

UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE CONTADURIA PUBLICA Y ADMINISTRACION
DIVISION DE ESTUDIOS DE POSTGRADO



ANALISIS Y EVALUACION DE SISTEMAS DE
SEGURIDAD PARA EL COMERCIO ELECTRONICO

POR

MA. MAGDALENA GARZA SANCHEZ

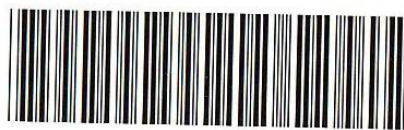
EN OPCION AL GRADO DE MAESTRO EN
INFORMATICA ADMINISTRATIVA

NOVIEMBRE 2001

W.M.G.S. ANALISIS Y EVALUACION DE SISTEMAS DE SEGURIDAD PARA EL COMERCIO ELECTRONICO

TM
Z7164
.C8
FCPYA
2001
.G377

01



1020146303

~~5~~

UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE CONTADURIA PUBLICA Y ADMINISTRACION
DIVISION DE ESTUDIOS DE POSTGRADO



ANALISIS Y EVALUACION DE SISTEMAS DE
SEGURIDAD PARA EL COMERCIO ELECTRONICO

POR

MA. MAGDALENA GARZA SANCHEZ

EN OPCION AL GRADO DE MAESTRO EN
INFORMATICA ADMINISTRATIVA

NOVIEMBRE 2001

970 866

TM

Z 7164

.C8

F074A

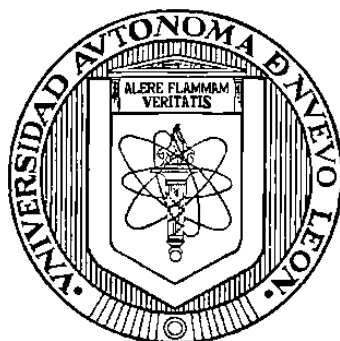
2001

.E377



FONDO
TESIS

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE CONTADURÍA PÚBLICA Y ADMINISTRACIÓN
DIVISIÓN DE ESTUDIOS DE POSTGRADO



**ANÁLISIS Y EVALUACIÓN DE SISTEMAS DE
SEGURIDAD PARA EL COMERCIO ELECTRÓNICO**

POR

MA. MAGDALENA GARZA SÁNCHEZ

EN OPCIÓN AL GRADO DE MAESTRO EN
INFORMÁTICA ADMINISTRATIVA

NOVIEMBRE 2001



FONDO
TESIS

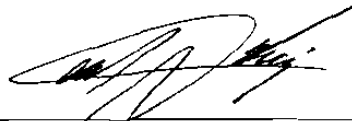
ANÁLISIS Y EVALUACIÓN DE SISTEMAS DE SEGURIDAD
PARA EL COMERCIO ELECTRÓNICO

Aprobación de la Tesis:



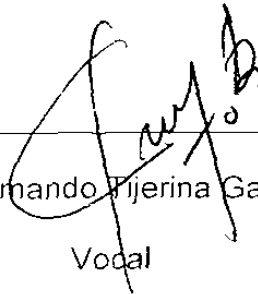
M.S. Juvencio Jaramillo Garza

Presidente y Asesor de Tesis



Lic. Francisco Cortés Cerda

Secretario



Lic. Armando Tijerina García

Vocal

M.A.P. Francisco Javier Jardines Garza

Subdirector de Postgrado

DEDICATORIA

A Dios...

Gracias por estar conmigo.

A mis Padres...

Eric Garza Garza (†) y Hortencia Sánchez Guajardo por haberme dado la vida, su amor y todo el apoyo en mis decisiones; por enseñarme que la vida es una serie de experiencias y retos con los cuales se forma el carácter de una persona.

A mi Esposo...

Quien fue mi guía y apoyo, por darme la seguridad, el amor y la comprensión que en muchos momentos necesité, por enseñarme que cuando uno siente que ya no se puede, siempre existe una luz a la cual seguir y lograr así nuestras metas.

A mi hijo...

El cual estuvo siempre conmigo, ya que durante su gestación vivió conmigo las desveladas y desesperaciones, así como los logros y alegrías.

AGRADECIMIENTOS

Quiero expresar mi agradecimiento al M.S. Juvencio Jaramillo Garza asesor de esta tesis, y a los coasesores, M.C. Armando Tijerina García, y M.C. Francisco Antonio Cortés Cerda por su valiosa ayuda, recomendaciones y sus acertadas guías para el desarrollo y conclusión del presente trabajo.

Así mismo, agradezco a la Facultad de Contaduría Pública y Administración de la Universidad Autónoma de Nuevo León por el apoyo que recibí durante mis estudios.

A la Universidad del Norte, quiero agradecerle la confianza que tuvieron en mí, el apoyo económico que me brindó, así como la oportunidad de mejorar mi formación académica.

Agradezco también a todos mis maestros que compartieron sus conocimientos y experiencias profesionales, además de su amistad y consejos brindados durante todos estos años.

TABLA DE CONTENIDO

Lista de figuras.....	ix
Lista de tablas.....	xi
Glosario.....	xii
Abreviaciones.....	xviii
Resumen.....	xx
Capítulo 1 Introducción	
1.1 Motivación.....	1
1.2 Antecedentes.....	5
1.3 Objetivos de la tesis.....	12
1.4 Limitaciones de la investigación.....	13
1.5 Estructura de la tesis.....	13
Capítulo 2 Características del comercio electrónico	
2.1 Aspectos generales.....	15
2.2 Redes de comunicación.....	17
2.3 Procesamiento de cómputo distribuido.....	18
2.4 Redes abiertas.....	20
2.5 Definición.....	25
2.6 Comercio electrónico como una red de comunicaciones.....	26
2.6.1 Comercio electrónico de productos digitales.....	28

2.6.2 Seguridad y privacidad en transacciones por Internet	31
2.7 Conclusiones del capítulo	32

Capítulo 3 Seguridad en redes de comunicación

3.1 Introducción.....	33
3.2 Importancia de la seguridad	34
3.3 Criptografía	38
3.3.1 Sistemas simétricos	39
3.3.2 Sistemas asimétricos	41
3.4 Autoridades de certificación	44
3.5 Integridad de los datos: Funciones Hash.....	46
3.6 Firmas digitales	51
3.7 Proceso de transmisión de un mensaje en forma segura	53
3.8 Firewall.....	55
3.8.1 Beneficios de un firewall	57
3.8.2 Limitaciones de un firewall	58
3.8.3 Decisiones de diseño básicas de un firewall.....	59
3.9 Estrategias de seguridad.....	61
3.9.1 Análisis de riesgos	62
3.9.2 Aspectos de la implementación de una política de seguridad	64
3.10 Conclusiones del capítulo	69

Capítulo 4 Sistemas de pago seguro

4.1 Características	70
4.2 Descripción general de un sistema de pago seguro	74
4.3 Proceso de pago y compra	75
4.4 Protocolos de transporte seguro	81
4.4.1 MIME (Multipurpose Mail Enhancements)	81
4.4.2 PEM - MOSS (Privacy Enhanced Mail y MIME Object Security Objects)	82
4.4.3 SSL (Secure Sockets Layer)	82
4.4.4 S-HTTP (Secure HTTP)	84
4.4.5 iKP (Internet Keyed Payment Protocols)	85
4.5 Esquemas de pago electrónico	86
4.5.1 Netscape	86
4.5.2 Microsoft	86
4.5.3 Checkfree	87
4.5.4 CyberCash	87
4.5.5 VeriSign	88
4.5.6 DigiCash	88
4.5.7 First Virtual	90
4.5.8 NetCash	91
4.5.9 CommerceNet	91
4.5.10 JEPI	92
4.5.11 Otros	93
4.6 Estándar SET	94

4.7 Conclusiones del capítulo	98
-------------------------------------	----

Capítulo 5 Comparación de sistemas de seguridad para el comercio electrónico

5.1 Introducción.....	99
5.2 Criterios de comparación	100
5.3 Resultados	101
5.4 Observaciones de la situación del comercio electrónico en México	106
5.5 Tendencias.....	108
5.6 Conclusiones del capítulo	108

Capítulo 6 Conclusiones

6.1 Conclusiones.....	110
6.2 Aportaciones	115
6.3 Recomendaciones para trabajos futuros	116
Bibliografía	117
Resumen autobiográfico	121

LISTA DE FIGURAS

Figura	Página
2.1 Áreas del comercio electrónico	30
3.1 Accesos no autorizados a una red, (a) pasivos, (b) activos	38
3.2 Sistema de criptografía simétrico	39
3.3 Algoritmo DES.....	40
3.4 Sistema de criptografía asimétrico	41
3.5 Usurpación de personalidad	46
3.6 Función Hash	46
3.7 Proceso de firma digital.....	52
3.8 Transmisión de un mensaje seguro entre dos usuarios: transmisión .	54
3.9 Transmisión de un mensaje seguro entre dos usuarios: recepción	55
3.10 Firewall.....	56
3.11 Funciones de un firewall	58
3.12 Descripción de las funciones del firewall.....	58
4.1 Proceso de registro de la cuenta del usuario.....	76
4.2 Conformación de la AC del registro de la cuenta del usuario	77
4.3 Proceso de orden de compra: usuario	79
4.4 Proceso de orden de compra: vendedor.....	80
4.5 Proceso de transacción electrónica CyberCash	88

4.6	Proceso de transacción electrónica de First Virtual	90
4.7	Modo de operación de JEPI.....	93

LISTA DE TABLAS

Tabla	Página
3.1 Técnicas de acceso no autorizado.....	37
5.1 Resultados de la evaluación	104

GLOSARIO

Autenticación. Se refiere a la habilidad para verificar la identidad de los agentes involucrados en la transacción.

Browser. Término aplicado normalmente a los programas que permiten acceder al servicio WWW.

Caballos de Troya. Virus almacenados dentro de programas, con el fin de rastrear información o realizar acciones destructivas en el sistema.

Certificado Digital. Es el que contiene la clave pública de la persona o entidad para la que se emite, junto con la información propia, y todo ello firmado electrónicamente por una autoridad de certificación.

Clave Privada. Clave que sólo conoce el usuario propietario de ella.

Clave Pública. Clave que se distribuye a todos los usuarios autorizados para enviar mensajes cifrados.

Comercio Electrónico. Es la automatización mediante procesos electrónicos de los intercambios de información, así como de transacciones, conocimientos,

bienes y servicios que en última instancia pueden conllevar o no la existencia de una contraprestación financiera, a través de un medio de pago.

Computadora Central (Host). Procesador responsable del control general de un sistema de computación.

Confidencialidad. Significa que la transacción es privada y sólo está disponible para los agentes participantes.

Correo Electrónico. Aplicación de computadora mediante la cual se transmiten mensajes por comunicación de datos a "buzones electrónicos".

Criptografía. Tecnología de comunicaciones para impedir delitos, basada en el cifrado y desciframiento de datos, para resolver los códigos transmitidos a través de canales de comunicación.

EDI (Electronic Data Interchange). Intercambio Electrónico de Datos.

Encriptación. Encriptar es hacer ilegible un escrito por medio de aplicar al texto un algoritmo matemático.

Extranets. Al igual que Intranet, son "hermanos menores" de Internet, es decir, que se utilizan los mismos protocolos, sistemas de páginas www, pero en este

caso sirven para unir sectores más amplios que las anteriores, tipo distintas empresas.

Firewall. Es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior de una red privada, por quienes pueden ser ejecutados estos servicios y también a que servicios tienen acceso los usuarios de la intranet hacia el exterior (Internet). El firewall da acceso a una máquina en una red local a Internet pero Internet no ve mas allá del firewall.

Función Hash. Es una función capaz de reducir un mensaje determinado en un conjunto de datos, denominado resumen, de longitud mucho menor que el mensaje, usualmente de 128 ó 254 bits.

iKP. Protocolo de pago que proporciona formas seguras de pago multiparte, se implementa sobre tarjetas de crédito.

Integridad. Significa que los datos transferidos durante la transacción no pueden ser modificados o almacenados en el proceso.

Internet. Es una red de redes, compuesta por un gran número de computadoras conectadas entre sí por medios alámbricos e inalámbricos.

Intranet. Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizará protocolo *TCP/IP* y servicios similares como *WWW*.

MIME. Multipurpose Internet Mail Extensions. Extensiones Multipropósito de Correo Internet. Extensiones del protocolo de correo de internet que permiten incluir información adicional al simple texto.

MOSS. Es una extensión del protocolo de pago MIME.

No-repudiación. Significa que ninguno de los agentes involucrados pueden negar la transacción una vez que ésta se realiza.

Password. Clave de acceso o contraseña necesaria para acceder a un determinado sistema.

PEM. Private Enhanced Mail. Correo Privado Mejorado. Sistema de correo con encriptación.

Procesamiento Distribuido. Configuración de un sistema donde dos o más computadoras geográficamente dispersas en una red, acomodan o comparten aplicaciones.

Protocolo de comunicación. Reglas establecidas para dirigir la forma en que se transmiten los datos a través de la red.

Protocolo IP. Es el protocolo básico de Internet que permite direccionar la transmisión de datos.

Protocolo TCP. Es un protocolo de control de transmisión que tiene la función de asegurar la integridad de los mensajes.

Red Abierta. Es una red donde todos los usuarios tienen acceso a los recursos disponibles con un mínimo de restricciones para salvaguardar la integridad de la red.

Red Privada. Es una red en la cual los usuarios tienen acceso a los recursos a través de contraseñas que son asignadas por el administrador de la red.

Robo de Acceso. Acceso a contraseñas y passwords sin autorización

Robo de Recursos. Uso de recursos de la red para almacenar software y datos sin autorización.

S-HTTP. Secure HTTP. HTTP seguro. Protocolo *HTTP* mejorado con funciones de seguridad con clave simétrica

Servidor. Componente de una red de área local que es compartido por los usuarios.

SSL. Secure Sockets Layer. Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

Suplantación. Asumir la identidad de un usuario a través del uso de direcciones IP y contraseñas de acceso.

Tecnología de Información. Es una colección de elementos que están en constante evolución y tienen un amplio rango de aplicaciones, que abarcan el hardware, el software, las redes de comunicación, estaciones de trabajo, la automatización y el desarrollo informático.

Virus. Programa parásito, diseñado como una broma o para sabotaje y que generalmente causa daño, escondido dentro de un programa legítimo y guardado en el sector de arranque (boot) de un disco.

WWW, WEB ó W3 - World Wide Web. Telaraña mundial, para muchos la WWW es Internet, para otros es solo una parte de esta. Podríamos decir estrictamente que la WEB es la parte de Internet a la que accedemos a través del protocolo *HTTP* y en consecuencia gracias a *Browsers* normalmente gráficos como Netscape.

ABREVIACIONES

AMECE	Asociación Mexicana de Estándares para el Comercio Electrónico
AUP	Política de uso aceptable
CA	Autoridad Certificadora
CIRD	(Direcciones sin clase)
DC	Documento certificado
DES	Data Encryption Standard
DSS	Digital Signature Standard
EAN	International Article Numering Association
ECC	Elliptic Curve Criptography
EDI	Electronic Data Interchange
EIT	Enterprise Integration Technologies
HTTP	HyperText Transport Protocol
IDEA	International Data Encryption Algorithm
iKP	Internet Keyed Payment Protocols
IP	Internet Protocol
JEPI	Joint Electronic Payment Initiative
LAN	Local Area Network
MIME	Multipurpose Mail Enhancements
MOSS	MIME Object Security Objects
NAT	Network Address Traslator

NIST	National Institute of Standards and Technology
NSA	National Security Agency
PEM	Private Enhanced Mail
PEP	Protocol Extension Protocol
RSA	RIVEST-Shamir-Adelman
S-HTTP	Secure - HyperText Transport Protocol
SET	Secure Electronic Transactions
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Tecnología de Información
UCC	Uniform Code Council
UPP	Universal Payment Preamble
VAN	Redes privadas de valor añadido
W3C	World-Wide Web
WAN	Wide Area Network
WWW	World-Wide Web

RESUMEN

La seguridad de los sistemas de comunicación utilizados en el comercio electrónico es un problema de negocio, y no solo un problema asociado a la tecnología. Las organizaciones no solo requieren implementar políticas de seguridad para proteger sus recursos, sino para permitirles tomar ventajas ante nuevas oportunidades de mercado. Por lo tanto, las organizaciones requieren desarrollar los mismos niveles de seguridad en un ambiente electrónico, similar a los alcanzados en las transacciones convencionales.

En muchos aspectos, los sistemas de comercio electrónico están sustentados en sistemas de pago electrónico. La incorporación de capacidades de pago electrónico conlleva una considerable complejidad para los sistemas de información, ya que deben ser capaces de proteger las aplicaciones del sistema, deben proporcionar un alto grado de integridad para cualquier tipo de transacción y deben admitir diversas opciones de pago de acuerdo a las preferencias de los consumidores. Esta diversidad de los sistemas de pago seguro por Internet, y la falta de un estándar único para la implementación de mecanismos de seguridad, ha ocasionado que la mayoría de los usuarios no tengan la suficiente confianza para realizar transacciones en forma electrónica. De ello se desprende la necesidad de explorar los diversos aspectos de seguridad en los sistemas de pago por Internet.

El objetivo de este trabajo de tesis es realizar un análisis de los diversos aspectos de seguridad de los sistemas de pago por Internet. El análisis se enfoca a estudiar las características de operación, así como las ventajas y desventajas de sistemas de transacciones comerciales en forma electrónica. Para ello se realizó una revisión de los sistemas de pago tradicionales, analizando los distintos métodos de encriptación para resolver los problemas de seguridad en estos sistemas. Posteriormente, se estudiaron las características de los nuevos sistemas de pago, su forma de operación y protocolos de seguridad. En este sentido, este trabajo solo aborda los mecanismos de seguridad utilizados en transacciones a través del Internet, excluyendo del estudio los mecanismos de seguridad que se utilizan a nivel empresa para proteger la integridad de sus recursos e información.