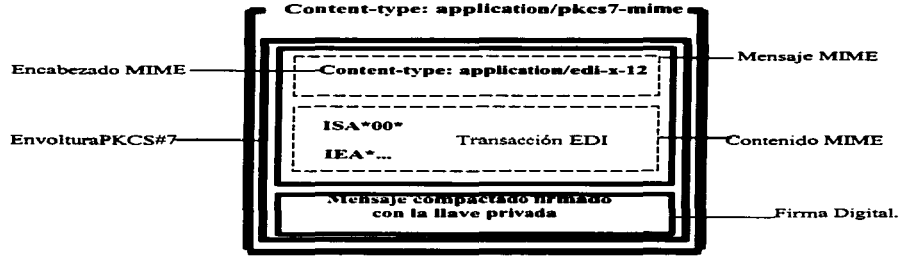
Autentificación , No repudiación y Firmas Digitales

Los socios comerciales que desean niveles adicionales de seguridad para la encripción pueden utilizar las características de seguridad como son: la autenticación y no repudiación de Templar.

Para la autentificación, Templar usa una llave única y sistemas de llaves públicas /privadas RSA, así como una firma digital.

Templar utiliza firmas digitales para:

Firmar un mensaje que va a mandar; empleando el formato S/MIME PKCS # 7. La siguiente figura ilustra el formato de un mensaje firmado.



Primero Templar computa un valor matemático, llamado "mensaje sintetizado" (message digest), de una parte del cuerpo MIME. El mensaje sintetizado es el resultado de un cálculo que toma un conjunto de datos de tamaño variable y retorna una cadena de caracteres de longitud fija, el mensaje sintetizado. Este mensaje es una síntesis matemática de los datos utilizados en su cálculo.

Después de computar el mensaje sintetizado, Templar, lo encripta con la llave privada del emisor. El resultado es una firma digital, la cual es enviada junto con la transacción EDI encriptada y encapsuladas en un formato de mensaje S/MIME PKCS # 7.

Aplicando la Autentificación y la No Repudiación del Origen

Cuando Templar recibe una transacción firmada con una firma digital, aplica la autentificación y la no repudiación de origen como sigue:

Primeramente desencripta el mensaje MIME con la llave privada del receptor y computa un mensaje sintetizado. Éste, es utilizado para verificar la integridad del mensaje MIME. Entonces emplea la llave pública del emisor para desencriptar la firma digital contenida en el paquete S/MIME PKCS # 7. La firma digital desencriptada es el mensaje sintetizado de el mensaje MIME. Templar computa un nuevo mensaje sintetizado de el mensaje MIME

recibido y lo compara con el valor de la firma digital desencriptada. Si estos dos valores concuerdan, la integridad del mensaje MIME y la identidad de su emisor son verídicas.

Aplicando la No Repudiación del Receptor

Después de aplicar la autentificación y la no repudiación del origen, Templar, aplica la no repudiación del receptor. Una vez que la integridad de la transacción EDI y la identidad de su emisor han sido verificadas, Templar, envía un AUTACK verificando que la transacción EDI fue recibida por el recipiente a la cual fue destinada.

Para enviar un recibo AUTACK, Templar crea un AUTACK y lo firma con la llave privada del receptor de la transacción EDI. Después pone esta firma en el AUTACK y lo transmite a el emisor verificado de la transacción EDI.

Templar utiliza el mensaje AUTACK cuando firma la recepción de un mensaje.

Cuando el recibo AUTACK llega, Templar primero verifica su integridad. Después desencripta la firma digital y la llave pública del emisor contenida en el AUTACK. El valor de este mensaje sintetizado es el valor del AUTACK recibido. A continuación, Templar computa un mensaje sintetizado del AUTACK y compara el valor de este mensaje sintetizado con el valor del mensaje sintetizado en la firma digital desencriptada. Si estos valores corresponden, la integridad del AUTACK y la identidad de su emisor son verídicas.

Ya completados estos pasos, Templar compara la información rastreada contenida en el AUTACK con la información original rastreada de la transacción. Si hacen juego, es decir, si el AUTACK es positivo, lo siguiente está implícito:

La transacción EDI es conocida por el emisor y el receptor. El AUTACK contiene el mensaje sintetizado de la transacción EDI y el número de la transacción EDI, por lo tanto templar reconoce estos valores.

La autenticidad e integridad de la transacción EDI recibida son verídicos.

El recipiente destino recibió la transacción EDI.

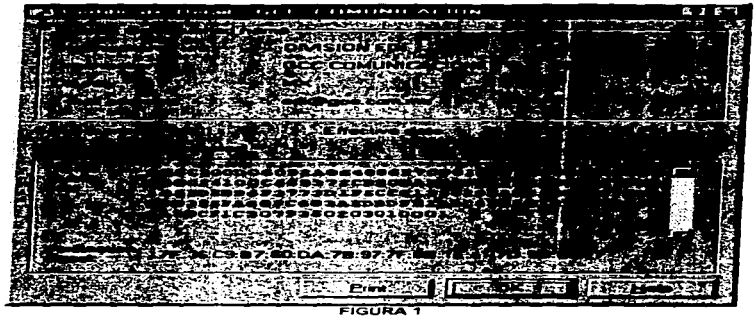


FIGURA 1

Pantalla que muestra los datos utilizados en la autentificacion

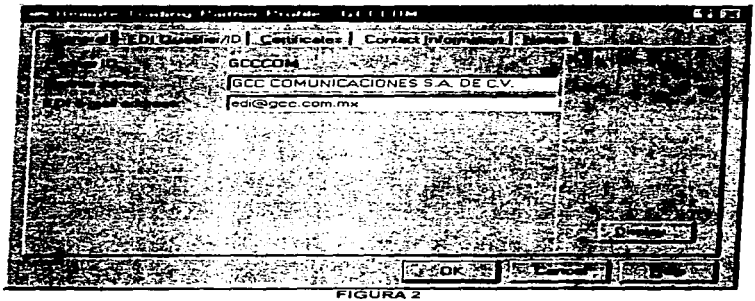


FIGURA 2

Muestra la configuracion de uno de los socios comerciales

2.2 FORMAS ELECTRÓNICAS

2.2.1 Definición

Las formas electrónicas son programas basados en computadoras capaces de desplegar un formato en la pantalla como si fuera una forma de papel. Estas formas permiten una adecuada captura, impresión y un correcto desplegado de la información a través de la computadora. Las formas electrónicas pueden ser enviadas electrónicamente a un punto de destino donde pueden ser procesadas directamente por computadoras automáticamente.

Mientras las formas electrónicas son similares en concepto a sus primas las formas en papel, éstas ofrecen muchísimas ventajas, ya que las formas electrónicas permiten desplegar convenientemente documentos que han sido recibidos y llenar documentos para poder ser enviados.

El uso de formas electrónicas provee un simple y poderoso método para crear, manipular y procesar documentos y reportes comerciales.

El hecho de que desarrolladores de software hayan pensado en el uso de formas electrónicas para el intercambio electrónico de datos se debe a las ventajas o capacidades que puede tener una empresa. Estas ventajas se presentan a continuación:

- Bajo costo por concepto de formas.
- Registro exacto (No se desperdician formas cuando no se llenan correctamente).
- Superior calidad de impresión (Todas las formas son originales).
- Impresión rápida de las formas.
- Eliminación de obsolecencia.
- Una forma electrónica puede usarse en 1 o más impresoras.
- Validación en los datos de captura.
- Poco tiempo para su intercambio.

Las formas electrónicas pueden ser utilizadas en muchas áreas de la industria y también para sustituir varias formas de papel. Algunos ejemplos son:

FORMAS DE PAPEL	INDUSTRIAS
Aplicaciones de crédito	Medica
Facturas	Seguros
Ordenes de Compra	Manufactura
Solicitudes de empleo	Aereoespacio
Exámenes de Admisión	Gobierno Municipal y Federal
Estimaciones	Bancaria y Financiera
Formas de Inspección, etc.	Ventas y Mercadeo, etc.

2.2. WebDox , software que utiliza Páginas Electrónicas para la realización de EDI a través de Internet.

WebDox es un software que permite a las grandes empresas incrementar los beneficios derivados del intercambio electrónico de datos así como expandir sus programas de comercio electrónico a un gran número de socios comerciales. Este software utiliza el poder de Internet y de la World Wide Web para transportar mensajes de datos estructurados entre socios comerciales.

WebDox tiene dos componentes:

- *WebDox Central*, el cual, reside en un servidor NT como lugar primario y consta de dos elementos el WebDox Admin y el WebDox Server.

- *WebDox Remote* aplicación con formas basadas en Windows para la PC fáciles de usar por los socios comerciales.

Requerimientos Técnicos

WebDox Server

RECURSOS	REQUERIMIENTOS
Procesador	Pentium o superior
RAM	64 MB
Sistema Operativo	Microsoft Windows NT Server 4.0 o superior
Software de Internet	Microsoft Internet Information Server 2.0 o superior. Microsoft SQL Server 6.5 o superior
Comunicaciones	Conexión Internet dedicada-ISDN o superior
Software de Seguridad	Digital Certificate for IIS

WebDox Admin

RECURSOS	REQUERIMIENTOS
Procesador	486 o superior
RAM	12 MB
Sistema Operativo	Windows 95, Windows NT 4.0 o superior
Comunicaciones	Conexión TCP/IP al WebDox Server

WebDox Remote

RECURSOS	REQUERIMIENTOS
Procesador	486 o superior
RAM	16 MB
Sistema Operativo	Windows 95, Windows NT Server 4.0 o superior
Comunicaciones	Conexión a Internet de 14,400 bauds o superior
Módem	14,400 bauds o superior
Monitor	VGA o superior
Software para Internet	Browser Internet

Las facilidades sofisticadas de WebDox permiten operaciones online y offline. Los socios comerciales pueden automáticamente durante la transmisión (online) intercambiar documentos con los hubs, y después los documentos (offline). El tiempo de las conexiones de los socios comerciales pueden ser muy cortas, mientras al mismo tiempo se minimiza la capacidad requerida del hub.

WebDox hace uso de los protocolos de la industria estándar del Web, de las características inherentes a los productos browser y server Internet de Microsoft para prevenir la intromisión y el engaño de personas ajenas. Por su parte el WebDox Central utiliza confirmaciones certificadas de un sitio Web para que otros sitios Web no puedan asumir la identidad de la ubicación del WebDox Central. Todas las comunicaciones entre los socios comerciales son protegidas por el protocolo SSL (Secure Sockets Layer). WebDox genera documentos de acuse de recibo para confirmar que cada transacción fue completada exitosamente.

El registro de socios comerciales es totalmente automático. Ellos solamente envían una forma de registro al sitio del WebDox Central y escoge las formas electrónicas que desea activar. El WebDox Central automáticamente las da de alta y las empieza a rutear en las formas adecuadas.

Los socios comerciales además de hacer uso de las aplicaciones de formas también pueden hacer uso del Web.

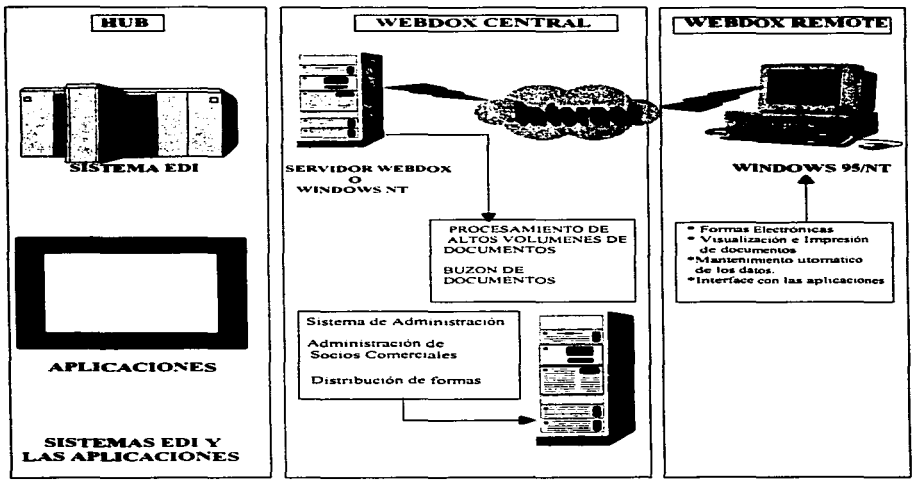
Cómo trabaja WebDox

El WebDox Central toma las transacciones comerciales, como ordenes de compra, de alguna aplicación del emisor o traductor EDI y las convierte en formas electrónicas. Las formas son enviadas a socio comercial receptor a través de Internet. El socio comercial receptor visualiza las transacciones y las formas en el WebDox Remote. Después WebDox Automáticamente crea documentos como facturas y avisos de embarque y puede imprimir documentos requeridos como etiquetas para empaque y etiquetas de código de barra.

Arquitectura

Arquitectura de Sistema

La arquitectura de sistema de WebDox se muestra a continuación en la siguiente figura. En el centro está el WebDox Central, consistiendo del Servidor WebDox y los componentes del WebDox Admin. En el lado derecho de la ilustración muestra el WebDox Remote en el sitio del Socio Comercial.



Procesos de Sistema

Flujos de Datos Operacionales

Los siguientes diagramas muestran como los documentos fluyen entre el hub del usuario y los socios comerciales. La secuencia de la figuras comienza con el envío de la forma de registro del socio comercial después de instalar WebDox Remote, como se muestra en la figura 2. La figura 3 muestra al WebDox Admin enviando electrónicamente el formato de la aplicación al WebDox Remote del socio comercial. la figura 4 ilustra el flujo de las transacciones comerciales entre el WebDox Server y el WebDox Remote. Por último la figura 5 tipifica el flujo de los mensajes de acuse de recibo.

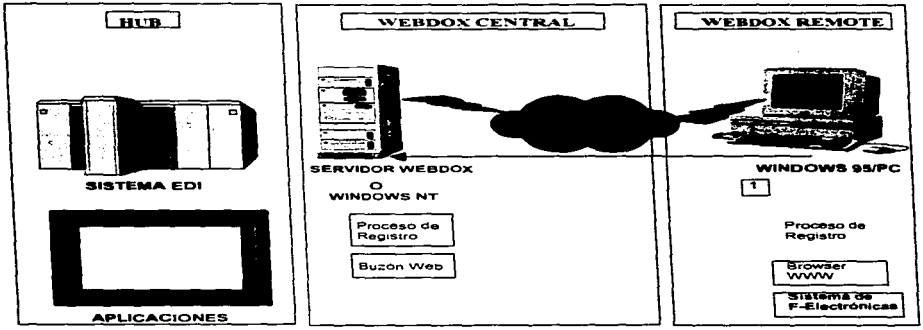


Figura 2

Flujo de Registro del Socio comercial. 1. Este es el flujo de la forma de registro desde el WebDox del Socio Comercial al Sistema del WebDox Server. El Sistema del WebDox Admin puede ser usado para visualizar y modificar la información del socio comercial.

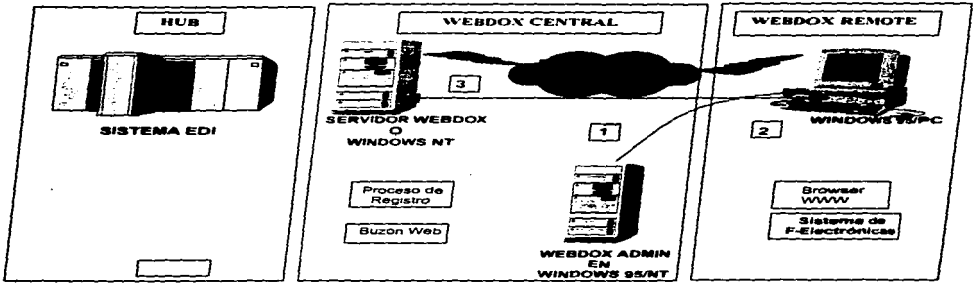


Figura 3

Flujo de los formatos en blanco. 1. Despues que el socio comercial es registrado, el sistema del WebDox Admin en vía al WebDox Remote una notificacion para que automaticamente de cargue la forma de la aplicación del WebDox Server. 2. El WebDox Remote despliega las notificaciones y carga las formas de WebDox Server. 3. La forma en blanco es entonces utilizada para recibir y crear documentos para el intercambio con el WebDox Server.

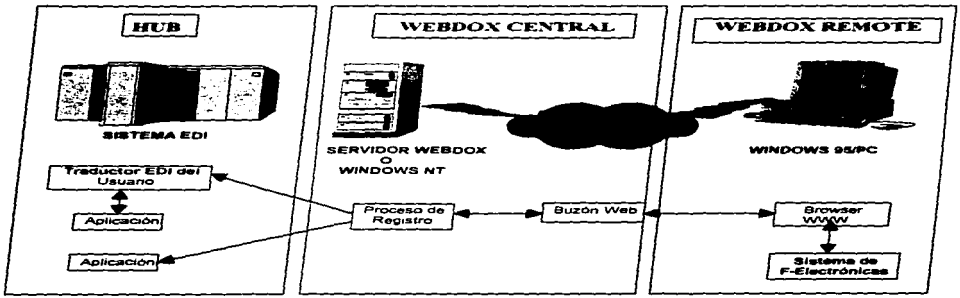


Figura 4

Flujo del Documento Comercial. Los flujos de un documento comercial entre los componentes del sistema WebDox son ilustrados.

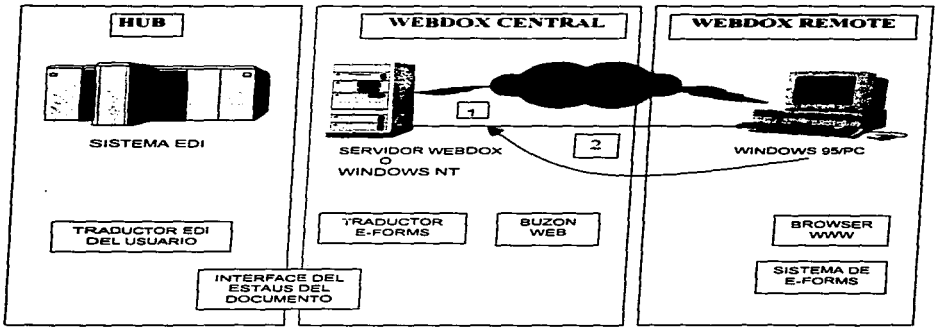


Figura 5

Flujo del Acuse de Recibo. 1. WebDox Server envía al socio comercial un mensaje notificando que el documento enviado ha sido recibido. 2. WebDox Remote envía un mensaje de acuse de recibo al WebDox Server por cada documento que es recibido. Esta información es usada para mantener auditada la información cuando los mensajes son intercambiados.

CAPITULO

3

WORLD WIDE WEB

3.1 Conceptualización

El World Wide Web es un sistema de navegación por Internet, que administra y distribuye la información a través de formatos dinámicos para la comunicación masiva y personal.

El Web integra diferentes formatos de información: imágenes fijas, texto, audio y video; además de integrar los mayores recursos que existen en Internet.

3.2 Orígenes

El origen del WWW se remonta al año de 1989, cuando un físico llamado Tim Berners-Lee del Laboratorio Europeo de Partículas Físicas (CERN), propuso el concepto del Web como un sistema para transferir ideas e investigación entre la comunidad de científicos relacionados con la física y la energía de alto nivel; teniendo como fundamento, ésta, el uso del hipertexto, una forma de presentar y relacionar información con enlaces en lugar de líneas secuenciales, para transmitir documentos y comunicación por las redes de cómputo.

A finales de 1990, funcionó el primer software Web en una computadora NeXT de Steven Job´s, el cual permitía visualizar y transmitir documentos de hipertexto en Internet y facilitaba la edición a los usuarios.

A partir de su conocimiento, el Web se ha expandido con un ritmo acelerado.
En 1993, el WWW era un proyecto que apenas tenía una presencia moderada entre el público en general. Ya para 1995, era mencionado frecuentemente por los medios de comunicación, principalmente la televisión. En 1997, el WWW es uno de los principales medios de comunicación entre la personas, empresas y países, ahora la mayoría de la gente hace uso de él.

Anteriormente fue mencionado que el WWW estaba fundamentado en el hipertexto, además de la hipermedia pero, ¿Qué es cada uno de estos conceptos?

El término *hipertexto* se refiere a la información de referencia cruzada en la que sólo hay que apuntar y hacer clic en un elemento apara ir a otro, es decir, es una interfaz amigable. La *hipermedia* es una extensión natural del hipertexto, pero con la diferencia, que en la segunda los enlaces son conexiones gráficas, mensajes de audio y video además del texto.

El medio de transmisión de la información contenida en el Web lo realiza el protocolo HTTP (Protocolo de Transportación de Hipertexto), a través del cual los servidores Web permiten el acceso a la información hipermedia e hipertexto a la computadora que así lo solicita. Cuando una computadora se comunica con un servidor Web, se establece la conexión, se recupera la información inicial y rápido se cierra. Esta se abre cuando se necesita transmitir más información a la computadora local o cuando se apunta a un enlace que requiere más información del servidor.

La primera información que se recibe desde un servidor remoto Web es la *Página base* o mejor conocida como *Página Web*, la cual es una interface inicial a una serie de documentos, archivos y recursos que residen en la computadora o en otros servidores Web en todo el mundo. Para poder hacer una conexión Web se necesitan direcciones ocultas llamadas URL las cuales representan un enlace a cada documento o archivo en Internet. Una dirección URL está integrada por:

Método de acceso para recuperar el recurso	Computadora en donde reside la información y a donde se va a conectar	Ubicación detallada del recurso
http://	**www.unam.com/**	**tesis.html**

El URL (Localizador Uniforme de Recursos) es el elemento central para la navegación por el Web.

3.3 Manejo de las Páginas Web para la realización de EDI.

La visión para el comercio en Internet y el inherente conjunto de retos representan una gran oportunidad para las compañías quienes buscan operar en un creciente y competitivo espacio de mercado. Los bancos están compitiendo con procesadores financieros, las compañías de cable con las compañías de teléfonos, proveedores de servicios en línea con los proveedores de acceso a Internet- y este es sólo el principio.

Como la era electrónica continúa evolucionando, las compañías están bajo la presión de cambiar su manera de proveer servicios a los clientes y negocios a través del ofrecimiento de

servicios cómodos y seguros. Esto lo están logrando con el uso del World Wide Web de Internet, el cual, tiene todas las características necesarias para que las empresas realicen transacciones comerciales desde la comodidad de su propia computadora con la confianza de la integridad y privacidad de éstas. Pero, ¿cómo se realiza el intercambio electrónico de datos por medio del Web? En los siguientes párrafos se describirá esta nueva forma de realizar negocios, así mismo, se presentará el funcionamiento de software OM-TRANSACT, como un ejemplo de este tema.

3.3.1 Transacciones comerciales a través del Web.

El World Wide Web está construido en servidores HTTP que pueden brindar contenido o servicios, o a veces los dos.

Los servidores Web que proporcionan contenido pueden ofrecer noticias, exposiciones, material cultural, entretenimiento o diversión, que consiste en cualquier combinación de recursos multimedia (textos, imágenes, audio, video y appletes ejecutables). Este material en el Web, algunas veces contiene hiperenlaces a otros sitios de contenido o posiblemente a sitios de servicios. El contenido puede ser almacenado estáticamente por los servidores o computado dinámicamente para ser entregado. Una persona u organización que brinda contenido en el Web es llamada Proveedor de Contenido.

Los servidores que ofrecen servicios, en contraste, publican en el ciberespacio los eventos sintetizados o institucionales que forman la base para las sociedades humanas y económicas, tal como la comunicación, autentificación en el intercambio de bienes o servicios para una compensación financiera o el establecimiento de relaciones formales. En las páginas Web presentan información o confirmaciones de los servicios presentados y acciones tomadas por el servidor Web, posiblemente presentando hiperenlaces a otros servicios o posiblemente a algún contenido. La persona u organización que utiliza un servidor Web para proporcionar servicios se le conoce como Proveedor de servicios.

Es posible para una organización actuar tanto como proveedor de servicios como de contenido, pero en ocasiones es conveniente separar los dos roles en partidas diferentes con el fin de determinar las metas que se van a lograr.

El propósito principal para ofrecer contenido y servicios en la Web es por supuesto, el de satisfacer las demandas de las personas o de clientes Web de operación autómata.

Estas distinciones forman la base para visualizar a los participantes que conforman la actividad en el Web

- Proveedores de servicios.
- Proveedores de contenido
- Consumidores (contenido o servicios).

3.3.2 Autentificación de URLs

Authenticated-Payload URLs

Para implementar esta separación de conocimientos en el Web. Se han desarrollado especificaciones para una mejor manera de transmitir datos autentificados a través del Web utilizando los URL. Estas son llamadas Authenticated-payload URLs: APUs. Este método para comunicaciones autentificadas hace posible la comunicación directa entre los proveedores de contenido y los proveedores de servicios sin ningún nuevo protocolo especial.

Tres claves son las necesarias para que los APUs las direccionen:

1. *Transmisión de datos pequeños.*- Transmitir datos de longitud pequeña a un servidor Web, el cual está configurado para recibir y procesarlos en la iniciativa de los clientes Web.
2. *Verificar la integridad de los mensajes.*- Proveer al receptor con las armas necesarias para detectar si los datos fueron corrompidos en el tránsito, accidentalmente o maliciosamente.
3. *Verificar la autenticidad del mensaje.*- Proveer al receptor las herramientas necesarias para asegurarse que los datos fueron creados por alguien autorizado.

Las implementaciones actuales hechas por Open Market referentes a los APUs dependen de las propiedades del HTTP, las cuales son altamente usadas y conocidas. Algunas de estas son:

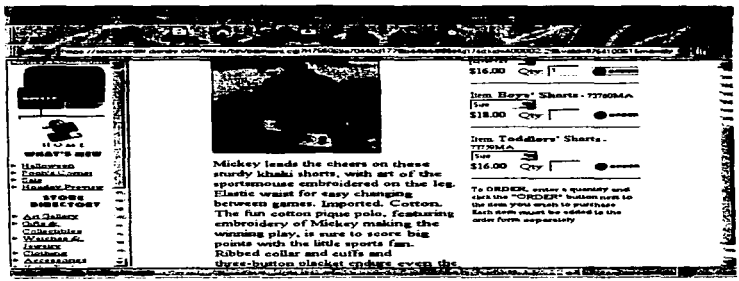
- Rutas a CGI ejecutables en los URLs.
- Uso de query strings en los URLs.
- Terminación parcial o relativa de los URLs.
- Redirección de cliente (HTTP retorna el código 302).

Estas propiedades son obviamente soportadas pero son menos conocidas que algunos otros mecanismos HTTP más comunes.

3.3.3 Tipos de APUs

Dentro del comercio electrónico en el Web existen dos tipos de APUs:
a) APUs basados en query strings
b) Ticketed APUs

3.3.3.1 APUs basados en query strings (query string-based APUs) o Digital Offers.
Los APUs basados en un query string son URLs que apuntan aun CGI (Common Gateway Interface) acarreando la información ingresada en un query string el cual, contiene los datos para un receptor conocido con el fin de autentificar al autor del query string y verificar la integridad del query string. A continuación se muestra una pantalla capturada de Disney, la cual utiliza esta tecnología para vender bienes con seguridad a través del Web usando una de las transacciones de proveedor de servicios en el Web.



Aquí está otro ejemplo de un particular tipo de APU basado en un query string, en el cual por definición, todo lo que se encuentra después del "?"" constituye el query string:

http://www.somewhere.com:80/cgibin/payment.cgi?194e7a75bcb66a464f0423ed697bb:kid=300009.200021&valid=824198763&ProdCode=61000&espire=2592000&goodstype=h&desc=68484%3A%20PULP%20FICTION%20%20PFICTION%3ALOGO%2FYOU%20WONT%20TSHIRT&domain=hardgoods&amt=12.99&cc=US&ss=env&fmt=get

La forma general de los APUs basados en query string es:

Protocolo://nombre del dominio:número de puerto/ruta?payload

Donde:

- El *protocolo* siempre es http.
- El *nombre del dominio* es el nombre del dominio DNS (la dirección IP) del servidor Web receptor. En el ejemplo anterior, el receptor es www.somewhere.com.
- El *número del puerto* es el número de puerto TCP/IP en el cual el servidor Web receptor espera ser escuchado para ingresar las peticiones (este no es requerido si el número del puerto es 80, el cual es el estándar por omisión). En el ejemplo el puerto es: 80.
- La *ruta* es la ruta completa al CGI que actúa como una **interface** para recibir y procesar el query string. Más de una interface debe existir en el mismo servidor Web, para direccionar a varios cuando se necesite. En el ejemplo la interface es: /cgi-bin/payment.cgi.
- El *payload* es un query string contenido en un largo string de dígitos hexadecimales por razones de seguridad (específicamente la autentificación y la verificación de integridad), llamada **MAC**, seguida de dos puntos (":") como un separador interno, y después el payload data estructurado como una **serie de pares de valores** de nombres de la forma nombre=valor, separados por ampersands ("&"). En el ejemplo anterior el MAC es: 194e7a75bcb66a464f0423ed697bb y el resto del payload URL constituye el actual ***payload data***. El MAC y el payload data en conjunto son referenciados como el **payload**.

Los APUs basados en los query strings hacen posible la siguiente secuencia de eventos:

1. Un cliente Web envía una requisición al servidor Web designado en un APU basado en un query string obtenido de un servidor Web capaz de generar URLs. Este URL puede ser el resultado de una redirección, o ser seleccionado de una página o de una lista de bookmarks o explícitamente ingresado.

2. El servidor Web receptor ejecuta el programa de interface direccionado a través del APU basado en un query string, pasándolo al payload como entrada.

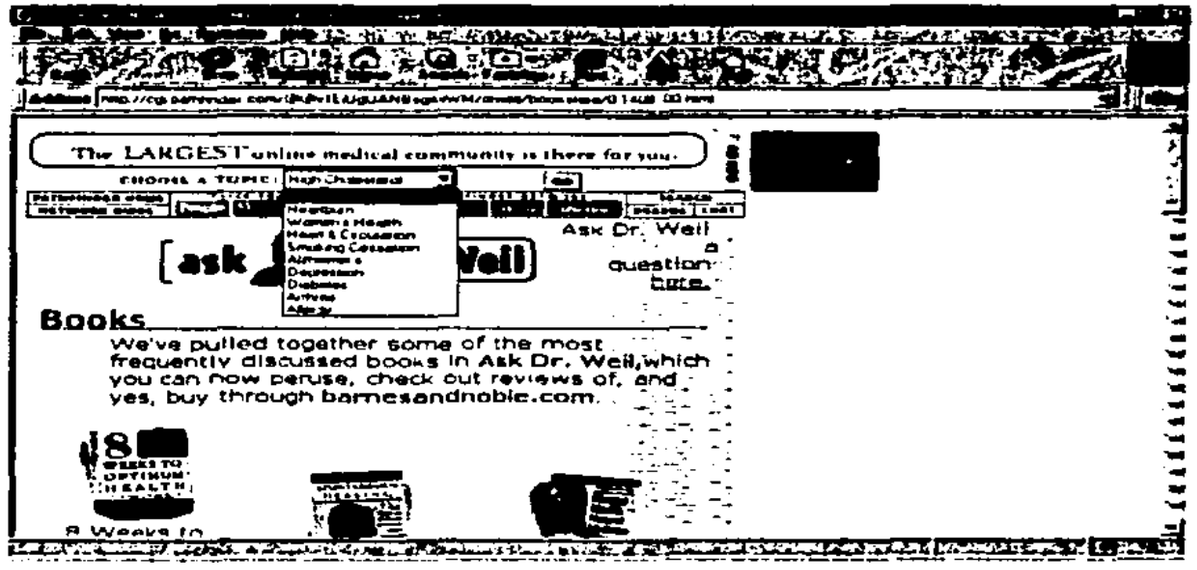
3. El programa de interface verifica la integridad y la autenticidad del payload ingresado.

4. Si la verificación falla, la interface produce una respuesta apropiada de servicio denegado la cual, el servidor Web retorna al cliente Web. Esta respuesta puede ser una página HTML describiendo el problema y posiblemente solicitando la entrada a través de una forma, o una redirección a otro URL habilitando el operador del cliente Web para obtener un APU basado en un query string válido. De otra manera, la interface procede a procesar el payload, posiblemente invocando a otros programas, y entonces produce la respuesta que es apropiada para empezar a proporcionar el servicio o contenido.

Los pasos 1 y 2 hacen referencia al primero de los tres requerimientos mencionados anteriormente: transmisión de datos pequeños entre el proveedor de contenido y el proveedor de servicios en demanda, posiblemente en la requisición de un comprador. Los pasos 3 y 4 referencian los dos siguientes requerimientos: verificar la integridad y autenticidad de los datos transmitidos.

3.3.3.2Ticketed APUs

Un ticketed APU es un URL sin restricciones en el recurso a la ruta que apunta o en el uso del query string, pero con un especial string de caracteres llamado un ticket prepended a su ruta. Para que un servidor Web sea capaz de responder a los requerimientos que usan los ticketed APUs, debe ser capaz de identificar la porción etiquetada del URL para ser procesado como sea necesario y cubrir el medio apuntado por la ruta del URL después de que la etiqueta ha sido removida de allí.
A continuación se muestra una pantalla capturada de un sitio Web que utiliza la Ticketed APU.



Aquí se muestra otro ejemplo de un Ticketed APU:

http://www.zine.com/@@Fz3H780g56kCSf2s/features/bookreviews.html

La forma general de un Ticketed APU es la siguiente:

Protocolo://nombre de dominio: No. Puerto/Ticket/ruta?query-string

El protocolo, el dominio y el número del puerto del URL trabajan de la misma manera que los APUs basados en query string. La ruta y el query string no son objeto de ninguna restricción. El query string es opcional. En general, la ruta puede ser omitida si el servidor Web está configurado para dar un recurso estándar cuando no es especificado (comúnmente la página base de un sitio Web). El ticket es el string: @@Fz3H780g56kCSf2s, donde un "@" o una secuencia de "@@" lo identifica como un ticket, de un elemento real de la ruta (por ejemplo el nombre de algún directorio), y el resto es el payload que contiene al MAC así como también al payload data, como en un APU basado en un query string. En contraste con el payload de un APU basado en un en query string, el payload aquí, el binario, el cual ha sido representado usando un radix64 codificado. Este no encripta el payload, sino que

meramente asegura que este no contenga caracteres, a los cuales el protocolo de transmisión HTTP les atribuya un significado especial.

Los Ticketed APUs hacen posible la siguiente secuencia de eventos:

1. Un cliente Web envía una requisición al servidor Web designado en un ticketed APU obtenido de un servidor Web capaz de generar URLs. Este URL puede ser el resultado de una redirección, o ser seleccionado de una página o de una lista de bookmarks o explícitamente ingresado.
2. El mecanismo de procesamiento de Tickets del servidor Web receptor identifica la existencia de un Ticket en la ruta y después verifica su integridad y la autenticidad.
3. Si la verificación falla, el mecanismo de procesamiento de Tickets del servidor Web receptor produce una respuesta apropiada de servicio denegado el cual, el servidor Web retorna al cliente Web. Esta respuesta puede ser una página HTML describiendo el problema y posiblemente solicitando la entrada a través de una forma, o una redirección a otro URL habilitando al operador del cliente Web para obtener un Ticketed APU, o cualquiera que sea apropiado para la aplicación. De otra manera, el mecanismo de procesamiento de Tickets procede a procesar el payload data, posiblemente invocando a otros programas, y entonces produce la respuesta que es apropiada para el servicio o contenido.

El paso 1 al primero de los tres requerimientos mencionados anteriormente: transmisión de datos pequeños entre el proveedor de contenido y el proveedor de servicios en demanda, posiblemente de la requisición de un comprador. Los pasos 2 y 3 referencian los dos siguientes requerimientos: verificar la integridad y autenticidad de los datos transmitidos.

3.3.4 Generación de APUs

Un APU nunca es escrito manualmente. Por lo que se han diseñado herramientas software con el fin de generar Ticketed APUs, las cuales utilizan los siguientes parámetros:

- El nombre del dominio o la dirección IP del servidor Web receptor, con el número del puerto (opcional).
- Una llave secreta para generar el MAC(Message Authentication Code).
- El payload data a ser transmitido.
- La ruta de la interface, si el APU a ser generado va a estar basado en un query string.

- Opcionalmente, la ruta y el query string del APU author's choosing si el APU a ser generado es un Ticketed APU.

Estos parámetros pueden ser reunidos de las siguientes formas:

- El usuario los ingresa en un programa que presenta una interface gráfica provisto de formas y otros controles gráficos.
- El usuario o una máquina los ingresan en forma de argumentos pasados en una línea de comando de un programa, también a través de un shell interactivo, en un script, o en un server-side que incluya la directiva #exec.
- Una máquina programada ingresa un conjunto de funciones API.
- Una máquina los ingresa, tomando de otra máquina de archivos leíbles los valores de entrada por omisión que tiene, los cuales van a ser usados cuando la entrada es requerida, pero no explícitamente suministrada por el usuario.

El nombre del dominio o la dirección IP del servidor receptor Web y la llave secreta son usados para generar los MAC, los cuales son generalmente reunidos de una máquina de archivos por omisión leíbles, visto que los medios para obtener el payload data típicamente varía mucho por estas posibilidades.

Habiendo obtenido estos datos, el software generador de APUs alimenta una representación binaria del payload, llamada mensaje, sólo con la llave secreta, a una función matemática especial conocida como one-way hash function o función para compactar mensajes (message digest function), para producir un valor llamado mensaje compactado con las siguientes características:

- Es mucho más pequeño que el mensaje.
- Siempre es del mismo tamaño, a pesar del tamaño del mensaje.
- Es único en el sentido de que aún cuando es más pequeño que el mensaje, podría ser diferente si un solo carácter en el mensaje ha sido diferente.
- Podría ser diferente si una llave secreta diferente fue usada.

Este mensaje compactado es llamado: Código de Autentificación de mensaje o MAC por su nombre en inglés Message Authentication Code.

Si el software generador de APUs crea un APU basado en un query string, entonces produce un URL válido para conectarse "http://" con el nombre del dominio o la dirección IP, opcionalmente el número del puerto precedido por ":". Después, el ticket delimitado entre slashes ("/"), seguido de cualquier ruta y el query string que fue (opcionalmente) proveído por el autor del APU.

El payload incluye identificadores de la llave y de la función para compactar mensajes usados para calcular el MAC. Estos identificadores son:

- El emisor y el receptor deben seguir un acuerdo en cómo el mensaje compactado y la llave son identificados en el payload data.

Los APUs pueden ser insertados en el HTML o en otro medio que soporte URLs, tal como VRML, o usados como respuestas de redirección para un requerimiento de un cliente Web.

El diseñador de un sitio Web que soporta APUs puede decidir que la generación de éstas sea dinámicamente at hit time, para que algunos o todos los valores que constituyen el payload puedan ser tolerados por las características particulares conocidas del visitante, factores externos tales como tiempo, hora, o ingresados de una base de datos relacional o un live data feed, para dar pocas posibilidades. Los APUs también pueden ser estáticos, calculados en el progreso de una área puesta en escena, antes de ser usados en un área de producción o por un programa de producción que requiere APUs pre calculados.

Calcular APUs dinámicamente resulta en un corto tiempo de respuesta a la petición del cliente Web. El escoger entre utilizar APUs dinámicos o estáticos o los dos, debe hacerse basado en el desempeño así como también en los requerimientos funcionales.

3.3.5 Validación de APUs

Cuando un cliente Web envia una petición a un servidor Web indicado por un APU, el payload del APU es validado por la interface señalada, en el caso de un APU basado en un query string, o por un mecanismo de procesamiento de Tickets, en el caso de un Ticketed APUs. Para Ticketed APUs, el mecanismo de procesamiento de Tickets primero debe decodificar el ticket, este representado usando el radix64.

Los pasos requeridos para validar el payload de un APU son los siguientes:

1. Localizar en el payload los identificadores usados para indicar que función para compactar archivos fue utilizada así como cual llave secreta fue empleada.
2. Alimentar el payload data y la llave secreta identificada a la función para compactar mensajes identificada para producir un MAC.
3. Comparar este MAC con el MAC traído en el payload.
4. Si los dos MACs concuerdan, entonces el APU es considerado válido, de otra manera el servidor Web conoce que el payload ha sido corrompido, ya sea accidentalmente o intencionalmente.

Para que esta técnica de autentificación de mensaje sea posible, la función para compactar mensajes debe ser fuerte, y la llave secreta debe ser compartida por las dos partes, cuidadosamente guardada a través del proceso al ser generada distribuida y usada, hasta que expire y sea remplazada con una nueva llave.

3.3.6 Procesamiento de APUs

Una vez que la APU ha sido exitosamente validada, el programa de interface o el mecanismo de procesamiento de Tickets puede procesar el resto del payload data como apropiado a la aplicación en particular.

3.3.7 Arquitectura para el Comercio de Tercera Capa

Como se vio anteriormente, los APUs posibilitan a los proveedores de contenido y a los proveedores de servicios para enviar y recibir datos con la seguridad de que cualquier falla de la integridad o autenticidad será detectado. Sobre la base de esta tecnología, se ha desarrollado un arquitectura de tercera capa para soportar transacciones comerciales que copien en el ciberespacio todos los aspectos que se desarrollan normalmente en las transacciones comerciales tradicionales.

En esta arquitectura, los tres aspectos son:

- Los vendedores ofreciendo bienes para su venta en una tienda Web y proporcionando información de éstos desde los servidores.

- Servicios de transacciones para todas las operaciones back-office envueltas en transacciones comerciales.
- Los compradores usando un software para clientes Web con el fin de realizar compras.

3.3.7.1 Tiendas Web (Web Stores)

Las expresiones "Tiendas Web" (Web Stores) o "tiendas en línea" (on-line store) son frecuentemente utilizadas para describir un alto rango de diferentes tipos de sitios Web, desde publicidad en línea, hasta catálogos, de vendedores de servicios al por menor y otros vendedores de bienes y servicios, algunas veces a gran escala.

Todos los sitios en el Web contienen páginas (generalmente presentadas en HTML) que describen productos textualmente o mostrados gráficamente. En muchas "tiendas", sólo se presentan las instrucciones de compra a lo largo de la información del producto solicitada por el visitante el cual actualmente desea adquirir éste, por fuera del Web(go out of band), contactando al vendedor por teléfono, e-mail u otro medio diferente al Web. Tales "tiendas" son comúnmente llamadas catálogos o simplemente publicidad.

Una tienda Web, precisamente definida, es un sitio que presenta contenido (imágenes, texto, etc., que describe productos para la venta) y ofrece acceso a los servicios requeridos por el comercio realizados en banda (not resorting to non-Web communication, como el teléfono). El comercio Web es entecos una instancia de la clase de actividades que envuelven tanto contenido como servicios.

Las tiendas Web pueden vender dos tipos de bienes: softgoods, tales como texto, imágenes, material multimedia, software, caracterizados por el hecho de que totalmente pueden ser mostrados electrónicamente, para ser entregados a través del Web, y hardgoods, tales como artículos de oficina, equipo, ropa, los cuales requieren entrega por los medios tradicionales. Los vendedores Web que ofrecen softgoods deben operar un servidor completo, desde el cual, los softgoods puedan ser obtenidos una vez que han sido comprados. Un servidor completo puede correr en el mismo host de la tienda Web o en uno diferente dependiendo las ventas de la tienda Web y del volumen manejado.

Las compras Web en banda son realizadas por un tipo de APU basado en un query string llamado Digital Offer o DO. El nombre del dominio al que el DO apunta debe designar un

servidor Web operado por una entidad denominada servicio de transacción el cual ofrece una interface capaz de procesar la información de la transacción a realizarse. Esta información de la compra es pasada como parte del payload data del DO.

Para implantar DOs en las tiendas Web, los vendedores proveen los medios para que los visitantes de la tienda realicen compras sin recurrir a otro medio que no sea el Web. Mientras la visita a una tienda Web contenga Dos, un comprador puede seleccionar un DO (o más precisamente, un hiperenlace en el que el valor del URL es un DO), indicando así la intención de hacer una compra. Los diseñadores de las tiendas Web deben tener mucho cuidado en escoger que van a usar como contenido del indicador origen del hiperenlace, por ejemplo: la descripción del producto, o su precio, o la imagen del producto, o una frase tal como "Oprima aquí para comprar", o alguna combinación de éstas.

3.3.7.1 Servicios de Transacción

Un servicio de transacción es un sistema capaz de procesar transacciones comerciales basadas en Digital Offers, y emitir otro tipo de APU como respuesta, llamado Digital Receipt o DR. Un DR actúa como una prueba de compra. También sirve en el caso de los softgoods, como la manera para obtener fulfillment of the purchase de un fulfillment server, ya sea directa o indirectamente (en el caso de una suscripción). Para hardgoods, DRs proveen acceso a la información de cualquier producto que haya sido enviado, cancelado o esté pendiente.

No es común encontrar reclamaciones por software que soporte transacciones comerciales en el Web.

3.4 OM-Transact

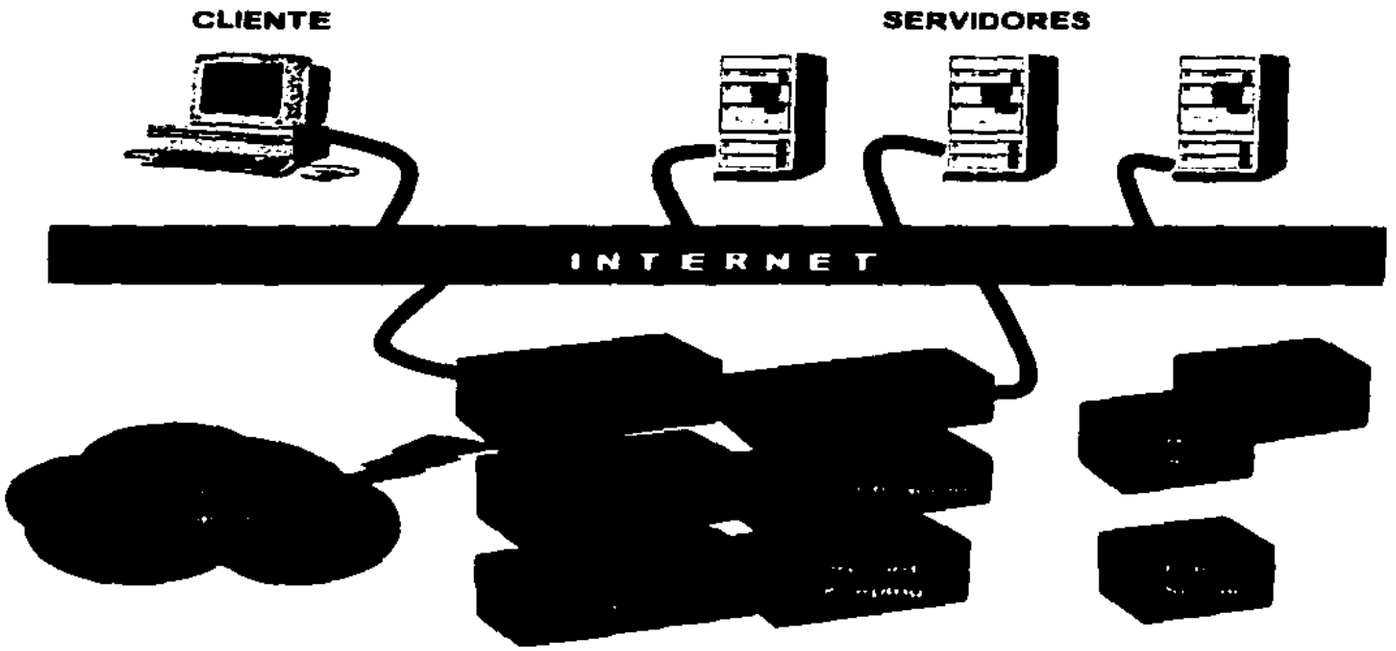
OM-Transact es un software desarrollado por Open Market, Inc., que proporciona una solución para aquellas compañías que desean cambiar su forma de realizar transacciones comerciales fijando su vista en el comercio por Internet. Utiliza la tradicional tecnología cliente/servidor y representa una aplicación de tercera capa que provee servicios con acciones obligatorias tales como: procesamiento de transacciones seguras y facilidades de servicio a los clientes tanto para los vendedores como para los compradores a través del World Wide Web.

OM-Transact está construido alrededor de una única arquitectura distribuida que separa las operaciones back-office de las actividades front-office con el fin de que los vendedores se centren en dar lo mejor de sí mismos para realizar sus negocios.

Con este diseño las empresas cuentan con una arquitectura flexible, extensible y escalable. Algunos de los servicios ofrecidos por OM-Transact están: protocolos de pago y el cálculo de impuestos internacionales, disponibles para todos los negocios y clientes consumidores a través del Web sin ningún costo adicional. También permite construir un ambiente de tiendas de autoservicio o centros comerciales para realizar compras desde la comodidad del hogar.

Otra característica de OM-Transact, es que está construido en un enfoque de sistemas abiertos; trabaja con todos los browsers populares (por ejemplo: Netscape, Mosaic, Microsoft),y con los métodos y protocolos de pago y seguridad tales como: CyberCash y SET. Así mismo, incorpora software para enlazar los actuales sistemas que se dedican al soporte de EDI.

La gran funcionalidad, personalización y extensibilidad a través de las APIs, proveen poderosas capacidades para el comercio negocio a negocio, el comercio negocio a consumidor, información publicitaria y proveedores de servicios comerciales (quienes brindan servicios comerciales a los vendedores).



OM-Transact es un software modular, que permite a las compañías extender sus sistemas funcionalmente y provee servicios únicos a sus negocios y a sus clientes. Los módulos plug-in que lo conforman son:

- *SalesTaxServer.*- Calcula impuestos estadounidenses y canadienses por concepto de ventas automáticamente, basados en la localización del comprador y del vendedor y de la categoría de los bienes en cuestión.
- *FaxServer.*- Aumenta el control de las ventas así como la administración de las mismas, faxeando reportes comprensivos para los vendedores.
- *EDI Server.*- Para los negocios que tienen un enlace EDI con una base de datos almacenada, OM-Transact puede fácilmente integrarse con ese sistema para brindar un messaging back-end electrónico con el fin de manipular ordenes de compra, suministrar un estatus de la mercancía e información completa.

Caracteristicas de OM-Transact

Seguridad

- Soporta los protocolos de seguridad estándares en Internet (ejemplo: S-HTTP y SSL) y los códigos de autentificación de mensajes codificados tales como: MACs codificados.

Autentificación

- Control de acceso sólo para los clientes registrados.
- Marcos de seguridad personalizables, con limites de crédito.

Bases de Datos de Clientes

- API para pre-cargar los registros de los clientes.
- Creación de cuentas en línea.
- Registro flexible de clientes
- Soporta compras de una sola vez o basadas en cuentas (con membresía).

Mercadeo uno a uno

- La API de configuración para el usuario soporta personalizar el contenido y el precio.

Record Keeping

- Reportes en línea de las transacciones en tiempo real para los vendedores.
- Reportes para auditar y seguir la actividad de las órdenes y transacciones.

Administración de Ordenes

- Aceptación segura de órdenes usando los protocolos Web estándar.
- Procesamiento de bienes físicos, bienes digitales y suscripciones.
- Shopping Carts para agregar productos a la compra.
- Cálculo automático de impuestos y cargos de embarque.
- Soporta los modelos de compra de una vez y en base a membresía.

Procesamiento de Pagos Seguros

- Acepta tarjetas de crédito, tarjetas de cargo, CyberCash y SET.
- Autorización en línea y por acuerdo.
- Acuerdos flexibles para la reconciliación de pagos en una tienda especifica.
- Soporta órdenes de compra para compras basadas en membresía.

- Suscripciones flexibles con pruebas, periodos de gracia, pey-per-view, créditos.
- Pagos múltiples.

Servicio al Cliente en línea.

- SmartStatements para el estatus de la orden en línea
- Facilidad para actualizar la información de los registros de los clientes.

Soporte de Operaciones OM-Transact

Los operadores pueden ejecutar las siguientes operaciones:

- Activar y desactivas compradores y tiendas.
- Promover un comprador al estatus de vendedor u operador.
- Visualizar una lista de tiendas.
- Visualizar las pre-autorizaciones pendientes.
- Emitir crédito totales o parciales.
- Visualizar todos los aspectos de la principal base de datos.
- Visualizar un catálogo de imágenes que puede ser utilizado para personalizar la interface del usuario presentada a los compradores y vendedores.

Integración de Sistemas Back-Office

- Integraciones con EDI, procesamiento de ordenes y sistemas ERP.

Soporte Internacional

- Cualquier lenguaje con alfabeto latino.
- Todos los estándares ISO.
- UK VAT
- Formatos de direcciones internacionales.

Arquitectura

OM-Transact está diseñado para soportar altos volúmenes de servicios de transacciones. Así mismo está construido para escalar de altos volúmenes a muy altos volúmenes de carga de trabajo. Operar un solo sistema de servicio OM-Transact requiere un mínimo de 2 hosts, con el fin de que uno de los hosts pueda estar mayormente protegido de accesos externos

fraudulentos como suele ocurrir a través de Internet y por lo tanto resguardar el host donde se encuentran los datos más sensibles, así como los procesos que forman parte de OM-Transact. Un gran servicio de transacciones puede requerir muchos (posiblemente docenas) de hosts a través de los cuales OM-Transact puede ser distribuido, para manejar el volumen de tráfico eficientemente.

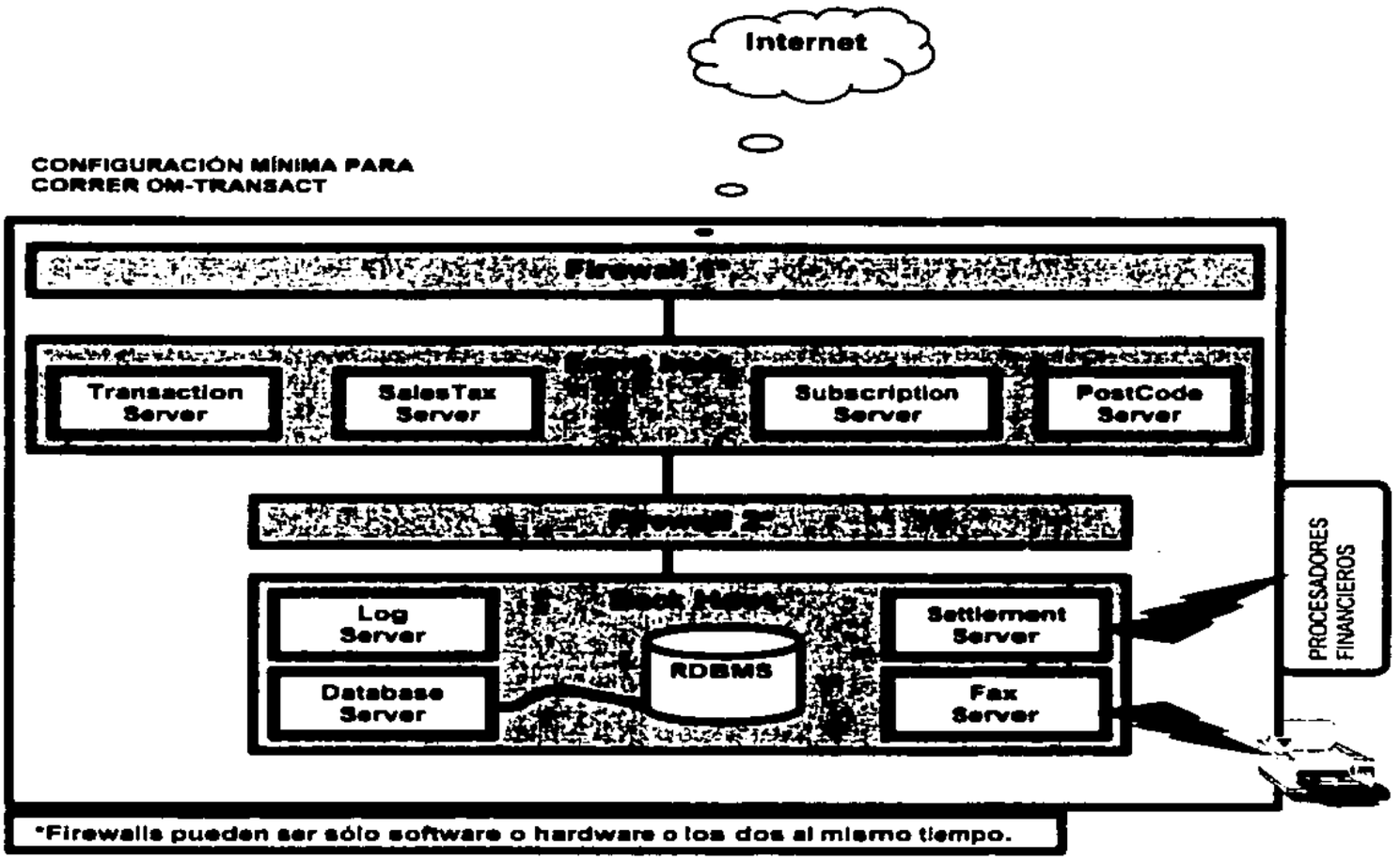
Para permitir este grado de distribución a través de muchos hosts, OM-Transact ha sido construido en un modo altamente modular, que consiste de una colección de servidores de componentes (component servers), cada uno de los cuales, es un conjunto de programas que juntos implementan un aspecto de la funcionalidad del sistema. Cada uno de estos component servers puede correr en un hosts separado, para distribuir la carga de acuerdo a las necesidades del alto volumen de procesamiento de transacciones. Muchos de los component servers pueden ser reduplicados.

OM-Transact corre en plataformas UNIX, incluyendo aquellas de Sun, SGI, Stratus y en HP-UX.

La comunicación entre los component servers se desarrolla vía HTTP sobre canales encriptados SSL, la mayor parte, con la excepción de que algunas comunicaciones de acceso a bases de datos que utilizan métodos optimizados por los vendedores de bases de datos para su particular RDBMS (OpenClient, de SYBASE es un claro ejemplo de esta situación).

OM-Transact incluye los siguientes servidores: TransactionServer, SubscriptionServer, SettlementServer, DatabaseServer, SalesTaxServer, PostCodeServer, LogServer y FaxServer. Algunos de estos component Servers son adicionales por lo que no es necesario que se compren con el producto central.

A continuación se muestra la configuración elemental del hardware de un OM-Transact:



El servidor Web base usado por OM-Transact es un Servidor Web de Seguridad de Open Market (Secure WebServer), un servidor multiprocesos que soporta al mismo tiempo S-HTTP y SSL y prove una gran flexibilidad para el control de acceso programable, el cual trabaja bajo altas cargas de trabajo lo cual ningún otro servidor Web en el mercado puede realizar.

Modelo de Datos (Data Model)

OM-Transact, ofrece un repertorio de servicios valiosos, todos basados alrededor de su modelo de datos, en otras palabras, su representación de entidades pasivas y activas y una variedad de posibles eventos a los cuales, diferentes respuestas son requeridas. El modelo del mundo de OM-Transact envuelve cuatro diferentes tipos de entidades activas (active entities):

- *Vendedores (Merchants)*.- Personas que desean vender productos a través de tiendas Web.
- *Compradores (Buyers)*.- Personas que desean comprar productos en el Web
- Procesos Financieros (Financial Processors).- Organizaciones con las cuales OM-Transact puede comunicarse en línea para originar la actual transacción de pago de tarjeta (ej. Envoy, Litle, Toronto Dominion).
- Operadores (Operators).- Personas que operan y controlan un servicio de OM-Transact (probablemente menos de una docena).

Las principales entidades pasivas que existen en el modelo del mundo de OM-Transact son:

- Tiendas
- Billeteras
- Instrumentos de pago
- Shopping carts

Los principales eventos que ocurren en el modelo del mundo de OM-Transact son:

- Entidades activas vienen en existencia para ser registradas (operadores, procesos financieros, vendedores).
- Los vendedores crean tiendas y las configuran.
- Los compradores crean billeteras, agregan instrumentos de pago a ellas, modifican varios aspectos de sus beneficios.

- Las transacciones de compra en el Web ocurren (generalmente referenciadas como transacciones): Un comprador compra algo de la tienda utilizando algún instrumento de pago.
- Las compras libres ocurren cuando los compradores hacen compras simplemente proveyendo un instrumento de pago sin ningún tipo de registro.
- Las transacciones de pago de tarjeta ocurren como pre y post autorizaciones, invalidas, créditos, etc.
- Las suscripciones son creadas.
- Los significados de la autorización son otorgados por material de suscripción.

Validación de APUs a través de Interfaces

Toda la comunicación de transacciones entre los vendedores y el servicio del OM-Transact con el cual ellos tienen registrado toma lugar por medio de los APUs. OM-Transact presenta un rango de interfaces a las cuales estos APUs pueden apuntar.

Todos los APUs que apuntan a las interfaces de OM-Transact contienen en su payload data (seguido del MAC) los siguientes campos:

- *Un único número de identificación de la tienda de donde se origina el APU.* Este número es utilizado por OM-Transact para buscar información de la tienda en su base de datos, incluyendo texto e imágenes utilizados para personalizar las páginas que se le presentan a los compradores en el contexto de una compra de una tienda dada, obtener información acerca de las reglas de la tienda para calcular el flete, los números de identificación de la tienda con uno o más procesos financieros, el número de servicio al cliente de la tienda, etc.
- *Un único número identificador de la llave secreta utilizada para crear el MAC (algunas llaves pueden estar en uso por una tienda en cualquier tiempo).* OM-Transact utiliza este número para buscar la llave secreta adecuada en su base de datos, con el fin de que pueda calcular el MAC, y compare sus resultados con el MAC recibido en APU, para determinar si el APU ha sido modificado accidentalmente o intencionalmente entre el tiempo de su creación y el tiempo en que OM-Transact lo recibió.
- *Identificador del esquema de seguridad.* Este identifica el algoritmo utilizado para calcular el MAC en el APU, para que OM-Transact pueda aplicar el algoritmo correcto cuando calcule el MAC para la comparación.
- La porción restante del payload data del APU, depende de la interface a la cual la ruta del APU apunte, así como también de la aplicación en particular por la cual la interface es invocada.
- *La validación es el primer paso realizado por OM-Transact para cualquier APU.*

Las interfaces que OM-Transact maneja para su funcionamiento son:

- Interface de Servicios para Vendedores
- Interfaces de pago por Digital Offer (DO)
- Interfaces de los Shopping Cart
- Interfaces para re-expedición de la firma digital
- Interface de Validación fallida

CASOS

DE

ESTUDIO

Como se mencionó en la introducción, el presente capítulo muestra tres de los más importantes casos en donde han sido aplicadas cada una de las tendencias para la realización del intercambio electrónico a través de Internet tema de este trabajo. Primeramente se presenta el caso de Chase Manhattan Bank, la cual desarrolla sus transacciones comerciales por medio del encriptamiento. A continuación, se muestra el caso de Canadian Tire, empresa que lleva a cabo sus transacciones comerciales a través del uso de las formas electrónicas; y por último, se ejemplificará la aplicación de las páginas Web para la realización del intercambio electrónico de datos, por medio de la compañía Disney.

ENCRIPTAMIENTO

Chase Manhattan Bank

Chase es el primer centro bancario de dinero en estructurar un programa de EDI financiero a través de Internet para incorporar un rango importante de productos que servirán a muchos clientes. La aplicación inicial piloto estuvo enfocada al pago ACH de dólares en EUA.. El primer socio comercial de Chase en participar en este programa piloto fue Diamond Shamrock, empresa líder en el mercadeo del petróleo en los EUA.

Chase, como empresa bancaria que realiza un sin fin de transacciones financieras con la mayoría de sus clientes, tenía el problema de que por este hecho, debía contar con muchas conexiones a las redes de valor agregado y esto le causaba grandes gastos de mantenimiento, renta, y todos aquellos gastos que se derivan del uso de estas redes. Viendo esta problemática y tomando en cuenta las características de la red de redes como medio de transmisión de información los directivos de Chase decidieron buscar una alternativa para derogar todos los gastos provenientes del uso de una VAN; fue entonces, cuando optaron por la utilización de Internet como medio para transmitir su información obteniendo las siguientes ventajas:

- La conexión a Internet ofrece un bajo costo y una red abierta para el amplio mundo de las comunicaciones.
- Darles la posibilidad de utilizar el comercio electrónico a un gran número de socios comerciales.

- El costo de Internet es más bajo que el de una VAN; La renta por el uso de Internet es muy baja.
- Realización un comercio electrónico basado en estándares.
- Tomar ventaja en la tecnología existente

Pero a pesar de estas grandes ventajas ofrecidas por Internet, había una desventaja mucho mayor que dejaba a un lado a estas y era: la "seguridad" de los datos. Por este motivo determinaron utilizar el encriptamiento de datos para un intercambio de transacciones seguro y a bajo costos a través de Internet. Con esta nueva opción ellos veían logrados los siguientes objetivos:

- Mantener la confidencialidad de los datos.
- Hacer posible la verificación de la identidad del emisor de los datos.
- Verificar la integridad de los datos
- Autentificar los datos para asegurarse que un archivo es recibido sin alteraciones en su contenido.
- Códigos de encriptación confiables con el fin de que la información no pueda leerse.
- Soportar el estándar de ecriptación de datos ASC X12.

Tomando en cuenta las ventajas que les trajo el uso de esta tecnología y la naturaleza de sus operaciones, los directivos de Chase Manhattan Bank, han pensado extender este programa piloto a pagos internacionales, a avisos de remesa, y a letras de crédito de cobro inmediato.

Como resultado de los grandes beneficios que trajo para Chase Manhattan Bank la utilización del encriptamiento para realizar transacciones comerciales, Diamond Shamrock optó por también utilizar esta tendencia para intercambiar información comercial con sus proveedores y clientes, lo cual le redituó en el incremento del número de relaciones comerciales con sus clientes y con sus proveedores de servicios. Con esta decisión, Los directivos de Diamond Shamrock esperan que en muy poco tiempo todos sus proveedores y clientes estén incorporados a la transferencia electrónica de ordenes de compra, facturas e instrucciones de pago usando EDI por Internet.

Acerca de Chase Manhattan Bank

Con 322 billones de dólares en bienes, el banco Chase Manhattan Corporation es la compañía bancaria más grande en los EUA. Tiene más relaciones primarias con otras empresas estadounidenses que otro competidor, haciéndolo el banco líder en la América corporativa.

La división de pagos globales y servicios interbancarios es un líder internacional en la administración de efectivo y valores, tratados financieros y pagos servicios de inversión a corporaciones, instituciones financieras, corredores de bolsa, y al amplio sector público. Chase es altamente reconocido por su habilidad para mover el dinero alrededor del mundo con seguridad y eficiencia. Es el proveedor número uno en servicios ACH en los Estados Unidos de Norteamérica, posición ganada desde 1974, y es el banco conciliador internacional líder del mundo.

Acerca de Diamond Shamrock

Diamond Shamrock, Inc., matriz en San Antonio, Texas, es un líder en el refinamiento y mercadeo de productos de petróleo en el Suroeste de los EUA con un crecimiento mixto de negocios relacionados a esta actividad. Diamond Shamrock, con ventas anuales de aproximadamente 4 billones de dólares, tiene dos refinerías en Texas con una capacidad de arriba de 225,000 barriles por día y vende gasolina aproximadamente a través de 2,700 establecimientos.

Algunas otras empresas que utilizan el encriptamiento para el intercambio de transacciones comerciales son:

- 3M
- Bank Of Boston
- Bank of New York
- The Gillette Company
- Hewlett Packard Company
- Lotus Development
- Mitsubishi Electric Corp.
- Coca-Cola Bottling Co.
- Dayton-Hudson Corpotration
- Nabisco
- Office Depot
- Pepsi Cola General Bottlers Inc.
- Silicon Graphics
- Sun Microelectronics
- Texas Instruments
- United States Postal Services, entre otros.

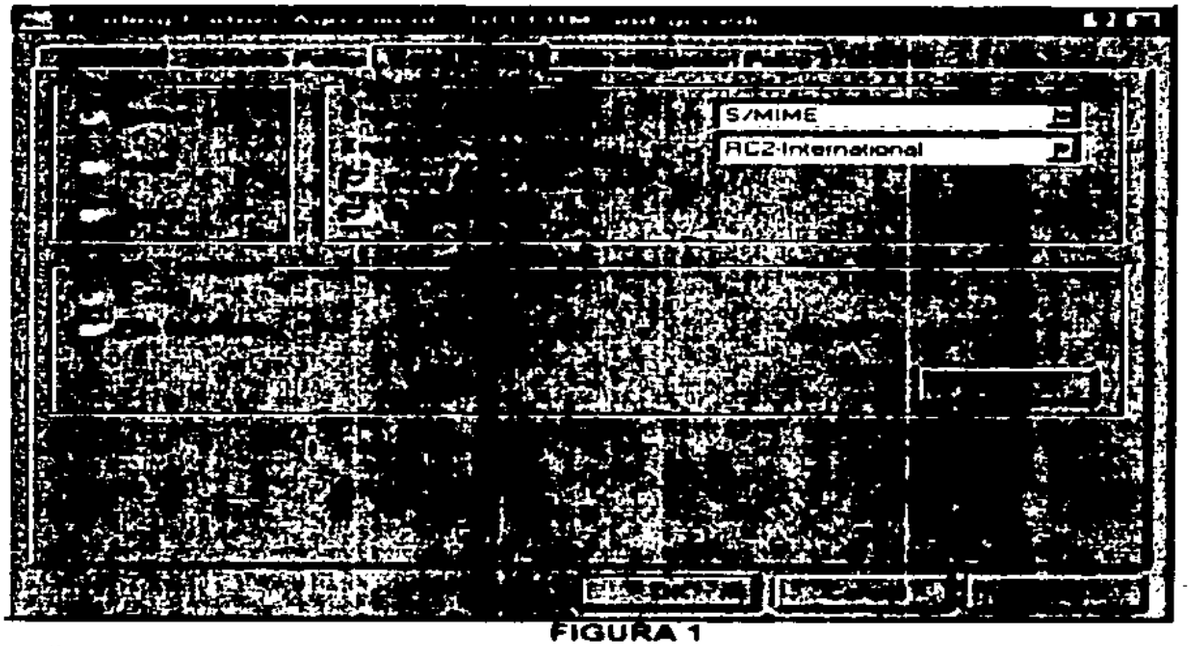


FIGURA 1

Esta pantalla muestra como se seleccionan los algoritmos de encriptamiento que se utilizarán en una transacción comercial.

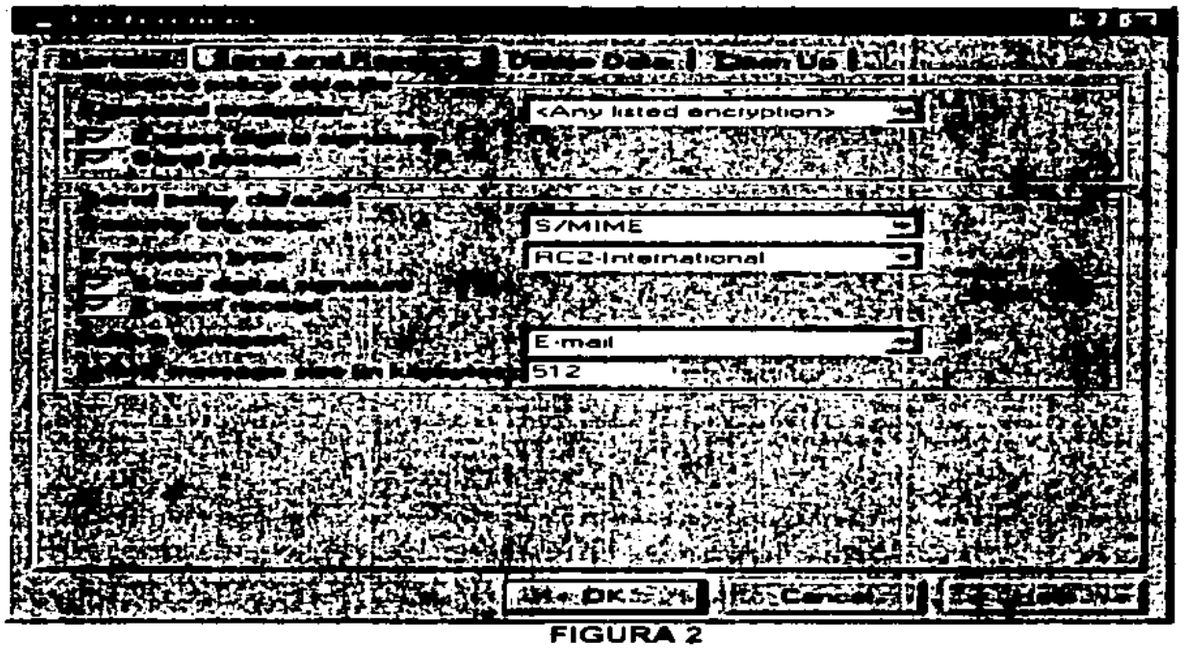


FIGURA 2

Configuración de las políticas de seguridad

FORMAS ELECTRONICAS

Canadian Tire Corporation, LTD.

Canadian Tire es una empresa especialista en la venta de herramientas que cuenta con la siguiente infraestructura tanto humana como material:

- 34,000 empleados
- 428 tiendas asociadas
- Alta expansión de tiendas
- 197 estaciones de gas
- 2 centros de distribución
- 20 almacenes
- 68,000 productos
- 490 millones de unidades
- 54,000 embarques
- 2,000 proveedores

Esta empresa tenía como meta que en 1998 debería ser una de las 10 primeras distribuidoras al menudeo en Norteamérica, con respecto al desarrollo efectivo de las técnicas de comercio electrónico y de las transacciones empleadas en é; para ello debería lograr vencer el siguiente reto:

"Implementar transacciones y medios de transmisión electrónicos con todos los socios comerciales incrementando la compra del producto, su movimiento y los procesos de pago.

Con el fin de lograr este objetivo, Canadian Tire evaluó diferentes formas para lograr el intercambio electrónico con sus diferentes proveedores, con el fin de encontrar una, la cual pudiera ser adoptada por todos, desde pequeñas empresas hasta grandes corporaciones. Fue entonces, cuando después de largos y arduos análisis, los encargados de dar solución a este problema llegaron a la conclusión de que la mejor opción para cumplir este cometido era la utilización de las formas electrónicas; por lo que trazaron un programa en donde primeramente se planteaba el problema que Canadian Tire tenía, el reto a vencer con este proyecto y la solución ante este problema, los cuales se describen a continuación;

Problema: El deseo de Canadian Tire de tener a todos sus proveedores comunicados electrónicamente no podía ser realizado a través del sólo uso del EDI.

Reto: ¿Cómo brindar las suficientes opciones para que los proveedores pudieran realizar negocios electrónicamente con un mínimo costo, esfuerzo y tiempo.?

Resultado: Las Formas electrónicas proveen más de una manera efectiva para comunicarse.

Después presentaba las implementaciones de los recursos necesarios para realizar la comunicación entre Canadian Tire y todos sus socios comerciales. Estas implementaciones fueron:

- Implementación del software a utilizar.
  - ✓ Instalación y configuración
- Implementación de las formas de las transacciones que se deseaban intercambiar:
  - ✓ Ordenes de compra
  - ✓ Cambio de la orden de compra
  - ✓ Avisos de embarque
  - ✓ Planeación de la orden
- Implementación del medio de transmisión para las transacciones.
  - ✓ Internet

Y por último se exponía los beneficios que Canadian Tire y sus proveedores obtendrían al desarrollar este proyecto.

Beneficios para Canadian tire:

- Transacciones y aplicaciones controladas
- Posibilidad de realizar grandes implementaciones en un corto período de tiempo.
- No se requiere realizar pruebas con los proveedores
- Un vehículo de comunicaciones completamente electrónicas.

Beneficios para los proveedores:

- Una alternativa de bajo costo para la realización del EDI.
- Fácil de usar
- Un vehículo de comunicaciones completamente electrónicas.
- Estar provistos con aplicaciones pre-construidas

Una vez presentado este proyecto y viendo los beneficios que trairían para la organización, los directivos de Canadian Tire lo aceptaron. Y ahora tras la completa implementación de esta técnica para realizar intercambio de transacciones comerciales Canadian Tire ha aumentado su productividad y está logrando el principal objetivo por el que se adoptó la utilización de las formas electrónicas.

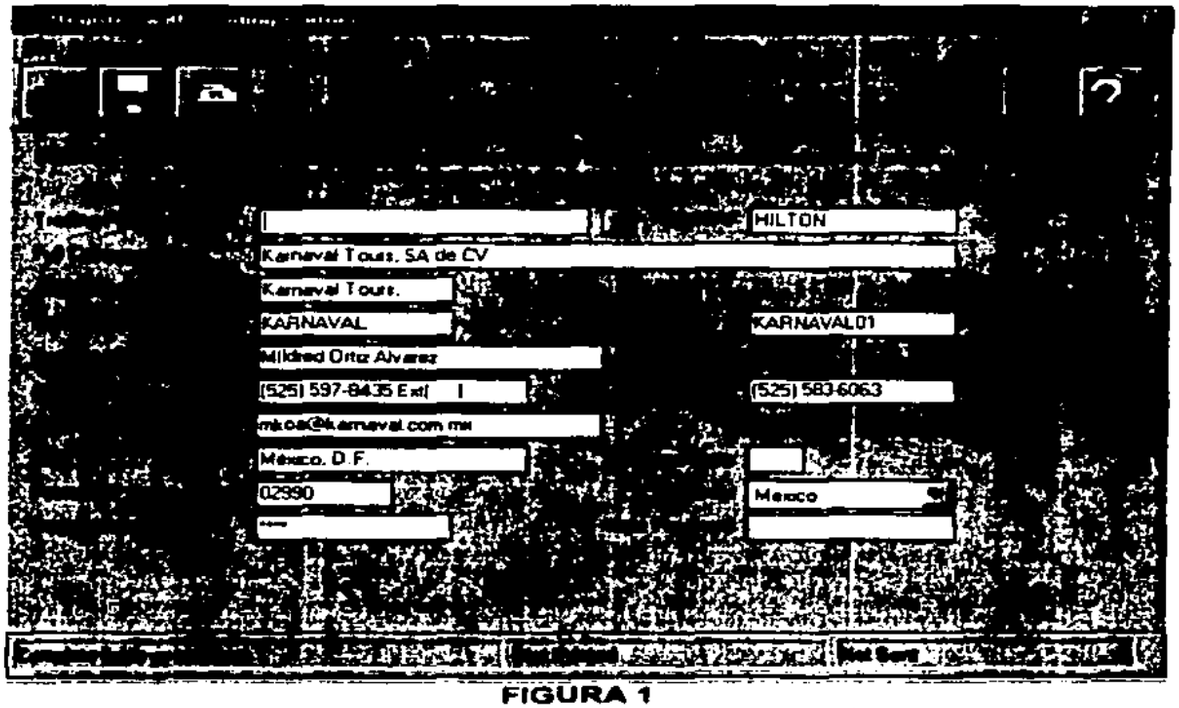


FIGURA 1
Ejemplo de una forma electrónica para el registro con el socio comercial

PAGINAS WEB

Disney On Line

La compañía Walt Disney es un claro ejemplo de la aplicación de las páginas Web en la realización del intercambio de transacciones comerciales. WaltDisney Company a través de su división Disney Online implementó una tienda virtual que es llamada Disney Store Online, a principios de 1997.,Esta implementación se desarrolló con el fin de que las personas puedan adquirir los productos Disney sin tener que desplazarse a Dineylandia, o algún lugar donde puedan ser adquiridos. Este proyecto en práctica con la adquisición de un software para realizar comercio electrónico a través de Internet, el cual, brinda todas las facilidades para crear bases de datos los productos, desarrollar las páginas Web que servirán como acceso a la tienda y a todas aquellas transacciones comerciales que se ven involucradas en la venta de los productos y sobre todo, mantiene segura la información que se maneja en cada transacción comercial.

Otra razón que tuvo la compañía Disney para llevar a cabo este proyecto fue el darse cuenta que la tecnología va cambiando día con día y por lo tanto la manera de realizar las actividades cotidianas tanto en el trabajo como el hogar también sufrían esta misma transformación. Tomando en cuenta esta situación y que Disney se caracteriza en utilizar tecnología de punta en todas sus áreas, pensó que era hora de adoptar una nueva forma para realizar sus ventas y qué mejor opción tenía sino el utilizar la supercarreta de la información como es llamada Internet, la cual actualmente, es uno de los medios de información que tiene mayor demanda, para efectuar este cambio.

A partir de la implantación de esta tienda virtual en las páginas Web, Disney vio realizadas todas las expectativas que se habían contemplado. Estas expectativas fueron:

- Facilidad de uso para los clientes
- Medidas de seguridad y anti-fraudes en el manejo de las transacciones comerciales, ejemplo: ordenes de compra, pagos por medio de las tarjetas de crédito, etc.
- Protección en los bienes de los negocios.
- Bajos riesgos financieros, al tener cuidado con los procesos de transacciones con tarjetas de crédito.

Y que mejor forma de visualizar esta implementación realizada por Disney Online, que mostrar algunas imágenes de esta nueva forma de realizar transacciones comerciales por medio de Páginas Web.

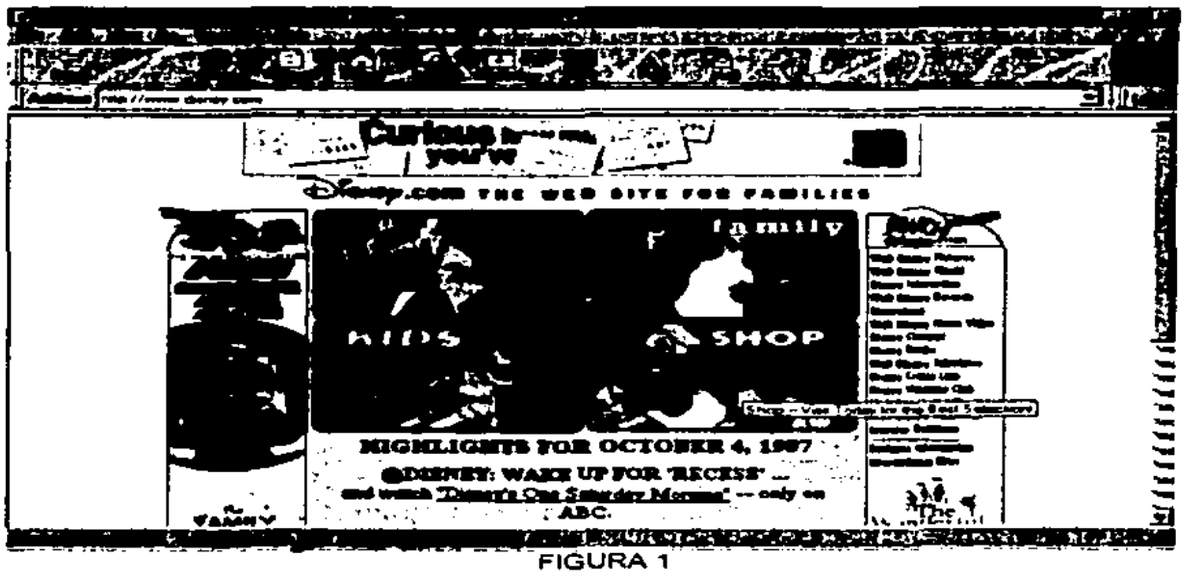


FIGURA 1
Página Web de Walt Disney Company. La selección a la Shop Online es muy sencilla, sólo se da un click en el dibujo del Shop.

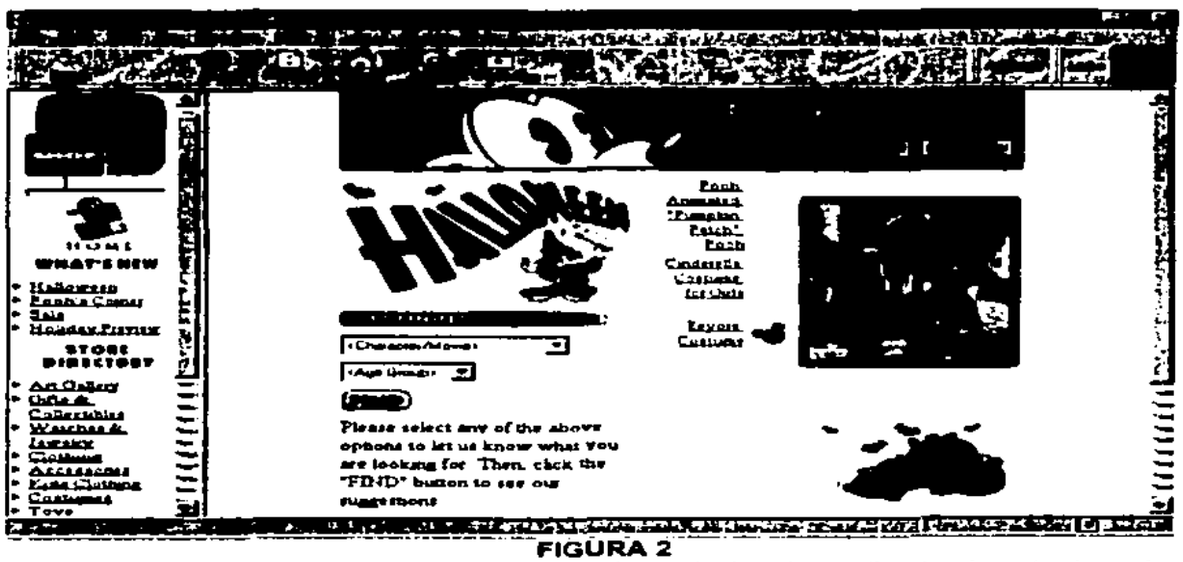


FIGURA 2
Dentro de la tienda se pueden seleccionar o buscar los artículos dependiendo al gusto de cada cliente.

FIGURA 3

Una vez seleccionado el artículo deseado, se escogen las características de este, como color, talla, cantidad, etc.

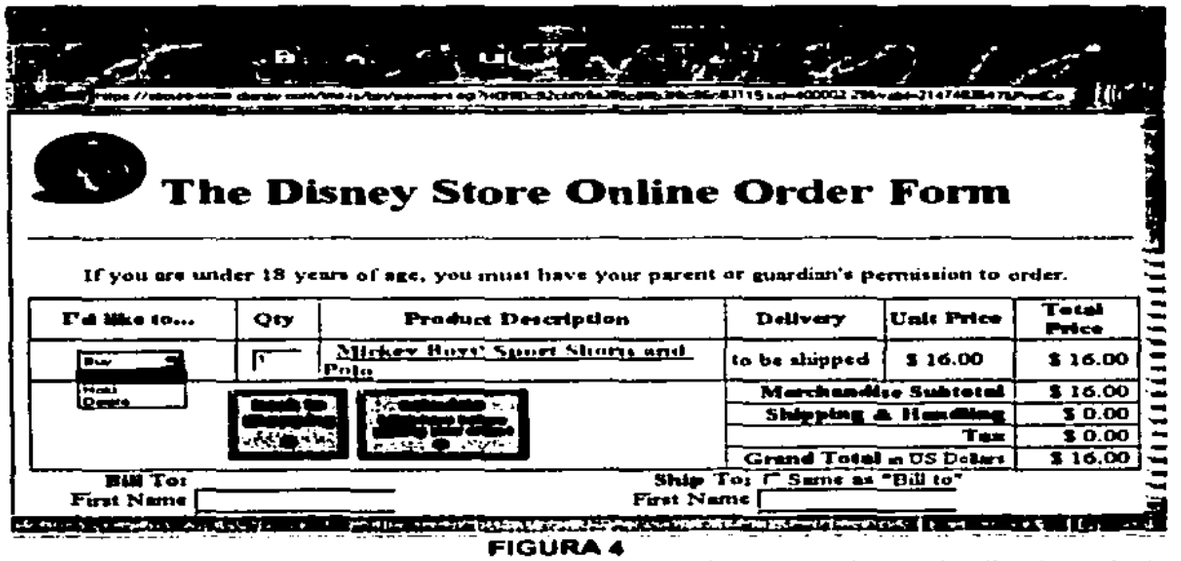


FIGURA 4

Si el cliente decidió comprar el artículo, entonces aparece la orden de compra donde detalla el precio, los cargos por envío, la descripción del producto, lugar de entrega, a nombre de quien se hará el cargo de la compra, etc.

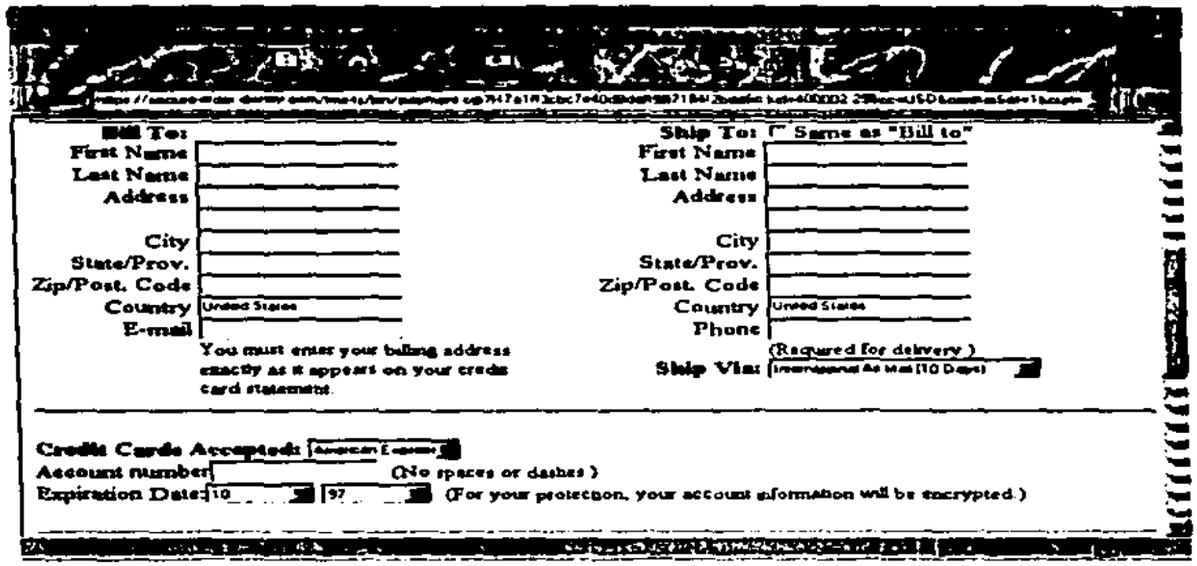


FIGURA 5
En la orden de compra también se introducen los datos concernientes a la tarjeta de crédito como: No. de cuenta, tipo de tarjeta, fecha de expiración, etc.

A cerca de Disney Online.

Disney Online es una parte de la Compañía Walt Disney, su casa matriz está en North Hollywood, California, cuenta con una sucursal en New York, NY. Fue fundada en 1995 para desarrollar la presencia de la compañía en el mundo online. En el estudio Inernet de Disney Online se han creado y producido páginas que han sido galardonados en el Web.

El primer sitio Web creado por Disney Online, Disney.com, fue lanzado en Febrero de 1996 y rápidamente se volvió uno de los más populares y altamente visitados sitios en el World Wide Web. Ubicado en el sitio www.disney.com, el sitio muestra los servicios y productos de la Compañía Walt Disney, con información innovadora y atractiva de una variedad de divisiones Disney incluyendo el Disney Channel, Walt Disney Pictures, Walt Disney Television, Disneyland, Walt Disney World, y la Disney Store Online .

CONCLUSIONES

A lo largo del presente trabajo, se cubrieron los objetivos marcados al inicio de éste:

1. Proponer las posibles áreas de aplicación de cada opción con base a sus características.

2. Precisar las ventajas y desventajas de cada una de las opciones para la ejecución del Intercambio Electrónico de Datos a través de Internet.

3. Dar una perspectiva de qué tendencia va en incremento y cual no.

La utilización del Intercambio Electrónico de Datos (EDI) por Internet en alguna de sus modalidades, resultará beneficiosa para las organizaciones en diversos aspectos tales como: costos, operabilidad, utilización de estándares y tecnología de punta, entre otros, ya que de acuerdo a los casos prácticos que se expusieron, las empresas que han adoptado alguna opción para realizar el intercambio electrónico de datos por Internet registraron beneficios sustanciales para su organización, y con base en la experiencia de éstas, otras compañías decidieron unirse al comercio electrónico por Internet.

De acuerdo a lo presentado en este trabajo, se obtuvieron las siguientes conclusiones::

- Las organizaciones están tendiendo al uso de Internet para el comercio principalmente por su, bajo costo, además de otras ventajas como: facilidad en su uso, , etc.

- Internet por si sola como red, no ofrece la seguridad para poder manejar o simplemente transportar información sensible y delicada y que por ende necesita un alto grado de seguridad en su trato.

- La concepción de lo que es EDI ha ido cambiando con el tiempo, ya que de ser un simple, llano y rígido intercambio de transacciones comerciales punto a punto basado en formatos estándares a veces difíciles de entender, se ha transformado primeramente en Softwares traductores sencillos en su manejo, desarrollados bajo un ambiente gráfico y amigable como lo es Windows, los cuales hacen uso de las redes VAN que emplean la

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

tecnología multipuntos. Ahora con la aparición de Internet y después con el desarrollo del World Wide Web el intercambio electrónico de datos empieza a adquirir otra conceptualización ya no tanto en el aspecto de emplear los estándares ANSI X12 y EDIFACT, además de las redes VAN, sino que, en estos tiempos EDI también es el intercambio electrónico de datos por medio de redes públicas, bajo los estándares apropiados para éstas y sin un software traductor.

- La opción para hacer EDI por Internet que tiene más futuro es el World Wide Web, ya que en esta tendencia se reúnen las otras dos: el encriptamiento y las formas electrónicas además de poder realizar el EDI en su forma tradicional. En cuanto al encriptamiento, éste, continuará en vigencia ya sea como encriptamiento en sí o como complemento de alguna aplicación, mientras no se encuentre otra forma de brindar seguridad a través de Internet. Por los que a las formas electrónicas se refiere, el uso de éstas irá menguando ya que de utilizar una simple hoja electrónica a usar una página Web es preferible optar por la segunda debido a que ofrece mayores ventajas que las primeras.

- Las tres tendencias pueden ser utilizadas en cualquier giro empresarial.

11. KARANJIT, Siyan & Chris Hare, *Internet y Seguridad en Redes*, México, Ed. PHH, 1995, 250 p.

12. KEHOE, Brendan P., El Arte de Internet, México, Ed. PHH, 1997,255p.

13. www.commercc.net

14. www.premenos.com

15. www.e-com.com

16. www.ecomworld.com

17. www.PCweek.com

18. www.openmarket.com

19. www.rsa.com

20. www.disney.com

21. www.pathfinder.com

22. www.ibm.com/NetworkComputing/es/index.html