00673
4

Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencias de la Administración

Facultad de Contaduría y Administración
Facultad de Química
Instituto de Investigaciones Sociales
Instituto de Investigaciones Jurídicas

T e s i s

La Firma Digital como un medio seguro para realizar negocios internacionales para las empresas mexicanas

Que para obtener el grado de:

Maestro en:

Administración De Negocios Internacionales

Presenta: Sergio Mauricio Martínez Monterrubio

Tutor (Director de la tesis): Marco Murray Lasso, PhD.

Asesor de apoyo: Carlos Hugo Rodas Morales, PhD.

México, D.F. Enero, 2003

TESIS CON
FALLA DE ORIGEN

2

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.

A la memoria de mi padre

SERGIO MARTINEZ RODRÍGUEZ

(3-06-1930 / 5-10-2001)

Gracias Papuchis por todo tu Amor y Cariño, por la dedicación que tuviste con mi mamá y conmigo, por tus valiosas enseñanzas y por hacerme un hombre de bien. Te Quiero Mucho. Tu hijuchito, Mauris.

A mi mamá tan querida,

Angelina Monterrubio Mazín,

Pilar en mi formación humana.

A mi segunda madre,

Susa

Por tu apoyo y cariño durante toda mi vida.

A cada uno de mis maestros de la UNAM en esta maestría que fue para mi descubrir el mundo tan rico en el que vivimos.

En especial a mis asesores de Tesis:

Dr. MARCO MURRAY LASSO, Asesor Tesis

Dr. CARLOS HUGO RODAS MORALES,
Asesor Metodológico

TESIS CON
FALLA DE ORIGEN

LA FIRMA DIGITAL COMO UN MEDIO SEGURO PARA REALIZAR NEGOCIOS INTERNACIONALES PARA LAS MACROEMPRESAS MEXICANAS

"... Y ustedes, no se dejen llamar Maestro, porque no tienen más que un Maestro, y todos ustedes son hermanos"

Lc. 20 [8]

TESIS CON
FALLA DE ORIGEN

INDICE

TESIS CON

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

ABSTRACT

The purpose of this thesis is to explain the business need for using a public-key infrastructure (PKI) and the benefits a PKI can provide in improving the operational effectiveness of an organization while providing an attractive return on security investment. A public-key infrastructure is a critical solution to ensure secure electronic business communication incorporating digital signatures and encryption technology. A PKI transparently manages keys and certificates enabling an organization to create and use a trustworthy networking environment. A trusted network allows organizations to take advantage of the following benefits:

- Confidential communication
- Ensures only intended recipients are able to read files.
- Files can not be intercepted.
- Authentication: validates the creation of a file by the sender.
- Recipients know the sender created the file.
- Non-repudiation: prevents the sender from denying involvement in the creation of a file.
- Integrity: guarantees the file was not altered during transmission.

The benefits of digital signatures and security of information is a mandatory option to enable e-commerce applications. With a PKI, organizations can take advantage of these benefits to gain competitive advantages by improving products and services

This thesis will elaborate on the elements that allow businesses to take advantage of a public-key infrastructure. In particular, it concentrates on the following items: the concept of a public-key infrastructure the requirements for implementing an effective, comprehensive public-key infrastructure for introduction in the Mexican market in order to make this country as competitive as others in the globalized world.

TESIS CON
FALLA DE ORIGEN

RESUMEN

El objetivo de esta tesis es la de presentar a la firma digital como una herramienta eficiente para realizar negocios internacionales por medio del WWW para las macroempresas en México debido al avance de las telecomunicaciones a nivel mundial, presentando así este país como un competidor de clase mundial.

En esta tesis se tratará de explicar la necesidad que requieren los negocios en México para usar una infraestructura de llave pública (PKI) en sus transacciones comerciales por Internet y las ventajas que un PKI puede proporcionar en mejorar la eficacia operacional de la organización mientras que hace atractiva su inversión en seguridad.

Una infraestructura de llave pública es una solución crítica para asegurar la comunicación electrónica segura del negocio que incorpora firmas digitales y tecnología de cifrado. Un PKI transparente maneja llaves secretas y seguras y certificados permitiendo a una organización crear y utilizar un ambiente de red digno de confianza. Una red confiable permite que las organizaciones se aprovechen de las siguientes ventajas:

- Una comunicación confidencial segura sin que otras personas puedan leer archivos confidenciales para los cuales no tienen permiso.
- Con el PKI se evita que los archivos puedan ser interceptados.
- La autentificación valida la creación de un archivo hecho por un usuario.
- Los recipientes saben que el remitente creo el archivo.
- La no negación evita que el remitente niegue su participación en la creación de un archivo.
- La integridad garantiza que los archivos no fueron alterados durante la transmisión.

Las ventajas de firmas digitales y de la seguridad de la información son una opción obligatoria para las aplicaciones del Comercio Electrónico en el mundo globalizado en el que vivimos. Con un PKI, las organizaciones pueden aprovechar estas ventajas para lograr ventajas competitivas mejorando productos y servicios.

Esta tesis detallará los elementos que permiten que los negocios internacionales aprovechen una infraestructura de llave pública y mostrará en detalle los elementos para proporcionar seguridad a las macro empresas mexicanas para darles la oportunidad de realizar transacciones seguras por Internet bajo el esquema de la firma digital.

TESIS CON
FALLA DE ORIGEN

INTRODUCCIÓN

Las organizaciones dependen cada vez más de las comunicaciones basadas en Internet. Internet es una solución de red de bajo costo que proporciona un medio estándar para la comunicación. El uso de aplicaciones para las empresas tales como E-mail, los servidores del Web, el acceso remoto y otras aplicaciones del comercio electrónico propensos a una variedad de ataques de computadoras. Una encuesta está reciente por el FBI y CSI (instituto de la seguridad de las computadoras, de sus siglas en inglés *Computer Security Institute*) en mas de 500 compañías encontró el 64% de las organizaciones sufrió un ataque en los últimos 12 meses: ataques provenientes de los saboteadores, los virus, los robos de computadoras portátiles, el fraude financiero, y la información propietaria robada. El FBI también señaló que la pérdida a las industrias en los E.E.U.U. debido al robo intelectual en las computadoras sumó $63 mil millones en 1997. A medida que la gente continúa confiando en el Internet, los intranets, y los extranets para la comunicación de misión-crítica, la necesidad de herramientas fáciles de utilizar totalmente implementadas para la seguridad son vitales

En la actualidad, la tecnología ha ido remplazando sistemáticamente los procesos manuales que ha utilizado el hombre a lo largo de su historia, haciéndolos hoy en día, más eficientes, y llegando a un mayor número de personas en tan solo segundos

Estos procesos se han desarrollado en el entorno de las tecnologías de información, principalmente en el WWW el cual ha sido el escenario mundial de la globalización y de la tecnología. Ahora las personas tienen la facilidad para comunicarse mas rápidamente a distancias que en toda la historia de la humanidad tomaban incluso años en dichos canales de comunicación

Sin embargo, quisiera adentrarme a un nuevo fenómeno específicamente para México en materia de Internet, el uso de la Firma Digital describiéndolo como un medio seguro para realizar negocios internacionales y colocando a nuestro país al mismo nivel de desarrollo que los países del primer mundo que ya utilizan esta herramienta como el caso de Canadá, Estados Unidos, El Reino Unido y Alemania, principalmente.

En esta tesis quiero enfocarme en la utilidad de la Firma Digital para las macroempresas mexicanas indagando sus ventajas y desventajas

En la actualidad muchas personas se inquietan con la tecnología de información debido a que piensan erróneamente que dichos sistemas remplazarán al hombre. Sin embargo, desde mi punto de vista ésta es una visión catastrófica de los adelantos tecnológicos que evolucionan para liberarnos para nuevas tareas. Es como si el hombre quisiera competir en las carreras con un automóvil, cuando el automóvil es una máquina que sirve para llevar al hombre a recorrer distancias mayores de una forma mas cómoda y rápida. La computadora y sus adelantos tecnológicos son también una herramienta que permite al hombre realizar procesos de forma sorprendentemente rápida en un entorno mundial, sin que esto atente contra su individualidad o bien, pretenda destruirlo como tantas películas de ciencia ficción nos hacen creer

Yo pienso que la tecnología puede ser utilizada tanto para el bien como para el mal. Sin embargo es el hombre quien controla dicha tecnología y él es quien la encauza con los fines que persigue. Puedo hacer hincapié que la tecnología puede y debe ser utilizada

para auxiliar al ser humano en las tareas que le costarían mas tiempo o esfuerzo conseguir. Es por esto que me he adentrado en la aventura, para mi, apasionante, de estudiar al Web en su aspecto de seguridad y no solamente en el lado del comercio electrónico, como lo puntualice en mi tesis de licenciatura. Pienso que para México y muchos países de América Latina y otros países emergentes, puede ser la pieza clave que le hace falta para entrar a una competencia mundial con los países líderes en estas tecnologías, especialmente los casos de Canadá, Estados Unidos y los países miembros de la comunidad económica europea.

He observado que las macro empresas mexicanas, sean del sector gobierno, financiero o telecomunicaciones, carecen de la infraestructura adecuada para proteger sus sistemas de computación, ya sea, por los ataques externos constantes de los hackers y crackers y de la competencia o bien, de los ataques internos de sus propios empleados, causándoles con esto perdidas millonarias, no solo económicas, sino también de información.

Esta es la razón por la cual, me he puesto la tarea crear a esta tesis denominada;

"LA FIRMA DIGITAL COMO UN MEDIO SEGURO PARA REALIZAR NEGOCIOS INTERNACIONALES PARA LAS MACROEMPRESAS MEXICANAS"

en la que elaborará un análisis profundo de la realidad contemporánea en materia de seguridad en nuestro país, comparándolo con países desarrollados los cuales cuentan ya con una infraestructura de seguridad en comercio electrónico, principalmente Canadá, Estados Unidos de América y los países miembros de la comunidad económica europea, con el fin de convertir a México en un país altamente competitivo en materia de seguridad, enfocándonos a la Firma Digital.

TESIS CON
FALLA DE ORIGEN

PLANTEAMIENTO DEL PROBLEMA

PROBLEMAS

PRINCIPAL

Se requiere investigar cuales son las causas por las que no ha sido aprovechado el WWW especificamente a la firma digital por las grandes empresas mexicanas ubicadas en el D.F para realizar negocios internacionales en México y así fomentar su multinacionalización por este medio.

¿Existe la infraestructura adecuada para el correcto uso de Internet de manera segura en nuestro pais con el fin de hacer negocios de manera internacional y que las empresas mexicanas no queden rezagadas con respecto a las empresas trasnacionales?

¿En qué medida se ha aprovechado o desaprovechado el WWW mediante el uso de la Firma Digital en la multinacionalización de las empresas mexicanas transnacionales del D.F. del ramo de comercio debido a su falta de seguridad y de una legislación apropiada?.

SECUNDARIOS

- ¿Es el desconocimiento de las empresas mexicanas del potencial del WWW y de la Firma Digital como una herramienta segura para realizar actos de comercio, lo que les impide realizar negocios internacionales en él?
- ¿Existen ventajas económicas en la Firma Digital para realizar negocios internacionales en Internet que puedan obtener las empresas mexicanas?
- ¿Existe competitividad e innovación tecnológica en el uso de Internet para abrir paso a la Firma Digital de manera segura en nuestro pais?

HIPÓTESIS

Las macro empresas mexicanas no poseen la infraestructura adecuada para competir en un mercado global e internacional para realizar negocios internacionales de una manera segura por Internet mediante el uso de la Firma Digital, por lo cual les coloca en una desventaja competitiva en comparación con otras empresas transnacionales de paises mas desarrollados.

OBJETIVOS DE LA INVESTIGACIÓN

TESIS CON
FALLA DE ORIGEN

OBJETIVOS

PRINCIPAL

Demostrar que es la falta de infraestructura, de cultura y de seguridad en México concerniente al ramo de las telecomunicaciones en Internet, especificamente para la Firma Digital, lo que ha sido la causa por la cual, las empresas mexicanas no han sabido explotar el Internet como una herramienta para los negocios internacionales.

Explicar que el correcto uso de Internet puede ser una herramienta competitiva para realizar negocios internacionales en México de una manera más rápida, eficiente, y económica. (Segura, rentable y confiable).

SECUNDARIOS

Indagar cuales son las ventajas económicas para realizar negocios (comercio electrónico *e-commerce*) internacionales de una forma segura por Internet, mediante el uso de la Firma Digital así como investigar cuales son el tipo de empresas que se beneficiarían mayormente con esta herramienta.

Explicar las ventajas y desventajas del uso de la Firma Digital para los negocios internacionales, desde el punto de vista legislativo, costos y de seguridad para las empresas Mexicanas.

TESIS CON
FALLA DE ORIGEN

CAPITULO PRIMERO

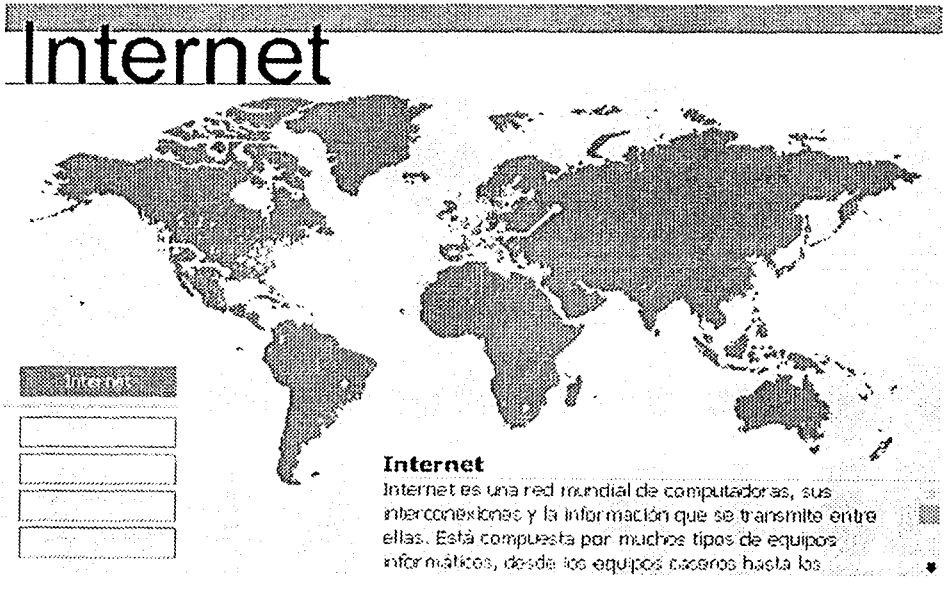
ANTECEDENTES

Lo que mas desean proteger las empresas es su información. La información se ha tornado critica pues desvirtuarla, alterarla o robarla puede lesionar grandemente a una organización.

Es por esto que se han buscado medios para cubrirnos de ataques de enemigos dentro y fuera de la empresa.

1.1 DEFINICIÓN DE INTERNET

Internet es un conjunto de redes de computadoras que emplean los mismos protocolos (TCP/IP principalmente) para comunicarse entre si. Podemos entender como protocolo un lenguaje de comunicación propio de las computadoras, de la misma manera como los seres humanos utilizan el lenguaje, como el idioma español, para entenderse entre sus semejantes. Las computadoras, sin embargo, mandan señales binarias en la red y de esta forma se comunican entre si sin importar la distancia en la que se encuentren. Como una carrera de relevos se transmiten las señales hasta llegar a la computadora indicada. Las redes que forman Internet están conectadas entre ellas mediante lineas telefónicas y otros medios



Fuente: dibujo tomado de la enciclopedia Encarta 2000. Microsoft (c)

TESIS CON FALLA DE ORIGEN

En Internet existen tres papeles importantes: el primero es el proveedor de información el cual coloca la información que maneja y la distribuye a los clientes (o usuarios), quienes juegan el papel secundario. El tercer papel lo tienen los proveedores de servicios de Internet, también conocidos como proveedores de conexión, quienes proveen el servicio de conexión a los dos anteriores.

1.2 ANTECEDENTES DEL WORLD WIDE WEB

RESUMEN

El documento más completo escrito acerca de la historia del Web fue redactado por Tim Barnes Lee en Paris en la ceremonia del lanzamiento del Consorcio del *World Wide Web*. Cuando el autor trabajaba en CERN, el laboratorio Europeo de partículas físicas, donde el World Wide Web fue concebido. Él ha trabajado con el Web desde el principio y ahora corre el servicio Web de CERN. El también es miembro fundador del IW3C2, el comité de conferencias internacionales de WWW. El formó parte de la diseminación del consorcio del WWW. Tim Barnes Lee, actualmente trabaja en laboratorio de ciencias computacionales del MIT

CERN es el laboratorio de física mas grande del mundo. Fundado por 19 miembros europeos. Esta localizado cerca de Ginebra, con las facilidades de los dos bordes tanto el Suizo como Francés.

Los físicos de CERN investigan la naturaleza de la energía y la materia en investigaciones científicas del ambiente. CERN provee a sus usuarios una gran cantidad de aceleradores de partículas nucleares. De ahí proviene su nombre: "*Conseil Européen pour la Recherche Nucléarie*", pero los laboratorios no involucran el poder nuclear ni las armas.

1.2.1 PREHISTORIA DEL WWW

La historia de cualquier gran invento esta basado en mucha prehistoria. En el caso del *World Wide Web*, existen dos líneas que mencionarse: el desarrollo del hipertexto, o la integración de lectura de los documentos electrónicos a las computadoras, y el desarrollo de protocolos de Internet los cuales hacen posible a una red global.

Tan cerca de 1945 Vannevar Bush, el científico consejero del presidente Roosevelt, escribe acerca del Memex, un dispositivo (basado en el microfilm) para contener muchos documentos en un solo escritorio, con mecanismos especiales de búsqueda, organización y con la facilidad de agregar datos.

En los años 60's Douglas Engelbart produce el primer sistema de hipertexto. Estos sistemas corrían en las costosas y enormes máquinas de los sesenta, con un poco mas costosos sistemas de despliegue. Engelbart es también el inventor del *Mouse*.

En 1968 Ted Nelson introduce el término de Hipertexto.

En 1962 DARPA inicia en su búsqueda líder al Internet. Originalmente convencidos de que se pueden conectar centros de investigación para cambiar información, mas tarde se convirtió con propósitos militares. Esta es la característica de los procesos de ruteo para

TESIS CON
FALLA DE ORIGEN

la información de paquetes, circulando los problemas de las redes, la vulnerabilidad a través de fallas de los nodos de transacciones simples.

1975 Alan Kay produce la primera computadora personal (Xerox PARC). Muchas ideas son traídas, Kay inventa la tecnología Windows para producir una maquina para usuario simple conducida por menús y comandos y accesados por el Mouse. Este es utilizado en muchas workstations en los inicios de los años 80's y popularizados por la Macintosh de Apple en 1984.

En 1979 Charles Goldfarb invierte en SGML. Esta idea separa de la estructura de contenido a la presentación. Por lo tanto, el mismo documento puede presentarse de diversas maneras. HTML, el lenguaje de marcación del Web es una aplicación SGML.

En 1981 "*Literary Machines*" (Ted Nelson) describe el proyecto Xanadu: una trabajo de red, un sistema de *World Wide* para publicaciones, incluyendo la colección de realidades y la inclusión del material existente.

En 1987 CERN y los laboratorios de Estados Unidos de América conectan el Internet como la principal fuente de intercambio de documentos entre laboratorios.

1989 La comunidad HEP es pequeña pero se encuentra en todo el mundo. Los físicos de los laboratorios del mundo hacen muchas colaboraciones e intercambian datos y documentos que es su actividad primordial. Este ambiente es aceptado como un sistema de facilidades de comunicación entre redes. La adopción de Internet como una red estándar académica por CERN y los laboratorios en los US hacen un campo fértil.

1990 CERN un propósito unido al sistema de hipertexto es presentado para su mantenimiento. Mike Sendall compra NeXT para evaluaciones y lo renombra Tim. El prototipo Tim se implementa en NeXSTep haciendo un espacio de unos pocos meses, gracias a las cualidades del desarrollo de sistemas del software NeXSTep. Este prototipo *WYSIWYG browsing/authoring* los actuales navegadores pueden sorfear por Internet. Como un mero espectador de Windows, daban la posibilidad al espectador de contribuir.

Durante algunas sesiones en la cafetería del CERN, Tim propuso como nombre del sistema World Wide Web.

1991 El prototipo fue muy impresionante, pero el sistema NeXSTep no era muy ancho. Una simplificación de la versión (sin facilidades de editar) el cual era muy fácilmente adaptado por cualquier computadora fue construido: el portable "Browser Modo en línea"

SLAC, el Centro lineal de aceleración de Stanford, el cual se encuentra en el centro de California, fue el primer servidor de Web en Estados Unidos de América (USA). El servidor contenia en existencia, una gran base de datos de resúmenes y papeles de física. La distribución del Software de Internet comienza. La conferencia del *Hipertext* (San Antonio) presenta el "póster"

1992. El *Browser* portable de CERN es puesto como *freeware*. Muchos laboratorios Hpe son ahora puestos como servidores: DESY (Hamburgo), NIKHEF (Amsterdam), FNAL (Chicago). El interés en Internet crece. Los sistemas Gopher de la Universidad de Minnesota, también conectados, simples de instalar pero sin la posibilidad de ligas, decaen rápidamente.

TESIS CON
FALLA DE ORIGEN

Se necesita implementar un *Browser* de Web para sistemas X, pero no se tiene un experto. Sin embargo, Viola (O'Reilly Assoc., California) y Midas (SLAC) hacen implementaciones *wysiwyg* (lo que deseas, eso es lo que obtienes de las siglas en ingles) para crear mayor interés.

El mundo tiene 50 servidores de Web.

1993 Viola y Midas enseñan su desarrollo de software del grupo NCSA (*The National Center for Supercomputing Applications*, Illinois). Marc Andreessen y Eric Bina escriben Mosaic para NCSA. Este es fácil de instalar, robusto, y provee de imágenes a color. Esto causa una explosión dentro de USA.

La ausencia del editor *wysiwyg* para páginas Web es muy frustante. Se comenzó a buscar por encontrar una tecnología SGML. Se obliga a los presidentes de la compañía Grif para que inviertan en publicidad para los negocios. Pero Europa no se encontraba lista para esta revolución. Sin embargo la compañía Grif es ahora uno de los principales miembros del consorcio del Web y tiene un Site para promocionar sus productos (Symposia).

CERN produce un software para servidor de Web con los básicos mecanismos de protección.

El servidor de Web con pinturas de una exhibición de dinosaurios en Honolulu se convierte en el servidor de entretenimiento del Web.

La comisión europea aprueba el primer proyecto basado en el WWW: "*Wise*" para la difusión de la información de proyectos grandes y medianos (DGXIII, *el Fraunhofer Gesellschaft* (Darmstadt/Rostock) the CCG (Potugal) y CERN). Se realiza y organiza la primera conferencia internacional de WWW Existen 250 servidores en el mundo.

1994 Jim Clark, predice la llegada de Internet. El funda MCC (posteriormente Netscape). Netscape se atrae a los mejores programadores de todo el mundo. La primera conferencia internacional de WWW se lleva a cabo en Ginebra, en CERN. Esto atrae alrededor de 600 entusiastas del Web. Solo 400 fueron admitidos *("Woodstock of the Web")*.

TESIS CON
FALLA DE ORIGEN

Una conferencia en Estados Unidos es una necesidad, se funda el IW3C2 (Comité International de conferencias del World Wide Web) para futuras conferencias.

El éxito del Web significa que CERN como laboratorio de física no continuará investigando proyectos informáticos sin ayuda. El propósito de un proyecto para la comisión europea para obtener fondos para continuar desarrollando tecnologías.

La segunda conferencia de WWW es organizada por NCSA, in Chicago. Esto atrae a 1800 personas, de los cuales solo 1300 son admitidas.

Tim Berners-Lee y el laboratorio de Ciencia de la *Computación (LCS Laboratory for Computer Science)* del MIT *(Massachusetts Institute of Tecnology)* comienza con el Consorcio del W3C en los Estados Unidos de América. Esto se modela posteriormente como el X consocio.

Tim Berners-Lee deja CERN por el MIT (Diciembre).

El concilio CERN aprueba unánimemente la construcción de un acelerador LHC. Este Larch Hadron Collider podrá ser construido en un túnel LEP, pero con un túnel estrecho. Esto es ahora posible para CERN para continuar adentrándose en el desarrollo del Web.

Existen en el mundo 2500 Servidores de World Wide Web.

También en 1994 se crea el primer banco de la Red: First Virtual. En Stanford University crean el buscador Yahoo. Surge en México la Red Tecnológica Nacional (RTN), soporte nacional de Internet.

1995 En enero CERN y la comisión Europea invitan a INRIA, el Instituto Nacional de Buscadores en Informática y Automatización a continuar el desarrollo europeo. INRIA tiene cinco sitios en Francia y sumamente involucrado en los proyectos y colaboraciones con institutos similares en Europa y en el mundo.

Sun Microsystems produce HotJava, un Browser el cual incorpora objetos interactivos.

La tercera conferencia es organizada por el FhG, *Darmstadt*. No hay camino para que individuos entren al consorcio del Web. Para dar una voz a los individuales, una organización se necesita. Esto lo lidera por una fundación de Web en Graz (Austria). Son organizadas las conferencias regionales (Portugal, Sydney...) ¡ Se registran 700 nuevos servidores por día !

TESIS CON FALLA DE ORIGEN

Durante el verano, muchas compañías Europeas, sobretodo usuarios, gozan del W3C. La presencia Europea en el mundo del Consorcio del Web es agrandado para ofrecer un día especial para las actividades en Europa. A este encuentro asisten 1300 personas que se albergan en Paris (organizado por INRIA).

La cuarta conferencia se llevará a cabo en Diciembre, organizada por MIT, Boston. La Quinta conferencia será organizada por INRIA que tendrá como sede en París en Mayo de 1996. Existen hasta 1995 aproximadamente 73,500 servidores de World Wide Web. WWW es generalmente certificado con el Internet.

También en 1995 sale al mercado Windows 95, el primer sistema operativo con Windows para los usuarios finales, que integra aplicaciones con el ambiente de Internet junto con el browser Internet Explorer. México anuncia oficialmente su dominio .mx y se crea el Centro de Información de Redes en México (NIC-México).

1996: Se descubren intromisiones a sitios de la CIA, la Fuerza Aérea y el Ministerio de Justicia de Estados Unidos de América. El número de usuarios de Internet asciende a 80 millones en 150 paises.

1997: Las grandes empresas dedicadas a la informática se dan cuenta del potencial económico de Internet y comienza la lucha por dominar este nuevo mercado, donde sus principales exponentes son IBM (e-commerce), Microsoft (con su navegador Internet Explorer), Sun Microsystems (con la tecnología Java) y las tarjetas Visa y Mastercard con SET. La búsqueda de un estándar para hacer transacciones comerciales seguras en todo el mundo es el paso que sigue, pues todavía no se encuentra ninguna solución a este problema, pero ya se prevé el potencial económico del World Wide Web.

También en este año, 1997 Bill Clinton, entonces presidente de los Estados Unidos de América propuso la Zona de Libre Comercio para Internet sin obstáculos legales. Para ese entonces existían más de 19 millones de páginas Web en el mundo.

1998 En enero la cantidad de Hosts o nodos conectados a Internet de fue de 29,670,000 y 68.69 millones de personas usan el Web, se estima que para finales de este año crecerá a 97.25 millones y que para el siglo XXI el número de usuarios de Internet crecerá a 319.79 millones.

1.3 CONCEPTO DE NEGOCIOS INTERNACIONALES

"Los negocios internacionales son el estudio de las transacciones que tienen lugar en el ámbito mundial con el fin de satisfacer las necesidades de los individuos y organizaciones. Estas actividades económicas son operaciones comerciales, como en el caso de exportar o importar bienes, y la inversión directa de fondos en compañías internacionales. Cerca del 80% de la inversión directa la realizan las 500 empresas."[1]

Aunque las multinacionales son el principal actor de los negocios internacionales, también las empresas medianas y los servicios participan en ellos, pero de una manera mas indirecta.

La mayor parte de esas inversiones se da en dos sentidos; Estados Unidos invierte en la comunidad europea y ésta a su vez lo hace en Estados Unidos; lo mismo sucede con las inversiones de Estados Unidos y Canadá, Japón y entre la Comunidad Europea.

1.3.1 Las 2 formas básicas que se llevan los negocios internacionales

Dos de los tipos mas comunes de estos negocios son las actividades de exportación e importación y la inversión extranjera directa. En los últimos años ambas han ido creciendo. En particular la inversión resulta de mucho interés porque la realizan las empresas multinacionales o transnacionales.

1.3.2 NEGOCIOS MUNDIALES: BREVE PANORAMA

La mayoría de los negocios internacionales se realizan por empresas multinacionales. Esta actividad la realizan en varias formas. Una es el comercio internacional; por ejemplo, las exportaciones e importaciones. Otra es la inversión directa en el extranjero. Una tercera son las licencias (concesiones), las empresas conjuntas y otras modalidades de inversión directa.

1.4 CONCEPTO DE FIRMA DIGITAL

Es un tipo de firma electrónica el cual está basado en la criptografía de llave pública (de sus siglas en inglés PKI lo que significa *Public Key Infraestructure*, lo que se traduce al español como; Infraestructura de Llave Pública) usada para proveer integridad y la autentificación.

TESIS CON
FALLA DE ORIGEN

[1] Fuente. Alan M. Rugman, Richard M. Hodgetts. "Negocios Internacionales, Un enfoque de administración estratégica" Mc Graw Hill, 1997

La seguridad en los negocios y comunicaciones a través de redes informáticas puede considerarse el equivalente electrónico de firmar una carta y sellarla dentro de un sobre. La firma prueba su autenticidad y el sobre cerrado proporciona confidencialidad.

No me adentrare a explicar profundamente el significado y la funcionalidad del PKI puesto que esto lo veremos en el capitulo siguiente.

TESIS CON
FALLA DE ORIGEN

CAPITULO SEGUNDO

LA INFRAESTRUCTURA DE LLAVE PUBLICA PKI

En este capitulo Identificaré cuales son las soluciones y productos que existen en materia de seguridad en el ámbito nacional e internacional y cuáles son las empresas que los proporcionan

La seguridad en los negocios actuales es un asunto que se está tornando crítico, en especial en aquellos negocios basados en Internet, ya que mucha de la información manejada es altamente confidencial y sensitiva. Muchas veces el proceso para determinar cuales controles de seguridad en las empresas puede resultar caro y complejo y muchas veces puede resultar subjetivo.

2.1 INTRODUCCIÓN A LA INFRAESTRUCTURA DE LLAVE PÚBLICA

Ésta Introducción al PKI será de gran utilidad para entender la Tecnología de Infraestructura de llave Pública. Proporcionare información exhaustiva sobre las opciones que se tienen que buscar cuando se evalúe una Infraestructura de llave Pública (PKI), así como los riesgos que debe tener cuando se desee implementarla.

Para crear las llaves de encripción secretas se utiliza un algoritmo llamado Asimétrico. En este tipo de encripción, el usuario posee dos tipos de llaves, una llave pública y una llave privada. Con la llave pública, el usuario encripta la información. Con la llave privada, la desencripta. La información no puede almacenarse, solamente enviarse. Por ejemplo, si Mauricio quiere enviarle a Ana un mensaje encriptato, lo que deberá hacer es encriptar el mensaje con la llave pública de Ana para que ella pueda leer el mensaje con su llave pública, pues ella es quien lo va a desencriptar. En la Firma Digital, lo que se busca es proteger es al documento. Yo debo de tener la certeza de que este documento lo creo quien dice que lo creo. La firma Digital utiliza una llave pública y una privada. Con la llave privada encripto la información y con la llave pública, la desencripto para que el mundo pueda ver que yo estoy enviando esta información, pues lo que me interesa es que el mundo sepa que yo lo envie. La Firma Digital garantiza que yo la firme y que la información no fue alterada por un tercero. Esto permite garantizar la integridad de la información enviada

TESIS CON
FALLA DE ORIGEN

Introducción a la Infraestructura de llave Pública

2.2 Seguridad de IT: Riesgos y Oportunidades

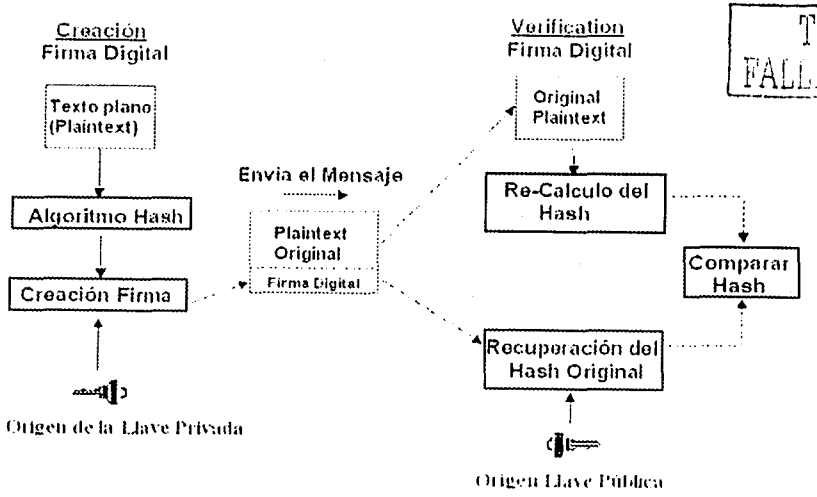
Estamos viviendo una época en la que se está produciendo una revolución del comercio electrónico. La nueva cultura global del intercambio electrónico de información y trabajo en red supone un riesgo mayor que nunca de fraude, de robo de datos del correo electrónico, tanto para las compañías como para los particulares.

La sociedad electrónica se enfrente hoy en dia al problema de la seguridad de la información. A medida que la autopista de la información cruza fronteras, las puertas cerradas ya no bastan para proteger uno de los activos más valiosos de las compañías: "la información"

Por otro lado, Internet ofrece a las empresas nuevas y emocionantes oportunidades para desarrollar un canal adicional para la entrega de servicios. La naturaleza omnipresente y económica de Internet ha provocado un auge en el comercio y negocio electrónico, creando un cambio paradigmático en el mundo de los negocios.

Modelo de la Firma Digital

TESIS CON
FALLA DE ORIGEN



Poner el negocio "en linea" abre todo un mundo lleno de posibilidades, como por ejemplo unos niveles de servicio mejorados, una mayor eficacia, la reducción de costos, una mejora en las comunicaciones de la empresa, menor tiempo de puesta en el mercado y un mayor alcance en el mismo.

Las organizaciones reconocen la necesidad de responder estratégicamente a este crecimiento explosivo, en vez de reaccionar en contra, equilibrando cuidadosamente la preocupación por la protección de los datos corporativos con el deseo de potenciar este nuevo método para obtener ventajas competitivas.

La seguridad de la información es un elemento imprescindible ante estas exigencias. Necesitamos seguridad de información, no sólo para proteger nuestros activos, sino también para aprovechar esta nueva oportunidad que nos brinda el mercado. Necesitamos tener los mismos niveles de confianza en el mundo electrónico que los que tenemos en el tradicional.

A medida que nos adentramos en el mundo electrónico, ¿cómo podemos reconocer y confiar en gente a la que no vemos, escuchamos, o ni siquiera conocemos su firma? Cómo mantenemos en secreto nuestras transacciones comerciales sin sobres sellados o llamadas telefónicas privadas? Cómo sabemos que el mensaje ha llegado intacto a la persona a la que iba destinada, y que ésta ha dado su aprobación al contrato?

La Infraestructura de llave Pública (PKI) proporciona la llave para abrir y descubrir las ventajas de un mundo electrónico plenamente seguro.

"Las previsiones indican que en una gran empresa, cuesta alrededor de 500 pesos distribuir y procesar en papel un solo informe de gastos. Ese costo se reduce a alrededor de 10 pesos por informe con el uso de firmas electrónicas." [2]

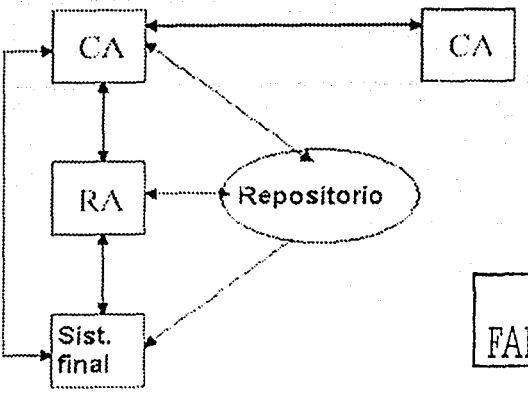
2.3 ¿Qué es una Infraestructura de llave Pública (PKI)?

La seguridad en los negocios y comunicaciones a través de redes informáticas puede considerarse el equivalente electrónico de firmar una carta y sellarla dentro de un sobre. La firma prueba su autenticidad y el sobre cerrado proporciona confidencialidad.

El PKI cuenta con tres características indivisibles; el Profile Server, el Directorio (o repositorio de datos) y la CA (Autoridad Certificadora)

2 Fuente: Data Communications, 7 de noviembre de 1998, número 7216

INTERAOPERABILIDAD ENTRE COMPONENTES



TESIS CON
FALLA DE ORIGEN

2.4 AUTORIDADES CERTIFICADORAS CA[3]

Es esa tercera parte fiable que acredita la unión entre una determinada clave y su propietario real. Actuaria como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Sin embargo ¿quién autoriza a dicha autoridad?, Es decir, ¿cómo sé que la autoridad es quién dice ser?, ¿Deberá existir una autoridad en la cúspide de la pirámide de autoridades certificadoras que posibilite la autenticación de las demás?

En USA la ley de Utah sobre firma digital da una importancia fundamental a las Autoridades Certificadoras, definidas como las personas facultadas para emitir certificados. Pueden ser personas físicas o empresas o instituciones públicas o privadas y deberán obtener una licencia de la *Division of Corporations and Commercial Code*. Están encargadas de mantener los registros directamente en línea (*on-line*) de claves públicas.

Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser fiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave. Esta solución da origen a diferentes niveles o jerarquías de CAs

En cuanto a los Certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un Registro (*repository*), considerado

[3] Autoridad Certificadora, de sus siglas en inglés: *Certification Authority*

como una base de datos a la que el público puede acceder directamente en línea (*on-line*) para conocer acerca de la validez de los mismos. Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.

2.5 La Autoridad Certificadora puede emitir distintos tipos de certificados:

1. Certificados de identificación: identifican y conectan un nombre a una clave pública.
2. Certificados de autorización: ofrecen otro tipo de información correspondiente al usuario, como por ejemplo la dirección comercial, antecedentes, catálogos de productos, etc.
3. Otros certificados colocan a la Autoridad Certificadora en el rol de notario, pudiendo ser utilizados para dar fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.
4. Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (*Digital time-stamp certificates*).

El interesado en operar dentro del esquema establecido por la ley, deberá, una vez creado el par de claves, presentarse ante la autoridad Certificadora (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita 'firmar' el documento de que se trate. Por ejemplo, para realizar una operación financiera de importancia con un banco, éste puede requerir al interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

Los *Repository* o Registros son la base de datos a la que el público puede acceder *on-line* para conocer la validez de los certificados, su vigencia o cualquier otra circunstancia que se relacione con los mismos. Dicha base de datos debe incluir, entre otras cosas, los certificados publicados en el repositorio, las notificaciones de certificados suspendidos o revocados publicadas por las autoridades Certificadoras acreditadas, los archivos de autoridades Certificadoras autorizadas y todo otro requisito exigido por la División. Para ser reconocido, el repositorio debe operar bajo la dirección de una autoridad Certificadora acreditada.

2.6 Servidores de Certificados

Son aplicaciones destinadas a crear, firmar y administrar certificados de claves, y que permiten a una empresa u organización constituirse en autoridad de certificación para subvenir sus propias necesidades. Los productos más famosos son *Netscape Certificate Server y OpenSoft*.

2.7 Situación actual de las autoridades de Certificación

Actualmente existen varias autoridades de certificación, Verisign es la más conocida Internacionalmente. En España nos encontramos con varias empresas que han introducido ya este tipo de servicio. La más utilizada en España es IPS (*Internet*

Publishing Services), seguida de la americana Verisign, sin embargo Banesto fue posiblemente la primera CA española, actualmente ya emite certificados para SSL y S/MIME (medios para garantizar la seguridad en las redes telemáticas). Posteriormente ACE (Autoridad de Certificación Española) ha comenzado a emitir también dichos certificados, pero su objetivo prioritario es emitir certificados SET. Está además participando en los desarrollos de PKIS (*Public Key Cryptography Standards*: estándares de criptografía de clave pública) o documentos que definen el estándar en el cifrado de clave pública, ya que se plantea un sistema de registro distribuido con la participación de los Bancos. Así tenemos que Argentaria utiliza una CA en Argenvia, su Banca electrónica. No obstante hay ya varias entidades financieras que utilizan la solución de banca electrónica de *Intercomputer*, éstas llevan más de un año usando una autoridad de certificación (SISCER) que próximamente va a ser relevada por FESTE (Fundación para el Estudio de la Seguridad de las Telecomunicaciones). Es una autoridad de certificación avalada por los notarios y corredores de comercio, es decir, por los fedatarios de las operaciones mercantiles. FESTE pone su énfasis en la garantía de las instituciones. De esta forma han aunado sus fuerzas para convertirse en la autoridad certificadora de la seguridad de los contratos mercantiles españoles. Como árbitro han elegido al ex-político y abogado Miguel Roca, y el camino a seguir incluye hablar con los ministros competentes para asegurárselos como garantes en la consecución de sus objetivos, entre los que se encuentra lograr la realización de la legislación pertinente en materia de seguridad mercantil telemática, ya que según comenta M. Roca "en España ni siquiera hay un proyecto legislativo en esta materia. Aunque esto no debe de extrañar porque el entorno europeo tiene la misma deficiencia, a excepción de Alemania e Italia que están desarrollando modelos muy distintos "

Por otro lado en el entorno académico y en distintas universidades Españolas se están produciendo interesantes avances. En la UPC (Universidad Politécnica de Cataluña), la UPM (Universidad Politécnica de Madrid), en Red IRIS y en el CSIC se han puesto en marcha diferentes autoridades de certificación, lo cual no hace sino demostrar que nuestro país es muy activo desde el punto de vista tecnológico.

Sin embargo las múltiples CA´s que hay a la larga puede derivar en:

1. Que existan una o dos autoridades fuertes que autoricen al resto.
2. Que existan muchas CA´s que se certifiquen mutuamente, es decir, que deberán a su vez estar certificadas por una autoridad superior llamada Root, única para todos.

Por tanto parece ser que la situación actual está por desarrollarse y reglamentarse, luego sólo podremos hablar de pruebas y tests hasta que exista una ley o se tome por la comunidad Internacional una solución al respecto

Requisitos De Las Autoridades De Certificación Según El Grupo De Trabajo Sobre Comercio Electrónico De La Comisión De Las Naciones Unidas Para El Derecho Mercantil Internacional

El plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI / UNCITRAL), que celebró su 29º periodo de sesiones en New York del 28 de marzo al 14 de Junio de 1996. Examinó el proyecto de ley Modelo sobre distintos aspectos del intercambio electrónico de datos(EDI), aprobándolo con la denominación de Ley Modelo sobre comercio electrónico. Tras un debate la Comisión encomendó al Grupo

TESIS CON
FALLA DE ORIGEN

de Trabajo, ahora denominado "sobre Comercio Electrónico" que se ocupara de examinar las cuestiones relativas a las firmas digitales y las autoridades de certificación.

La Comisión pidió a la secretaria que preparara un estudio de antecedentes sobre cuestiones relativas a las firmas digitales y a los proveedores de servicios, basándose en un análisis de las leyes que se estaban elaborando en varios paises. Dicho estudio quedó recogido en el documento A/CN.9/WGIV/WP.71 de 31 de Diciembre de 1996. El grupo de trabajo celebró su 31 periodo de sesiones en New York del 18 al 28 de febrero de 1997 centrando su debate en el proyecto de prácticas internacionales uniformes sobre autenticación y certificación de la Cámara de Comercio Internacional y las directrices sobre firmas digitales publicadas por la American Bar Asociation.

Dentro de esta sesión se abrió el debate sobre la necesidad o no de autorización y del establecimiento de requisitos, ya sean referidos a la propia entidad o al certificado. A tal efecto se ofreció el debate a partir de los criterios que se mencionan en el párrafo 44 del WP 71:

1. Independencia (ausencia de interés financiero o de otro tipo en las transacciones subyacentes).
2. Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida
3. Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.
4. Longevidad (conservación de certificados).
5. Aprobación del equipo y los programas.
6. Mantenimiento de un registro de auditoria y realización de auditorias por una entidad independiente.
7. Existencia de un plan para casos de emergencia.
8. Selección y administración del personal.
9. Disposiciones para proteger su propia clave privada.
10. Seguridad interna.
11. Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.
12. Garantías y representaciones.
13. Limitación de la responsabilidad.
14. Seguros.
15. Capacidad para intercambiar datos con otras autoridades certificadoras.
16. Procedimientos de revocación.

El valor otorgado por el grupo de trabajo sobre estos principios es el de factores a tener en cuenta en la confiabilidad de una determinada Autoridad de Certificación.

2.8 VeriSign como ejemplo de Autoridad Certificadora

VeriSign es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma digital. Para el logro de este objetivo, las autoridades de emisión (*Issuing Authorities, "IA"*) autorizadas por VeriSign funcionan como terceras partes confiables, emitiendo, administrando, suspendiendo o revocando certificados de acuerdo con la práctica pública de la empresa.

Las IA facilitan la confirmación de la relación existente entre una clave pública y una persona o nombre determinado. Dicha confirmación es representada por un certificado: un mensaje firmado digitalmente y emitido por una IA.

El proceso de certificación incluye servicios de registro, "*naming*", autenticación, emisión, revocación y suspensión de los certificados. Esta empresa ofrece tres niveles de servicios de certificación. Cada nivel o clase de certificados ofrece servicios específicos en cuanto a funcionalidad y seguridad. Los interesados eligen entre estos grupos de servicios el que más le conviene según sus necesidades, debiendo especificar qué clase de certificado desean

Dependiendo de la clase de certificado requerido, los interesados pueden solicitarlos y obtenerlos electrónicamente siguiendo las instrucciones detalladamente indicadas, o deberán concurrir personalmente a una Autoridad de Registro Local o LOCAL REGISTRATION AUTHORITY (LRA), o a un delegado, que puede ser un notario.

Pueden existir varias "IA" para cada uno de los distintos niveles. Cumplidos los requisitos exigidos se emite el certificado o se envía un borrador para su aceptación por el interesado, según el caso

2.9 Tipos de certificados:

A. **Certificados Clase 1:** son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indubitable el nombre del usuario o su "alias" y su dirección de E-mail con el registro llevado por VeriSign. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing y E-mail, afianzando la seguridad de sus entornos. En general, no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.

B. **Certificados Clase 2:** son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que ella no difiere de la que surge de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones via E-mail; transacciones comerciales de bajo riesgo, validación de software y suscripciones *on-line*. Después del acuerdo del usuario, realizado on line ante una LRA, los datos contenidos en la aplicación son confirmados comparándolos con una base de datos reconocida. Teniendo en cuenta dicha confirmación la LRA puede aprobar o rechazar la aplicación. En caso de aprobación, la conformación es enviada por correo. Debido a las limitaciones de las referidas bases de datos, esta clase de certificados está reservada a residentes en los Estados Unidos y Canadá.

C. **Los Certificados Clase 3:** son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, asegura la identidad del suscriptor, requiriendo su presencia física ante una LRA o un notario. En el caso de organizaciones asegura la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes. Son utilizados para determinadas aplicaciones de comercio electrónico como *'electronic banking'* y ELECTRONIC DATA INTERCHANGE (EDI). Como las autorizadas por VERISIGN firman digitalmente los certificados que emiten, la empresa asegura a los usuarios que la clave privada utilizada no está comprometida, valiéndose para ello de productos de hardware. Asimismo, recomiendan que las claves privadas de

TESIS CON FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

los usuarios sean encriptadas vía software o conservadas en un medio físico (*smart cards o PC cards*).

2.10 CRIPTOGRAFÍA

La criptografía garantiza la confidencialidad encriptando un mensaje mediante una clave secreta en conjunto con un algoritmo. Esto da como resultado una versión "codificada" del mensaje que el receptor puede desencriptar, utilizando la clave original, para recuperar su contenido. La clave empleada debe mantenerse en secreto entre las dos partes. El problema principal en la mayoria de las aplicaciones criptográficas es gestionar estas claves y mantenerlas secretas.

La criptografía mediante clave pública resuelve este problema sustituyendo la clave secreta con dos claves: una privada y otra pública.

2.10.1 Información

La información encriptada mediante la clave pública sólo puede recuperarse mediante la clave privada complementaria. Con este sistema, las claves públicas de todos los usuarios pueden publicarse en directorios abiertos, facilitando las comunicaciones entre todas las partes. Además de la encriptación, las claves públicas y privadas pueden emplearse para crear y verificar "firmas digitales". Éstas pueden agregarse a los mensajes para autentificar el mensaje y el remitente.

Pero la criptografía mediante clave pública, de por si, no basta si deseamos reproducir en un mundo electrónico las condiciones del comercio tradicional basado en el papel.

También necesitamos:

- Políticas de seguridad para definir las reglas según las cuales deben funcionar
- Productos para generar, almacenar y gestionar las claves
- Procedimientos para establecer cómo generar, distribuir y emplear las claves y certificados

En resumen: necesitamos una Infraestructura de llave Pública (PKI).

La PKI proporciona el marco de acción para un amplio conjunto de componentes, aplicaciones, políticas y prácticas para combinar y obtener las cuatro funciones principales de seguridad para transacciones comerciales:

- **Confidencialidad:** mantener privada la información
- **Integridad:** demostrar que la información no ha sido manipulada
- **Autentificación:** demostrar la identidad de una persona o aplicación
- **No repudiación:** garantizar que no se puede negar el haber hecho una acción.

La falta de seguridad, a menudo, se cita como una de las mayores trabas para el crecimiento del comercio electrónico, el cual sólo puede basarse en la confianza que procede de saber que todas las transacciones están protegidas por estas funciones centrales.

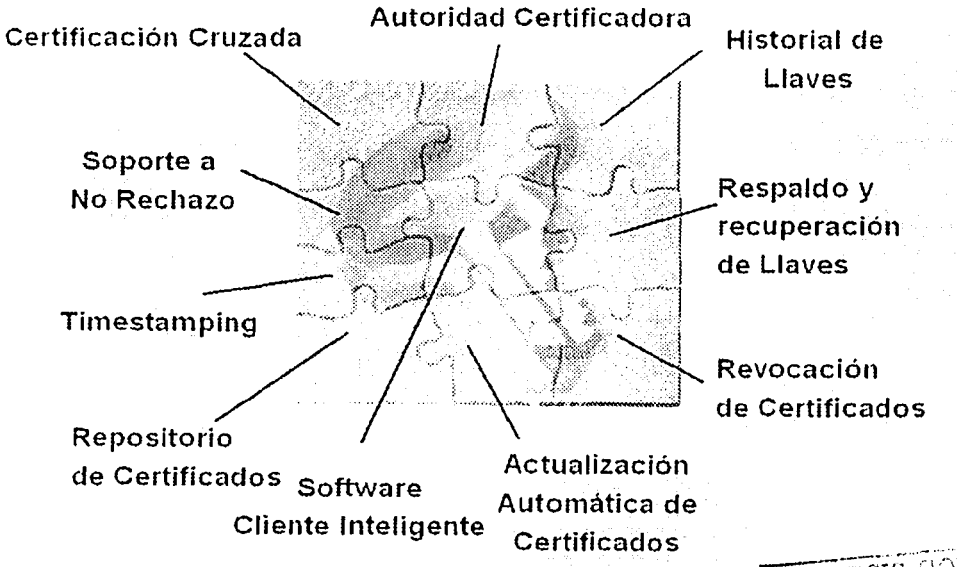
Al igual que cualquier tecnología nueva y crítica para el negocio, la evaluación e implementación de una solución PKI es un proceso complicado e intrincado, que requiere una buena planificación, gestión y guía clara.

Dataquest, del Grupo Gartner, estima que el mercado de Software de Certificados Digitales y de Servicios de CA (Autoridad Certificadora, de sus siglas en inglés: *Certification Authority*) experimentará un índice de crecimiento anual compuesto del 80% entre 1998 y el 2002. *"Dataquest, del Grupo Gartner, estima que el mercado de Software de Certificados Digitales y de Servicios de CA experimentará un índice de crecimiento anual compuesto del 80% entre 1998 y el 2002."*

2.11 COMPONENTES DE UNA PKI

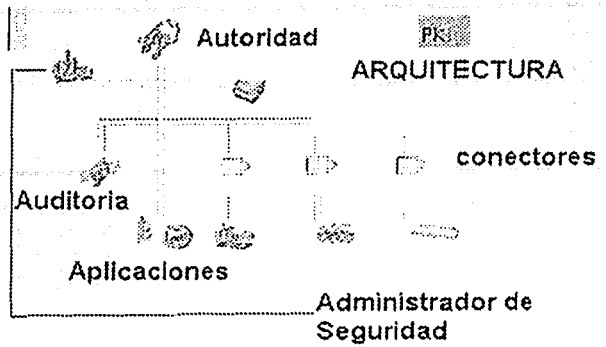
Una Infraestructura de llave Pública es una combinación de productos de hardware y software, políticas y procedimientos. Ofrece la seguridad básica requerida para llevar a cabo negocios electrónicos de forma que los usuarios, que no se conocen entre sí, o están muy alejados entre sí, pueden comunicarse con seguridad a través de una cadena de confianza. La PKI se basa en identidades digitales conocidas como "certificados digitales", que actúan como "pasaportes electrónicos", y vinculan la firma digital del usuario a su clave pública.

2.12 COMPONENTES DE LA PKI:



- Una Política de Seguridad
- Autoridad de Certificación (CA)
- Autoridad de Registro (RA)
- Sistema de Distribución de Certificados
- Aplicaciones habilitadas por PKI

TESIS CON
FALLA DE ORIGEN



2.13 Política de Seguridad

Una política de seguridad establece y define la dirección de máximo nivel de una organización sobre seguridad de información, así como los procesos y principios para el uso de la criptografía. Por lo general, incluye declaraciones sobre cómo gestionará la empresa las claves y la información valiosa, y establecerá el nivel de control requerido para afrontar los niveles de riesgo.

2.14 Declaración de Práctica de Certificados (CPS)

Algunos sistemas de PKI se gestionan mediante Autorizadores de Certificados Comerciales (CCA) o Terceras Partes Seguras, y, por lo tanto, requieren un CPS. Éste es un documento en el que se detallan los procedimientos operativos sobre cómo ejecutar la política de seguridad y cómo aplicarla en la práctica. Por lo general, incluye definiciones sobre cómo se construyen y operan los CA, cómo se emiten, aceptan y revocan certificados, y cómo se generan, registran y certifican las claves, dónde se almacenan y cómo se ponen a disposición de los usuarios.

2.15 Autoridad de Certificación (CA)

El sistema de CA es la base de confianza de una PKI, ya que gestiona los certificados de clave pública durante toda su vida. La CA:

- Emite certificados vinculando la identidad de un usuario o sistema a una clave pública con una firma digital
- Programa las fechas en la que expiran los certificados
- Garantiza que los certificados se revocan cuando sea necesario, publicando Listados de Revocación de Certificados (CRL).

Al implantar una PKI, una organización puede manejar su propio sistema de CA, o emplear el servicio de CA de un CA Comercial o Tercera Parte Segura.

2.16 Autoridad de Registro (RA)

TESIS CON
FALLA DE ORIGEN

Una RA proporciona el interfaz entre el usuario y el CA. Captura y autentifica la identidad de los usuarios y entrega la solicitud de certificado al CA. La calidad de este proceso de autentificación establece el nivel de confianza que puede otorgarse a los certificados.

2.17 Sistema de Distribución de Certificados

Los certificados se pueden distribuir de varias formas, dependiendo de la estructura del entorno PKI. Se pueden distribuir, por ejemplo, por los propios usuarios o a través de un servicio de directorios. Puede que ya exista un servidor de directorios dentro de una organización, o se pude suministrar uno como parte de la solución PKI.

2.18 Aplicaciones habilitadas por PKI

Una PKI es un medio para conseguir un fin, que proporciona el marco de seguridad con el que se pueden distribuir las aplicaciones habilitadas por PKI para obtener ventajas finales.

Algunos ejemplos de aplicaciones pueden ser:

- Comunicaciones entre servidores y buscadores de Internet
- Correo electrónico
- Intercambio Electrónico de Datos (EDI)
- Transacciones con tarjeta de crédito en Internet
- Redes Privadas Virtuales (VPN)

TESIS CON
FALLA DE ORIGEN

2.19 PASOS PARA EVALUAR SOLUCIONES DE PKI:

2.19.1 Flexibilidad

Es esencial que todos los componentes de una PKI sean compatibles, ya que es improbable que todos provengan de un único proveedor. Por ejemplo, el CA deberá poderse interconectar con los sistemas existentes, como servidores de directorios instalados previamente en la organización. La PKI debe emplear interfaces estándar abiertos como LDAP y X.500 (DAP) para garantizar que puede funcionar con todos los servidores de directorios que cumplen los estándares.

Asimismo, muchas organizaciones se han decantado por proveedores de tarjetas inteligentes y módulos de seguridad de hardware (HSM). También en este caso, los interfaces estándar, como el PKCS#11 (Cryptoki), la PKI tiene la flexibilidad necesaria para funcionar con una amplia gama de señales de seguridad.

En muchos sistemas de PKI, es necesario hacer el registro cara a cara, para proporcionar el nivel necesario de confianza. Sin embargo, tal vez esto no sea siempre apropiado, por lo que es posible que se necesite un registro desde un punto remoto. La PKI debe permitir a los usuarios solicitar certificados a través del correo electrónico, empleando un buscador web estándar, o automáticamente a través de dispositivos de comunicación en red para VPN

Para algunas implementaciones a gran escala, los certificados deben emitirse por lotes, por ejemplo, para tarjetas de banco o documentos nacionales de identidad. En esos

casos, la PKI exige la flexibilidad de un proceso automatizado de RA vinculado a la base de datos de tarjetas.

2.19.2 Sencillez de manejo

Aunque los principios con los que funciona un sistema de PKI pueden ser complicados, su gestión no debe serlo. La PKI debe permitir a personal no especializado, como administradores comerciales, manejarla con confianza. Estos operadores no tienen por qué entender las complicaciones de los algoritmos criptográficos, claves y firmas. Debe resultar tan fácil como pulsar iconos y dejar a la aplicación de software que se encargue del resto. El interfaz debe ser gráfico e intuitivo, ayudando a la tarea de gestión, en lugar de dificultarla con complejos registros de la base de datos.

La flexibilidad y sencillez de manejo aportarán un gran rendimiento a la inversión en un sistema de PKI, ya que repercuten en aspectos como la formación, el mantenimiento, la configuración del sistema, la integración y, por supuesto, el futuro crecimiento en el número de usuarios. Estos aspectos pueden elevar el costo de una PKI muy por encima del costo inicial de implementación y, por lo tanto, se deben estudiar atentamente en la fase de evaluación.

Soporte para la Política de Seguridad de una Organización

La PKI se está convirtiendo en un elemento imprescindible en las estructuras de seguridad de las empresas y todo CA debe ser capaz de reflejar e implantar la política de seguridad de la organización

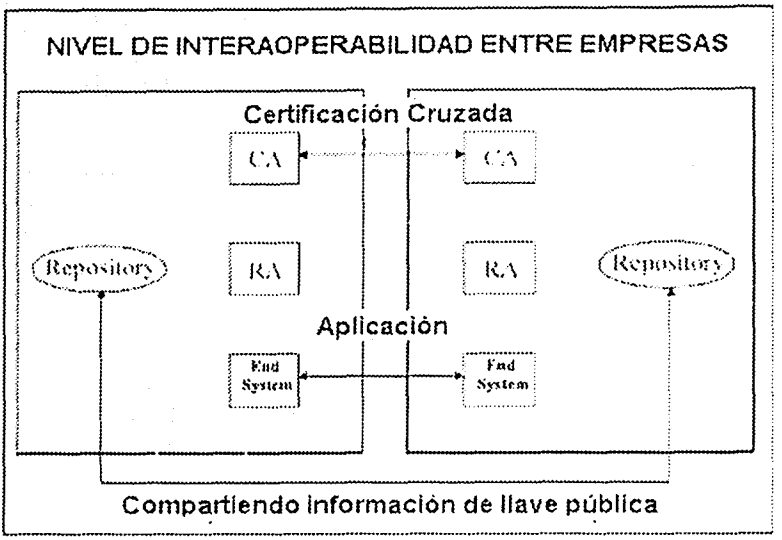
Por este motivo, un sistema de PKI basado en políticas es crítico para garantizar que el proceso de gestión de certificados refleja con precisión los papeles de los Operadores de CA y RA y de los usuarios de certificados. Por ejemplo, el Operador de CA puede decidir delegar la revocación de certificados de usuarios finales en los Operadores de RA, al tiempo que retiene el derecho de revocación de los certificados de los Operadores de RA.

2.19.3 Ampliabilidad

A medida que una organización emplea y depende cada vez más de la PKI, es esencial que dicho sistema PKI pueda ampliarse para adaptarse a su crecimiento. Inicialmente, una PKI sólo puede soportar una sola aplicación. Sin embargo, debe tener la suficiente versatilidad como para soportar más aplicaciones a medida que aparecen en línea.

También debe ser posible añadir componentes de CA y RA adicionales para soportar un número creciente de certificados a medida que crece la PKI. Asimismo, es posible que se necesiten diversos tipos de certificados y mecanismos de registros, a medida que la PKI se amplíe para incluir nuevos servicios.

TESIS CON
FALLA DE ORIGEN



2.19.4 Compatibilidad[4]

La tecnología de PKI aún se encuentra en fase de desarrollo y resulta difícil predecir con certeza los usos y requisitos futuros para los sistemas de PKI. Los estándares para PKI aún están evolucionando y, en algunos casos, no existen todavía.

Por lo tanto, para proteger la inversión y evitar futuros problemas de compatibilidad, es fundamental crear una PKI que sea totalmente abierta y construida para cumplir los estándares comerciales más comunes y avanzados. Esto debe estudiarse en la fase de diseño, para garantizar una integración armoniosa con el resto de la infraestructura de IT.

2.19.5 La Seguridad del CA / RA

Los sistemas de CA / RA se encuentran en el núcleo de cualquier PKI. La seguridad de estos sistemas es de primordial importancia y si se pone en entredicho, correrá peligro toda la solución PKI

2.19.6 El PKI debe garantizar lo siguiente:

La clave privada del CA debe situarse en un módulo de seguridad a prueba de manipulaciones y se deben realizar copias de seguridad para la recuperación de desastres

El acceso a la CA y a la RA debe vigilarse muy atentamente, por ejemplo, empleando tarjetas inteligentes para garantizar una mejor autentificación de usuarios.

TESIS CON
FALLA DE ORIGEN

[4] http //www entrust com/entrust/features.htm

También debe ser posible configurar el proceso de gestión de certificados de forma que un operador deba autorizar las solicitudes de certificación.

Todas las solicitudes de certificación deben firmarse digitalmente mediante una fuerte autentificación criptográfica para detectar e impedir a los piratas informáticos que generen deliberadamente certificados falsos. Todas las acciones llevadas a cabo por el sistema de CA / RA deben registrarse en un registro de auditoria seguro, en el que cada entrada tenga asignada una fecha / hora y reciba una firma, para asegurar que las entradas no pueden falsificarse.

La CA debe ser aprobada y verificada por un organismo independiente, por ejemplo al menos hasta ITSEC E2, pero preferiblemente hasta ITSEC E3 (Criterios de Evaluación de Seguridad de Tecnología de la Información). ITSEC es un estándar global reconocido para la medición de productos de seguridad y la evaluación E3 representa el mayor nivel de seguridad comercial actual.

2.19.7 Las mejores Soluciones de PKI

"El comercio electrónico está creando una sensación creciente de urgencia y demanda de soluciones de seguridad mediante "clave pública" altamente ampliables. Las compañías Fortune 1000 están invirtiendo en tecnología y servicios de PKI para soportar redes privadas virtuales, mensajes seguros, acceso inmediato, autentificación de socios en extranets, y servidores Web seguros para el comercio seguro." [5]

TESIS CON
FALLA DE ORIGEN

[5] Fuente: revista Fortune, Junio 2002, http://www.fortune.com/companies/

2.20 PROCESO DE LA FIRMA DIGITAL

He seleccionado un producto único en el mercado de firma digital, True Pass (software de la compañía Entrust Technologies), el cual puede hacer que se pueda utilizar la firma digital en cualquier máquina y ofrece un esquema sencillo para el usuario y con la facilidad del Roaming, es decir, se puede utilizar en cualquier computadora y en cualquier parte del mundo con solo estar en un navegador conectado a Internet y haciendo una llamada a la pagina principal donde el servidor, quien posee las llaves y dialoga con el web server quien sirve de intermediario en el intercambio entre el navegador (ya sea Nestcape Navigator o Internet Explorer).

2.20.1 SIMBOLOGIA

NAVEGADORES

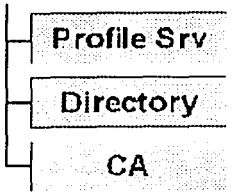
Conexión SSL (Secure Socket Layer) en el navegador.

Firewall

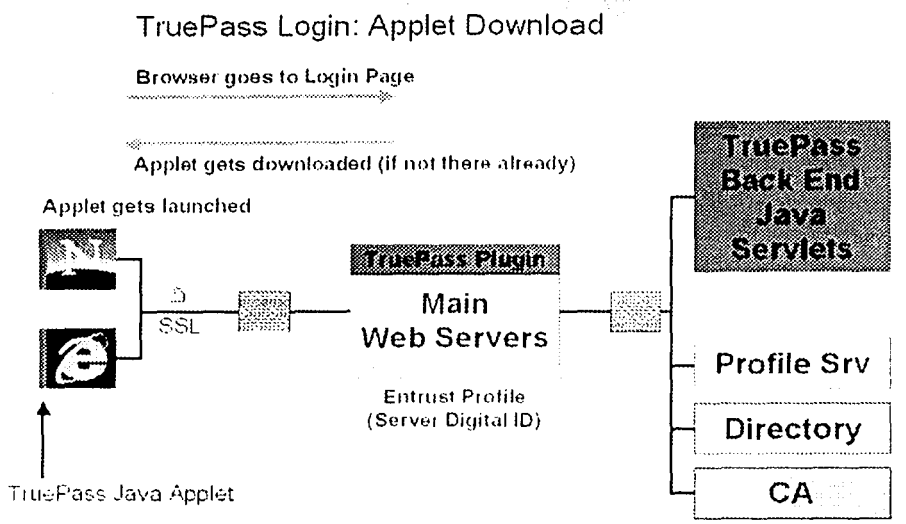
Servidor Web (donde interactua TruePass)

El Back End de TruePass donde se concentran los servlets de Java

TESIS CON
FALLA DE ORIGEN



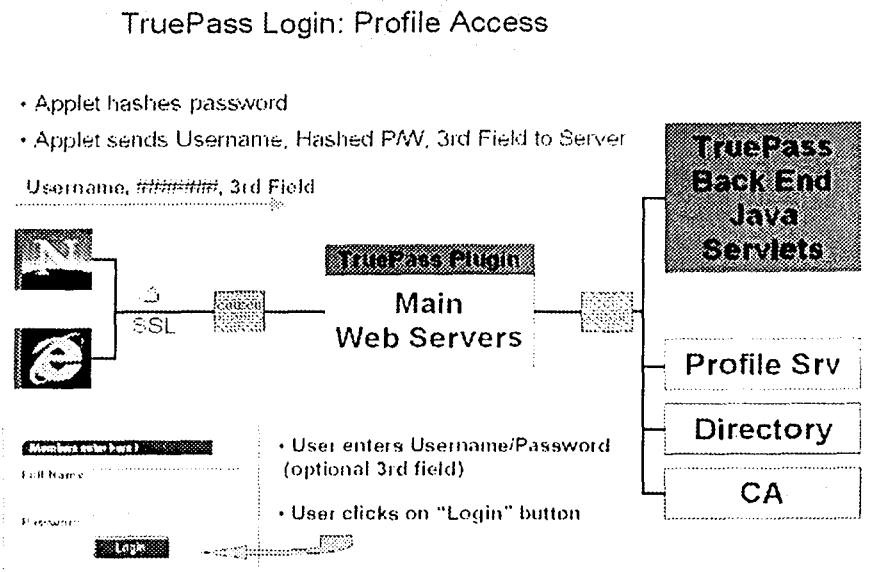
Aquí se encuentra el PKI con sus tres características indivisibles; el Profile Server, el Directorio y la CA (Autoridad Certificadora)



2.20.2 Primer paso: Definición.

En el presente esquema tenemos un servidor donde se encuentra el PKI (compuesto por; Profile Server, Directory y CA) y la aplicación que se llama True Pass, el cual es un software que permite hacer uso de la Firma Digital el cual puede ser usado como Roaming, es decir, en cualquier computadora que este conectada a Internet y cuente con un navegador, ya sea Netscape o Internet Explorer. El navegador hace una llamada al servidor quien revisa que exista dicha firma digital y que sea correcto, previamente manda applets de java al navegador para que se cree un canal seguro de comunicación por medio del cifrado

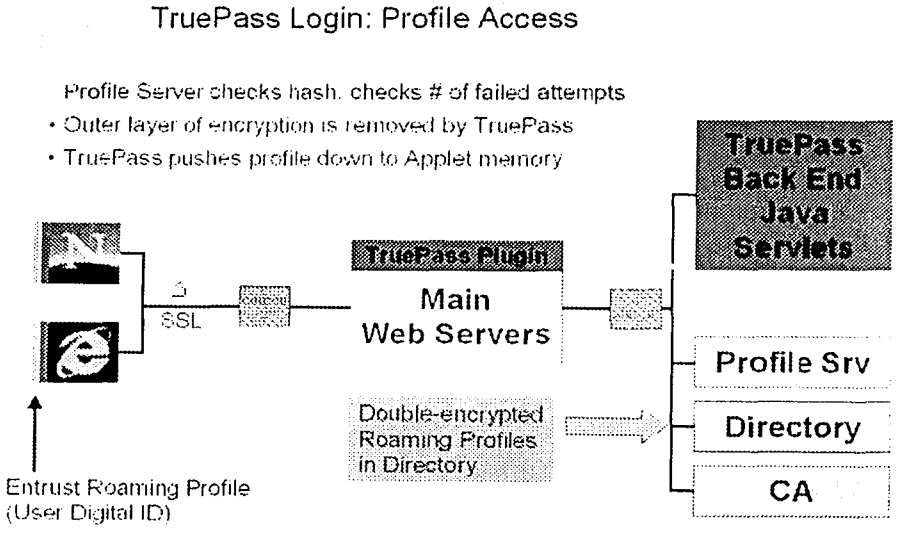
TESIS CON
FALLA DE ORIGEN



2.20.3 Segundo paso: password.

El usuario escribe su nombre y su password el cual nunca sale de la computadora del usuario, sino que es un algoritmo de hash el que viaja por Internet aumentando y modificando 24 veces el pasword de tal forma que no viaje por la red de manera plana, sino encriptada.

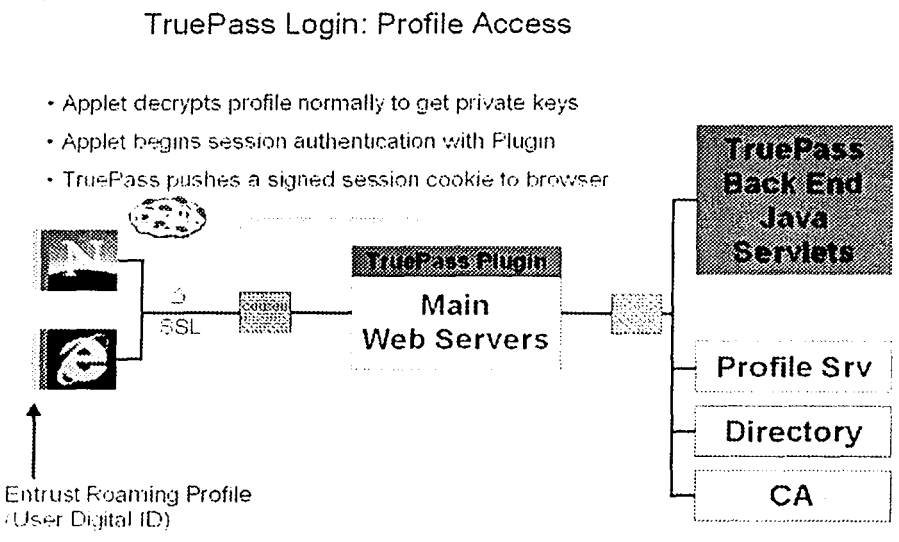
TESIS CON
FALLA DE ORIGEN



2.20.4 Tercer paso: Algoritomo de hash

El servidor revisa el algoritmo de hash y se revisa en el servidor, para mas tarde dar la respuesta de acceso a la transacción.

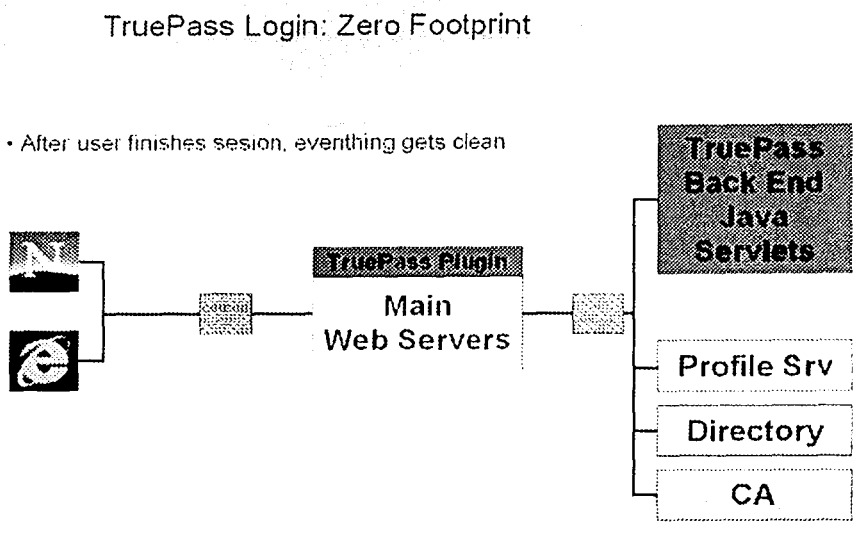
TESIS CON
FALLA DE ORIGEN



2.20.5 Cuarto paso: Envío de la información.

el applet envia una sesión de autentificación con un plugin y True Pass manda una cookie al navegador.

TESIS CON
FALLA DE ORIGEN



2.20.6 Quinto paso: cierre de la sesión.

Finalmente el usuario cierra la sesión y todo se remueve del navegador quedando completamente limpio y sin rastros de la sesión.

Para finalizar el presente capitulo podemos confirmar que el comercio electrónico es ya una realidad. Con su crecimiento acelerando actualmente a una velocidad vertiginosa, la PKI pronto será tan habitual que las organizaciones emitirán certificados digitales y tarjetas inteligentes como práctica habitual.

Por lo tanto, a la hora de evaluar un sistema PKI potencial, es fundamental realizar un estudio minucioso para tomar decisiones fundamentadas para garantizar que se han cumplido los requisitos fundamentales.

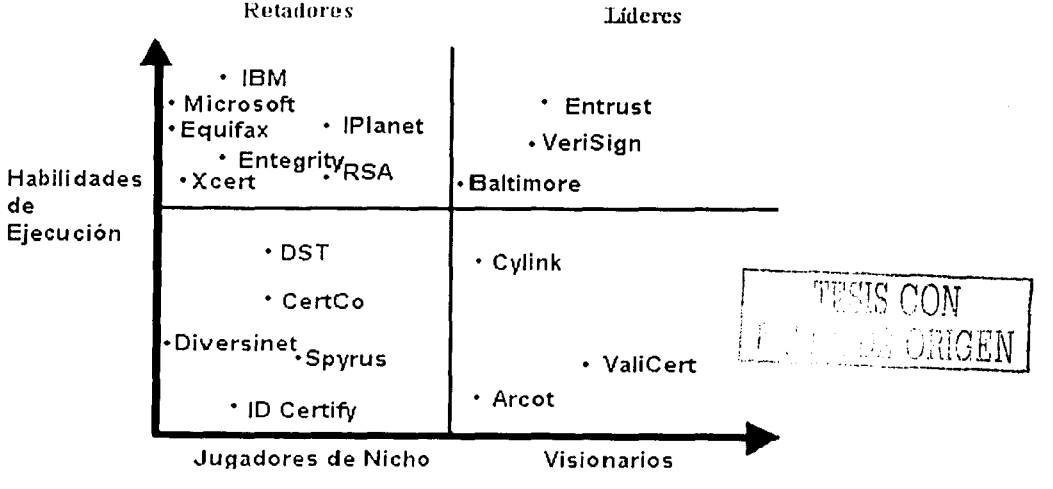
Para triunfar en el mundo del comercio electrónico, las organizaciones deben volver a diseñar sus prácticas de trabajo, e implantar sistemas para llevar a cabo actividades comerciales electrónicas con total seguridad, con lo cual se adoptará la tecnología del futuro en la actualidad.

TESIS CON
FALLA DE ORIGEN

2.21 ANÁLISIS DE PROVEEDORES DE TECNOLOGÍA

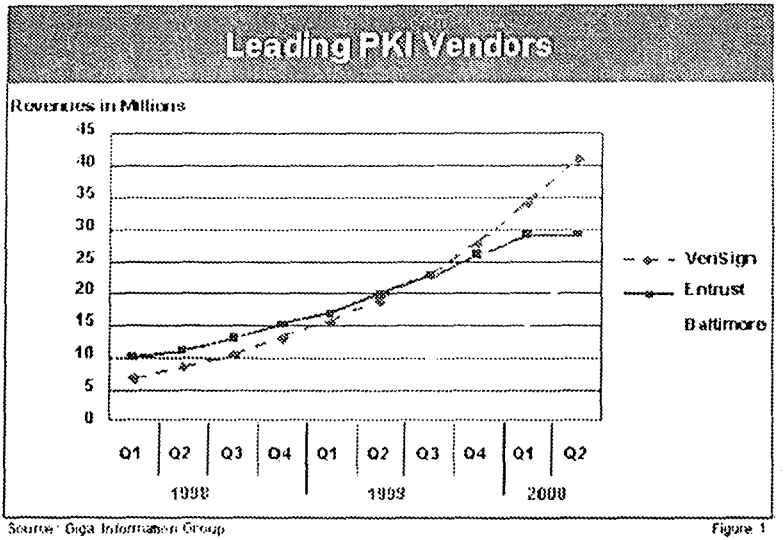
INDICADORES CLAVE	ENTRUST	VERISIGN	BALTIMORE	SPYRUS
Integración	✓	✓	✓	✓
Jerarquía	✓	✓	✓	✗
Certificación Cruzada	✓	✓	✓	✗
Roaming	✓	✗	✗	✗
Seguridad para formato WAP	✓	✗	✓	✗
Recuperación de Llaves	✓	✗	✗	✗
Escalabilidad	✓	✗	✗	✗

2.22 Los cuadrantes de Gartner



Fuente: Gartner Research

TESIS CON ORIGEN



Source: Giga Information Group

Figure 1

TESIS CON
FALLA DE ORIGEN

CAPITULO TERCERO

ESTÁNDARES DE SEGURIDAD

En el presente capitulo me adentrare a mostrar cuales son los principales estándares de seguridad en el ámbito mundial, los cuales debe cumplir México o cualquier otro país que pretenda ingresar a realizar comercio electrónico seguro mediante la firma digital con el PKI en los mercados internacionales.

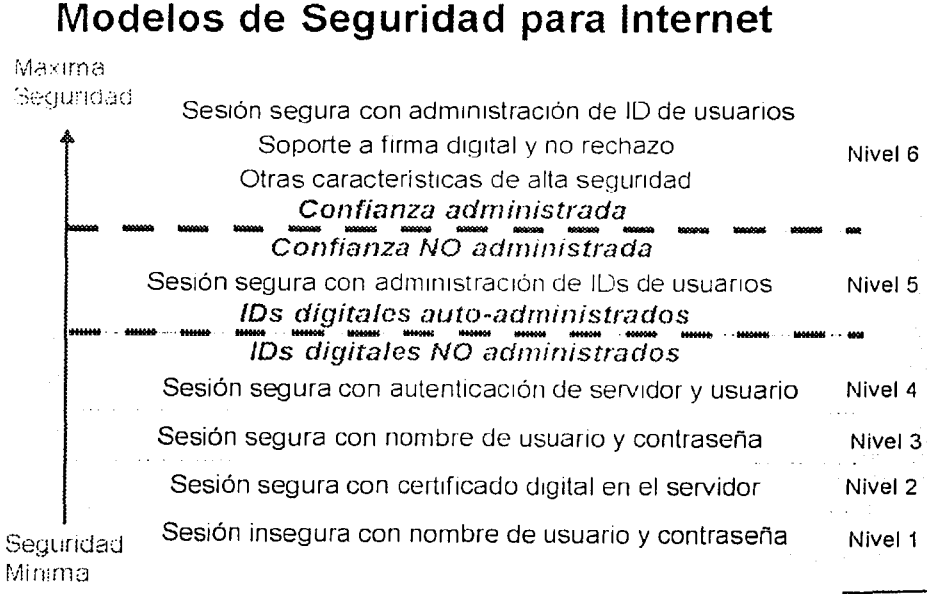


FIGURA 1.MODELOS DE SEGURIDAD PARA INTERNET

TESIS CON
FALLA DE ORIGEN

3.1 INTRODUCCIÓN A LOS ESTANDARES Y LA INTEROPERATIBILIDAD

Lo que provee la interoperatibilidad es el suporte de los estándares de la industria a través de la administración de llaves y certificados mediante múltiples aplicaciones y plataformas. Este soporte facilita la relación de trabajo entre las redes existentes y los productos. Como resultado, las empresas pueden implementar la infraestructura de la seguridad la cual soporta la interoperatibilidad entre la empresa y las organizaciones externas a ella.

La meta de la Infraestructura de Llave Pública (de sus siglas en inglés, *Public-Key Infrastructure* y con las siglas abreviadas, *PKI*), es la de proveer el mejor tipo de Infraestructura para establecer la interoperativilidad entre los diferentes proveedores del PKI's haciendo uso al máximo de estos estándares abiertos. Existen las siguientes organizaciones las cuales emiten estándares mundiales y se obtiene con ello, los siguientes beneficios:

- Internet Engineering Task Force (IETF) Working Groups, (including PKIX Working Group, Common Authentication Technologies Group, S/MIME, LDAPExt group, entre otros).
- Compañías las cuales elaboran este tipo de tecnologia podemos mencionar a Entrust Technologies, Microsoft, IBM, VeriSign, Baltimore Technologies, RSA-Security, Spyrus y LJL entre otros.
- Ofreciendo estándares basados en herramientas y APIs sin costo alguno para construir aplicaciones de PKI las cuales podrán trabajar con múltiples PKI y Autoridades Certificadoras (de sus siglas en inglés, Certification Authority, CA) ofreciendo productos y servicios a otros fabricantes.
- Estableciendo una red confiable a nivel mundial lo cual proveerá una arquitectura que permitirá a las CA s de múltiples fabricantes tener una interoperatibilidad como lo son Entrust Technologies, Baltimore Technologies, Microsoft, Netscape, VeriSign entre otros.

3.2 Compendio de los Estándares Abiertos

Los estándares que surgen y se convierten en los estándares de la industria cuando ellos llegan a la madurez se pueden mencionar los siguientes: IETF's PKIX, NIST's MISPC, Microsoft's CryptoAPI, entre otros. El PKI es un estándar abierto, un producto inter operable el cual debe soportar los estándares impuestos por la industria los cuales son S/MIME, X 509V3, PKIX, PKCS, GSS-API, IDUP-GSS-API, IPSec y muchos otros. En esta sección encontraremos un repaso breve de los estándares mas reconocidos por la industria y los protocolos.

La siguiente tabla muestra una lista de estándares y protocolos mas usados por la industria:

TESIS CON
FALLA DE ORIGEN

Estándar de la Industria	Descripción
X 509 v 3	Los certificados X 509 v3 y sus extensiones X 509 v3 Adicionalmente, se debe incorporar una arquitectura en el certificado para que se provea la flexibilidad para adecuar al usuario X 509 v3 para muchos servicios y dispositivos Sería recomendable que este certificado
LDAP	Es un directorio de servicios el cual viene de sus siglas en ingles *Lightweight Directory Access Protocol (LDAP)* el cual provee muchos directorios del tipo X 500
PKCS **(PKCS 1, 3, 5, 7, 8, 10, 11)**	***PKCS standards*** • **PKCS#1** - firma digital RSA y llave de transferencia de acuerdo con el PKCS#1, • **PKCS#3** - Acuerdo de llaves Diffie-Hellman mediante el PKCS#3, • **PKCS#5** Almacenamiento privado basado en PKCS#5 and PKCS#8, • **PKCS#7** – Seguridad de archivos de acuerdo con el PKCS#7 • **PKCS#10** - Certificado de protocolo de peticion soportado en la industria de los navegadores web browsers de acuerdo con el PKCS#10, • **PKCS#11** - CRYPTOKI interfase de hardware criptográfico que soporta los mas comunes son los "tokens"
PKIX	El protocolo de intercambio seguro el cual es la base de los IETF's PKIX-CMP (de sus siglas en inglés, *Certificate Management Protocol*)
Algoritmos de Encripción	Podemos mencionar los siguientes CAST-128 CAST-80 y CAST-64, DES, Triple- DES, RC2-128 y RC2-40
Algoritmos para Firma	***RSA-1024 y DSA-1024***
Algoritmos de Hashing	***SHA-1 y MD5.***
S/MIME	El protocolo S/MIME es un estandar de la industria el cual es usado para transacciones de e-mail seguras
IPSEC	El protocolo IPSEC provee un alto nivel para las APIs donde los desarrolladores tienen la facultar de habilitar sus dispositivos IPSEC para tomar ventaja de los servicios de administración de las llaves y certificados
SSL	Es un proceso que provee autentificación para los certificados web basados en la autentificación de un servidor web con un browser o navegador La version actual es SSL V3 la cual implementa una autentificación tanto del lado del browser como la del servidor mediante los sockets SSL
Transacciones Electrónicas Seguras ***Secure Electronic Transaction (SET)***	Los certificados X 509 v3 se utilizan para el protocolo SET (de sus siglas en inglés, Secure Electronic Transaction)
FIPS 140-1	La validación FIPS-140 provee la seguridad de que el diseño del crypto kernal, incluyendo el Número Generado Secuencial (de sus siglas en inglés, the Random Number Generator (RNG) el cual es utilizado, ha sido provisto y acreditado por una tercera parte La Validacion al FIPS 140 es requerida para todos los productos criptográficos usados por el gobierno de los Estados Unidos de América

[7] Un Token es un dispositivo de hardware el cual habilita funciones con la computadora, por ejemplo, las tarjetas inteligentes o de sus siglas en ingles, "smart cards" se consideran un token pues interactuan con un sistema de verificación de acceso de seguridad ademas del password tradicional lo que hace mas difícil al duplicar el acceso de la entrada a dicho sistema

Para realizar operaciones de interoperatibilidad entre el PKI y los productos de la CA además de los proveedores de servicios, podemos tener iniciativas las cuales proveen posteriormente los estándares en la industria, los cuales construyen la interoperatibilidad y el soporte para la participación y cooperación entre el Mercado.

3.2.1 Iniciativas a nivel mundial

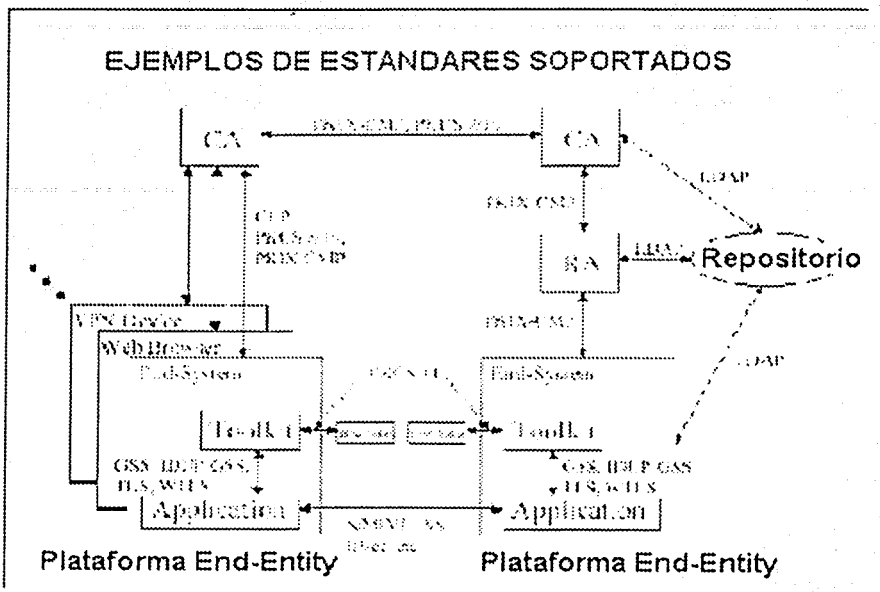
El uso de las redes con la facilidad del comercio electrónico y de comunicación por medio del PKI encontramos a los líderes mundiales en el e-commerce incluyendo a ABAecom, Bell Emergis/MPACT Immedia, BNL Multiservizi, Digital Signature Trust Co., Entrust Technologies, Japan, SECOM Co. Ltd., el Royal Mail, PriceWaterhouseCoopers y Deloitte & Touche los cuales participan en estas iniciativas. Estas organizaciones ofrecen productos y fundamentos para hacer de la confianza en las redes algo flexible y abierto permitiendo a las CAs de numerosas empresas como Entrust Technologies, Baltimore Technologies, Microsoft, Netscape, VeriSign y otros la habilidad para interactuar entre ellos mismos.

3.2.2 Estrategia de apertura de VPN

Esta estrategia incluye englobar todas las aplicaciones para los productos los cuales incluirán el soporte necesario para todos los dispositivos de VPN los cuales se emplean en la industria como un estándar como IPSec, IKE, PKCS #7 y PKCS #10, y Cisco's Certificate Enrollment Protocol (CEP).

Esto resulta en una solución sencilla basada en la seguridad de los certificados para todos los dispositivos de VPN disponibles en el mercado incluyendo routers, firewalls y VPN gateways. Los Productos de mas de 18 compañías también serán capaces de operar con los productos PKI para VPN. Estos incluyen 3Com, Axent/Raptor, Bay Networks, Cisco Systems, Lucent Technologies™, Check Point Software Technologies Ltd., Hewlett-Packard, Hi/fn, IRE, SLM Software Inc. (formerly Milkyway Networks), Network Associates, Nortel Networks, Radguard, Red Creek, TimeStep, Shiva, V-ONE y VPNet

TESIS CON
FALLA DE ORIGEN



En la gráfica anterior se describen los estándares soportados en cada una de los componentes del PKI, estas son:

- Para la CA (CERTIFICATION AUTHORITY)
  PKIX-CMP, PKS7/10, PKIX-CMP
- Para el REPOSITORIO
  LDAP
- De la CA a la RA
  PKIX-CMP
- De CA a EndSystem
  CFP, PKCS 7710, PKIX-CMP
- De TOOLKIT a la APLICACIÓN
  GSS, IDUP-GSS, TLS, WTLS
- De APLICACIÓN a APLICACIÓN
  S/MIME, SSL, IPsec, entre otros.
- De TOOLKIT a TOOLKIT
  PKS II

TESIS CON
FALLA DE ORIGEN

3.3 ORGANISMOS INTERNACIONALES PARA EL CUMPLIMIENTO DE ESTÁNDARES

NOMBRE DEL ORGANISMO INTERNACIONAL	FUENTE
El Open Group (formalmente OSF y X/Open)	http://www.opengroup.org
ISO/IEC JTC1/SC21/WG4 y ITU-T SG7 Directory	http://www.iso.org
ISO/IEC JTC1/SC27/WG2 Information Technology Security Techniques	
ANSI X9F1 Cryptographic Algorithms for the Financial Industry	http://www.ansi.org
ANSI X9F3 Cryptographic Protocols for the Financial Industry	
IEEE P1363	http://grouper.ieee.org/groups/1363/index.html
Federal PKI Technical Working Group (TWG)	http://csrc.nist.gov/pki/twg
MISPCv2 (Minimum Interoperability Specification for PKI Components Version 2) Working Group	
PKCS Technical Working Groups	http://www.rsasecurity.com/rsalabs/pkcs
Secure Digital Music Initiative (SDMI)	http://www.sdmiorg
The Wireless Application Protocol (WAP) y Wireless Security Group(WSG)	http://www.wapforum.org
Several Internet Engineering Task Force (IETF)	http://www.ietg.org

- Grupos de trabajo incluyendo
  - Public-Key Infrastructure X.509-based (PKIX);
  - Common Authentication Technologies (CAT);
  - Secure/Multi-purpose Internet Mail Extensions (S/MIME);
  - XML Digital Signature (XMLDigSig); y
  - LDAP Extensions (LDAPExt).

3.4 LISTA DE LOS ESTÁNDARES DE LA INDUSTRIA [7]

Nota. Esta lista se encuentra en inglés debido a que en todo el mundo se les conoce en este idioma y el traducirlo implicaría cometer un error de interpretación.

- OpenGroup (formerly OSF and X/Open).
- ISO/IEC JTC1/SC33 and ITU-T SG7 Directory.
- ISO/IEC JTC1/SC27/WG2 Information Technology Security Techniques.
- ISO TC68 (Banking)
- ANSI X9F1 Cryptographic Techniques for Financial Industry.
- IEEE P1363
- NIST CRADA MISPC (Minimum Interoperability Specification for PKI Components)
- PKCS#11 Technical Working Group.
- Electronic Messaging Association (EMA).

TESIS CON
FALLA DE ORIGEN

Fuente: www.entrust.com

- Internet Engineering Task Force (IETF) working groups incluyendo: PKIX group (Public-Key Infrastructure, X.509-based). CAT group (Common Authentication Technologies), S/MIME, LDAPExt group, y otros.
- American Bar Association.
- National Automated Clearing House Association (NACHA) Working Group on Authentication and Network of Trust.
- International Law and Policy Forum.
- National Association of State Information Resource Executives (NASIRE).

Reconociendo que muchos de los aspectos de la seguridad en redes aun no se encuentran estandarizados, se pueden consultar estos foros para crear iniciativas para la creación de estándares emergentes, mientras estos maduran, incluyendo a IETF's PKIX, NIST's MISPC, Microsoft's CryptoAPI, entre otros.

3.5 RESUMEN DE ESTANDARES

En este punto, citaré algunos ejemplos de estándares que se manejan en el mundo:

3.5.1 Algoritmos de Encripción Simetrica (*Symmetric Encryption Algorithms*)

- U.S. Data Encryption Standard (DES) de acuerdo con el U.S. FIPS PUB 46-2 y el ANSI X3.92
- CAST de acuerdo al RFC 2144 (64-bit, 80-bit, y variaciones de 128-bits)
- Triple-DES de acuerdo al ANSI X9.52 (3-key una variante del tamaño de la llave de 168-bits)
- RC de acuerdo al RFC 2268 (de 40-bit y variaciones de 128-bits);
- IDEA como lista en la ISO/IEC 9979 Registrados como algoritmos criptográficos (128-bit)
- Nota: DES, CAST, Triple-DES, RC2 y la encripción IDEA usan el modo de operación CBC de acuerdo a los Estados Unidos (U.S.)
- FIPS PUB 81, ANSI X3.106 y ISO/IEC 10116.

3.5.2 Algoritmos de la Firma Digital (*Digital Signature Algorithms*)

- RSA de acuerdo al estándar Public Key Cryptographic (PKCS) especifico PKCS#1 Versión 2.0, ANSI
- X9.31, IEEE P1363, ISO/IEC 14888-3 y U.S. FIPS PUB 186-2 (de 1024-bit y 2048-bit)
- DSA de acuerdo al estándar de Firma Digital, U.S. FIPS PUB 186-2, ANSI X9.30 Part 1, IEEE P1363
- ISO/IEC 14888-3 (1024-bit)
- ECDSA de acuerdo con ANSI X9.62, IEEE P1363, ISO/IEC 14888-3 y U.S. FIPS PUB 186-2 (192-bit)

3.5.3 Funciones de un solo sentido de Hash (*One-Way Hash Functions*)

- SHA-1 de acuerdo a los Estados Unidos FIPS PUB 180-1 y ANSI X9.30 Parte 2
- MD5 Message-Digest algorithm de acuerdo con RFC 1321
- MD2 Message-Digest algorithm de acuerdo con RFC 1319
- RIPEMD-160 de acuerdo con ISO/IEC 10118-3:1998

3.5.4 Algoritmos de intercambio de llaves (*Key Exchange Algorithms*)

- RSA key transfer de acuerdo con RFC 1421 y RFC 1423 (PEM), PKCS#1 Versiones 2.0, y IEEE P1363
- Diffie-Hellman key agreement de acuerdo con PKCS#3
- Mecanismo simple de autenticación de llave pública Public-Key GSS-API (SPKM) y acuerdo de llave (key agreement) de acuerdo con RFC 2025,
- ISO/IEC 9798-3 y U.S. FIPS PUB 196

3.5.5 Técnicas simétricas integrales (*Symmetric Integrity Techniques*)

- MAC de acuerdo con U.S. FIPS PUB 113 (for DES-MAC) y X9.19
- HMAC de acuerdo con RFC 2104

3.5.6 Psuedo Random Number Generator

- Psuedo random number generator de acuerdo con ANSI X9.17

3.5.7 Certificados para la revocación de listas (*Certificate Revocation Lists (CRLs)*)

- Versión 3 public-key certificates and Versión 2 CRLs de acuerdo con ITU-T X.509 y de las recomendaciones ISO/IEC 9594-8 (Versión 1997)
- Versión 3 del certificado de llave pública y extensiones de la Versión 2 CRL de acuerdo con el RFC 2459
- Versión 3 del certificado de llave pública y extensiones de la Versión 2 de CRLs de acuerdo con los estándares "de-facto" para Web browsers (navegadores) y servidores"
- WTLSCertificate de acuerdo con WAP WTLS Versión 1.1.
- identificadores del algoritmo RSA y los formatos de llave pública de acuerdo con el RFC 1422, el 1423 (PEM) y el PKCS#1

3.5.8 Formatos para cerrar Archivos (*File Envelope Formats*)

- RFC 1421 (PEM) Formato de archive estándar basado en Internet
- PKCS#7 Versión 1.5 basada en el RFC 2315 y la versión 2 de S/MIME basadas en el RFC 2311

3.5.9 Formatos para sesiones seguras (*Secure Session Formats*)

- Implementación del mecanismo de Llave pública On-line GSS-API usando SPKM de acuerdo con Internet la entidad autentificadora RFC 2025 y SPKM de acuerdo con el FIPS 196

3.5.10 Repositorios de datos (*Repositories*)

- LDAP Versión 2 de acuerdo a lo acordado en el RFC 1777 y RFC 2559
- LDAP Versión 3 de acuerdo a lo acordado en el RFC 2251-2256

3.5.11 Almacenamiento de llaves privadas (*Private Key Storage*)

- Almacenamiento de llave privada, (*Private key storage)* de acuerdo a los estándares PKCS#5 y PKCS#8

3.5.12 Administración de Certificados (*Certificate Management*)

- Protocolo seguro de intercambio de sus siglas en ingles; *Secure Exchange Protocol (SEP)*, utilizando los estándares *Generic Upper Layers Security (GULS)* ITU-T Recs X.830, X.831, X.832 e ISO/IEC 11586-1, 11586-2, 11586-3 (SEP continua siendo soportado solamente como compatibilidad del tipo backward)

- PKIX-CMP de acuerdo al RFC 2510 y PKIX-CRMF de acuerdo con RFC 2511 PKCS 7/10 (basado para soluciones de clientes Web y soluciones VPN [8])
- Certificados Cisco Enrollment Protocol (CEP) (para soluciones VPN)

3.5.13 Interfaces de aplicaciones de programación (*Application Programming Interfaces (APIs)*)

- Interfase criptográfica de (*Hardware cryptographic interface*) de acuerdo al estándar PKCS#11
- Servicios genéricos de seguridad (Generic Security Services API (GSS-API)) de acuerdo al RFC 1508 y 1509
- IDUP-GSS-API de acuerdo al Internet Draft draft-ietf-cat-idup-gss-08.txt

TESIS CON

TABLA DE ESTANDARES MAS UTILIZADOS

Estándares mas utilizados
ALGORITMOS CRIPTOGRÁFICOS Y ESTÁNDARES
ENCRIPCIÓN
DES (U.S. Data Encryption Standard) de acuerdo a los U.S. FIPS PUB 46-2 y ANSI X3.92
CAST encriptador de bloque de acuerdo con el Internet RFC 2144
Triple-DES de acuerdo con ANSI X9.52
RC2 de acuerdo con el Internet Draft "Una Descripción del Algoritmo de encriptamiento RC2(r)", R. Rivest, 06/24/1997.
Encripción DES, CAST, RC2 y Triple-DES utilizando el modo de operación CBC de acuerdo con el U.S. FIPS PUB 81, ANSI X3.106 y el ISO/IEC 10116
FIRMAS DIGITALES
Firma Digital RSA de acuerdo con PKCS#1.
DSA de acuerdo con el estándar de Firma Digital de U.S. FIPS PUB 186 y ANSI X9.30 (Part 1)
FUNCIONES DE HASH
SHA-1 de acuerdo con U.S. FIPS PUB 180-1 y ANSI X9.30 (Part 2)
Algoritmo MD5 Message-Digest de acuerdo con el Internet RFC 1321
ADMINISTRACIÓN DE LLAVES *(Key Management)*
Transferencia de llaves RSA de acuerdo con el Internet RFC 1421 y 1423 (PEM), y PKCS#1
Acuerdo de llaves de Diffie-Hellman de acuerdo con PKCS#3.
Autentificacion y acuerdo de llaves de acuerdo con el ISO/IEC 9798-3 y US FIPS PUB 196
INTEGRIDAD POR TECNICAS SIMÉTRICAS
Código de autentificación de Mensajes *(Message Authentication Code (MAC))* de acuerdo con el U.S. FIPS PUB 113, ANSI X9.9 y X9.19
GENERACIÓN DE NÚMEROS PSEUDO-RANDOM
de acuerdo con el ANSI X9.17
FORMATOS DE DATOS Y PROTOCOLOS
CERTIFICADOS Y FORMATOS DE LISTAS DE REVOCACIÓN DE CERTIFICADOS
Certificados Versión 3 y extensiones de Certificados de acuerdo con el ITU-T Rec. X.509 (1997) y el estándar comun ISO/IEC 9594-8 (1997)
Certificate Revocation Lists Version 2 and CRL extensions in accordance with ITU-T Rec. X.509 (1997) and common standard ISO/IEC 9594-8 (1997).

[8] Red Privada de datos, de sus siglas en ingles, Virtual Private Network (VPN)

Estándares mas utilizados
Certificate and CRL extensions in accordance with the IETF PKIX-1 profile specification.
Certificate and CRL extensions in accordance with the SET 1.0 specification.
Certificate and CRL profiles in accordance with de-facto standards for web browsers and servers.
RSA algorithm identifiers and public-key formats in accordance with Internet RFC 1422 and 1423 (PEM) and PKCS#1
File Envelope Format
Standard file envelope format based on Internet RFC 1421 (PEM).
Secure file enveloping in accordance with PKCS#7 and S/MIME
Secure Session Format
On-line GSS-API public-key implementation mechanism using Simple Public Key Mechanism (SPKM in accordance with Internet RFC 2025 and SPKM entity authentication in accordance with FIPS 196.
Directory Protocols
LDAP (Lightweight Directory Access Protocol, version 2) in accordance with RFC 1777.
PKI operational protocol in accordance with PKIX-2.

3.6. ISO 17799

La norma ISO 17799 es un estándar de seguridad internacional el cual se le conoce como la piedra angular de seguridad de información dentro de las organizaciones.

En el Mundo de Política de seguridad, las Políticas de Seguridad de Información podrían hacer las siguientes preguntas:

- ¿Las políticas implantadas en la organización son lo bastante comprensivas?
- ¿Están actualizadas?
- ¿Obedece su empresa a la norma ISO17799?
- ¿Como apoya la organización en la efectividad de las políticas?

3.7 BS 7799

La norma BS 7799 es también un estándar de seguridad de uso en el Reino Unido.

Dentro de los estándares de seguridad podemos realizar un proceso de Consultoría para la seguridad en el PKI, del cual esta basado la Firma Digital, de esto hablaremos en el capítulo quinto.

TESIS CON
FALLA DE ORIGEN

CAPITULO CUARTO

LEGISLACIÓN INTERNACIONAL EN MATERIA DE SEGURIDAD INFORMÁTICA

En el presente capitulo nos adentraremos a la legislación en materia de seguridad *(como la firma digital y la regulación de las transacciones comerciales en el WWW)* y comercio electrónico existe actualmente en México, para promover los actos de comercio por medio del WWW.

También podremos comparar otras legislaciones de otros paises los cuales son emitidos por la ONU por medio de la UNCITRAL en materia de la Firma Digital y qué es lo que esta haciendo AMITI, responsable en México de la UNCITRAL en materia de legislar los actos comerciales por medio del WWW.

4.1 LAS PRIMERAS EXPERIENCIAS LEGISLATIVAS EN INTERNET [9]

Enero 1997

Uno de los aspectos decisivos para afianzar el comercio electrónico en Internet está constituido por el entorno jurídico, es decir, las leyes que sirvan de soporte para las transacciones, e introduzcan el concepto de seguridad jurídica en el mercado digital.

Existe una opinión generalizada de que, si ya es complicado, en la vida presencial, demostrar la existencia de una deuda que no se formalizado en un titulo ejecutivo, la dificultad probatoria será mayor en una plataforma contractual en la que el consentimiento se transmite en forma de bits.

Es evidente que los que basan sus compromisos comerciales en el célebre apretón de manos, tendrán que recurrir a la realidad virtual para poder sellar así sus acuerdos a través de Internet.

Pero los que tienen por norma documentar sus transacciones con contratos escritos podrán comprobar en poco tiempo, que la firma digital aporta una eficacia probatoria igual, o incluso superior a la que aporta la firma original en papel.

La firma digital es el instrumento que permitirá, entre otras cosas, determinar de forma fiable si las partes que intervienen en una transacción son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente.

La primera ley que ha regulado los aspectos jurídicos de la firma digital como instrumento probatorio se aprobó el año pasado en Utah. Posteriormente surgieron proyectos

[9] Tomado de la página de RIBAS & RODRIGUEZ Abogados Asociados, en España, http //www.asertel.es/cs/ RIBAS & RODRIGUEZ Abogados Asociados, Ronda Sant Pere, 25 Principal 08010 BARCELONA

legislativos en Georgia, California y Washington. En Europa, el primer país que ha aprobado una Ley sobre la materia ha sido Alemania.

Es evidente que la eficacia de estas leyes radica en su uniformidad, ya que si su contenido difiere en cada estado, será difícil su aplicación a un entorno global como Internet. Por ello, el esfuerzo a realizar a partir de ahora deberá centrarse en la consecución de un modelo supra estatal, que pueda ser implantado de manera uniforme en las leyes nacionales. Tal tarea puede encomendarse a organismos internacionales como UNCITRAL, que ya dispone de experiencia en iniciativas similares en materia de EDI.

4.2 ENTIDADES CERTIFICADORAS

Enero 1997

La emisión de certificados y la creación de claves privadas para firmas digitales acostumbra a depender de una pluralidad de entidades que están jerarquizadas de una manera que las de nivel inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Finalmente, en la cúspide de la pirámide suele hallarse una autoridad certificadora, que puede pertenecer al Estado, y que en el proyecto alemán coincide con el organismo que controla las telecomunicaciones

Las autoridades certificadoras tienen la función de emitir, suspender y revocar certificados, así como dar a conocer la situación actual de un certificado y crear claves privadas. Los certificados indican la autoridad certificadora que lo ha emitido, identifican al firmante del mensaje o transacción, contienen la clave pública del firmante, y contienen a su vez la firma digital de la autoridad certificadora que lo ha emitido

De esta manera, las partes que intervienen en una transacción aportan como credencial los certificados de su correspondiente entidad certificadora. Por ejemplo, la entidad certificadora A da fe de la identidad del usuario A1 cuando éste adquiere un bien al usuario B1, que es a su vez identificado por la entidad certificadora B.

Para llegar a ser una entidad certificadora deberá mediar una solicitud a una autoridad certificadora de nivel superior, que podrá denegar la licencia si el solicitante no ofrece la fiabilidad o los conocimientos necesarios, ni cumple los requisitos establecidos en la ley.

4.3 LEY ALEMANA SOBRE FIRMA DIGITAL

Octubre 1996

La ley alemana está divida en dos partes, un texto principal y una reglamento que desarrolla aspectos concretos de la ley, como el procedimiento de concesión, transferencia y revocación de una licencia de entidad certificadora, así como los deberes de los certificadores, el periodo de validez de los certificados, los métodos de control de los certificados, los requisitos de los componentes técnicos y el procedimiento de examen de los mismos

Un certificado deberá contener obligatoriamente, el nombre del propietario de la firma digital, que deberá estar identificado de forma inequívoca, la clave pública atribuida, el nombre de los algoritmos utilizados, el número del certificado, la fecha de inicio y final de

la validez del certificado, el nombre de la entidad certificadora, información sobre las limitaciones que se hayan establecido para su utilización e información relativa a certificados asociados.

Una entidad certificadora deberá bloquear un certificado en el momento en que compruebe que está basado en información falsa, cuando la entidad cese en su actividad sin que otra entidad la suceda, o cuando reciba la orden de bloqueo de la autoridad certificadora

La entidad certificadora podrá recabar datos personales del afectado, pero sólo directamente del mismo, y con la única finalidad de emitir un certificado. Si el propietario de la firma digital utiliza un seudónimo, la entidad certificadora sólo podrá transmitir datos relativos a su identidad a requerimiento de la autoridad judicial y en los casos establecidos por la ley

También establece un sistema de auditoria que permitirá a la autoridad certificadora inspeccionar los equipos de la entidad, con el fin de comprobar el cumplimiento de los requisitos técnicos y el plan de seguridad exigidos para el desarrollo de dicha actividad.

Dichos requisitos se refieren a los procedimientos de creación, almacenamiento y comprobación de firmas digitales, que deberán permitir la detección inmediata de cualquier uso no autorizado de una firma digital y la alteración del contenido de los datos, mensajes o transacciones que se hayan efectuado con dicha firma.

4.4 COMUNICACIÓN DE LA COMISIÓN EUROPEA SOBRE FIRMA DIGITAL

Octubre 1997

La Comunicación de la Comisión Europea de fecha 8 de octubre de 1997 persigue el fin de sensibilizar a los Estados miembro sobre el creciente uso de Internet como plataforma de comunicación y de comercio, así como de la necesidad de establecer un marco uniforme en materia de cifrado de la información y firma digital.

La Comunicación recuerda que los mensajes en Internet pueden ser interceptados y manipulados, y esta circunstancia puede impedir que se conceda validez a los documentos enviados a través de la red. Las tecnologías de cifrado pueden resolver este problema, ya que constituyen una herramienta esencial para garantizar la seguridad y la fiabilidad de las comunicaciones y transacciones electrónicas

Dos aplicaciones importantes de estas tecnologías son las firmas digitales y el cifrado de mensajes. Varios Estados miembro han anunciado su intención de promulgar leyes específicas relativas a la encriptación, y algunos ya lo han hecho. Pero la divergencia legal y técnica de estas regulaciones podría constituir un serio obstáculo para el Mercado Interior e impedir el desarrollo de nuevas actividades económicas relacionadas con el comercio electrónico

4.4.1 Los objetivos de la Comunicación de la CE

1 El desarrollo de un marco legal que asegure el funcionamiento de los productos y servicios de cifrado en el Mercado Interior.

2. Establecer un marco europeo para las firmas digitales

Esta Comunicación anuncia la intención de la Comisión de proponer una legislación que cubra estos dos objetivos durante el primer semestre de 1998.

4.4.2 Situación actual de la firma electrónica en Europa

El uso de firmas digitales exige el ajuste y la harmonización de diversas áreas. Actualmente, la mayor parte de los problemas se centran en los siguientes puntos:

1. Ausencia de requisitos uniformes para las autoridades de certificación.
2. Ausencia de requisitos uniformes para los productos de firma digital.
3. Ausencia de normas uniformes en materia de responsabilidad.
4. Ausencia de normas uniformes respecto al reconocimiento legal de las firmas digitales y su eficacia probatoria.

La evidente naturaleza transfronteriza de las firmas digitales exige el reconocimiento mutuo de los requisitos legales establecidos en esta materia por cada Estado, con el fin de evitar la fragmentación del comercio electrónico en el Mercado Interior.

Acciones especificas en el campo de las firmas digitales

4.4.3 La Comisión propone la siguiente estrategia:

- Establecer un marco comunitario para las firmas digitales con el fin de que la regulación de cada Estado no genere barreras internas para el comercio electrónico.
- Determinar unos requisitos comunes para las autoridades de certificación en Europa.
- El sistema jurídico de cada Estado debe reconocer y tratar las firmas digitales de manera idéntica a las firmas convencionales
- La interoperabilidad entre diferentes sistemas de cifrado y firma digital es absolutamente necesaria.

4.4.4 DIRECTIVA SOBRE VENTA A DISTANCIA

Junio 1997

El Diario Oficial de las Comunidades Europeas del cuatro de junio de 1997 publicó la Directiva 97/7/CE relativa a la protección de los consumidores en materia de contratos a distancia. El tema ofrece un gran interés en la actualidad, ya que afecta a las operaciones de comercio electrónico que de manera progresiva van realizándose a través de Internet.

Si hasta ahora podía ponerse en duda el carácter de venta a distancia de una transacción efectuada a través del correo electrónico, a partir de la transposición de esta Directiva, los contratos celebrados mediante este tipo de comunicaciones entrarán de lleno en el regimen establecido por la misma

Las principales repercusiones que se derivan de la aplicación de la normativa citada se resumen a continuación:

El consumidor dispondrá de un plazo mínimo de siete días laborables, a partir de la recepción del producto, para rescindir el contrato sin penalización alguna, y sin indicación

de los motivos. El único gasto que podría imputarse al consumidor es el coste directo de la devolución de las mercancías al proveedor.

Quedarán exceptuados del derecho de arrepentimiento los productos que puedan ser reproducidos fácilmente: grabaciones sonoras o de vídeo, programas informáticos, publicaciones periódicas, etc.

Salvo pacto en contrario, el proveedor deberá suministrar el pedido en el plazo máximo de treinta días a partir del día siguiente a aquél en que el consumidor le haya comunicado su pedido.

El consumidor podrá solicitar la anulación de un pago en caso de utilización fraudulenta de su tarjeta de pago en el marco de contratos a distancia. En caso de utilización fraudulenta, se restituirán las sumas abonadas en concepto de pago. Se prohíbe el suministro de bienes o servicios que no hayan sido solicitados previamente por el consumidor, cuando dichos suministros incluyan una petición de pago. La falta de respuesta en tales situaciones no podrá considerarse como consentimiento. Los servicios financieros quedan excluidos del ámbito de la Directiva.

4.4.5 MODELO DE TEXTO DISUASORIO RELATIVO A TARJETAS FALSAS

Junio 1997

Las páginas Web destinadas a comercio electrónico disponen de formularios específicos para la recogida de los datos correspondientes a la tarjeta de crédito o débito que el usuario utilizará para efectuar el pago del producto o servicio contratado.

Es recomendable incluir una advertencia que señale las responsabilidades penales en las que el usuario puede incurrir si utiliza datos correspondientes a una tarjeta falsa o ajena.

Este modelo de texto disuasorio incluye dichas advertencias y puede resultar eficaz para prevenir actos ilícitos en la formalización de transacciones electrónicas en entornos no garantizados por protocolos de seguridad.

4.4.6 DECLARACIÓN CONJUNTA UNIÓN EUROPEA-ESTADOS UNIDOS DE AMÉRICA SOBRE COMERCIO ELECTRÓNICO

5 de diciembre de 1997

1. El comercio electrónico global, promovido por el desarrollo del Internet, será un motor importante para el crecimiento de la economía mundial del siglo XXI. El comercio electrónico ofrece nuevas oportunidades para los negocios y los ciudadanos de todas las regiones del mundo. En particular, las compañías pequeñas podrán conseguir un acceso sin precedentes a los mercados mundiales a bajo coste bajos y los consumidores podrán escoger entre un amplio abanico de productos y servicios. El comercio electrónico aumentará la productividad en todos los sectores de nuestras economías, además de promover el intercambio de bienes y servicios y la inversión, creará nuevos sectores de actividad, nuevas formas de marketing y venta, nuevos sistemas de obtención de ingresos y, lo más importante, nuevos puestos de trabajo. La liberalización de los servicios, particularmente de los servicios básicos de telecomunicaciones, juega un papel clave en el crecimiento de comercio electrónico.

2. Proponemos un diálogo abierto entre los gobiernos y el sector privado mundial para construir un entorno legal y comercial idóneo para la realización de negocios en Internet. Reconocemos que el comercio electrónico requiere una aproximación coherente, coordinada internacionalmente. Cuando los acuerdos gubernamentales sean apropiados, nosotros nos comprometemos a trabajar de forma constructiva con nuestros socios en el seno de las instituciones multilaterales apropiadas y otros foros para alcanzar soluciones coherentes y eficaces preferentemente a nivel global. En este aspecto, estamos de acuerdo en la importancia de involucrar a todos los países, incluyendo los países en vías de desarrollo.

3. Acordamos trabajar para el desarrollo de un mercado global donde la competencia y la capacidad de elección del consumidor dirijan la actividad económica, de acuerdo con las siguientes recomendaciones:

La expansión del comercio electrónico global estará orientada esencialmente al mercado y será manejada por la iniciativa privada. Debe tener en cuenta los intereses de todos los actores, en particular de consumidores, bibliotecas, escuelas y otras instituciones públicas, así como la necesidad de asegurar el uso más amplio posible de las nuevas tecnologías.

El papel de los gobiernos es proporcionar un marco legal claro y consistente, promover un entorno competitivo en el que el comercio electrónico pueda florecer y asegurar la protección adecuada de objetivos de interés público como la intimidad, los derechos de propiedad intelectual, la prevención del fraude, la protección del consumidor y la seguridad nacional.

La autorregulación de la industria es importante. Dentro del marco legal puesto por los gobiernos, los objetivos de interés públicos pueden estar previstos en códigos de conducta internacionales o recíprocamente compatibles, contratos tipo, recomendaciones, etc. que sean el resultado de un acuerdo entre la industria y otras ramas del sector privado.

Las barreras legales y reguladoras que resulten innecesarias deben ser eliminadas y debe impedirse la aparición de otras nuevas. Cuando una acción legislativa se juzgue necesaria, las ventajas o desventajas del comercio electrónico no deben ser comparadas con otras formas de comercio.

Los impuestos en materia de comercio electrónico deben ser claros, consistentes, neutrales y no discriminadores.

Es importante aumentar el conocimiento y la confianza de los ciudadanos y las PYME en el comercio electrónico y apoyar el desarrollo de actividades de formación respecto a la red.

La interoperabilidad, la innovación y la competencia son importantes para el desarrollo de un mercado global, y, en este contexto, los estándares voluntarios, basados en un acuerdo, preferentemente a nivel internacional, pueden jugar un papel importante.

4 Especificamente, nosotros acordamos trabajar hacia:

Un reconocimiento global, lo antes posible, de que, cuando los productos se soliciten electrónicamente y se entreguen físicamente, no deberá aplicarse aranceles adicionales que graven el uso de medios electrónicos. En los demás casos relacionados con el comercio electrónico, la ausencia de aranceles en las importaciones debe permanecer.

La efectiva aplicación a partir del 1 de enero de 1998 de los compromisos adoptados en materia de servicios básicos de telecomunicaciones e incluidos en los programas y anexos del GATS y la finalización de la segunda fase del Acuerdo en materia de Productos de Tecnologías de la Información en verano de 1998.

La ratificación y aplicación, lo antes posible, de los tratados de la OMPI sobre Derechos de Autor y sobre Derechos de Ejecución y Fonogramas. Asegurar la protección eficaz del derecho a la intimidad con respecto al tratamiento automatizado de datos personales en redes de información globales.

La creación de un sistema de registro, asignación y gestión de los dominios en Internet basado en el mercado global que refleje en su totalidad la diversidad geográfica y funcional de Internet

5. Además, acordamos Apoyar activamente el desarrollo, preferentemente a nivel global, de códigos de conducta basados en la autorregulación y de tecnologías que permitan aumentar la confianza del consumidor en el comercio electrónico, involucrando a todos los actores del mercado, incluso aquellos que representan los intereses del consumidor

Cooperación y ayuda mutua para asegurar una administración eficaz de los impuestos y para combatir y prevenir actividades ilegales en Internet.

El papel positivo que el comercio electrónico puede jugar en el desarrollo de una estrategia que permita mejorar el mercado de trabajo internacional y el comercio.

Cooperación en las áreas de I+D definidas conjuntamente y en las tecnologías del comercio electrónico, en el marco del Acuerdo sobre Ciencia y Tecnología suscrito entre la Unión Europea y los Estados Unidos de América, así como en los proyectos piloto en materia de negocios que resulten apropiados.

Continuar las discusiones bilaterales a nivel de expertos, incluyendo a participantes de los gobiernos y del sector privado, respecto los temas antes expresados y otros, como las compras publicas. Las leyes en materia de contratos y las profesiones reguladas; la responsabilidad civil, la comunicación comercial; los pagos electrónicos; las técnicas de cifrado de la información, la autentificación electrónica y la firma digital; y las tecnologías de filtrado y calificación de contenidos.

Cooperacion dirigida a potencias el intercambio de datos estadísticos en materia de comercio electrónico

6. En la medida en que sea necesario para lograr estos objetivos, continuaremos las discusiones con el fin a alcanzar un acuerdo general en los foros multilaterales apropiados, que puede incluir, por ejemplo, la OIC, la OCDE, la OMPI y UNCITRAL. Proponemos un trabajo continuado en el seno de EU-U.S. *Information Society Dialogue, the Trans-Atlantic Business Dialogue and the EU-U.S. Joint Study.*

7. Analizaremos el progreso conseguido en la consecución de estos objetivos y de próximas metas.

4.4.7 INICIATIVA DE LA ONU EN MATERIA DE COMERCIO ELECTRÓNICO

24 de febrero de 1998

La Organización de las Naciones Unidas acaba de crear un grupo de trabajo formado por juristas de los estados miembros, especializados en comercio electrónico, que se denominará LWG *(Legal Working Group)* y auxiliará a las organizaciones CEFACT, UNCITRAL e ICC en la generación de las normas que regularán el comercio electrónico a nivel Internacional.

La representación española correrá a cargo del despacho RIBAS & RODRIGUEZ, a propuesta de la CEOE. Las tareas prioritarias en el calendario de actuaciones son las siguientes:

Asunto	Acción a desarrollar	Descripción
Modelo de Contrato de Comercio Electrónico	Revisión de la recomendación 26 de la ONU y propuesta de una nueva recomendación	Revisión del actual modelo de Contrato de Intercambio con el fin de proponer una nueva recomendación que cubra el comercio electrónico en Internet y contenga las directrices necesarias para el desarrollo de los anexos técnicos relativos a un entorno genérico de comercio electrónico.
Mensajes UN/EDIFACT	Advertencias de limitación de responsabilidad	Preparar mensajes de limitación de responsabilidad, de acuerdo con el análisis de ciertos mensajes UN/EDIFACT en el Informe Portia encomendado por la Unión Europea
Autentificación electrónica	Nueva recomendación de la ONU	La lista de convenios internacionales y acuerdos contenida en el documento R 1096, que contiene una referencia a la generación y firma de documentos debe ser revisada con el fin de permitir sus equivalencias en medios electrónicos. Se propondrá una nueva Recomendación sobre firmas digitales y sistemas de autentificación que tenga en cuenta las implicaciones para la legislación de cada Estado
Modelo de acuerdo de TTP	Nueva recomendación de la ONU	Redacción de un modelo de "Trusted Third Party", a incluir en una nueva Recomendación de la ONU
Protección de datos	Guía de referencia	Preparar una guía sobre el efecto de la Directiva europea sobre protección de datos.
Material divulgativo	Guías legales	Desarrollar documentos divulgativos que ayuden a entender los aspectos jurídicos relacionados con el comercio electrónico.
Barreras legales	Análisis de leyes estatales	Utilizando los recursos de UNCITRAL, se revisarán las respuestas a los

		cuestionarios realizados para conocer la existencia de posibles barreras al comercio electrónico en las legislaciones nacionales, y considerar la necesidad de una acción posterior.
Colaboración internacional	Relación con otras organizaciones	Relación con otras organizaciones como CEFACT, UNCITRAL, ICC, EU, WTO (OMC), ECA/EDIA, ICS, ISO, IMO, NSO y los respectivos ministerios de cada Estado.

Iniciativa de la ONU en materia de comercio electrónico, la representación española correrá a cargo del despacho RIBAS & RODRIGUEZ, a propuesta de la CEOE.

4.4.8 La Iniciativa G-7 [10]

A principios de 1995 las naciones del Grupo de los 7, asumieron un grupo de once iniciativas que colectivamente intentaban demostrar el potencial de la sociedad de la información y estimular su desarrollo. Una de estas iniciativas "Un Mercado Global para las PYMEs", tiene el objetivo general de facilitar el incremento de la competitividad y la participación en el mercado global de las PYMEs, explotando las posibilidades ofrecidas por el desarrollo de la sociedad de la información global. Sus objetivos específicos son:

Contribuir al desarrollo de un entorno electrónico global para el intercambio abierto y no discriminatorio de información beneficiosa para las PYMEs (sobre tecnologías, productos, recursos humanos), por encima de obstáculos como la distancia, el tiempo o las fronteras entre países; extender el comercio electrónico global para establecer plataformas que sustenten sus operaciones comerciales y las gestionen de forma más eficaz y provechosa

La iniciativa, que está previsto se complete para finales de 1998, tiene tres temas, cada uno con su coordinador propio:

Tema 1. redes globales de información para PYMEs
Este tema contribuirá al desarrollo de un entorno abierto y no discriminatorio que permita a las PYMEs acceder a la información que necesitan y difundir información de sus productos, tecnologías, etc., usando las redes internacionales de información. El coordinador del tema es Japón.

Tema 2. requerimientos de las PYMES (legales, institucionales y técnicos)
Este tema trata de asegurar que la apertura sistemática asociada con una mercado global para las PYMES está dirigida y proporciona una plataforma basada en sistemas abiertos que asegure que el proyecto como un todo responda a las necesidades explícitas de las PYMEs. El coordinador del tema es la Comisión Europea.

Tema 3. soporte internacional para el comercio electrónico
Este tema pretende:
(1) Promocionar la compensación de las iniciativas dirigidas a poner en marcha un "mercado global para las PYMEs" por medio del comercio electrónico global;

[10] Grupo de los 7, tomado de la página http://www.sopde.es/cajon/comercio/g7.html

(2) Fomentar el desarrollo de estudios, proyectos piloto y otras acciones cooperativas que evalúen o demuestren soluciones para los problemas aún sin resolver;
(3) Dar publicidad a las demostraciones satisfactorias de comercio electrónico global que impliquen a PYMEs. El coordinador del tema es USA.

La iniciativa está abierta a la participación de países no miembros del Grupo y a las organizaciones internacionales.

4.5 ESTUDIO COMPARATIVO DE ALGUNAS LEYES INTERNACIONALES RELATIVAS A LA FIRMA DIGITAL [11]

4.5.1 INTRODUCCIÓN

En los últimos años los avances científicos han revolucionado el uso de los sistemas informáticos, redes electrónicas e Internet, los cuales han incidido en el desarrollo del comercio, la producción y la prestación de servicios. A esta nueva forma de intercambio se le ha denominado comercio electrónico, en el cual se ven involucrados tanto el sector público como el sector privado.

El comercio electrónico se caracteriza porque las operaciones se realizan por vía electrónica o digital, en las que se presentan diversas situaciones, como las siguientes: se prescinde del lugar donde se encuentran las partes, no se lleva a cabo un registro en papel (facturas), en algunos casos la importación del bien no pasa por las aduanas (audio, software, videos, etc.); se reducen los intermediarios y se realizan más rápidamente las transacciones

En el mundo, el comercio electrónico es un fenómeno que está creciendo y desarrollandose rápidamente, principalmente por las facilidades que brinda a los usuarios, entre ellas la flexibilidad y la disminución en el costo de las operaciones.

No obstante el notable incremento en las relaciones comerciales, existen factores que impiden un mayor desarrollo del comercio electrónico, uno de ellos es la inseguridad al momento de realizar transacciones electrónicas, debido a un sistema jurídico que no está suficientemente instrumentado para recoger las exigencias del mismo.

La mayoría de las organizaciones internacionales están estudiando nuevas reglas y formas de regular estos aspectos. Algunos países más desarrollados ya tienen normas en funcionamiento, las cuales permiten crear documentos seguros, mediante el denominado sistema de firmas electrónicas, basado en certificados electrónicos emitidos por entidades de certificación

La regulación de la firma electrónica o digital significa un avance en el establecimiento de un marco jurídico respecto de las tecnologías de la información; sin embargo, es importante considerar y no perder de vista otros aspectos como la propiedad intelectual, el pago de impuestos, los delitos y sus respectivas sanciones, los nombres de dominio, la protección al consumidor, los problemas de ley y jurisdicción aplicable. Para ello, se

[11] La información relativa a las leyes que hace referencia este artículo fue recabada por medio de Internet, a través de la página http://www.vlex.com. La información contenida en este artículo fue coordinada por Guillermina González Durand, Subdirectora de Análisis Jurídicos y Administrativos e integrada por Sandra Gomez Pérez, especialista del Departamento de Análisis Jurídicos en Informática, Dirección de Políticas y Normas en Informática, INEGI.

tendrán que revisar los diferentes ordenamientos con el fin de reformarlos, o en su caso expedir normas y lineamientos que complementen el tema.

En relación con la situación del uso de la firma electrónica o digital, cabe señalar que aunque está plenamente justificada su existencia, a partir de la celebración de contratos o de transacciones económicas o compras que se realizan a través de medios electrónicos, todavía es perceptible que existe un rechazo social a la utilización de éstos. Esto se debe en parte al nivel de inseguridad que impera entre los usuarios al momento de realizar una operación de este tipo, por desconocer la identidad del destinatario y receptor de los mensajes o documentos electrónicos, en la veracidad y autenticidad de su contenido y en cuanto a la validez del documento electrónico, entre otros.

Con la finalidad de tener un panorama general de la situación en que se encuentra regulada la firma electrónica o digital, a continuación se presenta un cuadro en el que se hace una comparación del contenido de algunas legislaciones emitidas en países de América y de Europa.

Para ello, se escogieron como principales rubros: el nombre de la ley, objetivo, ámbito de aplicación o cobertura, definiciones, supervisión y control, instancias que intervienen en la emisión de certificados, protección de datos, elementos de seguridad, valor probatorio, reconocimiento de certificados extranjeros, responsabilidad por daños y perjuicios y, sanciones.

Los países que se incluyen, en orden de aparición por su fecha de publicación son: Estados Unidos en el Estado de Utah, Colombia, Perú, Venezuela, Alemania, España, la Comunidad Europea, Argentina y Chile.

4.5.2 PAÍSES AMERICANOS

4.5.2.1 ESTADOS UNIDOS

Ley del Estado de Utah sobre la Firma Digital. Código comentado Título 46, Capítulo 3 (1996)

Objetivo
Facilitar las transacciones mediante mensajes electrónicos y firmas digitales; reducir al mínimo la posibilidad de fraguar firmas digitales y el fraude en las transacciones electrónicas; instrumentar jurídicamente la incorporación de normas pertinentes; establecer, en coordinación con diversos Estados, normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos.

Ámbito de aplicación o cobertura
Transacciones mediante mensajes electrónicos y firmas digitales autenticación y confiabilidad de los mensajes de datos.

Definiciones

a) *Firma digital:* transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la

clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación.

b) *Criptosistema asimétrico:* algoritmo o serie de algoritmos que brindan un par de claves confiable.
c) *Certificado:* registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.
d) *Repositorio:* sistema para almacenar y recuperar certificados y demás información pertinente a las firmas digitales.

Supervisión y control
Corresponde a la División, cuyo papel principal es actuar como autoridad certificante en sí misma, además de formular políticas, facilitando la adopción de la tecnología necesaria para la firma digital y realizando una labor de supervisión regulatoria.

Instancias que intervienen en la emisión de certificados
Autoridad certificante acreditada: es quien emite certificados.
Repositorios: operan bajo la dirección de una autoridad certificante acreditada.

Protección de datos
No hace referencia

Elementos de seguridad
Uso de sistemas confiables: equipos y programas de computación que sean razonablemente confiables contra la posibilidad de intrusión o uso indebido; que brinden un razonable grado de disponibilidad, confiabilidad y correcto funcionamiento, y que se adapten debidamente al desempeño de sus funciones específicas.

Por lo menos una vez al año se evaluarán a las autoridades certificantes acreditadas con el fin de determinar si se cumplen las normas exigidas por la ley.

Valor probatorio
Un mensaje tiene la misma validez y puede ser exigido judicialmente y es efectivo como si estuviera escrito en papel si aporta en su totalidad una firma digital y si ésta es verificada mediante la clave pública mencionada en un certificado que haya sido emitido por una autoridad certificante acreditada y haya sido válido al momento en que se efectuó la firma digital

Reconocimiento de certificados extranjeros
No lo contempla, sin embargo señala que la División puede reconocer la acreditación o autorización de autoridades certificantes que realicen otros organismos gubernamentales, siempre y cuando los requisitos para la acreditación sean substancialmente similares a los que rigen en el Estado

Responsabilidades por daños y perjuicios
Al aceptar un certificado, el suscriptor se compromete a indemnizar a la autoridad certificante por daños y perjuicios en la emisión o publicación de un certificado con base en una declaración falsa y significativa realizada por el suscriptor; o bien, un hecho significativo no revelado por el suscriptor.

Salvo que la autoridad certificante renuncie a ello, se considerará que no será responsable por pérdidas causadas por haberse confiado en una firma falsa o fraguada, si con respecto a dicha firma, la autoridad hubiera cumplido con los requisitos establecidos; que no será responsable por un monto mayor al que se menciona en el certificado como límite recomendado de confianza; será responsable sólo por daños directos emergentes de una acción promovida por resarcimiento de daños debido a haber confiado en el certificado

Sanciones
No hace referencia

4.5.2.2 COLOMBIA

Ley de Comercio Electrónico en Colombia (Ley 527 de 1999)

Objetivo
Definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como establecer las entidades de certificación.

Ámbito de aplicación o cobertura
Uso de firmas digitales en todo tipo de información en forma de mensaje de datos.

Definiciones

a) *Firma digital*: valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
b) *Mensaje de datos*: la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax
c) *Entidad de certificación*: persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.
d) *Sistema de información*: sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Supervisión y control
Entidades de certificación autorizadas por la Superintendencia de Industria y Comercio.

Instancias que intervienen en la emisión de certificados
Entidad de certificacion, una de sus obligaciones es llevar un registro de los certificados.

Protección de datos
Es obligacion de las entidades de certificación garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.

Elementos de seguridad

La información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.
El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Valor probatorio
El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Reconocimiento de certificados extranjeros
Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Responsabilidades por daños y perjuicios
Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor

Sanciones
La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

1. Amonestación
2. Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.
3 Suspender de inmediato todas o algunas de las actividades de la entidad infractora.
4. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.
5 Revocar definitivamente la autorización para operar como entidad de certificación.

4.5.2.3 PERÚ

Ley No. 27269 Ley de Firmas y Certificados Digitales (2000)

Objetivo
Utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Ámbito de aplicación o cobertura
Firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

Definiciones
a) *Firma digital:* firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
b) *Certificado digital:* documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.
c) *Entidad de certificación:* cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general; podrán igualmente asumir las funciones de Entidades de Registro o Verificación.
d) *Entidad de registro o verificación:* cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales.

Supervisión y control
El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.

Instancias que intervienen en la emisión de certificados
Entidad de certificación, la cual puede asumir las funciones de entidades de registro o verificación

Entidad de registro o verificación
Cada entidad de certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado

Protección de datos
La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la ley.
Asimismo, la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Elementos de seguridad
No hace referencia

Valor probatorio

No hace referencia

Reconocimiento de certificados extranjeros
Los certificados de firmas digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la ley, siempre y cuando sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

Responsabilidades por daños y perjuicios
No hace referencia

Sanciones
No hace referencia

4.5.2.4 VENEZUELA

Ley sobre Mensajes de Datos y Firmas Electrónicas (2001)

Objetivo
Otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos

Ámbito de aplicación o cobertura
Mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro.

Definiciones
a) *Firma electrónica:* información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado
b) *Mensajes de datos:* toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
c) *Certificado electrónico:* mensaje de datos proporcionado por un proveedor de servicios de certificación que le atribuye certeza y validez a la firma electrónica.
d) *Proveedor de servicios de certificación:* persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en este Decreto-Ley.
e) *Sistema de información:* aquel utilizado para generar, procesar o archivar de cualquier forma mensajes de datos.

Supervisión y control
Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Instancias que intervienen en la emisión de certificados
Proveedor de Servicios de Certificación.

Protección de datos
Los mensajes de datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal.

Elementos de seguridad
La Superintendencia de Servicios de Certificación Electrónica podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los proveedores de servicios de certificación (uso de estándares o prácticas internacionalmente aceptadas o que el proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio).

Los proveedores de servicios de certificación tienen la obligación de garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione como mantener un respaldo confiable y seguro de dicha información, garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas que proporcionen.

Valor probatorio
La firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. La firma electrónica podrá formar parte integrante del mensaje de datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Reconocimiento de certificados extranjeros
Los certificados electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el Decreto-Ley, siempre que sean garantizados por un proveedor de servicios de certificación, debidamente acreditado conforme a lo previsto en el Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado. Los certificados electrónicos extranjeros no garantizados por un proveedor de servicios de certificación debidamente acreditado conforme a lo previsto en el Decreto-Ley, carecerán de los efectos jurídicos; sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica

Responsabilidades por daños y perjuicios
El Signatario de la Firma Electrónica tendrá las siguientes obligaciones:

1) Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.
2) Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello.

El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

Sanciones
Los proveedores de servicios de certificación serán sancionados con multa de Quinientas Unidades Tributarias a Dos Mil Unidades Tributarias, cuando incumplan las obligaciones o con los requisitos establecidos en el Decreto-Ley.

Las sanciones serán impuestas en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes o atenuantes existentes.
Son circunstancias agravantes: reincidencia y reiteración; gravedad del perjuicio causado al usuario; gravedad de la infracción; resistencia o reticencia del infractor para esclarecer los hechos.

Son circunstancias atenuantes: no haber tenido la intención de causar el hecho imputado de tanta gravedad; las que se evidencien de las pruebas aportadas por el infractor en su descargo.

4.5.2.5 ARGENTINA

Decreto Nº 427/98, que permite el uso de Firma Digital para los actos internos del Sector Público Nacional (1998)

Objetivo
Optimizar la actividad de la Administración Pública Nacional adecuando sus sistemas de registro de datos, tendiendo a eliminar el uso del papel y automatizando sus circuitos administrativos.

Ámbito de aplicación o cobertura
Uso de la firma y el documento digital dentro del Sector Público Nacional.

Definiciones

a) *Firma digital:* resultado de una transformación de un documento digital empleando un criptosistema asimétrico y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza:
    1. Si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio
    2. Si el documento digital ha sido modificado desde que se efectuó la transformación, lo que garantiza su integridad. La conjunción de los dos requisitos anteriores garantiza su no repudio y su integridad.
b) *Documento digital:* representación digital de actos, hechos o datos jurídicamente relevantes.
c) *Documento digital firmado:* documento digital al cual se le ha aplicado una firma digital

Supervisión y control
La autoridad de aplicación del Decreto es la Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros, cumpliendo las funciones de organismo licenciante.

Instancias que intervienen en la emisión de certificados
Autoridad certificante licenciada: Órgano administrativo que emite certificados de clave pública. Ente organismo auditante: Órgano administrativo encargado de auditar la actividad del ente organismo licenciante y de las autoridades certificantes licenciadas.

Protección de datos

El organismo auditante deberá evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos.

Elementos de seguridad
El organismo auditante deberá evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como el cumplimiento con las especificaciones del manual de procedimientos y el plan de seguridad aprobados por el organismo licenciante, y verificar que se utilicen sistemas técnicamente confiables.

La autoridad certificante licenciada tiene la obligación de notificar al solicitante sobre las medidas necesarias que éste está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable; y de las obligaciones que éste asume por el sólo hecho de ser suscriptor de un certificado de clave publica.

Valor probatorio
En el régimen del Decreto la firma digital tendrá los mismos efectos de la firma ológrafa.

Reconocimiento de certificados extranjeros
No hace referencia

Responsabilidades por daños y perjuicios
No hace referencia

Sanciones
No hace referencia

4.5.2.6 CHILE
Normatividad que regula el Uso de la Firma Digital y los Documentos Electrónicos en la Administración del Estado (1999)

Objetivo
Regular la utilización de la firma digital y los documentos electrónicos como soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos de la administración del Estado.

Ámbito de aplicación o cobertura
Firma digital y documentos electrónicos utilizados en la Administración del Estado, salvo la Contraloría General de la República, el Banco Central y las Municipalidades.

Definiciones
a) *Firma electrónica*: código informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su transmisor desconocer la autoría del mensaje en forma posterior.
b) *Firma digital*: especie de firma electrónica que resulta de un proceso informático validado, implementado a través de un sistema criptográfico de claves públicas y privadas.
c) *Documento electrónico*: toda representación informática que da testimonio de un hecho.

d) *Certificado de firma digital:* documento electrónico por el ministro de fe del servicio respectivo que acredita la correspondencia entre una clave pública y la persona que es titular de la misma.

Supervisión y control
Ministerio Secretaria General de la Presidencia asesorará a los organismos de la Administración del Estado en la implementación de sistemas de firma digital y diseñará y coordinará planes piloto para emplear la firma digital en servicios determinados.

Instancias que intervienen en la emisión de certificados
No hace referencia

Protección de datos
No hace referencia

Elementos de seguridad
La utilización de soportes, medios y aplicaciones electrónicos, informáticas y telemáticas en las actuaciones administrativas, requerirá la adopción de medidas técnicas y de organización necesarias para garantizar la autenticidad confidencialidad, integridad y conservación de la información.

Las autoridades de cada órgano o servicio deberán adoptar medidas de seguridad para que los soportes, medios y aplicaciones informáticas cumplan con estándares internacionalmente reconocidos.

Valor probatorio
Los documentos de los órganos señalados en la ley escritos en un soporte electrónico, producirán los mismos efectos que los escritos en un soporte de papel. En dichos documentos, la firma digital sustituirá a la firma ológrafa del funcionario que lo emite y producirá los mismos efectos que aquélla.

La firma digital sustituirá el uso de cualquier sello, timbre, visto bueno u otra marca distinta que fuere necesaria para la validez del documento, si este hubiere sido escrito sobre un soporte de papel

Reconocimiento de certificados extranjeros
No hace referencia

Responsabilidades por daños y perjuicios
No hace referencia

Sanciones
No hace referencia

4.5.3 PAÍSES EUROPEOS

4.5.3.1 COMUNIDAD EUROPEA

Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica (1998)

Objetivo
Garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo y adecuado para la Comunidad Europea, y definiendo criterios que fundamenten su reconocimiento legal.

Ámbito de aplicación
La Directiva regula el reconocimiento legal de la firma electrónica.
La Directiva no regula otros aspectos relacionados con la celebración y validez de los contratos u otras formalidades no contractuales que precisen firma.
La Directiva establece un marco jurídico para determinados servicios de certificación accesibles al público.

Definiciones

a) *Firma electrónica:* la firma en forma digital integrada en unos datos, ajena a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:
   1. Estar vinculada al signatario de manera única;
   2. Permitir la identificación del signatario;
   3. Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control;
   4 Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.
b) *Dispositivo de creación de firma:* los datos únicos, como códigos o claves criptográficas privadas, o un dispositivo físico de configuración única, que el signatario utiliza para crear la firma electrónica.
c) *Dispositivo de verificación de firma:* los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.
d) *Certificado reconocido* el certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad, y que cumple los requisitos establecidos en el Anexo Y.
e) *Proveedor de servicios de certificación:* la persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica.

Supervisión y control
La Comisión estará asistida por un comité denominado "Comité de Firma Electrónica", de carácter consultivo, compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

Instancias que participan en la emisión de certificados
Proveedor de servicios de certificación: persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica.

Protección de datos
Se contempla un artículo relacionado con la protección de datos en el que se señalan cuatro puntos, entre ellos está el que los Estados miembros velen porque los proveedores de servicios de certificación únicamente puedan recabar datos personales directamente del titular de los mismos, y sólo con el alcance necesario a efectos de la expedición del certificado Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento de su titular.

Seguridad, integridad y confiabilidad
Es deber de los prestadores de servicios de certificación el que utilicen sistemas dignos de confianza y productos de firma electrónica que garanticen la protección contra toda alteración de los mismos que posibilite su uso con fines diferentes de aquellos para los que fueron concebidos; también deberán utilizar productos de firma electrónica que garanticen la seguridad técnica y criptográfica de los procesos de certificación sustentados por los productos.

Valor probatorio
Los Estados miembros velarán porque la firma electrónica basada en un certificado reconocido que haya expedido un proveedor de servicios de certificación, que cumpla con los requisitos establecidos, sea por un lado, considerada como firma que cumple los requisitos legales de una firma manuscrita y sea, por otro, admisible como prueba a efectos procesales de la misma forma que una firma manuscrita.

Reconocimiento de certificados extranjeros
Los Estados miembros velarán porque los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país gocen de equivalencia legal con los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si se cumple que:

El proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el marco de un sistema voluntario de acreditación establecido por un Estado miembro;

Un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones del Anexo II, avala el certificado en la misma medida que los suyos propios,

El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales

La Comisión podrá tomar medidas a fin de facilitar tanto la prestación de servicios de certificación transfronterizos con terceros países como el reconocimiento legal de las firmas electrónicas originarias de estos últimos, la Comisión presentará, en su caso, propuestas para la aplicación de normas y acuerdos internacionales relacionados con los servicios de certificación. Llegado el caso, presentará propuestas al Consejo en solicitud de mandatos de negociación de acuerdos bilaterales y multilaterales con terceros países y organizaciones internacionales. El Consejo se pronunciará por mayoría cualificada.

Responsabilidades por daños y perjuicios
Los Estados miembros velarán porque el proveedor de servicios de certificación que expida un certificado reconocido sea responsable, ante cualquier persona que de buena fe confíe en el certificado, a efectos de: la veracidad de toda la información contenida en el certificado reconocido a partir de la fecha de su expedición; la conformidad con todos los requisitos en la expedición del certificado reconocido; la garantía de que, en el momento de la expedición del certificado reconocido, obra en poder de la persona identificada en el mismo el dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado; en caso de que el proveedor de

servicios de certificación genere los dispositivos de creación y de verificación de firma, la garantía de que ambos funcionen conjunta y complementariamente.

El proveedor de servicios de certificación no será responsable de eventuales inexactitudes en el certificado reconocido que resulten de la información facilitada por la persona a la que se expidió el mismo, a condición de que el proveedor demuestre haber actuado siempre con la máxima diligencia para comprobar tal información.

El proveedor de servicios de certificación no será responsable de los daños y perjuicios causados por el uso indebido de un certificado reconocido en el que consten tales límites en cuanto a sus posibles usos cuando éstos se hayan transgredido.

El proveedor de servicios de certificación no será responsable de los eventuales daños y perjuicios que excedan de valor límite de las transacciones válidas.

Sanciones
No hace referencia

4.5.3.2 ALEMANIA

Ley de Firma Digital Alemana (SigG) (1997)

Objetivo
Crear las condiciones generales para las firmas digitales bajo las cuales se las pueda considerar seguras y que las falsificaciones de firmas digitales y las falsificaciones de información firmada puedan ser verificadas sin lugar a duda.

Ámbito de aplicación
Uso de firmas digitales, verificación y falsificación.

Definiciones
a) *Firma digital*: sello creado con una clave privada de firma sobre información digital, tal sello permite, mediante el uso de la clave pública asociada rotulada por un certificado de clave de un certificador, o de una Autoridad, que sean verificados el propietario de la clave de firma y el carácter de no falsificado de la información.
b) *Certificador*: persona física o jurídica la cual da fe a la atribución de claves públicas de firma de personas físicas y mantiene una licencia para ese motivo.
c) *Certificado*: certificación digital rotulada con una firma digital respecto a la atribución de una clave de firma pública a una persona física (certificado de clave de firma), o una certificación digital especial que se refiere inequívocamente a un certificado de clave de firma y contiene información adicional (certificado de atributos)

Supervisión y control
Sólo se menciona que el otorgamiento de licencias, la emisión de certificados, los certificadores, así como la supervisión del cumplimiento de la Ley, yacen bajo la Autoridad del Artículo 66 de la Ley de Telecomunicaciones.

Instancias que participan en la emisión de certificados
Certificador: es una persona física o jurídica la cual da fe a la atribución de claves públicas de firma a personas físicas y mantiene una licencia para ello.

Protección de datos
Se maneja como protección a la información y se señala que el certificador puede recopilar información personal sólo directamente de la persona afectada y sólo en la medida que sea necesario para los propósitos de un certificado. La recopilación de información de un tercero se permite sólo con el consentimiento de la persona afectada.
También se señala que se deberá aplicar la sección 38 de la Ley de Protección de Información Federal, con la condición de que también puede llevarse a cabo una revisión si no hay bases para la previsión de violaciones de la protección de información.

Seguridad, integridad y confiabilidad
Para el adecuado cumplimiento de la Ley los certificadores, deberán establecer las medidas de seguridad que se requieren en un plan de seguridad, el cual debe ser examinado y verificado por una instancia reconocida por la Autoridad.
También se señala que el certificador deberá informar al solicitante lo referente a las medidas necesarias para contribuir a asegurar la firma digital y su verificación confiable.

Valor probatorio
No hace referencia

Reconocimiento de certificados extranjeros
Se establece que las firmas digitales que se puedan verificar con una clave pública de firma para la cual exista un certificado extranjero de otro estado miembro de la Unión Europea o de otro Estado firmante del tratado en el Área Económica Europea son equivalentes a firmas digitales según la ley, en tanto puedan demostrar un nivel de seguridad equivalente. Lo anterior también se aplica a otros estados en la medida en que se suscriban acuerdos internacionales relativos al reconocimiento de certificados.

Responsabilidades por daños y perjuicios
No hace referencia

Sanciones
No hace referencia

4.5.3.3 ESPAÑA

Real Decreto Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica (1999)

Objetivo
Establecer una regulación clara del uso de firma electrónica, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación.

Ámbito de aplicación
Uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al publico de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

Definiciones

a) *Firma electrónica:* conjunto de datos, en forma electrónica, ajenos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

b) *Firma electrónica avanzada:* firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.
c) *Certificado:* certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.
d) *Prestador de servicios de certificación:* persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Supervisión y control
El Ministerio de Fomento controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos.

Instancias que participan en la emisión de certificados
Prestador de servicios de certificación": Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España. Su regulación se desarrollará por Real Decreto.

Protección de datos
Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito y serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

El tratamiento los datos se sujeta a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

Seguridad, integridad y confiabilidad
Un dispositivo de creación de una firma electrónica es seguro, si garantiza que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto; si existe seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento; si los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros, y si el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al signatario antes del proceso de firma.

Valor probatorio

La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Reconocimiento de certificados extranjeros

Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste, expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumplan alguna de las siguientes condiciones:

a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.
b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.
c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

Responsabilidades por daños y perjuicios

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone el Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.
2. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.
3. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.
4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Sanciones

a) Por la comisión de infracciones muy graves, se impondrá multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio lo constituirá el límite del importe de la sanción pecuniaria.
b) La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

ESTA TESIS NO SAL
DE LA BIBLIOTEC

c) Por la comisión de infracciones graves, se impondrá multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria.
d) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 euros).

Análisis de la legislación internacional sobre la firma digital
De acuerdo con el contenido de los rubros señalados, los puntos relevantes son los siguientes:

Objetivo
El objetivo en general es regular el uso de la firma digital, otorgándole validez y eficacia jurídica. En el caso de Argentina y Chile, se busca optimizar la actividad de la Administración Pública por medio de la sustitución del papel por el uso de medios electrónicos.

El Estado de Utah contempla el reducir el fraude en las transacciones electrónicas, así como la falsificación de las firmas digitales.

Colombia dedica una parte al comercio electrónico de mercancías, es decir, integra en una misma ley el comercio electrónico, la firma digital y el acceso y uso de mensajes de datos.

Ámbito de aplicación
Las legislaciones se aplican al uso de firmas digitales que cumplan con lo establecido legalmente y que está previsto en cada una de sus respectivas leyes.

El ámbito de aplicación en Argentina y Chile es el Sector Público, es decir, los órganos de la Administración del estado que cada país reconoce.

Colombia señala que la Ley no será aplicable a aquella información relacionada con las obligaciones contraídas por el Estado en los Convenios y Tratados Internacionales, así como en las advertencias que deban ir impresas por disposición legal en ciertos productos, en razón del riesgo que implica su comercialización, uso o consumo.

La Comunidad Europea no regula aspectos relacionados con la celebración y validez de los contratos u otras formalidades no contractuales que precisen firma.

Definiciones
Las legislaciones contemplan los términos de "firma electrónica" y "firma digital":
"Firma electrónica". Chile, Venezuela y España, coinciden en que es la información creada o utilizada que permite determinar su autenticidad y ser atribuida a su autor.

Firma digital. El Estado de Utah, Colombia, Perú, Argentina, Chile, la Comunidad Europea, Alemania y España coinciden en la utilización de un criptosistema asimétrico basado en el uso de un par de claves, una pública y una privada relacionadas entre sí, de tal forma que, si una persona posee el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante y si el mensaje ha sido modificado desde que

se efectuó la transformación. España utiliza el término de firma electrónica avanzada en lugar de firma digital.

Chile define ambos términos.

Supervisión y control
Cada país establece o crea un organismo autónomo o dependiente de una Secretaría de Estado. Como funciones principales tienen las de acreditar, supervisar y controlar a las entidades de certificación o a los proveedores de servicios de certificación como se les denomina en Venezuela.

Los encargados de emitir, revocar o cancelar certificados se les conoce como entidades o autoridades de certificación o prestadores de servicios de certificación. Entre sus funciones están el garantizar la seguridad para la emisión y creación de firmas digitales, así como mantener un registro de firmas digitales certificadas de acceso público, entre otras.

Perú establece, además, una entidad de registro o verificación cuya función es levantar y comprobar los datos del solicitante de certificados digitales, aceptar y autorizar las solicitudes de emisión o cancelación de certificados digitales, aunque esta actividad la puede asumir la entidad de certificación.

En la legislación chilena sólo se señala que habrá un ente asesor de los organismos de la Administración del Estado en la implementación de sistemas de firma digital.

La Comunidad Europea integra un Comité de Firma Electrónica al cual se le podrán hacer consultas sobre los requisitos de los proveedores de servicios de certificación y normas aceptadas para los productos de firmas electrónicas.

Colombia, Chile y Venezuela señalan que podrán ser entidades de certificación las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la autoridad correspondiente en cada país.

Protección de datos
Este rubro se refiere a aquellos datos recabados que estén relacionados con la firma digital, es decir, la información personal que proporcione a la autoridad competente el solicitante de dicha firma.

Perú, Colombia, Argentina, España y la Comunidad Europea señalan que se podrán recabar datos personales del titular de los mismos a efectos de la emisión del certificado correspondiente, la información que se adquiera deberá de ser utilizada de manera adecuada y confidencialmente, y no podrán ser utilizados para otros fines sin el consentimiento del titular.

Venezuela contempla la protección de datos pero en los mensajes digitales.

El Estado de Utah, Chile y Alemania no lo contemplan.

Adicionalmente, la legislación española menciona que se deberá observar lo establecido en la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Elementos de seguridad
Las legislaciones señalan el deber de utilizar sistemas confiables en la prestación de los servicios de certificación que garanticen la integridad, disponibilidad, calidad, accesibilidad y conservación de la información.

Contemplan la adopción de medidas preventivas para evitar la falsificación tanto de los certificados como de las firmas electrónicas.

Establecen que se realicen evaluaciones a las autoridades certificantes para verificar que actúan conforme a lo establecido en sus legislaciones.

Colombia sólo considera la integridad y confiabilidad de los mensajes de datos.
Perú no lo contempla.

España establece el dispositivo de creación de firma y los define como un programa o un aparato informático que sirve para aplicar los datos de creación de firma, lo cual da seguridad al signatario.

Alemania contempla la realización de un plan de seguridad por parte de los prestadores de servicios de certificación en el que se incluyan las medidas de seguridad necesarias para el adecuado cumplimiento de la ley. Dicho plan deberá ser examinado por la autoridad.

Valor probatorio
Las legislaciones establecen que la firma digital tendrá la misma validez y eficacia probatoria que la que se le atribuye a la firma autógrafa, siempre y cuando cumpla con los requisitos establecidos.

Perú no hace referencia.

En el caso de Chile, la firma digital sustituirá el uso de cualquier sello, timbre, visto bueno u otra marca distinta que fuere necesaria para la validez del documento, si éste hubiere sido escrito sobre un soporte de papel.

Reconocimiento de certificados extranjeros
Estados Unidos y Colombia no lo contemplan; sin embargo, Estados Unidos reconoce la autorización de las autoridades certificantes que realicen otros organismos gubernamentales pero sólo dentro del país

Perú, Venezuela y las legislaciones europeas reconocen la misma validez y eficacia jurídica a los certificados extranjeros que los que se señalan en cada una de sus legislaciones siempre y cuando garanticen que son expedidos por una autoridad certificante, así como el cumplimiento de los requisitos, el procedimiento para su expedición, validez y vigencia

Argentina y Chile, por tener legislaciones enfocadas al Sector Público no lo contemplan.

Responsabilidades por daños y perjuicios
En este rubro, el Estado de Utah, Colombia y Venezuela contemplan la responsabilidad por daños y perjuicios por parte del suscriptor del certificado de firma electrónica en caso

de que se presente la pérdida de la clave privada, si ha sido expuesta o corre peligro de que se le dé un uso indebido, por lo que habrá de notificar a la entidad certificadora o al proveedor de servicios de certificación de los hechos mencionados. En caso de que no cumpla con dicha notificación será responsable de las consecuencias del uso no autorizado de su firma electrónica.

La Ley del Estado de Utah señala que cuando un suscriptor acepta un certificado se compromete a indemnizar a la autoridad certificante por daños y perjuicios en la emisión o publicación de un certificado si emitió una declaración falsa u omitió revelar un hecho significativo.

La misma Ley también establece la responsabilidad y riesgo de responsabilidad que recae sobre la autoridad certificante, que debe ser capaz de evaluar y manejar su riesgo frente a una posible responsabilidad. La Comunidad Europea señala que los Estados miembros velarán porque el proveedor de servicios de certificación que expida un certificado reconocido sea responsable, ante cualquier persona que de buena fe confíe en el certificado. Esto permitirá comprobar que la veracidad de toda la información contenida en el certificado, la conformidad con todos los requisitos establecidos.

España establece que los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone la ley o actúen con negligencia.

Sanciones

No todas las legislaciones establecen un apartado de sanciones. Colombia, Venezuela y España contemplan sanciones para las entidades de certificación o proveedores de servicios de certificación.

En Colombia las sanciones pueden consistir en amonestación, multa, suspensión de actividades hasta por el término de cinco años, o la revocación definitiva de la autorización para operar como entidad de certificación.

Las sanciones en Venezuela sólo consistirán en multas, las cuales podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes (reincidencia, gravedad del perjuicio causado al usuario, gravedad de la infracción, resistencia del infractor para esclarecer los hechos) o atenuantes (no haber tenido la intención de causar el hecho imputado, las que se evidencien de las pruebas aportadas por el infractor en su descargo) existentes. Para la imposición de las multas previstas se aplicará el procedimiento administrativo ordinario previsto en la Ley Orgánica de Procedimientos Administrativos

En España las sanciones pueden ser multas o la prohibición de la actuación de los prestadores de servicios de certificación.

Consideraciones finales

1) Es importante dar mayor difusión a las leyes en materia de firma electrónica, para lo cual sería conveniente que el órgano encargado de la supervisión y control de la ley realice una versión comentada o que sea más entendible para los ciudadanos, ya que es un tema complejo sobre todo por los términos que se manejan.

2) La difusión también tiene que llegar a las personas encargadas de la impartición de justicia y debería establecerse a detalle el procedimiento a seguir en la resolución de conflictos.
3) Debería hacerse una concientización de la importancia del uso de los medios electrónicos en las autoridades, por lo que sería conveniente que existiera una capacitación sobre aspectos relativos a las tecnologías de la información.
4) Es importante evaluar qué tan eficaz es la implementación de códigos de ética tanto para los empleados del órgano superior como para los prestadores de servicios de certificación.
5) Tomando en cuenta la globalización de las relaciones comerciales, sería conveniente unificar las normativas, así como reforzar las relaciones entre países mediante acuerdos o tratados internacionales.

CAPITULO QUINTO

LEGISLACIÓN EN MÉXICO EN MATERIA DE SEGURIDAD INFORMÁTICA

5.1 LEGISLACIÓN ELECTRÓNICA EN MÉXICO [12]

1999
mayo 17
Se modifica el código penal federal para incluir nuevos tipos de delitos informáticos como accesos ilícitos a sistemas particulares, de gobierno y del sector financiero.

2000
enero 4
se publican 2 nuevas leyes, la ley de obras públicas y servicios y la ley de arrendamientos, adquisiciones y servicios del sector público, que entre otras cosas, dan soporte legal al sistema de compranet.

Mayo 29
Se realizan reformas en materia de comercio electrónico en cuatro leyes: código de comercio, código civil federal, código federal de procedimientos civiles y ley federal de protección al consumidor.

Mayo 30
Se publica la reforma a la ley federal de procedimiento administrativo, que da la misma validez a los documentos electrónicos que a los firmados mediante autógrafo.

Octubre 6
Se firma un convenio de colaboración entre la SECOFI y el colegio nacional de correduría pública mexicana A.C. y la Asociación Nacional del Notariado Mexicano para establecer mecanismos de emisión y administración de los certificados digitales que se utilizarán para acceder al registro público de comercio.

Octubre 13
Se publicó en el DOF del Estado de Nuevo León reformas hechas al Código Civil estatal para realizar contratos electrónicos. Gracias a estas reformas, el art. 1758 del código en su capitulo II de la declaración unilateral de la voluntad, obliga a quien hace algún ofrecimiento a cumplirlo, "incluso a través de la utilización de medios electrónicos, ópticos o de cualquier otro medio tecnológico"

[12] Con información de Joel Gómez, presidente de la academia mexicana de derecho informático Sección A periódico reforma Lunes 2 de septiembre del 2002 articulo ¿quién me protege en línea?

2002

Junio 4
Se reforma la ley de instituciones de crédito, con lo que se permite a los bancos realizar operaciones con particulares por medios electrónicos.

Se expide la ley de sociedades de inversión, con lo que se hace posible dar a conocer información financiera no sólo por medios impresos, sino también electrónicos.

Norma oficial mexicana NOM-151-SCFI-2002, practicas comerciales-requisitos que deben observarse para la conservación de mensajes de datos

Salió publicado en el DIARIO OFICIAL firmado en México, D.F., a 20 de marzo de 2002. por el Director General, **Miguel Aguilar Romo** La Norma Oficial Mexicana Nom-151-Scfi-2002. Practicas Comerciales-Requisitos que deben observarse para la Conservación De Mensajes de Datos.

Notas adicionales:

La ley no ofrece ninguna protección al hacer una compra en una empresa ubicada fuera de México, según Eduardo Cantón, director de nuevas tecnologías de VISA.

Tampoco existe protección contra el SPAM.

La cámara de diputados en la actual legislatura dar impulso a la factura electrónica. Se tiene una iniciativa a la ley modelo presentada por la UNCITRAL *(de sus siglas en inglés; United Nations Comisión of International Trade Law)*

Según la Ley Federal de Protección al Consumidor en mayo del 2000, los proveedores de servicios o negocios electrónicos están obligados a proteger a los consumidores

El Art. 76 bis de esta ley, señala que el proveedor está obligado a tratar de manera confidencial la información que le proporciona al consumidor, sin venderla, traspasarla o arrendarla, a menos de que cuente con la autorización del usuario

Además se debe brindar seguridad en la transacción, así como proporcionar un domicilio físico y un número telefónico para aclaraciones. En caso de que se viole cualquiera de las disposiciones de esta ley, puede acudir a la PROFECO.

Las sanciones son multas de una a 2 mil veces el salario mínimo general vigente para el DF, lo que actualmente representa entre 40 y 100 mil pesos aproximadamente.

El Hackeo (intrusión a sistemas informáticos) y Craking (robo o destrucción de información) están contemplados en las leyes

El Código Penal Federal contempla, desde su reforma en 1999, en el título noveno, capítulo II, del artículo 211 Bis 1 a 211 Bis 7, las sanciones a quienes modifiquen, destruyan, copien o provoquen pérdida de información sin autorización en sistemas o equipos particulares, del estado o de las instituciones financieras que estén protegidos.

También contempla castigo para quienes teniendo autorización a entrar a los sistemas, protegidos por un mecanismo de seguridad, modifiquen o destruyan indebidamente la información.

Esto es si la computadora no tiene mecanismo de seguridad no está protegida para la ley, esto es para nosotros un grave defecto porque la mayoría de las computadoras en México no están protegidas.

5.2 LEGISLACIÓN EN MÉXICO, LEY DE LA SECRETARIA DE COMERCIO Y FOMENTO INDUSTRIAL[13]

29 DE MAYO DE 2000

DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO CIVIL PARA EL DISTRITO FEDERAL EN MATERIA COMÚN Y PARA TODA LA REPÚBLICA EN MATERIA FEDERAL, DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES, DEL CÓDIGO DE COMERCIO Y DE LA LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Presidencia de la República.
ERNESTO ZEDILLO PONCE DE LEON, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:
Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente
DECRETO
"EL CONGRESO DE LOS ESTADOS UNIDOS MEXICANOS, D E C R E T A:
REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CODIGO CIVIL PARA EL DISTRITO FEDERAL EN MATERIA COMUN Y PARA TODA LA REPUBLICA EN MATERIA FEDERAL, DEL CODIGO FEDERAL DE PROCEDIMIENTOS CIVILES, DEL CODIGO DE COMERCIO Y DE LA LEY FEDERAL DE PROTECCION AL CONSUMIDOR.

ARTICULO PRIMERO.- Se modifica la denominación del **Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal**, y con ello se reforman sus artículos 1o., 1803, 1805 y 1811, y se le adiciona el artículo 1834 bis, para quedar como sigue:

"CODIGO CIVIL FEDERAL
Artículo 1o - Las disposiciones de este Código regirán en toda la República en asuntos del orden federal
Artículo 1803 - El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente
I - Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y

[13] Transcribo el documento de manera integra debido a la importancia del mismo, ya que, hasta el año 2001, es el único documento de materia legal que norma el comercio electrónico y la firma digital en México

II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.
Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

Artículo 1811.- . . .
Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.

Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige."

ARTICULO SEGUNDO.- Se adiciona el artículo 210-A al **Código Federal de Procedimientos Civiles**, en los términos siguientes:

"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta."

ARTICULO TERCERO.- Se reforman los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205, y se adicionan los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32 bis 1298-A; el Título II que se denominará "Del Comercio

Electrónico", que comprenderá los artículos 89 a 94, y se modifica la denominación del Libro Segundo del Código de Comercio, disposiciones todas del referido **Código de Comercio**, para quedar como sigue:

"Artículo 18.- En el Registro Público de Comercio se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran.
La operación del Registro Público de Comercio está a cargo de la Secretaría de Comercio y Fomento Industrial, en adelante la Secretaría, y de las autoridades responsables del registro público de la propiedad en los estados y en el Distrito Federal, en términos de este Código y de los convenios de coordinación que se suscriban conforme a lo dispuesto por el artículo 116 de la Constitución Política de los Estados Unidos Mexicanos. Para estos efectos existirán las oficinas del Registro Público de Comercio en cada entidad federativa que demande el tráfico mercantil.
La Secretaría emitirá los lineamientos necesarios para la adecuada operación del Registro Público de Comercio, que deberán publicarse en el **Diario Oficial de la Federación**.

Artículo 20.- El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contarán con al menos un respaldo electrónico

Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral

Las bases de datos del Registro Público de Comercio en las entidades federativas se integrarán con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas.

El programa informático será establecido por la Secretaría. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal.

En caso de existir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en la base de datos de alguna entidad federativa, o sobre cualquier otro respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario.
La Secretaría establecerá los formatos, que serán de libre reproducción, así como los datos, requisitos y demás información necesaria para llevar a cabo las inscripciones, anotaciones y avisos a que se refiere el presente Capítulo. Lo anterior deberá publicarse en el **Diario Oficial de la Federación**.

Artículo 20 bis.- Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:

I. Aplicar las disposiciones del presente Capítulo en el ámbito de la entidad federativa correspondiente,
II. Ser depositario de la fe pública registral mercantil, para cuyo ejercicio se auxiliará de los registradores de la oficina a su cargo;

III. Dirigir y coordinar las funciones y actividades de las unidades administrativas a su cargo para que cumplan con lo previsto en este Código, el reglamento respectivo y los lineamientos que emita la Secretaría;
IV. Permitir la consulta de los asientos registrales que obren en el Registro, así como expedir las certificaciones que le soliciten,
V. Operar el programa informático del sistema registral automatizado en la oficina a su cargo, conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaría;
VI. Proporcionar facilidades a la Secretaría para vigilar la adecuada operación del Registro Público de Comercio, y
VII. Las demás que se señalen en el presente Capítulo y su reglamento.

Artículo 21.- Existirá un folio electrónico por cada comerciante o sociedad, en el que se anotarán:
I a XIX - . . .
Artículo 21 bis.- El procedimiento para la inscripción de actos mercantiles en el Registro Público de Comercio se sujetará a las bases siguientes:
I.- Será automatizado y estará sujeto a plazos máximos de respuesta;
II - Constará de las fases de:
Recepción, física o electrónica de una forma precodificada, acompañada del instrumento en el que conste el acto a inscribir, pago de los derechos, generación de una boleta de ingreso y del número de control progresivo e invariable para cada acto;
Análisis de la forma precodificada y la verificación de la existencia o inexistencia de antecedentes registrales y, en su caso, preinscripción de dicha información a la base de datos ubicada en la entidad federativa;

Calificación, en la que se autorizará en definitiva la inscripción en la base de datos mediante la firma electrónica del servidor público competente, con lo cual se generará o adicionará el folio mercantil electrónico correspondiente, y
Emisión de una boleta de inscripción que será entregada física o electrónicamente.
El reglamento del presente Capítulo desarrollará el procedimiento registral de acuerdo con las bases anteriores.

Artículo 21 bis 1.- La prelación entre derechos sobre dos o más actos que se refieran a un mismo folio mercantil electrónico, se determinará por el número de control que otorgue el registro, cualquiera que sea la fecha de su constitución o celebración.
Artículo 22.- Cuando, conforme a la ley, algún acto o contrato deba inscribirse en el Registro Público de la Propiedad o en registros especiales, su inscripción en dichos registros será bastante para que surtan los efectos correspondientes del derecho mercantil, siempre y cuando en el Registro Público de Comercio se tome razón de dicha inscripción y de las modificaciones a la misma.
Artículo 23.- Las inscripciones deberán hacerse en la oficina del Registro Público de Comercio del domicilio del comerciante, pero si se trata de bienes raíces o derechos reales constituidos sobre ellos, la inscripción se hará, además, en la oficina correspondiente a la ubicación de los bienes, salvo disposición legal que establezca otro procedimiento.
Artículo 24.- Las sociedades extranjeras deberán acreditar, para su inscripción en el Registro Público de Comercio, estar constituidas conforme a las leyes de su país de origen y autorizadas para ejercer el comercio por la Secretaría, sin perjuicio de lo establecido en los tratados o convenios internacionales.

Artículo 25.- Los actos que conforme a este Código u otras leyes deban inscribirse en el Registro Público de Comercio deberán constar en:

I. Instrumentos públicos otorgados ante notario o corredor público;
II. Resoluciones y providencias judiciales o administrativas certificadas;
III. Documentos privados ratificados ante notario o corredor público, o autoridad judicial competente, según corresponda, o
IV. Los demás documentos que de conformidad con otras leyes así lo prevean.

Artículo 26.- Los documentos de procedencia extranjera que se refieran a actos inscribibles podrán constar previamente en instrumento público otorgado ante notario o corredor público, para su inscripción en el Registro Público de Comercio.
Las sentencias dictadas en el extranjero sólo se registrarán cuando medie orden de autoridad judicial mexicana competente, y de conformidad con las disposiciones internacionales aplicables.
Artículo 27.- La falta de registro de los actos cuya inscripción sea obligatoria, hará que éstos sólo produzcan efectos jurídicos entre los que lo celebren, y no podrán producir perjuicio a tercero, el cual sí podrá aprovecharse de ellos en lo que le fueren favorables
Artículo 30.- Los particulares podrán consultar las bases de datos y, en su caso, solicitar las certificaciones respectivas, previo pago de los derechos correspondientes.
Las certificaciones se expedirán previa solicitud por escrito que deberá contener los datos que sean necesarios para la localización de los asientos sobre los que deba versar la certificación y, en su caso, la mención del folio mercantil electrónico correspondiente.
Cuando la solicitud respectiva haga referencia a actos aún no inscritos, pero ingresados a la oficina del Registro Público de Comercio, las certificaciones se referirán a los asientos de presentación y trámite.
Artículo 30 bis.- La Secretaría podrá autorizar el acceso a la base de datos del Registro Público de Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaría, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos registrales.
La Secretaría certificará los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio, así como la de los demás usuarios del mismo, y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.
Artículo 30 bis 1.- Cuando la autorización a que se refiere el artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, el envío de información por medios electrónicos al Registro y la remisión que éste efectúe al fedatario público correspondiente del acuse que contenga el número de control a que se refiere el artículo 21 bis 1 de este Código.
Los notarios y corredores públicos que soliciten dicha autorización deberán otorgar una fianza a favor de la Tesorería de la Federación y registrarla ante la Secretaría, para garantizar los daños que pudieran ocasionar a los particulares en la operación del programa informático, por un monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal.
En caso de que los notarios o corredores públicos estén obligados por la ley de la materia a garantizar el ejercicio de sus funciones, sólo otorgarán la fianza a que se refiere el párrafo anterior por un monto equivalente a la diferencia entre ésta y la otorgada.
Dicha autorización y su cancelación deberán publicarse en el **Diario Oficial de la Federación**.

Artículo 31.- Los registradores no podrán denegar la inscripción de los documentos mercantiles que se les presenten, salvo cuando:

- El acto o contrato que en ellos se contenga no sea de los que deben inscribirse;
- Esté en manifiesta contradicción con los contenidos de los asientos registrales preexistentes, o
- El documento de que se trate no exprese, o exprese sin claridad suficiente, los datos que deba contener la inscripción.

Si la autoridad administrativa o judicial ordena que se registre un instrumento rechazado, la inscripción surtirá sus efectos desde que por primera vez se presentó.
El registrador suspenderá la inscripción de los actos a inscribir, siempre que existan defectos u omisiones que sean subsanables. En todo caso se requerirá al interesado para que en el plazo que determine el reglamento de este Capítulo las subsane, en el entendido de que, de no hacerlo, se le denegará la inscripción.
Artículo 32.- La rectificación de los asientos en la base de datos por causa de error material o de concepto, sólo procede cuando exista discrepancia entre el instrumento donde conste el acto y la inscripción.

Se entenderá que se comete error material cuando se escriban unas palabras por otras, se omita la expresión de alguna circunstancia o se equivoquen los nombres propios o las cantidades al copiarlas del instrumento donde conste el acto, sin cambiar por eso el sentido general de la inscripción ni el de alguno de sus conceptos.
Se entenderá que se comete error de concepto cuando al expresar en la inscripción alguno de los contenidos del instrumento, se altere o varíe su sentido porque el responsable de la inscripción se hubiere formado un juicio equivocado del mismo, por una errónea calificación del contrato o acto en él consignado o por cualquiera otra circunstancia similar.
Artículo 32 bis - Cuando se trate de errores de concepto, los asientos practicados en los folios del Registro Público de Comercio sólo podrán rectificarse con el consentimiento de todos los interesados en el asiento.
A falta del consentimiento unánime de los interesados, la rectificación sólo podrá efectuarse por resolución judicial.
El concepto rectificado surtirá efectos desde la fecha de su rectificación.
El procedimiento para efectuar la rectificación en la base de datos lo determinará la Secretaría en los lineamientos que al efecto emitan.
Artículo 49 - Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.
Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

LIBRO SEGUNDO
DEL COMERCIO EN GENERAL

...

Artículo 80.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

TITULO II
DEL COMERCIO ELECTRONICO
Articulo 89.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos.
Articulo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:

I.- Usando medios de identificación, tales como claves o contraseñas de él, o
II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente

Articulo 91.- El momento de recepción de la información a que se refiere el artículo anterior se determinará como sigue:

I.- Si el destinatario ha designado un sistema de información para la recepción, ésta tendrá lugar en el momento en que ingrese en dicho sistema, o
II.- De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado, en el momento en que el destinatario obtenga dicha información

Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.
Articulo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo.
Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.
Articulo 93.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.
En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.
Articulo 94.- Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.

Artículo 1205.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.
Artículo 1298-A - Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada."

ARTICULO CUARTO.- Se reforma el párrafo primero del artículo 128, y se adiciona la fracción VIII al artículo 1o., la fracción IX bis al artículo 24 y el Capítulo VIII bis a la **Ley Federal de Protección al Consumidor**, que contendrá el artículo 76 bis, para quedar como sigue
"Artículo 1o -
.....
I a VII - ...
VIII - La efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.
Artículo 24 - ...
I a IX - ...
IX bis - Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por esta Ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología;
X a XXI - ...

CAPITULO VIII BIS DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVES DEL USO DE MEDIOS ELECTRONICOS, OPTICOS O DE CUALQUIER OTRA TECNOLOGIA
Artículo 76 bis - Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.
El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.
El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;

El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;
El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.
Artículo 128.- Las infracciones a lo dispuesto por los artículos 8, 10, 12, 60, 63, 65, 74, 76 bis, 80 y 121 serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal.
..."

TRANSITORIOS
Primero.- El presente Decreto entrará en vigor a los nueve días siguientes de su publicación en el **Diario Oficial de la Federación**.
Segundo.- Las menciones que en otras disposiciones de carácter federal se hagan al Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, se entenderán referidas al Código Civil Federal.
Las presentes reformas no implican modificación alguna a las disposiciones legales aplicables en materia civil para el Distrito Federal, por lo que siguen vigentes para el ámbito local de dicha entidad todas y cada una de las disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, vigentes a la entrada en vigor del presente Decreto.
Tercero.- La operación automatizada del Registro Público de Comercio conforme a lo dispuesto en el presente Decreto deberá iniciarse a más tardar el 30 de noviembre del año 2000.
Para tal efecto, la Secretaría de Comercio y Fomento Industrial proporcionará a cada uno de los responsables de las oficinas del Registro Público de Comercio, a partir de la entrada en vigor del presente Decreto y a más tardar el 31 de agosto del año 2000, el programa informático del sistema registral automatizado a que se refiere el presente Decreto, la asistencia y capacitación técnica, así como las estrategias para su instrumentación, de conformidad con los convenios correspondientes.
Cuarto.- En tanto se expide el Reglamento correspondiente, seguirán aplicándose los capítulos I a IV y VII del Título II del Reglamento del Registro Público de Comercio, publicado en el **Diario Oficial de la Federación** el 22 de enero de 1979, en lo que no se opongan a lo dispuesto en el presente Decreto.
Quinto.- La captura del acervo histórico del Registro Público de Comercio deberá concluirse, en términos de los convenios de coordinación previstos en el artículo 18 del Código de Comercio a que se refiere el presente Decreto, a más tardar el 30 de noviembre del 2002.
Sexto.- La Secretaría, en coordinación con los gobiernos estatales, determinará los procedimientos de recepción de los registros de los actos mercantiles que hasta la fecha de entrada en vigor del presente Decreto efectuaban los oficios de hipotecas y los jueces de primera instancia del orden común, así como los mecanismos de integración a las bases de datos central y a las ubicadas en las entidades federativas. Dicha recepción deberá efectuarse en un plazo máximo de ciento ochenta días contados a partir de la entrada en vigor del presente Decreto.

Séptimo.- Las solicitudes de inscripción de actos mercantiles en el Registro Público de Comercio y los medios de defensa iniciados con anterioridad a la entrada en vigor del presente Decreto, se substanciarán y resolverán, hasta su total conclusión, conforme a las disposiciones que les fueron aplicables al momento de iniciarse o interponerse.

Octavo.- La Secretaría deberá publicar en el **Diario Oficial de la Federación** los lineamientos y formatos a que se refieren los artículos 18 y 20, que se reforman por virtud del presente Decreto, en un plazo máximo de noventa días, contados a partir de la fecha de su entrada en vigor.

5.3 NORMA OFICIAL MEXICANA NOM-151-SCFI-2002, PRACTICAS COMERCIALES-REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACION DE MENSAJES DE DATOS

El Martes 4 de junio de 2002 salió publicado en el DIARIO OFICIAL firmado en México, D.F., a 20 de marzo de 2002. por el Director General, **Miguel Aguilar Romo** La Norma Oficial Mexicana Nom-151-Scfi-2002, Practicas Comerciales-Requisitos Que Deben Observarse Para La Conservación De Mensajes De Datos

Por su importancia la transcribo de manera integra:

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaria de Economía.
La Secretaria de Economia, por conducto de la Dirección General de Normas, con fundamento en los artículos 34 fracciones XIII y XXX de la Ley Orgánica de la Administración Pública Federal; 39 fracción V, 40 fracciones III y XVIII, 47 fracción IV de la Ley Federal sobre Metrologia y Normalización, y 23 fracciones I y XV del Reglamento Interior de esta Secretaría, y

CONSIDERANDO
Que es responsabilidad del Gobierno Federal procurar las medidas que sean necesarias para garantizar que los servicios que se comercialicen en territorio nacional contengan los requisitos necesarios, con el fin de garantizar los aspectos de información para lograr una efectiva protección del consumidor; Que con fecha 28 de septiembre de 2001 el Comité Consultivo Nacional de Normalización de Seguridad al Usuario, Información Comercial y Prácticas de Comercio aprobó la publicación del proyecto de Norma Oficial Mexicana PROY-NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, lo cual se realizó en el **Diario Oficial de la Federación** el 16 de noviembre del mismo año, con objeto de que los interesados presentaran sus comentarios; Que durante el plazo de 60 dias naturales contados a partir de la fecha de publicación de dicho proyecto de Norma Oficial Mexicana, la Manifestación de Impacto Regulatorio a que se refiere el artículo 45 de la Ley Federal sobre Metrología y Normalización estuvo a disposición del público en general para su consulta; y que dentro del mismo plazo, los interesados presentaron sus comentarios al proyecto de norma, los cuales fueron analizados por el citado Comité Consultivo, realizándose las modificaciones procedentes. Que con fecha 20 de marzo de 2002 el Comité Consultivo Nacional de Normalizacion de Seguridad al Usuario, Información Comercial y Prácticas de Comercio, aprobó por unanimidad la norma referida; Que la Ley Federal sobre Metrología y Normalización establece que las Normas Oficiales Mexicanas se constituyen como el instrumento idóneo para la protección de los intereses del consumidor, se expide la siguiente Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos.

México, D.F., a 20 de marzo de 2002.- El Director General, **Miguel Aguilar Romo**.- Rúbrica

NORMA OFICIAL MEXICANA NOM-151-SCFI-2002, PRACTICAS COMERCIALES-REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACION DE MENSAJES DE DATOS

PREFACIO

En la elaboración de la presente Norma Oficial Mexicana participaron las siguientes empresas e instituciones:

- ACERTIA NETWORKS, S.A. DE C.V.
- ALESTRA, S. DE R.L. DE C.V.
- ASOCIACION MEXICANA DE ESTANDARES PARA EL COMERCIO ELECTRONICO, A.C.
- ASOCIACION MEXICANA DE LA INDUSTRIA DE TECNOLOGIAS DE INFORMACION, A.C.
- ASOCIACION NACIONAL DE TIENDAS DE AUTOSERVICIO Y DEPARTAMENTALES, A.C.
- BANCO DE MEXICO.
- BANCO INTERNACIONAL, S.A.
- BANCO NACIONAL DE MEXICO, S.A.
- BBVA BANCOMER, S.A.
- CAMARA NACIONAL DE COMERCIO DE LA CIUDAD DE MEXICO.
- CAMARA NACIONAL DE LA INDUSTRIA ELECTRONICA, DE TELECOMUNICACIONES E INFORMATICA.
- CECOBAN, S.A. DE C.V.
- CONSEJO MEXICANO DE LA INDUSTRIA DE PRODUCTOS DE CONSUMO, A.C.

Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 33
- COMISION FEDERAL DE TELECOMUNICACIONES.
- COMPAÑIA PROCTER & GAMBLE MEXICO, S. DE R.L. DE C.V.
- HEWLETT PACKARD DE MEXICO, S.A. DE C.V.
- IBM DE MEXICO, S.A. DE C.V.
- INSTITUTO NACIONAL DE ESTADISTICA, GEOGRAFIA E INFORMATICA.
Dirección General de Politicas y Normas en Informática.
- KPMG CARDENAS DOSAL, S.C.
- PEGASO COMUNICACIONES Y SISTEMAS, S.A. DE C.V.
- PETROLEOS MEXICANOS.
Gerencia de Informática y Sistemas Financieros.
- PODER JUDICIAL FEDERAL.
Instituto Federal de Especialistas de Concursos Mercantiles.
- PROMOCION Y OPERACION, S.A. DE C.V.
- SECRETARIA DE ECONOMIA.
-Dirección General de Normas.
-Dirección General de Fomento al Comercio Interior.
-Dirección General de Politica de Comercio Interior y Abasto.
- SEGURIDATA PRIVADA, S.A. DE C.V.
- SERVICIO DE ADMINISTRACION TRIBUTARIA.
Administración General de Grandes Contribuyentes.
Administración General de Tecnología de la Información.
- SOFTWARE AG, S.A. DE C.V.
- VERA ABOGADOS, S.C.
- WAL-MART DE MEXICO, S.A. DE C.V.
- XEROX MEXICANA, S.A. DE C.V.
- X WEB ADOBE, S.A. DE C.V.

INDICE

0. Introducción

De conformidad con lo dispuesto por los artículos 40 de la Ley Federal sobre Metrología y Normalización en relación con el 49 del Código de Comercio, la Secretaría de Economía deberá emitir una Norma Oficial Mexicana que permita el cumplimiento de la obligación, a cargo de los comerciantes que Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 34 utilicen mensajes de datos para realizar actos de comercio, de conservar por el plazo establecido en dicho Código, el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, y cuyo contenido debe mantenerse íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta

1. Objetivo

La presente Norma Oficial Mexicana establece los requisitos que deben observarse para la conservación del contenido de mensajes de datos que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones

2. Campo de aplicación

La presente Norma Oficial Mexicana es de observancia general para los comerciantes que deban conservar los mensajes de datos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

3. Definiciones

3.1 Aceptación de autoría
A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente.
3.2 Acto de comercio
A todo acto que la legislación vigente considera como tal.
3.3 Autenticación
Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros
3.4 Archivo parcial
Al mensaje de datos representado en formato ASN.1, conforme al apéndice de la presente Norma Oficial Mexicana
3.5 ASN.1
A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis).

3.6 Bits
A la unidad mínima de información que puede ser procesada por una computadora.
3.7 Bytes
A la secuencia de 8 bits.
3.8 Clave pública
A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada.
3.9 Clave privada
A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.
3.10 Certificado digital
Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública.
3.11 Código
Al Código de Comercio
3.12 Código de error
Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 35. A la clave indicativa de un suceso incorrecto.
3.13 Comerciantes
A las personas físicas o morales a los que la legislación les otorga tal carácter.
3.14 Compromiso
A cualquier acto jurídico diferente del contrato o del convenio, que genere derechos y obligaciones.
3.15 Confidencialidad
Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada.
3.16 Contrato
Al acuerdo de voluntades que crea o transfiere derechos y obligaciones.
3.17 Convenio
Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones
3.18 Constancia del prestador de servicios de certificación
Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.
3.19 Criptografía
Al conjunto de técnicas matemáticas para cifrar información.
3.20 Destinatario
A aquella entidad a quien va dirigido un mensaje de datos.
3.21 Emisor
A aquella entidad que genera y transmite un mensaje de datos.
3.22 Entidad
A las personas físicas o morales.
3.23 Expediente electrónico
Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente norma oficial mexicana.
3.24 Firma digital
A la firma electrónica que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital es una especie de firma electrónica

TESIS CON
FALLA DE ORIGEN

que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.

3.25 Firma electrónica

A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre los datos y la identidad del firmante.

3.26 Formato

A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información.

3.27 Legislación

A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo.

3.28 Mensaje de datos

Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 36. A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

3.29 Objetos

A las definiciones del lenguaje ASN.1

3.30 Original

A la información contenida en un mensaje de datos que se ha mantenido íntegra e inalterada desde el momento en que se generó por primera vez en su forma definitiva.

3.31 Prestador de servicios de certificación

A la entidad que presta los servicios de certificación a que se refiere la presente Norma Oficial Mexicana.

3.32 Red

Al sistema de telecomunicaciones entre computadoras.

3.33 Resumen o compendio

Al resultado de aplicarle a un mensaje de datos una función de criptografía del tipo *hash*.

3.34 Sello del prestador de servicios de certificación

Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.

3.35 Secretaría

A la Secretaría de Economía.

4. Disposiciones generales

4.1 Los comerciantes deberán conservar los mensajes de datos de acuerdo al método que se describe en el Apéndice de la presente Norma Oficial Mexicana.

4.2 La información que se desee conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras.

4.3 Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre soportada en un medio físico similar o distinto a aquéllos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana. La migración de la información deberá ser cotejada por un tercero legalmente autorizado, que constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera

vez en su forma definitiva. El tercero legalmente autorizado deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente
y cumpla con los requisitos legales aplicables.
4.4 Los programas de cómputo (*software)* para la conservación de los mensajes de datos deberán dar cumplimiento a lo establecido por la presente Norma Oficial Mexicana.

5. Elementos que intervienen en la conservación de mensajes de datos
5.1 Para la emisión de la firma electrónica y/o digital, así como el prestador de servicios de certificación, deberán observar los requisitos que la normatividad aplicable señale para su operación.
5.2 La constancia emitida por el prestador de servicios de certificación deberá observar los términos establecidos en el Apéndice de la presente Norma Oficial Mexicana.
5.3 Los programas informáticos en y con los que se almacenen los mensajes de datos a los que se refiere la presente Norma Oficial Mexicana, utilizarán los formatos para mensajes de datos en los términos establecidos en el Apéndice del mismo.

6. Vigilancia
La vigilancia de la Norma Oficial Mexicana estará a cargo de la Secretaría conforme a sus atribuciones y la legislación aplicable.

TESIS CON
FALLA DE ORIGEN

7. Apéndice Normativo

INTRODUCCION
En este Apéndice normativo se presentan los elementos necesarios para la implantación de la presente Norma Oficial Mexicana; la descripción del algoritmo de conservación de información y la definición ASN.1 de los objetos usados.
Se describe brevemente el algoritmo y se muestran dos archivos de texto que serán usados para construir los objetos ASN.1 resultantes de aplicar la presente Norma Oficial Mexicana a estos dos archivos. Los objetos ASN.1 creados son mostrados a través de un vaciado hexadecimal de su contenido en formato BER. Se incluyen las claves de criptografía que se usaron en la creación de los ejemplos con el propósito de que se pueda verificar la implantación de la presente Norma Oficial Mexicana.

El contenido de los archivos, las definiciones pertenecientes al lenguaje ASN.1 y los archivos ASN.1 aparecen con el tipo Courier New. Cuando se use el nombre de un objeto ASN.1 dentro del texto, éste aparecerá en *itálicas*. Como referencia se presenta el juego de caracteres ISO 8859-1 (Latin 1)

FORMACION DE ARCHIVOS PARCIALES
Para formar un *archivo parcial* se crea un mensaje en formato ASN.1 que contiene (i) el nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo, (ii) el tipo del archivo, y (iii) el contenido del mismo; con el objetivo de guardar la relación lógica que existe entre estos tres elementos.

OBTENCION DE LOS COMPENDIOS O RESUMENES DIGITALES
Se calcula el compendio o resumen digital del *archivo o archivos parciales* resultado del proceso anterior, usando el algoritmo MD5.

INTEGRACION DELEXPEDIENTE ELECTRONICO
Para conformar un *expediente electrónico* se creará un mensaje ASN.1 que contiene **(i)** el nombre del *expediente*, que debe de coincidir con el nombre con el que se identifica en el

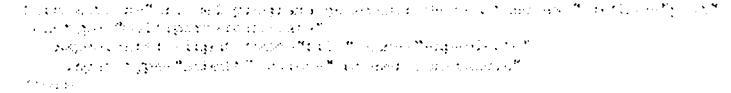
sistema de información en donde está o estuvo almacenado, **(ii)** un índice, que contiene el nombre y el compendio de cada *archivo parcial* que integra el *expediente*, **(iii)** la identificación del operador del sistema de conservación, y **(iv)** su firma digital de acuerdo a la definición correspondiente en la presente Norma Oficial Mexicana.

OBTENCION DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACION

Para la obtención de la *constancia* el sistema de conservación deberá usar el protocolo de aplicación descrito en este apéndice para enviar el *expediente* al prestador de servicios de certificación, quien emitirá una *constancia* en formato ASN.1 y la regresará al sistema de conservación, haciendo uso del mismo protocolo.

El expediente opcionalmente podrá enviarse como un anexo de correo electrónico, siendo aplicables en este caso los protocolos Internet correspondientes.

También podrá usarse la transmisión vía Web siempre que el expediente se reciba como un archivo y siempre que se utilice un directorio protegido por nombre de usuario y contraseña. Para ello, la forma en que lo envíe deberá ser como la siguiente:



La constancia deberá regresar al cliente como un archivo de tipo mime application/octet-stream1. El prestador de servicios de certificación podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes.

FORMACION DE LA CONSTANCIA

El prestador de servicios de certificación formará una *constancia* en formato ASN.1 que contendrá **(i)** el nombre del archivo en donde está almacenada la *constancia*, **(ii)** el *expediente* enviado por el sistema de conservación, **(iii)** fecha y hora del momento en que se crea la *constancia*, **(iv)** la identificación del prestador de servicios de certificación y **(v)** su firma digital de acuerdo a la definición correspondiente de esta Norma Oficial Mexicana.

METODO DE VERIFICACION DE AUTENTICIDAD

La verificación de la autenticidad de una *constancia* se realizará por medio del uso de un sistema de verificación que lleve a cabo los pasos siguientes:

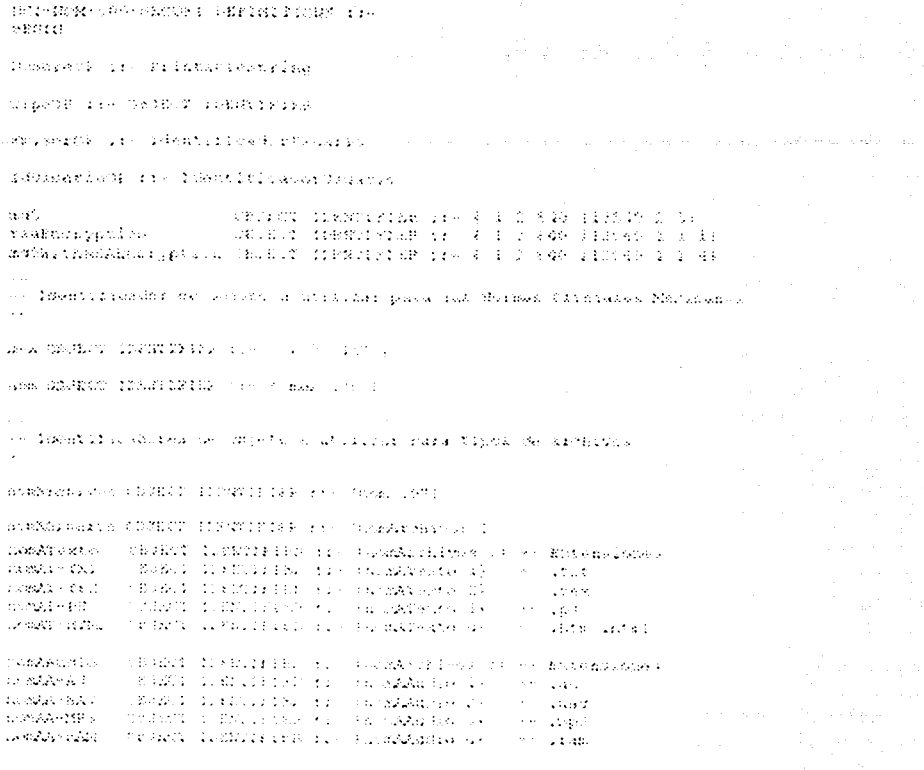
i) verificar la firma digital del prestador de servicios de certificación en la *constancia*;

ii) verificar la firma digital del operador del sistema de conservación en el *expediente* contenido en la *constancia*, y

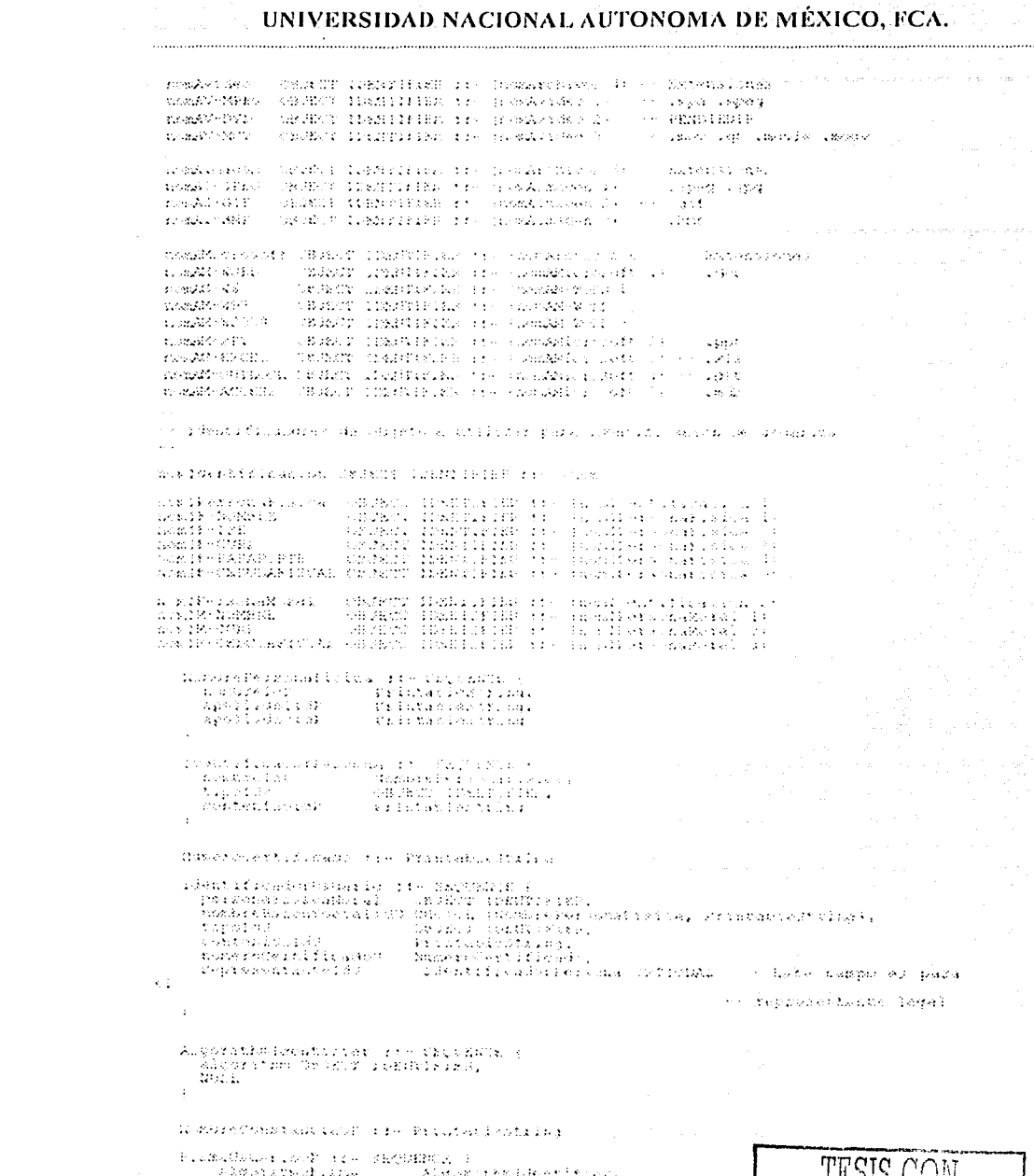
iii) recalcular el compendio de él o los *archivos parciales* y verificar que coincidan con los compendios asentados en el *expediente*.

TESIS CON
FALLA DE ORIGEN

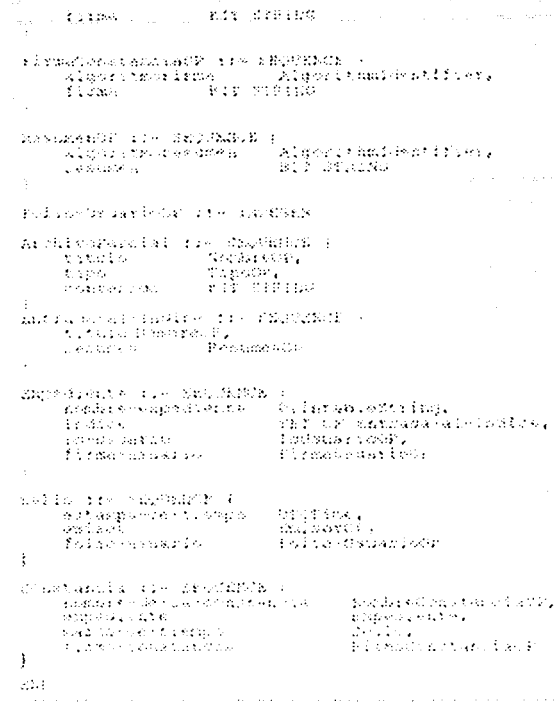
Definición ASN.1



TESIS CON
FALLA DE ORIGEN



TESIS CON
FALLA DE ORIGEN



TESIS CON
FALLA DE ORIGEN

En el programa ASN.1 se definen primeramente los identificadores de objeto necesarios para identificar los tipos de archivo que se podrán almacenar observando la presente Norma Oficial Mexicana; estas definiciones podrian ser objeto de revisiones periódicas para incluir nuevos formatos, luego los objetos necesarios para almacenar los archivos o mensajes de datos que serán conservados. A lo largo del programa se definen diferentes objetos ASN.1 cuyo uso dentro del programa aclara su función.

El campo *firma-usuario* del objeto *expediente* es la firma digital de los campos *nombre-expediente*, *índice* e *id-usuario* concatenados en ese orden, vistos como una secuencia de bytes. En el objeto *sello*, el campo *estampa-de-tiempo* es la fecha y hora en formato GMT o IMT con la cual se creó el *sello*, *emisor* es el representante del prestador de servicios de certificación que está creando el *sello* y *folio-usuario* es un número secuencial ascendente para cada usuario registrado del prestador de servicios de certificación. Es decir, cada usuario llevará un registro numerado consecutivamente de cada operación que registra el prestador de servicios de certificación.

El objeto *Constancia* contiene un campo *nombre-de-la-constancia* que almacena el nombre del archivo de computadora donde se guardará dicha *constancia* en el sistema de información del prestador de servicios

de certificación, *expediente* que es de tipo *Expediente* y es la información que se registra con el prestador de servicios de certificación con un *sello* emitido por ella, este *sello*

contiene la fecha y la hora del momento en que se crea la *Constancia*. El campo *firma-constancia* es la firma digital de los campos *nombre-de-la constancia*, *expediente*, *marca-de-tiempo* concatenados en ese orden y vistos como una secuencia de bytes.

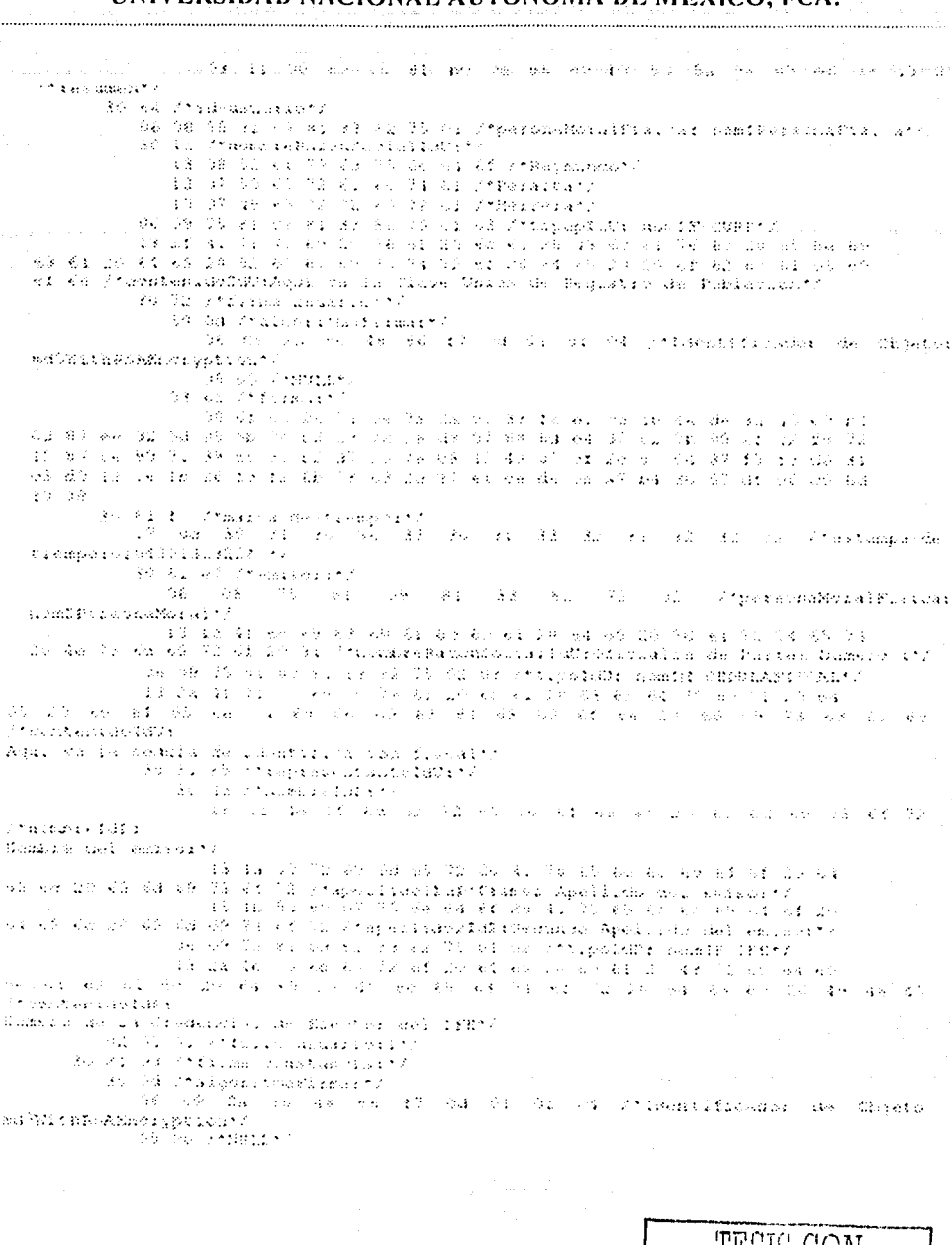
El ejemplo de codificación está organizado de la siguiente forma: primero se presentan dos archivos que se desea conservar, a continuación se construyen cada uno de los objetos ASN.1 correspondientes, **(i)** los *archivos parciales*, **(ii)** el *expediente* que está almacenado en un archivo de nombre "docusuario.ber" y **(iii)** la *Constancia* que está en el archivo "recibo.ber". Los nombres de los archivos que almacenan al *expediente*, *constancia* y *archivos parciales* están almacenados en los campos nombre-expediente, nombre-de-la-constancia y titulo respectivamente (ver Definición ASN.1).

Enseguida se presenta el contenido de los objetos ASN.1 correspondientes. La línea "==========" representa el principio y el fin del archivo respectivamente y no forma parte del archivo.
Los objetos ASN.1 que se presentan están en formato BER y se muestra un vaciado hexadecimal comentado.

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN



TESIS CON
FALLA DE ORIGEN

Claves privadas usadas para firmar

Con el propósito de poder verificar los objetos ASN.1 definidos en este documento se incluyen las claves privadas que fueron usadas para generar las firmas de los documentos mencionados. Durante el proceso de generación de claves no se generó la clave pública y ya se ha perdido la información de generación de dichas claves. Las claves y los resultados presentados pueden ser usadas únicamente para verificar los formatos de este ejemplo.

Clave privada de usuario

Clave privada de usuario

Clave privada del prestador de servicios de certificación

TESIS CON
FALLA DE ORIGEN

Front End de Comunicaciones (FEC, referencia de implantación para el prestador de servicios de certificación)

Introducción

El FEC es un programa desarrollado para manejar las comunicaciones en aplicaciones con arquitectura cliente/servidor, fue diseñado pensando en aplicaciones que requieran intercambiar mensajes en tiempo real. Se puede usar la definición de este sistema para especificar el protocolo de comunicación entre los clientes del prestador de servicios de certificación y los sistemas que se indican en la presente Norma Oficial Mexicana. La Secretaría de Economía deberá contar con un sistema de referencia para que el o los prestadores de servicios de certificación tengan un estándar contra el cual verificar que la implantación de la norma es correcta. Los objetivos del FEC son:

Simplificar la programación de los sistemas con arquitectura cliente / servidor, de tal manera que al desarrollar un sistema se dejen a un lado los detalles relacionados al manejo de las comunicaciones y el esfuerzo se centre en los detalles propios del sistema.

Lograr un ambiente de operación flexible que permita la interacción de programas desarrollados en distintas plataformas, sistemas operativos y lenguajes.

Optimizar el uso de los recursos y permitir que los sistemas que lo usen operen en tiempo real. El FEC se encarga de realizar algunas tareas que, en la arquitectura cliente/ servidor tradicional, serían realizadas por el servidor, por ejemplo:

- Autenticar a los clientes que desean establecer comunicación con algún servidor.
- Notificar la conexión o desconexión de un cliente al servidor adecuado.
- Notificar a los clientes si un servidor está o no en servicio.
- Verificar continuamente el estado de los clientes y servidores conectados.

Es por ello que su uso proporciona las siguientes ventajas:

- Provee de transparencia en la localización de clientes y servidores.
- Simplifica la programación de servidores.
- Permite la interacción de programas desarrollados en distintas plataformas.
- Minimiza el uso de recursos de la red de comunicaciones.

Esquema de operación

El modelo básico de operación del FEC se muestra en la figura 1, en ella se esquematiza un programa cliente, el FEC y un programa servidor. El esquema de operación es simple: el FEC se encarga de aceptar las conexiones de los clientes, autentificar y, en caso de que el servicio al que se deseen conectar se encuentre en operación, avisar a este último de la conexión del cliente.

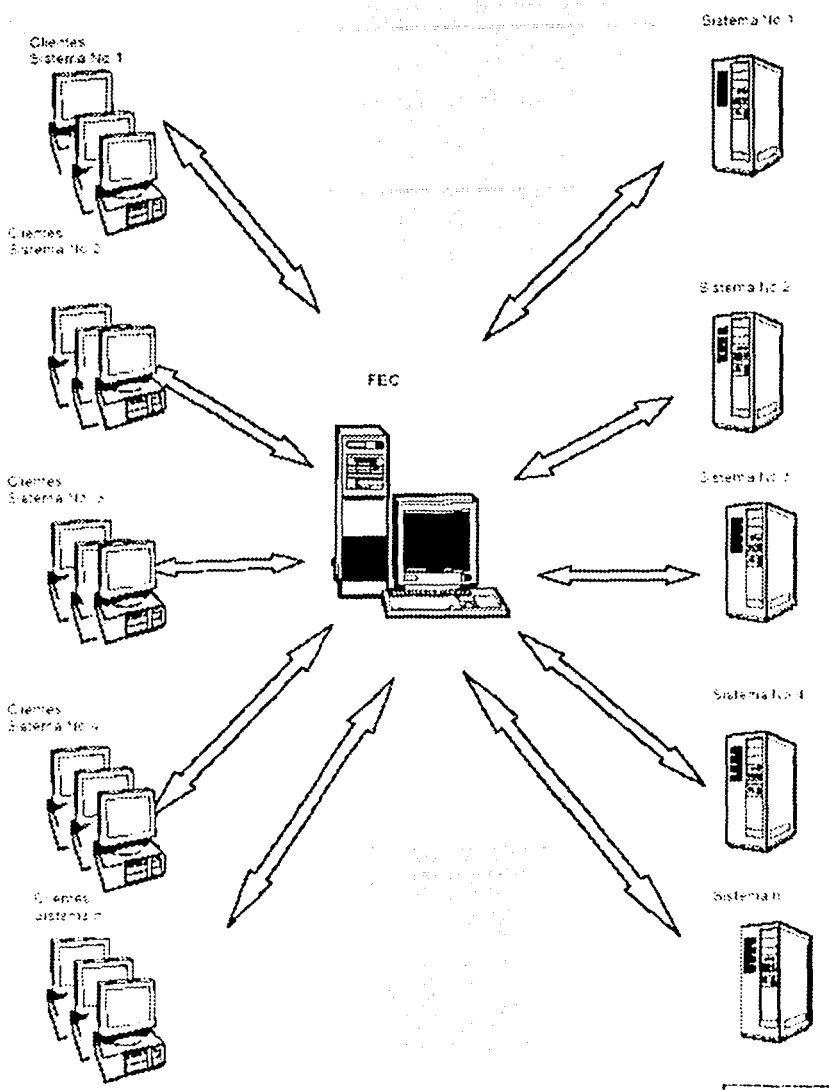
TESIS CON
FALLA DE ORIGEN

Figura 1. Esquema básico de operación del FEC

En este esquema los clientes no establecen comunicación directa con el servidor, en lugar de ello envían sus mensajes a través del FEC, éste los toma y los entrega al servidor

Del mismo modo, el FEC recibe los mensajes del servidor y los entrega al cliente indicado por éste. Visto a grandes rasgos, una vez realizada la autenticación de clientes y servidores, la labor del FEC se limita a registrar y transmitir los mensajes de los clientes al servidor adecuado y viceversa, es decir, el FEC es únicamente un mecanismo de enlace entre clientes y servidores.

TESIS CON
FALLA DE ORIGEN



En la figura 2 se muestra un esquema de la operación del FEC

TESIS CON
FALLA DE ORIGEN

Comunicaciones en el FEC

Manejo de Comunicaciones en el FEC

A fin de minimizar el tráfico en la red de comunicaciones y permitir el intercambio de información entre programas desarrollados en distintos lenguajes y sistemas operativos, el FEC utiliza un protocolo de comunicación abierto.

En este protocolo todos los mensajes constan de dos partes: encabezado y cuerpo, como se muestra en la figura 3.

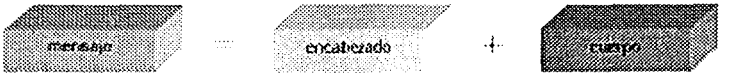


Figura 3. Todos los mensajes están formados por encabezado y cuerpo

Tanto el encabezado como el cuerpo de los mensajes se construyen con los tipos de datos básicos de todos los lenguajes de programación: char, int, short, string. Es importante mencionar que el protocolo utilizado permite, a partir de los tipos de datos mencionados y respetando ciertas reglas (similares a las de las expresiones regulares), construir cualquier tipo de mensaje. La única restricción para que los programas intercambien información es que acuerden de antemano el "formato" de los mensajes que se enviarán durante la operación.

Encabezado de los Mensajes

En el protocolo del FEC, la longitud del encabezado de un mensaje depende del destinatario, por ejemplo, en los mensajes que envían los clientes y servidores hacia el FEC, así como los mensajes que envía el FEC a los clientes, el encabezado tiene una longitud de 4 bytes con la estructura que se muestra en la figura 4.

Encabezado
FEC Cliente

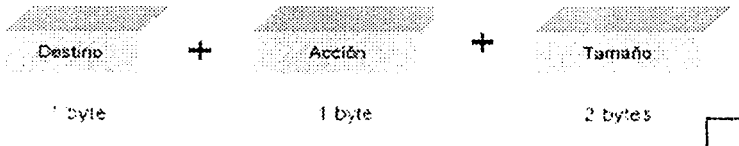


Figura 4. Encabezado de un mensaje FEC ### Cliente

TESIS CON
FALLA DE ORIGEN

A continuación se explican los campos que lo forman:

- *Destino*. Servidor o Cliente a quien se desea enviar el mensaje (1 byte).
- *Acción*. Instrucción o procesamiento que se desea realizar (1 byte).
- *Tamaño*. Longitud en bytes del cuerpo del mensaje, sin incluir el encabezado (2 bytes).

Por otra parte, el encabezado de los mensajes que el FEC envía a los servidores tiene una longitud de 12 bytes y la estructura que se muestra en la figura 5.

Los elementos que conforman este encabezado son:

- *Origen*. Cliente que envía el mensaje (1 byte).
- *Acción*. Instrucción o procesamiento que se desea realizar (1 byte).
- *Año, Mes, Día*. Fecha en que el FEC recibió el mensaje (2 bytes cada campo).
- *Hora*. Hora en que el FEC recibió el mensaje.
- *Tamaño*. Longitud en bytes del cuerpo del mensaje, sin incluir el encabezado (2 bytes).

La existencia de estos dos tipos de encabezado se debe a la necesidad de llevar un registro detallado de los mensajes que se transfieren a los servidores a través del FEC, además de proveer un cierto grado de seguridad. Es por ello que antes de transferir un mensaje a un servidor, el FEC debe colocarle una estampa de tiempo que certifique la fecha y hora en que se recibió.

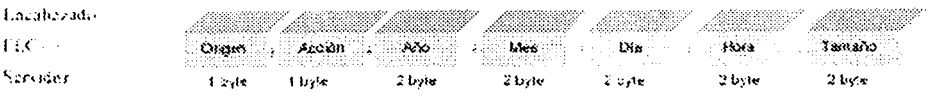


Figura 5. Encabezado de un mensaje FEC => Servidor

Cuerpo de los mensajes

Esta parte del mensaje es de longitud variable y puede construirse como una expresión regular a partir de los tipos de datos mencionados anteriormente.

El elemento *Acción* en el encabezado de un mensaje indica la solicitud de que se ejecute una determinada instrucción o procesamiento. En algunos casos, para realizar dicha *Acción* se requiere de información adicional. El contenido e interpretación del cuerpo de un mensaje depende de la *Acción* indicada en su encabezado, es decir, el cuerpo de un mensaje debe respetar un "formato" previamente establecido entre quien lo envía y quien debe ejecutar la acción solicitada.

Como este "formato" se establece de antemano entre los interesados, cuando se recibe un mensaje basta conocer la *Acción* del encabezado para deducir la forma en que debe interpretarse el cuerpo, es decir, su "formato".

El "formato" de un mensaje es una secuencia de tipos de datos básicos que describe su contenido Para facilitar la lectura e interpretación de estas secuencias, a cada tipo de dato se le ha asignado un símbolo, el
cual se muestra a continuación[14] :

Tipo de dato	Símbolo	Tamaño en bytes
Char	%c	1
Int	%l	4
Short	%d	2
String	%s	Libre
N	n	4

Nota: Dado que el protocolo de comunicación del FEC es abierto, toda la información viaja en formato de red.

Interpretación del formato de un mensaje

Para reafirmar la idea de "formato", a continuación se muestra el "formato" del encabezado y cuerpo de algunos mensajes utilizados por el protocolo del FEC.

[14] El tipo de dato string que se maneja en el protocolo no tiene una longitud fija e incluye el carácter de fin de cadena Es muy importante que se considere la longitud de cada tipo de dato al desarrollar su software, sobretodo si utiliza un sistema operativo diferente a Linux

Formato del encabezado de 4 bytes: "%c%c%d". En una trama de bytes con este formato viajan tres datos. El primer y segundo dato vienen en el primer y segundo bytes de la trama respectivamente.

El valor del tercer dato debe obtenerse de los dos últimos bytes de la trama. Lo anterior puede deducirse de la tabla donde se muestra la longitud de los elementos que conforman los mensajes[15]

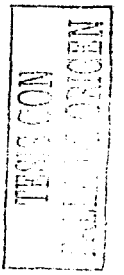
Formato del encabezado de 12 bytes: "%c%c%d%d%d%d%d". En una trama de bytes con este formato contiene siete datos. Los dos primeros tienen una longitud de un byte y los restantes 5 de dos bytes cada uno.

Formato del mensaje Greeting "%s %l". Este mensaje se utiliza para avisar a un servidor de la conexión de un cliente. Contiene dos datos: el nombre del cliente en una cadena de longitud indefinida, pero terminada con el carácter de fin de cadena, y a continuación su clave en un valor de 4 bytes.

Formato del mensaje Login: "%s". Se utiliza cuando un cliente envía su login a un servidor, contiene una cadena con la información.

Formato cualquiera: "%c %d %l %s n(%c %d %l %s)". Este formato contiene un número variable de datos. Podemos deducir que primero viene un dato que ocupa un byte (es decir un valor entre 0 y 255), después un dato que ocupa 2 bytes, luego uno que ocupa 4 bytes, a continuación una cadena cuya longitud se desconoce y después una serie de "n" elementos, este número "n" es un valor de 4 bytes. A continuación vienen "n" elementos de un byte, "n" elementos de 2 bytes, "n" elementos de 4 bytes y finalmente "n" cadenas.

Este último formato muestra el potencial del protocolo de comunicación, el cual permite construir mensajes de longitud y contenido variable.



Construcción de mensajes

Dado que el campo Acción en el encabezado de un mensaje tiene una longitud de 1 byte, existen únicamente 255 acciones válidas en la operación de un sistema.
Aunque cada aplicación es la encargada de determinar el número de acciones que requiere y la información que debería incluirse en el cuerpo de los mensajes a enviar, resulta evidente que existe un conjunto de acciones comunes a todos los sistemas que interactúen con el FEC (por ejemplo los mensajes para establecer o terminar la conexión con el FEC), es por ello que algunos de los 255 posibles mensajes están reservados a estas acciones comunes a todos los sistemas. En esta sección se indican cuáles son estos mensajes reservados y se dan ejemplos de su construcción.

Mensajes reservados

En esta sección se muestran los mensajes que deben usar los programas que se desee establecer comunicación con el FEC y el formato de éstos el hecho de que no aparezca un formato asociado a un tipo de mensaje indica que no se requiere información adicional para realizar la acción solicitada, es decir, este tipo de mensajes tienen un cuerpo nulo.

[15] Tome en cuenta las longitudes de los tipos de datos mostrados en la tabla de la sección anterior y además recuerde que los datos viajan en formato de red, es decir, una vez obtenidos deberán transformarse al formato de la computadora receptora.

En la siguiente sección se muestra la manera de construirlos.

Mensajes reservados para el FEC

Acción	Nombre	Formato	Descripción
236	CONFPASSWD		Confirma a un cliente que su contraseña fue cambiada exitosamente
243	DEADSRVR		Avisa a un cliente que el servidor ha dejado de operar
244	BYE		Avisa a un servidor que un cliente se desconectó
245	AREYOUALIVE		Pregunta a un cliente/servidor si opera correctamente
247	GREETING	%s%s	Avisa a un servidor de la conexión de un cliente incluye nombre y clave del cliente
249	CHPSWDFAIL		Avisa a un cliente que su contraseña no pudo ser cambiada
251	LOGINFAIL		Avisa a un cliente que su conexión fue rechazada
252	NOSERVICE		El servidor al que desea conectarse esta fuera de servicio
253	LOGGED	%d	Avisa a un cliente que su conexión fue aceptada
254	LOGINREQ		Solicita a un cliente su clave de usuario para autenticarlo
255	PASSWREQ		Solicita a un cliente su contraseña para autenticarla

Mensajes comunes a todos los clientes

Acción	Nombre	Formato	Descripción
0	LOGOUT		Avisa al FEC del fin de la conexión
1	LOGIN	%s	Envía clave de usuario al FEC
2	PASSWD	%s	Envía contraseña al FEC
7	IAMALIVE		Avisa a FEC que opera sin problemas
16	CONEXION		Solicita conexión al FEC
212	CHANGEPASS	%s	Solicita cambio de contraseña envía nueva contraseña al FEC

Ejemplos de construcción de mensajes

Para lograr que nuestro protocolo sea abierto debemos enviar los datos en una forma tal que cualquier computadora pueda interpretarlos adecuadamente. Por ejemplo, cuando una computadora envía un entero de 32 bits a otra. El hardware se encarga de transportar los bits desde la primer computadora a la segunda sin cambiar el orden, sin embargo, no todas las computadoras almacenan los enteros de 32 bits de la misma manera.

En algunos casos la dirección más baja de memoria contiene el byte menos significativo del entero (formato Little Endian). En otros, la dirección más baja de memoria contiene el byte más significativo del entero (Formato Big Endian). Estas dos maneras de almacenar datos se ilustran en la figura 6 [16]. Internet resuelve el problema del orden de los bytes al definir un estándar de red que debe utilizarse para intercambiar datos. Las computadoras que intercambian información deben convertir sus datos de la representación local a la

[16] En la figura 6 el contenido de cada byte se ha representado en formato hexadecimal unicamente con fines ilustrativos, **esto no significa que en el protocolo los valores deban enviarse en formato hexadecimal.**

TESIS CON

representación estándar de red antes de enviarlos. Al recibir datos deben convertirlos de la representación estándar de red a la representación local.

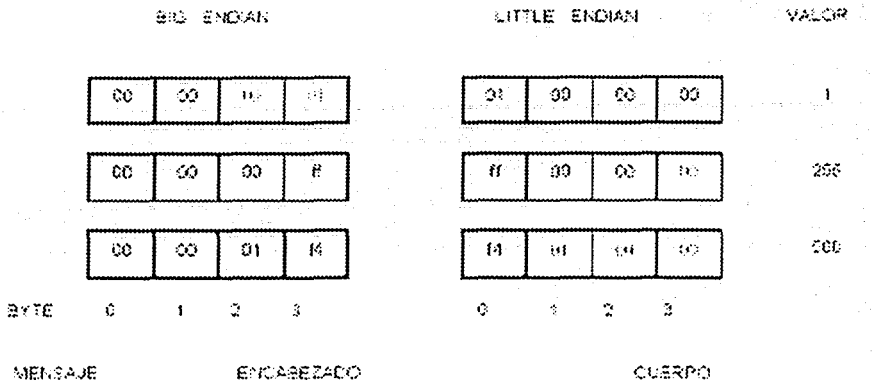
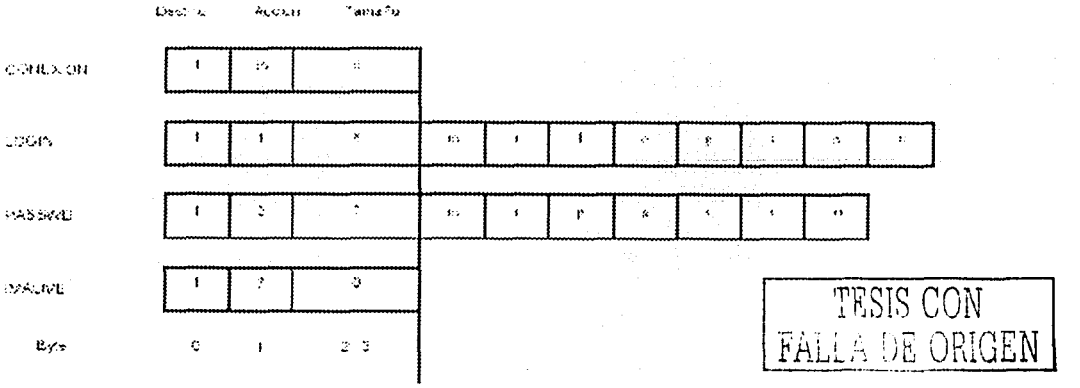


Figura 6. Diferentes Representaciones de Datos

El estándar de red de Internet indica que primero debe enviarse el byte más significativo de un entero, es decir, si uno considera los bytes sucesivos de un paquete viajando de una computadora a otra, los enteros en ese paquete tienen su byte más significativo cerca del inicio y el byte menos significativo cerca del final del paquete.

Nuestro protocolo utiliza el estándar de red de Internet para intercambiar información. En la figura 7 representamos los mensajes necesarios para que un cliente establezca comunicación con el FEC siguiendo el estándar antes mencionado[17] . No olvide que los valores deben enviarse en formato de red.



TESIS CON
FALLA DE ORIGEN

Figura 7. Construcción de Mensajes para Conectarse al FEC

[17] Observe que en el campo Destino se ha colocado el valor "1", esto indica que se quiere establecer comunicacion con un servidor cuya clave de identificación es "1" Todos los servidores conectados al FEC tienen asignada una clave de identificación.

Secuencia de Conexión
Recepción y transmisión de mensajes en el FEC

La secuencia de recepción y transmisión de mensajes en el FEC se muestra en la figura 8.
El mecanismo es el siguiente:

1. El cliente C envía al FEC un mensaje destinado al servidor S, este mensaje tiene un encabezado de 4 bytes.
2. El FEC recibe el mensaje y analiza el encabezado para determinar a quién debe transferirlo, incluye en el encabezado original una estampa de tiempo y lo envía al destinatario adecuado.
3. El servidor S recibe un mensaje del FEC cuyo encabezado es de 12 bytes, en él se indica quien lo originó y a que hora se recibió en el FEC.
4. El servidor S envía un mensaje dirigido al cliente C, este mensaje tiene un encabezado de 4 bytes.
5. El FEC recibe el mensaje del Servidor S, analiza el encabezado, determina a quién debe transferirlo y lo envía.

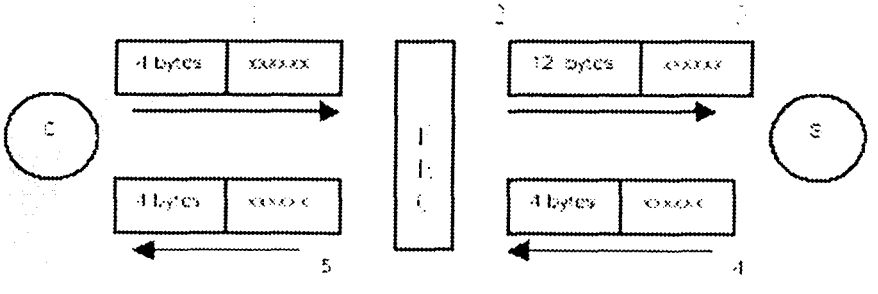


Figura 8. Secuencia de transmisión y recepción de Mensajes en el FEC

Conexión entre un Cliente y el FEC
El intercambio de mensajes que debe llevarse a cabo para que un cliente establezca conexión con el FEC se esquematiza en la figura 9.

TESIS CON
FALLA DE ORIGEN

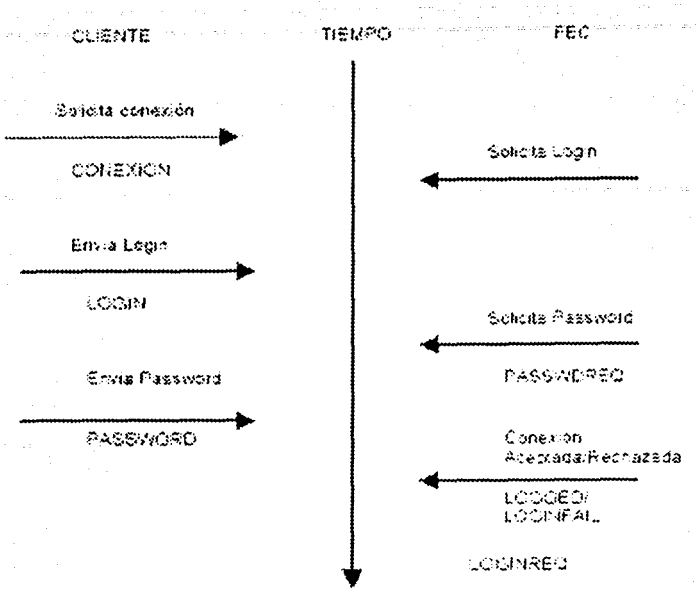


Figura 9. Esquema de conexión de un cliente con el FEC

Protocolo de comunicación entre el software de almacenamiento y el prestador de servicios de certificación

Se define el protocolo para solicitar una constancia como el procedimiento siguiente:

1. El usuario genera, a partir de sus mensajes de datos los *archivos parciales* necesarios para hacer con ellos un *expediente* el cual enviará al prestador de servicios de certificación Solicitud de conexión por parte del usuario ante el prestador de servicios de certificación e identificación entre ellos usando un esquema seguro de identificación con certificados digitales (este proceso puede darse mediante un esquema de clave de usuario y contraseña en una primera etapa)

2. El prestador de servicios de certificación genera una *Constancia* a partir del *Expediente* recibido, dicha constancia se registra en las bases de datos del prestador de servicios de certificación y se envía una copia de ese mensaje ASN.1 al usuario.

3. El usuario almacena su *Constancia* como considere conveniente.

MENSAJES TIPO FEC

Mensajes del usuario al prestador de servicios de certificación.

TESIS CON
FALLA DE ORIGEN

MENSAJES TIPO FEC

Mensajes del usuario al prestador de servicios de certificación:

Nombre	Acción	Formato	Descripción	Posible respuesta
SolConsta	12	%l %d n(%c)	Envío de un *Expediente* a la OP El campo %l contiene un identificador del documento (por sesión) para la transmisión El campo %d puede tener los siguientes valores 0 - Primer y único envío 1 - Primero de varios envíos 2 - Envío intermedio 3 - Último envío El campo n(%c) representa el *Expediente* como una secuencia de caracteres, en formato ASN.1	ConstaOP DocNoVal

Mensajes del prestador de servicios de certificación al usuario:

Nombre	Acción	Formato	Descripción
ConstaOP	22	%l %d n(%c)	La OP envía una *Constancia* al usuario El campo %l contiene un identificador del documento (por sesión) para la transmisión, este es el mismo valor que el enviado por el usuario en el mensaje SolConsta El campo %d puede tener los siguientes valores 0 - Primer y único envío 1 - Primero de varios envíos 2 - Envío intermedio 3 - Último envío El campo n(%c) representa el *Constancia* como una secuencia de caracteres, en formato ASN.1
DocNoVal	23	%d	Contiene un código de error que indica el motivo por el cual no se llevó a cabo la creación de la constancia solicitada Los posibles valores son -1 Error en los tipos de datos básicos -2 Expediente electrónico de usuario incompleto -3 Algoritmo de resumen o compendio de firma desconocido -4 Identificador de usuario inválido -5 Firma de usuario inválida

TESIS CON
FALLA DE ORIGEN

Juego de caracteres ISO 8859-1 (Latin 1)

Char	Code (código) (en decimal)	Name (nombre)	Description (descripción)
	32	-	Normal space
!	33	-	Exclamation
"	34	quot	Double quote
#	35	-	Hash or pound
$	36	-	Dollar
%	37	-	Percent
&	38	-	Ampersand
'	39	-	Apostrophe
(	40	-	Open bracket
)	41	-	Close bracket
*	42	-	Asteri.

TESIS CON
FALLA DE ORIGEN

+	43	-	Plus sign
,	44	-	Comma
-	45	-	Minus sign
.	46	-	Period
/	47	-	Forward slash
0	48	-	Digit 0
1	49	-	Digit 1
2	50	-	Digit 2
3	51	-	Digit 3
4	52	-	Digit 4
5	53	-	Digit 5
6	54	-	Digit 6
7	55	-	Digit 7
8	56	-	Digit 8
9	57	-	Digit 9
:	58	-	Colon
;	59	-	Semicolon
<	60	lt	Less than
=	61	-	Equals
>	62	gt	Greather than
?	63	-	Question mark
@	64	-	At sign
A	65	-	A
B	66	-	B
C	67	-	C
D	68	-	D
E	69	-	E
F	70	-	F
G	71	-	G
H	72	-	H
I	73	-	I
J	74	-	J
K	75	-	K
L	76	-	L
M	77	-	M
N	78	-	N
O	79	-	O
P	80	-	P
Q	81	-	Q
R	82	-	R
S	83	-	S
T	84	-	T
U	85	-	U
V	86	-	V
W	87	-	W
X	88	-	X
Y	89	-	Y
Z	90	-	Z
[	91	-	Open square bracket
\	92	-	Backslash
]	93	-	Close square bracket
^	94	-	Pointer
_	95	-	Underscore

TESIS CON FALLA DE ORIGEN

`	96	-	Grave accent
a	97	-	a
b	98	-	b
c	99	-	c
d	100	-	d
e	101	-	e
f	102	-	f
g	103	-	g
h	104	-	h
i	105	-	i
j	106	-	j
k	107	-	k
l	108	-	l
m	109	-	m
n	110	-	n
o	111	-	o
p	112	-	p
q	113	-	q
r	114	-	r
s	115	-	s
t	116	-	t
u	117	-	u
v	118	-	v
w	119	-	w
x	120	-	x
y	121	-	y
z	122	-	z
{	123	-	Left brace
|	124	-	Vertical bar
}	125	-	Right brace
~	126	-	Tilde
	160	nbsp	Non-breaking space
¡	161	iexcl	Inverted exclamation
¢	162	cent	Cent sign
£	163	pound	Pound sign
¤	164	curren	Currency sign
¥	165	yen	Yen sign
¦	166	brvbar	Broken bar
§	167	sect	Section sign
¨	168	uml	Umlaut or dieresis
©	169	copy	Copyright sign
ª	170	ordf	Feminine ordinal
«	171	laquo	Left angle quotes
¬	172	not	Logical not sign
-	173	shy	Soft hypher
®	174	reg	Registered trademark
¯	175	macr	Spacing macron
°	176	deg	Degree sign
±	177	plusmn	Plus-minus sign
²	178	sup2	Superscript 2
³	179	sup3	Superscript 3
´	180	acute	Spacing acute
µ	181	micro	Micro sign

TESIS CON
FALLA DE ORIGEN

¶	182	para	Paragraph sign
·	183	middot	Middle dot
¸	184	cedil	Spacing cedilla
¹	185	sup1	Superscript 1
º	186	ordm	Masculine ordinal
»	187	raquo	Right angle quotes
¼	188	frac14	One quarter
½	189	frac12	One half
¾	190	frac34	Three quarters
¿	191	iquest	Inverted question mark
À	192	Agrave	A grave
Á	193	Aacute	A acute
Â	194	Acirc	A circumflex
Ã	195	Atilde	A tilde
Ä	196	Auml	A umlaut
Å	197	Aring	A ring
Æ	198	AElig	AE ligature
Ç	199	Ccedil	C cedilla
È	200	Egrave	E grave
É	201	Eacute	E acute
Ê	202	Ecirc	E circumflex
Ë	203	Euml	E umlaut
Ì	204	Igrave	I grave
Í	205	Iacute	I acute
Î	206	Icirc	I circumflex
Ï	207	Iuml	I umlaut
Ð	208	ETH	ETH
Ñ	209	Ntilde	N tilde
Ò	210	Ograve	O grave
Ó	211	Oacute	O acute
Ô	212	Ocirc	O circumflex
Õ	213	Otilde	O tilde
Ö	214	Ouml	O umlaut
×	215	times	Multiplication sign
Ø	216	Oslash	O slash
Ù	217	Ugrave	U grave
Ú	218	Uacute	U acute
Û	219	Ucirc	U circumflex
Ü	220	Uuml	U umlaut
Ý	221	Yacute	Y acute
Þ	222	THORN	THORN
ß	223	szlig	sharp s
à	224	agrave	a grave
á	225	aacute	a acute
â	226	acirc	a circumflex
ã	227	atilde	a tilde
ä	228	auml	a umlaut
å	229	aring	a ring
æ	230	aelig	ae ligature
ç	231	ccedil	c cedilla
è	232	egrave	e grave
é	233	eacute	e acute
ê	234	ecirc	e circumflex

TESIS CON
FALLA DE ORIGEN

ë	235	euml	e umlaut
ì	236	igrave	i grave
í	237	iacute	i acute
î	238	icirc	i circumflex
ï	239	iuml	i umlaut
ð	240	eth	eth
ñ	241	ntilde	n tilde
ò	242	ograve	o grave
ó	243	oacute	o acute
ô	244	ocirc	o circumflex
õ	245	otilde	o tilde
ö	246	ouml	o umlaut
÷	247	divide	divis or sign
ø	248	oslash	o slash
ù	249	ugrave	u grave
ú	250	uacute	u acute
û	251	ucirc	U circumflex
ü	252	uuml	u umlaut
ý	253	yacute	y acute
þ	254	thorn	thorn
ÿ	255	yuml	y umlaut

8. Concordancia con normas internacionales

- La presente Norma Oficial Mexicana no tiene concordancia con norma internacional por no existir referencia alguna al momento de su elaboración.

TRANSITORIO

UNICO.- La presente Norma Oficial Mexicana entrará en vigor una vez que la Secretaría de Economía por conducto de la Dirección General de Normas, publique en el **Diario Oficial de la Federación** el aviso mediante el cual dé a conocer la existencia de infraestructura para llevar a cabo la evaluación de la conformidad en los términos de la Ley Federal sobre Metrología y Normalización y su Reglamento. México, D.F., a 20 de marzo de 2002 - El Director General, **Miguel Aguilar Romo**.- Rúbrica. Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 61

DECLARATORIA de vigencia de la Norma Mexicana NMX-E-043-SCFI-2002.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Economía - Dirección General de Normas.

DECLARATORIA DE VIGENCIA DE LA NORMA MEXICANA QUE SE INDICA

La Secretaría de Economía, por conducto de la Dirección General de Normas, con fundamento en lo dispuesto por los artículos 34 fracciones XIII y XXX de la Ley Orgánica de la Administración Pública Federal; 51-A, 51-B, 54 de la Ley Federal sobre Metrología y Normalización, 46, 47 del Reglamento de la Ley Federal sobre Metrología y Normalización y 23 fracciones I y XV del Reglamento Interior de esta Secretaría y habiéndose satisfecho el procedimiento previsto por la ley de la materia para estos efectos, expide la declaratoria de vigencia de la norma mexicana que se enlista a continuación, misma que ha sido elaborada y aprobada por el "Comité Técnico de Normalización Nacional de la Industria del Plástico". El texto completo de la norma que se indica puede ser consultado gratuitamente en la biblioteca de la Dirección General de Normas de esta Secretaría,

LA FIRMA DIGITAL COMO UN MEDIO SEGURO PARA REALIZAR NEGOCIOS INTERNACIONALES FRENTE A LAS MAYORES EMPRESAS MEXICANAS

COPIA CON FALLA DE ORIGEN

ubicada en Puente de Tecamachalco número 6, Lomas de Tecamachalco, Sección Fuentes, Naucalpan de Juárez, código postal 53950, Estado de México, o en el Catálogo Mexicano de Normas que se encuentra en la página de Internet de la Dirección General de Normas, cuya dirección es: http://www.economia-normas.gob.mx. La presente norma entrará en vigor 60 días después de la publicación de esta Declaratoria de vigencia en el **Diario Oficial de la Federación**.

CLAVE O CODIGO TITULO DE LA NORMA
NMX-E-043-SCFI-2002 INDUSTRIA DEL PLASTICO-TUBOS DE POLIETILENO (PE) PARA LA CONDUCCION DE GAS NATURAL (GN) Y GAS LICUADO DE PETROLEO (GLP)-ESPECIFICACIONES (CANCELA A LA NMX-E-043-1977).

Campo de aplicación
Esta Norma Mexicana establece las especificaciones que deben cumplir los tubos de polietileno de alta densidad (PEAD) y polietileno de media densidad (PEMD) utilizados en canalizaciones subterráneas, para la conducción de gas natural y gas licuado de petróleo (GLP) en estado gaseoso a presiones menores o iguales a las establecidas en las normas oficiales mexicanas NOM-002-SECRE y NOM-003-SECRE. Esta Norma Mexicana es aplicable a los tubos de polietileno serie métrica e inglesa, de fabricación nacional e importación que se comercialicen en el territorio nacional.

Concordancia con normas internacionales
Esta norma mexicana es parcialmente equivalente a la Norma Internacional ISO 4437:1997. México, D.F., a 24 de mayo de 2002.- El Director General, **Miguel Aguilar Romo**.- Rúbrica.

TESIS CON
FALLA DE ORIGEN

CAPITULO SEXTO

LA FIRMA DIGITAL EN MÉXICO

Para fomentar el comercio electrónico en México es requisito fundamental que exista una legislación de la firma digital, por lo cual, propongo la siguiente iniciativa de ley en materia de la firma digital para que en el contexto internacional puedan existir intercambios comerciales entre otros países, y ponga a nuestro país a la vanguardia en el comercio internacional, aprovechando todos los tratados comerciales que tenemos

INICIATIVA DE LEY DE LA FIRMA DIGITAL EN MÉXICO

EXPOSICIÓN DE MOTIVOS

El objetivo de esta iniciativa de Ley presentando a la Firma Digital como una herramienta eficiente para realizar negocios internacionales por medio de Internet (WWW) es la de describir las ventajas de las firmas digitales asegurando la información informática. La firma digital se ha convertido en una herramienta obligatoria para las aplicaciones del Comercio Electrónico tanto nacional e internacional. Mediante la Firma Digital, las organizaciones pueden aprovechar esta herramienta para lograr ventajas competitivas mejorando productos y servicios.

El propósito de esta iniciativa de Ley es la de explicar la necesidad que se requiere en materia legal en México para utilizar una infraestructura de llave pública (PKI), mejor conocida como la Firma Digital en sus transacciones comerciales por Internet y las ventajas que esta puede proporcionar para mejorar la eficacia operacional de cualquier organización mientras se hace atractiva su inversión en seguridad

Una infraestructura de llave pública es una solución crítica para asegurar la comunicación electrónica segura del negocio que incorpora firmas digitales y tecnología de cifrado.

Una Firma Digital maneja llaves secretas y seguras y certificados permitiendo a una organización crear y utilizar un ambiente de red digno de confianza. Una red confiable permite que las organizaciones aprovechen las siguientes ventajas:

- Una comunicación confidencial segura sin que otras personas puedan leer archivos confidenciales para los cuales no tienen permiso.
- Con la Firma Digital se evita que los archivos puedan ser interceptados.
- La autentificación valida la creación de un archivo hecho por un usuario.
- Los recipientes saben que el remitente creo el archivo.
- La no negación evita que el remitente niegue su participación en la creación de un archivo.
- La integridad garantiza que los archivos no fueron alterados durante la transmisión.

La legislación en materia de seguridad para la firma digital y la regulación de las transacciones comerciales en el WWW a nivel internacional fomentan por esta vía el comercio electrónico en México para promover los actos de comercio por medio del WWW utilizando la seguridad de la Firma Digital.

TESIS CON
FALLA DE ORIGEN

Esta Ley detallará los elementos para que las empresas en México aprovechen una infraestructura de llave pública dándoles la oportunidad de competir en un mundo globalizado realizando transacciones seguras por Internet bajo una legislación en la Firma Digital.

LEY DE LA FIRMA DIGITAL EN MÉXICO

ORDENAMIENTO VIGENTE, Publicado el día ___ en la *Gaceta Oficial del Distrito Federal.*
Al margen superior izquierdo obra un escudo nacional.- Ciudad de México.- JEFE DE GOBIERNO DEL DISTRITO FEDERAL

_____, Jefe del Gobierno del Distrito Federal, a sus habitantes sabed:

Que la Honorable Asamblea Legislativa del Distrito Federal II Legislatura, se ha servido dirigirme la siguiente **INICIATIVA DE LEY**

LA ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL, II LEGISLATURA DECRETA:

Nombre de la ley
De acuerdo con el Artículo 122, sobre las Facultades de la Asamblea Legislativa

Definida por el artículo 44 de este ordenamiento la naturaleza jurídica del Distrito Federal, su gobierno está a cargo de los Poderes Federales y de los órganos Ejecutivo, Legislativo y Judicial de carácter local, en los términos de este artículo.

Son autoridades locales del Distrito Federal, la Asamblea Legislativa, el Jefe de Gobierno del Distrito Federal y el Tribunal Superior de Justicia.

BASE PRIMERA.- Respecto a la Asamblea Legislativa:
ñ) Presentar iniciativas de leyes o decretos en materias relativas al Distrito Federal, ante el Congreso de la Unión,

LEY DE LA FIRMA DIGITAL EN MÉXICO

CAPITULO PRIMERO
DISPOSICIONES GENERALES

MEDIOS ELECTRÓNICOS Y LA FIRMA DIGITAL EN EL COMERCIO

Artículo 1o.- Las disposiciones de la presente Ley son de orden público e interés general y tienen por objeto regular los servicios de seguridad informática mediante la Firma Digital prestados por empresas públicas y privadas que operen en el Distrito Federal.

Artículo 2o.- Corresponde al Jefe de Gobierno del Distrito Federal la aplicación de esta Ley, a través de la Asamblea Legislativa.

TESIS CON
FALLA DE ORIGEN

Artículo 3o.- Para los efectos de esta Ley se entenderá por:

ACEPTACIÓN DE AUTORÍA	A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente
ACTO DE COMERCIO	A todo acto que la legislación vigente considera como tal
ADMINISTRADOR	El responsable de mantener en operación continua los recursos de cómputo con los que cuenta un sitio
AGENTE ELECTRÓNICO	El término de Agente Electrónico se refiere a los programas de computadora o electrónicos o cualquiera que sea automatizado independientemente de que inicie una acción que responda a un registro electrónico o rendimiento en todo o en parte sin revisión o intervención de un individuo al tiempo que sucede dicha acción o respuesta
ARCHIVO PARCIAL	Al mensaje de datos representado en formato ASN 1, conforme al apéndice de la presente Norma Oficial Mexicana
ASN 1	A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis)
ATAQUE	Un incidente cuyo objetivo es causar daño a un sistema, robar información del mismo, o utilizar sus recursos de forma no autorizada
AUDITORIA	Deben conocerse en cada momento las actividades de los usuarios dentro del sistema
AUTENTICACIÓN	Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros
AUTENTIFICADO	Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos
BITS	A la unidad mínima de información que puede ser procesada por una computadora
BYTES	A la secuencia de 8 bits
CERT	El CERT® Equipo de Respuesta para Emergencias Informáticas de sus siglas en ingles, *(Computer Emergency Response Teams)* es un centro de seguridad informática especializada localizada en el Instituto de Ingeniería de Software *(Software Engineering Institute)*, operado por la universidad de Carnegie Mellon University bajo un fondo federal de investigación y desarrollo de los EEUU
CERTIFICADO	Registro basado en la computadora que identifica a la autoridad certificante que lo emite, nombra o identifica a quien lo suscribe, contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite
CERTIFICADO DIGITAL	Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública
CLAVE PRIVADA	A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos
CLAVE PÚBLICA	A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada
CÓDIGO	Al Código de Comercio

CÓDIGO DE ERROR	Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 35 A la clave indicativa de un suceso incorrecto
COMERCIANTES	A las personas físicas o morales a los que la legislación les otorga tal carácter
COMPROMISO	A cualquier acto jurídico diferente del contrato o del convenio, que genere derechos y obligaciones
CONFIDENCIAL	La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo
CONFIDENCIALIDAD	Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada
CONSISTENTE	El sistema, al igual que los datos, debe comportarse como uno espera que lo haga
CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN	Al mensaje de datos representado en formato ASN 1 conforme al Apéndice de la presente Norma Oficial Mexicana
CONSUMIDOR	El término consumidor se refiere al individuo que obtiene, por medio de una transacción, productos o servicios los cuales son utilizados de manera personal, familiar o con propósitos de posesión, igualmente aplica al representante legal del individuo
CONTRATO	Al acuerdo de voluntades que crea o transfiere derechos y obligaciones
CONTROL DE ACCESO	Debe conocerse en todo momento quién entra al sistema y de dónde procede
CONVENIO	Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones
CRIPTOGRAFÍA	Al conjunto de técnicas matemáticas para cifrar información
CRIPTOSISTEMA ASIMÉTRICO	algoritmo o serie de algoritmos que brindan un par de claves confiable
DESTINATARIO	A aquella entidad a quien va dirigido un mensaje de datos
DISPONIBLE	La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos
ELECTRÓNICO	El término electrónico se refiere a la tecnología ya sea, eléctrica, digital, magnética, óptica, electromagnética, inalámbrica o alguna con características similares
EMISOR	A aquella entidad que genera y transmite un mensaje de datos
ENTIDAD	A las personas físicas o morales
EXPEDIENTE ELECTRÓNICO	Al mensaje de datos representado en formato ASN 1 conforme al Apéndice de la presente norma oficial mexicana
FIREWALL	Un dispositivo de hardware y software que actúa como una barrera protectora entre una red privada y el mundo exterior, se usa para proteger el acceso a los recursos internos desde el exterior, así como para controlar los recursos externos que son accedidos desde la red privada
FIRMA ELECTRÓNICA	A la firma electrónica que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se

TESIS CON
FALLA DE ORIGEN

	refiere de modo que cualquier cambio ulterior de los mismos sea detectable La firma digital es una especie de firma electrónica que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relacion con el mensaje de datos e indicar que dicho firmante aprueba la informacion recogida en el mensaje de datos La firma electrónica establece la relación entre los datos y la identidad del firmante Es la información creada o utilizada que permite determinar su autenticidad y ser atribuida a su autor El término de Firma Electrónica se refiere al símbolo o proceso electronico agregado o lógicamente asociado a un contrato u otro registro y atribuido o adoptado por una persona que firma un registro Son los datos en forma electronica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relacion con el mensaje de datos e indicar que dicho firmante aprueba la informacion recogida en el mensaje de datos La firma electronica establece la relacion entre los datos y la identidad del firmante La utilizacion de un criptosistema asimétrico basado en el uso de un par de claves, una publica y una privada relacionadas entre si, es fundamental debido a que, si una persona posee el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformacion se creó usando la clave privada que corresponde a la clave publica del firmante y si el mensaje ha sido modificado desde que se efectuo la transformación
FIRMA DIGITAL	Ver Firma Electrónica
FORMATO	A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información
HERRAMIENTAS DE SEGURIDAD	Programas que nos permiten incrementar la fiabilidad de un sistema de cómputo Existe una gran variedad de ellas, casi todas de libre distribución Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son ➢ Para el manejo de contraseñas anlpasswd, passwd+, crack, John The Ripper S/Key ➢ Para el manejo de autenticación Kerberos, SecureRPC ➢ Para el monitoreo de redes Satan ISS ➢ Para auditoria interna COPS, Tiger, Tripwire ➢ Para control de acceso TCP-Wrapper, PortSentry
HERRAMIENTAS DE SEGURIDAD	Programas que nos permiten incrementar la fiabilidad de un sistema de cómputo Existe una gran variedad de ellas, casi todas de libre distribución Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son ➢ Para el manejo de contraseñas anlpasswd passwd+, crack, John The Ripper, S/Key ➢ Para el manejo de autenticación Kerberos, SecureRPC ➢ Para el monitoreo de redes Satan, ISS ➢ Para auditoria interna COPS, Tiger, Tripwire ➢ Para control de acceso TCP-Wrapper, PortSentry
INCIDENTE	Un evento que pone en riesgo la seguridad de un sistema de cómputo
INFORMACIÓN	El término de Información se refiere al dato, texto, imágenes, sonidos, código, programas de computadora, software bases de datos o lo similar
INTEGRO	La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo

TESIS CON
FALLA DE ORIGEN

LEGISLACIÓN	A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo
MENSAJE DE DATOS	Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 36 A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología
OBJETOS	A las definiciones del lenguaje ASN 1
ORGANIZACIÓN AUTO-REGULADORA	El término de Organización Auto-Reguladora se refiere a la organización o entidad que no es una agencia reguladora federal o estado, pero que se encuentra bajo la supervisión de la ley federal para adoptar y administrar reglas aplicables a sus miembros los cuales son reconocidos por dicha organización u entidad, por la agencia federal reguladora o por otra organización de auto-regulación
ORIGINAL	A la información contenida en un mensaje de datos que se ha mantenido íntegra e inalterada desde el momento en que se genero por primera vez en su forma definitiva
PERSONA	El término de Persona se refiere al individuo, corporación, negociación, estado, confiable asociación, fusión, agencia gubernamental, corporación pública o cualquier otra entidad comercial
PRESTADOR DE SERVICIOS DE CERTIFICACIÓN	A la entidad que presta los servicios de certificacion a que se refiere la presente Norma Oficial Mexicana
RED	Al sistema de telecomunicaciones entre computadoras
REGISTRO	El término de Registro se refiere a la información la cual está inscrita en un medio tangible el cual es almacenado en un medio electrónico u otro medio el cual es recuperable y posee una forma perceptible
REGISTRO ELECTRÓNICO	El término de Registro Electrónico se refiere al contrato u otro registro creado, generado, enviado, comunicado recibido o almacenado bajo medios electrónicos
REPOSITORIO	Sistema para almacenar y recuperar certificados y demás información pertinente a las firmas digitales
REQUIREMENTO	El término de Requerimiento incluye prohibición
RESUMEN O COMPENDIO	Al resultado de aplicarle a un mensaje de datos una función de criptografía del tipo hash
SECRETARÍA	A la Secretaría de Economía
SEGURIDAD EN CÓMPUTO	Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoría
SELLO DEL PRESTADOR DE SERVICIOS DE CERTIFICACION	Al mensaje de datos representado en formato ASN 1, conforme al Apéndice de la presente Norma Oficial Mexicana
SITIO (SITE)	Cualquier organización (militar gubernamental, comercial, académica, etc) que posea recursos relativos a redes y computadoras
TRANSACCIÓN	El término de TRANSACCIÓN se refiere a la accion o al conjunto de acciones relativas al negocio, consumidor o relaciones comerciales entre dos o mas personas incluyendo cualquier otro tipo de las siguientes conductas

	1) La venta, intercambio, licenciamiento o cualquier otra disposición de: a. Propiedad personal, incluyendo bienes e intangibles b. Servicios c. Cualquier combinación entre ellas 2) La venta, intercambio, licenciamiento o cualquier otra disposición de cualquier interés de una propiedad real o cualquier combinación sobre la misma
TRANSFERENCIA ELECTRÓNICA	Es un registro electrónico que a) El usuario de los registros electrónicos expresados como un acuerdo de registros transferibles b) Relativos a adquirir una como una propiedad real c) Una transferencia electrónica puede ser ejecutado usando una firma electrónica
USUARIO	Cualquier persona que hace uso de alguno de los recursos de cómputo con los que cuenta una organización

Articulo 4o.- Regla general de validez
No importando cualquier reglamento, regulación o cualquier otra ley en lo que compete a cualquier transacción dentro o fuera del país:

I. Una firma, contrato u otro registro relativo a una transacción no puede ser repudiada legalmente, invalidada o desincorporada de la ley por el hecho de ser de una forma electrónica.
II. Un contrato relativo a una transacción no puede ser repudiada legalmente, invalidada o desincorporada de la ley por el hecho de haber sido elaborada en un medio electrónico.

Articulo 5o.- Preservación de los derechos y obligaciones
Este título no:

I. Limita, altera o afecta cualquier otro requerimiento impuesto por un estatuto, regulación o legislación relativa a los derechos y obligaciones de las personas bajo el estatuto, regulación o reglamento que los contratos u otros registros que fueron escritos, firmados en una forma no electrónica.
II. Se requiere que cualquier persona que acepte a utilizar los medios electrónicos o firmas digitales, distintos al gobierno con respecto a esta contrato del cual es participe.

TESIS CON
FALLA DE ORIGEN

CAPITULO SEGUNDO
REQUISITOS Y OBJETIVOS

Articulo 6o.- Requisitos y objetivos
La presente iniciativa de ley establece los requisitos que deben observarse para la Firma Electrónica que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones

I. Facilitar las transacciones mediante mensajes electrónicos y firmas digitales; reducir al mínimo la posibilidad de fraguar firmas digitales y el fraude en las transacciones electrónicas; instrumentar jurídicamente la incorporación de normas pertinentes; establecer, en coordinación con diversos Estados, normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos.
II. Definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como establecer las entidades de certificación.

III. Utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.
IV. Otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.
V. Optimizar la actividad de la Administración Pública Nacional adecuando sus sistemas de registro de datos, tendiendo a eliminar el uso del papel y automatizando sus procesos administrativos.
VI. Regular la utilización de la firma digital y los documentos electrónicos como soporte alternativo al uso del papel de las actuaciones de los órganos de la administración del Estado.
VII. Garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo y adecuado y definiendo criterios que fundamenten su reconocimiento legal.
VIII. Crear las condiciones generales para las firmas digitales bajo las cuales se las pueda considerar seguras y que las falsificaciones de firmas digitales y las falsificaciones de información firmada puedan ser verificadas sin lugar a duda.
IX. Establecer una regulación clara del uso de firma electrónica, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación.

CAPITULO TERCERO
CAMPO DE APLICACIÓN

Articulo 7o.- Campo de aplicación
La presente iniciativa de ley es de observancia general para todas aquellas empresas públicas o privadas que desean o necesiten utilizar la firma electrónica en los mensajes de datos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

Articulo 8o.- Disposiciones generales

Se podrán utilizar programas de software públicos o privados que cumplan con los requisitos de la seguridad descritos en el siguientes puntos:

I. Todo sistema informático basado en la Firma Digital debe contener las siguientes características:
   a. Confidencialidad. La información es revelada únicamente a las personas autorizadas.
   b. Integridad. La información no destruida o alterada sin permiso.
   c. Autenticación. La persona que está del otro lado de la red sea quien dice ser.
   d. No-repudio. Evitar que las personas nieguen haber realizado transacciones.
   e. Registro para auditorias. Información para rastrear y observar las transacciones realizadas.
   f. Disponibilidad. Los servicios y datos están disponibles cuando se requieren.
II. La información que se desee conservar se podrá almacenar en una Base de Datos cifrada *(encriptada)* y deberá estar protegida por uno o mas Firewalls así como su almacén en una o varias computadoras utilizadas como repositorio de datos protegidas y aseguradas para tal fin.
III. Los programas de cómputo *(software)* para la conservación de los mensajes de datos deberán dar cumplimiento a lo establecido por la presente ley.
IV. La información deberá de ser auditable llevando un registro de todas las transacciones que se realicen por medio de la Firma Electrónica.

CAPITULO CUARTO
SUPERVISIÓN Y CONTROL

Artículo 9o.- Supervisión y Control

I. La Asamblea Legislativa, por Decreto Presidencial, determinará la autoridad administrativa competente y señalará sus funciones y facultades.
II. Se podrá crear la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente de la Comisión de Ciencia, Tecnología e Informática.

Artículo 10o.- Instancias que intervienen en la emisión de certificados

I. Autoridad certificante acreditada: es quien emite certificados.
II. Repositorios: operan bajo la dirección de una autoridad certificante acreditada.
III. Entidad de certificación, una de sus obligaciones es llevar un registro de los certificados.
IV. Autoridad certificante licenciada: Órgano administrativo que emite certificados de clave pública. Ente organismo auditante: Órgano administrativo encargado de auditar la actividad del ente organismo licenciante y de las autoridades certificantes licenciadas.
V. Entidad de certificación, la cual puede asumir las funciones de entidades de registro o verificación.

Artículo 11o.- Protección De Datos

I. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito y serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado
II. La recopilación de información de un tercero se permite sólo con el consentimiento de la persona afectada.
III. Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento de su titular.
IV. El organismo auditante deberá evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos
V. Los mensajes de datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal.
VI. La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la ley.
VII. Asimismo, la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.
VIII. Es obligación de las entidades de certificación garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor

Artículo 12o.- Elementos De Seguridad

I. Las Autoridad certificante acreditada deberán adoptar medidas de seguridad para que los soportes, medios y aplicaciones informáticas cumplan con estándares internacionalmente reconocidos
II Es requisito utilizar sistemas confiables en la prestación de los servicios de certificación que garanticen la integridad, disponibilidad, calidad, accesibilidad y conservación de la información
III. Uso de sistemas confiables: equipos y programas de computación que sean razonablemente confiables contra la posibilidad de intrusión o uso indebido; que brinden un razonable grado de disponibilidad, confiabilidad y correcto funcionamiento, y que se adapten debidamente al desempeño de sus funciones específicas.

IV. Por lo menos una vez al año se evaluarán a las autoridades certificantes acreditadas con el fin de determinar si se cumplen las normas exigidas por la ley, evaluando si contemplan la adopción de medidas preventivas para evitar la falsificación tanto de los certificados como de las firmas electrónicas.

V. Es requisito contemplar la realización de un plan de seguridad por parte de los prestadores de servicios de certificación en el que se incluyan las medidas de seguridad necesarias para el adecuado cumplimiento de la ley. Dicho plan deberá ser examinado por la autoridad.

VI. El organismo auditante deberá evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como el cumplimiento con las especificaciones del manual de procedimientos y el plan de seguridad aprobados por el organismo licenciante, y verificar que se utilicen sistemas técnicamente confiables.

VII. La autoridad certificante licenciada tiene la obligación de notificar al solicitante sobre las medidas necesarias que éste está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable; y de las obligaciones que éste asume por el sólo hecho de ser suscriptor de un certificado de clave pública.

VIII. Los proveedores de servicios de certificación tienen la obligación de garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione como mantener un respaldo confiable y seguro de dicha información; garantizar la adopción de las medidas necesarias para evitar la falsificación de certificados electrónicos y de las firmas electrónicas que proporcionen.

IX. La información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

X. La utilización de soportes, medios y aplicaciones electrónicos, informáticas y telemáticas en las actuaciones administrativas, requerirá la adopción de medidas técnicas y de organización necesarias para garantizar la autenticidad confidencialidad, integridad y conservación de la información.

Artículo 13o.- Valor Probatorio

I. Un mensaje tiene la misma validez y puede ser exigido judicialmente y es efectivo como si estuviera escrito en papel si aporta en su totalidad una firma digital y si ésta es verificada mediante la clave pública mencionada en un certificado que haya sido emitido por una autoridad certificante acreditada y haya sido válido al momento en que se efectuó la firma digital.

II. La Firma Electrónica tendrá una caducidad de un año y esta deberá reemplazarse al vencimiento de la misma.

III. Los documentos de los órganos señalados en la ley escritos en un soporte electrónico, producirán los mismos efectos que los escritos en un soporte de papel. En dichos documentos, la firma digital sustituirá a la firma autógrafa de quien lo emite y producirá los mismos efectos que aquélla.

IV. La firma electrónica es válida siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en cualquier juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

V. La firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. La firma electrónica podrá formar parte integrante del mensaje de datos, o estar asociada a éste; enviarse o no en un mismo acto.

CAPITULO QUINTO
CONCORDANCIA CON NORMAS INTERNACIONALES

Artículo 14o.- Reconocimiento de Certificados Extranjeros

I. Los certificados extranjeros tienen la misma validez y eficacia jurídica que los señalados en cada una de sus legislaciones siempre y cuando garanticen que son expedidos por una autoridad certificante acreditada, así como el cumplimiento de los requisitos, el procedimiento para su expedición, validez y vigencia.
II. Se establece que las firmas digitales que se puedan verificar con una clave pública de firma para la cual exista un certificado extranjero de otro estado miembro de la Unión Europea o de otro Estado firmante del tratado en el Área Económica Europea son equivalentes a firmas digitales según la ley, en tanto puedan demostrar un nivel de seguridad equivalente. Lo anterior también se aplica a otros estados en la medida en que se suscriban acuerdos internacionales relativos al reconocimiento de certificados.

Artículo 15o.- Requisitos de los Certificados

I. Los certificados expedidos por una autoridad certificante acreditada establecida en un tercer país que gocen de equivalencia legal con los expedidos por un proveedor de servicios de certificación serán validos si cumplen con los requisitos que establece la autoridad certificante acreditada en México.
II. El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre México y terceros países u organizaciones internacionales.
III. Los certificados electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica siempre que sean garantizados por una autoridad certificante acreditada, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado.
IV. Los certificados electrónicos extranjeros no garantizados por un proveedor de servicios de certificación debidamente acreditado, carecerán de los efectos jurídicos.
V. Los certificados de firmas digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la ley, siempre y cuando sean reconocidos por una entidad de certificación nacional o bien, por una entidad de certificación internacional autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia, garantizando en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

CAPITULO SEXTO
COMERCIO ELECTRONICO INTERNACIONAL

TESIS CON
FALLA DE ORIGEN

Artículo 16o.- Acciones requeridas para la Promoción de las Firmas Electrónicas

I. La Secretaría de Relaciones Exteriores promoverá el uso y aceptación, desde una perspectiva internacional, el uso de las firmas electrónicas de acuerdo con los principios estipulados en esta iniciativa de ley.
II. El Secretario de Relaciones Exteriores tomará las acciones necesarias para eliminar o reducir al máximo posible, los impedimentos del comercio en las firmas electrónicas, con el propósito de facilitar el desarrollo de los estados y del comercio en el extranjero.

TESIS CON
FALLA DE ORIGEN

Artículo 17o.- Los principios regulatorios para el uso de las firmas digitales en las transacciones internacionales servirán para:

I. Quitar los obstáculos basados en el papel para adoptar las transacciones electrónicas adoptadas en la presente ley.
II. Regularse por la ley del comercio electrónico adoptado en 1996 por la ley de la Comisión internacional de comercio estipulada por las Naciones Unidas.
III. Permitir a las partes realizar una transacción que determine su apropiada autentificación con las tecnologías y los modelos implementados para dichas transacciones reconocidos y certificados.
IV. Permitir a las partes de una transacción la oportunidad de probar ante una corte internacional sus procedimientos de autentificación y la validez de sus transacciones.
V. Realizar actos no discriminatorios de las firmas electrónicas y los métodos de autentificación de otras jurisdicciones.

CAPÍTULO SEPTIMO
VIGILANCIA: RESPONSABILIDADES POR DAÑOS Y PERJUICIOS

Artículo 18o.- Responsabilidades del usuario (Signatario de la Firma Electrónica)

I. El usuario tendrá la responsabilidad por daños y perjuicios por parte del suscriptor del certificado de firma electrónica en caso de que se presente la pérdida de la clave privada, si ha sido expuesta o corre peligro de que se le dé un uso indebido, por lo que habrá de notificar a la entidad certificadora o al proveedor de servicios de certificación de los hechos mencionados.
II. Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello. En caso de que no cumpla con dicha notificación será responsable de las consecuencias del uso no autorizado de su firma electrónica.
III. El Signatario deberá actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.
IV Cuando un suscriptor acepta un certificado se compromete a indemnizar a la autoridad certificante por daños y perjuicios en la emisión o publicación de un certificado si emitió una declaración falsa u omitió revelar un hecho significativo.
V. La autoridad certificante debe ser capaz de evaluar y manejar su riesgo frente a una posible responsabilidad.
VI. El proveedor de servicios de certificación no será responsable de los daños y perjuicios causados por el uso indebido de un certificado reconocido en el que consten tales límites en cuanto a sus posibles usos cuando éstos se hayan transgredido.
VII. Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.
VIII. El proveedor de servicios de certificación no será responsable de los eventuales daños y perjuicios que excedan de valor límite de las transacciones válidas.

Artículo 18o.- Responsabilidades de los prestadores de servicios de certificación

I. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone la ley Mexicana o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.
II. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

III. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en esta ley.
IV. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.
V. La Ley Mexicana velará porque el proveedor de servicios de certificación que expida un certificado reconocido sea responsable, ante cualquier persona que de buena fe confíe en el certificado. Esto permitirá comprobar que la veracidad de toda la información contenida en el certificado, la conformidad con todos los requisitos establecidos.
VI. El proveedor de servicios de certificación que expida un certificado reconocido sea responsable, ante cualquier persona que de buena fe confíe en el certificado, a efectos de: la veracidad de toda la información contenida en el certificado reconocido a partir de la fecha de su expedición; la conformidad con todos los requisitos en la expedición del certificado reconocido; la garantía de que, en el momento de la expedición del certificado reconocido, obra en poder de la persona identificada en el mismo el dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado; en caso de que el proveedor de servicios de certificación genere los dispositivos de creación y de verificación de firma, la garantía de que ambos funcionen conjunta y complementariamente.

CAPÍTULO OCTAVO
DE LAS SANCIONES Y DEL RECURSO DE INCONFORMIDAD

La Autoridad Certificadora Acreditada para el debido proceso, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

Artículo 19o.- Sanciones

I. Amonestación.
II. Multas institucionales hasta por el equivalente a doce mil veces (12,000) el salario mínimo vigente, y personales a los administradores y representantes legales de las entidades de certificación, hasta por mil trescientos veces (1,300) el salario mínimo vigente, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.
III. Suspensión inmediata de todas o algunas de las actividades de la entidad infractora.
IV. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.
V. Revocar definitivamente la autorización para operar como entidad de certificación.

Artículo 20o.

I Las sanciones a que se refiere el artículo anterior podrán ser aumentadas en atención a las circunstancias agravantes existentes.
II. Son circunstancias agravantes: reincidencia y reiteración; gravedad del perjuicio causado al usuario, gravedad de la infracción; resistencia o reticencia del infractor para esclarecer los hechos.

Artículo 21o.

I. Si del incumplimiento de la presente ley, se deriva una acción delictiva o de responsabilidad civil serán las autoridades judiciales las que impongan la sanción que en el ejercicio de sus facultades compete.

TESIS CON
FALLA DE ORIGEN

TRANSITORIOS

PRIMERO.- La presente Ley entrará en vigor al día siguiente de su publicación en la Gaceta Oficial del Distrito Federal.

SEGUNDO.- Los ordenamientos y acuerdos en materia de servicios de seguridad Informática mediante la Firma Digital expedidos con anterioridad a la entrada en vigor de la presente Ley, permanecerán vigentes en todo lo que no se oponga a la misma mientras no se expida el Reglamento correspondiente.

TERCERO.- Las personas físicas o morales que presten servicios de seguridad Informática en el Distrito Federal sin contar con la autorización respectiva, gozarán de un plazo hasta de noventa días hábiles improrrogables, contados a partir de la entrada en vigor de la presente Ley, para solicitar y obtener dicha autorización.

CUARTO.- Publíquese en la Gaceta Oficial del Distrito Federal, para su debida aplicación y observancia y en el Diario Oficial de la Federación, para su mayor difusión.

Salón de sesiones de la Asamblea Legislativa del Distrito Federal, a veinticuatro de Noviembre de año dos mil dos.- **POR LA MESA DIRECTIVA.- DIP. ¿?, PRESIDENTE.- DIP. ¿?, SECRETARIO.- DIP. ¿?, SECRETARIA.- FIRMAS.**

En cumplimiento de lo dispuesto en el artículo 122, apartado C, Base Segunda, fracción II, inciso b), de la Constitución Política de los Estados Unidos Mexicanos; 48, 49 y 67, fracción II, del Estatuto de Gobierno del Distrito Federal, y para su debida publicación y observancia, expido el presente Decreto Promulgatorio en la Residencia del Jefe de Gobierno del Distrito Federal, en la Ciudad de México, a los cinco días del mes de enero de mil novecientos noventa y nueve.- **EL JEFE DE GOBIERNO DEL DISTRITO FEDERAL,_____.- FIRMA.- LA SECRETARIA DE GOBIERNO, _____.- FIRMA.- EL SECRETARIO DE SEGURIDAD PÚBLICA, _____.- FIRMA.**

TESIS CON
FALLA DE ORIGEN

CONCLUSIONES

Después de realizar la presente investigación para esta tesis de maestría, estoy proponiendo cambiar la visión de hacer negocios internacionales en nuestro país poniéndonos a la vanguardia y a la par con los países quienes ya son nuestros socios comerciales.

Las ventajas de utilizar la Firma Digital son amplias y como conclusión veo que hace falta una legislación adecuada en esta materia, es por esto que dedico íntegramente el capítulo sexto a elaborar una iniciativa de ley que regule la Firma Electrónica en México.

Podemos concluir lo que nos planteamos en el inicio de nuestra investigación:

TESIS CON
FALLA DE ORIGEN

PROBLEMAS

PRINCIPAL

Según los resultados de esta investigación, hemos concluido que las causas por las que no ha sido aprovechado el WWW mediante la Firma Digital por las Grandes Empresas Mexicanas para realizar negocios internacionales en México y así fomentar su multinacionalización por este medio es la falta de una legislación para la Firma Digital pues ni las empresas ni los usuarios podrán tener seguridad si no están amparados en un marco jurídico estable. Es por esto, que como propongo una iniciativa de ley en el capítulo sexto para fomentar el comercio electrónico entre los países y México. Otro factor es el desconocimiento de esta herramienta.

También pudimos ver que existe la infraestructura adecuada para el correcto uso de Internet de manera segura en nuestro país con el uso de la firma digital, pues es, después de Brasil, el país de América Latina que mejor infraestructura posee en materia de telecomunicaciones. Esto proporciona una gran ventaja con el fin de hacer negocios de manera internacional por este medio ya que las empresas mexicanas implementando el uso de esta tecnología no tardarán mucho tiempo rezagadas con respecto a las empresas trasnacionales que ya utilizan la Infraestructura de llave Pública para sus transacciones comerciales de manera segura y confiable por medio del Web.

No obstante, pienso que se ha desaprovechado el WWW mediante el uso de la Firma Digital en la multinacionalización de las empresas mexicanas del D.F. inscritas en el ramo de comercio debido a su falta de seguridad, pues desconocen el cifrado para realizar transacciones de manera segura y que su información permanezca íntegra y no sea vista por un tercero.

Esta tesis ayuda a conocer mas lo que significa la firma digital, su historia y su utilidad para ser utilizada en el Web como un acontecimiento muy reciente, pero que esta cambiando drásticamente, en el ámbito mundial, la forma de hacer negocios, principalmente en los Estados Unidos de América, en Europa y Canadá, quien es el país mas importante en el e-government realizando transacciones para sus ciudadanos y reduciendo los costos operativos y la corrupción en el gobierno.

Podemos contestar también a la pregunta que nos planteamos en un inicio; ¿Es el desconocimiento de las empresas mexicanas del potencial del WWW y de la Firma Digital como una herramienta segura para realizar actos de comercio, lo que les impide realizar negocios internacionales en él? Con una respuesta afirmativa y agregar que no solo el desconocimiento lo que hace falta, sino una regularización jurídica aplicable a nivel nacional e internacional lo que promovería el uso de la Firma Digital y fomentar con esto el comercio electrónico internacional.

Pude descubrir que la mayoría de las empresas en México desconocen el concepto de la firma digital y por lo tanto su uso y beneficio. Sin embargo, también pudimos descubrir en empresas tan importantes como Grupo Carso, en Eficentrum que conocen perfectamente las bondades de este software, sin embargo, es el alto costo lo que también ha reprimido su compra y uso

También podemos ya responder a la pregunta ¿Existen ventajas económicas en la Firma Digital para realizar negocios internacionales en Internet que puedan obtener las empresas mexicanas? Con un si, pues, no obstante a su alto costo de instalación y puesta en marcha, el PKI resulta una inversión para las empresas mas que un gasto debido a que, como pudimos observar en el capitulo quinto, que es una inversión muy rentable pues el retorno a la inversión resulta, en ocasiones hasta en solo dos meses, lo que Perot Systems pudieron conseguir encriptando el canal haciendo una VPN y reduciendo los costos de llamadas y papelería.

Finalmente podemos contestar la siguiente pregunta ¿Existe competitividad e innovación tecnológica en el uso de Internet para abrir paso a la Firma Digital de manera segura en nuestro país? En nuestro país solo existe una compañía que ha efectuado una ingeniosa solución para resolver el problema de la firma digital y esta es Seguridata. Esta empresa 100% mexicana ha invertido en innovación tecnológica y actualmente acapara el mercado en México con mas del 90% pues su software resulta barato aunque también tiene sus limitaciones

Como pudimos observar en el capitulo segundo, la comparación entre empresas extranjeras y mexicanas de acuerdo a quienes proveen la firma digital principalmente Entrust, líder en el mercado internacional de PKI, seguido por Verising, Baltimore y RSA security. Sin embargo, el gigante del software, Microsoft ya posee su propio PKI el cual esta integrado a su sistema operativo, Windows 2000 de manera manual. También IBM, la empresa mas importante del mercado de la informática está poniendo sus ojos en el jugoso negocio de la firma digital y no se esperara mucho para ver una competencia muy feroz para ver quien controla finalmente este mercado tan rentable a nivel internacional

También pude demostrar la hipótesis de esta tesis de maestría en donde me refería que "Las macro empresas mexicanas no poseen la infraestructura adecuada para competir en un mercado global e internacional para realizar negocios internacionales de una manera segura por Internet mediante el uso de la Firma Digital, por lo cual les coloca en una desventaja competitiva en comparación con otras empresas transnacionales de países mas desarrollados." Con un descubrimiento importante, efectivamente las empresas mexicanas no poseen la infraestructura de llave pública, es decir, el PKI para competir en un mercado que cambia segundo a segundo y nos pone en clara desventaja si deseamos realizar negocios internacionales con los países con los cuales poseemos tratados como el TLC (de sus siglas en inglés; NAFTA) y los tratados con la Comunidad Económica

TESIS CON
FALLA DE ORIGEN

Europea quienes son dos de los tres los principales bloques económicos mundiales y con quienes realizamos el 93% del comercio de manera internacional, y quienes ya llevan una ventaja de innovación tecnológica de 15 años en este tipo de software.

También pude, por medio de esta investigación, demostrar los objetivos principales de esta investigación donde precisamente es la falta de infraestructura, cultura y seguridad concerniente al ramo de las telecomunicaciones en Internet en México, especificamente para la Firma Digital, las principales causas por las cuales las empresas mexicanas no han explotado el uso de Internet como una herramienta para realizar negocios internacionales

También en la presente Tesis pudimos explicar de manera detallada que el correcto uso de Internet puede ser una herramienta competitiva para realizar negocios internacionales en México de una manera más rápida, eficiente, y económica, así como Segura, rentable y confiable mediante el uso de la Firma Digital como pudimos ver en el capitulo segundo. Así mismo, pudimos indagar cuales son las ventajas económicas para realizar negocios de comercio electrónico (*e-commerce*) internacionales de una forma segura por Internet, mediante el uso de la Firma Digital y observando que las macro empresas mexicanas son el tipo de empresas que se beneficiarían mayormente con esta herramienta pues ellas poseen el capital y la infraestructura necesarias para implantar el PKI de manera exitosa en sus empresas y beneficiar con esto el intercambio electrónico de información de forma segura a nivel nacional e internacional.

También en esta investigación pudimos explicar las ventajas y desventajas del uso de la Firma Digital para los negocios internacionales desde el punto de vista legislativo, tanto nacional como internacional como lo pudimos observar en el capitulo tercero en la legislación en materia de seguridad para el e-business donde México tiene la ley del 19 de Mayo de 1999 un acercamiento a la regularización de este medio para su uso en este país. Además pudimos ver los costos aproximados que tiene que invertir una empresa en materia de seguridad para su corporativo o firma.

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

BIBLIOGRAFIA

Karanjit Siyan y Chris Hare., *Firewalls y la seguridad en Internet*, segunda edición. Ed. Prentice Hall. 1997

Charles Cresson Wood. *Information Security Policies Made Easy*, 1997

Barbara L.Dijker. *A Guide to Developing Computing Policy Documents - Series: Short topics in system administration N° 2* USENIX Association for SAGE (System Administration Guild) 1996

RFC (Request for Comments) 1281, 1244 - *Site Security Handbook, Internet Engineering Task Force (IETF)*, 1991

Site Security Policy Development - Rob McMillan, Information Technology Services - Griffith University, Australia, 1995

Garfinkel & Spafford. *Practical UNIX & Internet Security* -, O'Reilly

Consideraciones para la elaboración de políticas de seguridad en cómputo para una organización - César Vega Calderón, Dia Internacional de la Seguridad en Cómputo 1998

Internet Security Policy: A Technical Guide - NIST Special Publication 800-XX - Barbara Guttman, Robert Bagwill, 1997

Security Policies for the Internet - Stephen L. Arnold, Ph.D

CAF "Academic Computing Policy Statements" Archive (ejemplos de políticas seguidas en diversos sitios) – The Electronic Frontier Foundation (EFF) – 1999

Área de Seguridad en Cómputo, UNAM

SOON-YONG Choi, O. STAHL Dale y B. WHINSTON Andrew. *The Economics of Electronic Commerce, the essential economics of doing business in the electronic marketplace*. EUA, Macmillan Technical Publishing. Indianapolis, Indiana, 1997

WAYNER Peter. *Digital cash, commerce on the net*, EUA, Ap professional, 1997

COOK, David y SELLERS, Deborah, A SIMON y SCHUSTER Company. *Inicie su negocio en Web, launching a business on the web, 2nd. edition*, México Prentice Hall hispanoamericana, 1997.

VASSOS, Tom. *Estrategias de Mercadotecnia en Internet*, México, Prentice Hall. 1996

HANCE Olivier, DIONNE BALZ Susan. *Leyes y negocios en Internet*, México, Mc. Graw-hill, 1996

BRANWYN Gareth, CARTON Sean, TURLINGTON Shannon. *Internet roadside attractions*, EUA, Ventana Press, 1996.

R D QUENTIN, traducción ROBLA ROMERO Jesús. *Diccionario Ilustrado de la Informática Everest. longman ilustrated diccionary of computing science, España*, Everest S.A., 1997.

KARANJIT, Siyan. *Firewalls y La Seguridad en Internet.* México, Prentice Hall Hispanoamericana, S.A. Segunda Edición, 1997.

Código de Comercio.

Ley Federal sobre Metrología y Normalización.

Reglamento de la Ley Federal sobre Metrología y Normalización.

NMX-Z-13-1997, Guía para la redacción, estructuración y presentación de las normas oficiales mexicanas.

Schneier, Bruce. Applied Cryptography.

Leyes Modelo de la CNUDMI sobre las Firmas Electrónicas y sobre Comercio Electrónico en General.

ISO/IEC 8859-1:1998 Information technology-8bit single-byte coded graphic character sets-Part 1: Latin alphabet No. 1.

STOUT, Rick. *Optimización De Servidores Web, análisis y estadísticas.* España, OSBORNE Mc Graw-Hill, 1997.

McAFEE, R.P. y J. McMILLAN. Electronic Markets, readings in electronic commerce, EUA, R. Kalakota y A.B. Whinston, 1997.

TESIS CON
FALLA DE ORIGEN

FUENTES ELECTRÓNICAS

El organismo que se encarga de regular, establecer estándares, administrar y hacer operacional a Internet es la **ISOC** ***(Internet Society)***. La ISOC esta compuesta por múltiples organismos:

Organismos encargados de establecer estándares:
IETF. Grupo de Trabajo de Ingeniería de Internet *(Internet Engineering Task Force)* que es un grupo voluntario que investiga y desarrolla estándares.

IESG. Grupo de Dirección de Ingeniería de Internet. *(Internet Engineering Steering Group)*. Grupo voluntario que se encarga de considerar los estándares propuestos por el Internet *Engineering Task Force* (IETF) que posteriormente serán establecidos por el IAB.

IAB. Consejo de Arquitectura de Internet *(Internet Architecture Board)*. Es el consejo reglamentador que toma decisiones sobre estándares que regirán a Internet. Determina las necesidades técnicas a medio y largo plazo, y toma las decisiones sobre la orientación tecnológica de la Internet. Aprueba las recomendaciones y estándares de la Internet a través de una serie de documentos denominados RFC *(Request for Comments* - Solicitud Para Comentarios)

Organismo encargados administración de Internet
IANA *(Internet Assigned Number Authority)*. Se encarga de llevar el control de las direcciones IP (que son las direcciones que se asignan a cada computadora en Internet) y la definición de los dominios en Internet.

Operación de Internet
IEPG.-*(Internet Engineering Planning Group)* Organismo que lleva el control de la operación de Internet.

Seguridad en Internet
CERT. Equipo de Respuesta para Emergencias Informáticas *(Computer Emergency Response Teams)*. Existen varios CERT en el planeta. Cada uno de ellos se encarga de auxiliar a usuarios y administradores de redes en cuestiones de seguridad de la información.

DEPARTAMENTOS DEL WEB

W3C
El consorcio del World Wide Web. Unidos a INRIA en Europa y al MIT en Estados Unidos de América cuyos miembros se encuentran en todo el mundo. Los miembros firman un contrato por tres años y pagan un porcentaje, por el cuál ellos obtienen un sin fin de beneficios como el acceso a información más reciente, la participación en el desarrollo de estándares y protocolos. Los miembros deben ser organizaciones o compañías, no existen membresías individuales. http //www w3 org

TESIS CON
FALLA DE ORIGEN

IW3C2
El comité de conferencias internacionales de WWW. Este organiza una serie de conferencias académicas acerca de la tecnología del Web y su desarrollo. Esto implica conferencias regionales con las mismas oportunidades. http://jeeves.ncsa.uiuc.edu/Public/IV2C2/

Web Society
Una asociación para usuarios del Web como individuos. Compañías y organizaciones no pueden ser miembros. http://www.websoc.at/

Internet Society
Un foro donde se discuten temas de Internet, uss protocolos, la arquitectura de internet, su ingeniería, etc. No es un sitio Web específico o relacionado al W3C. http://www.isoc.org/

LA BIBLIOTECA DEL CONGRESO
http://lcweb.loc.gov/

CIA
http://www.odci.gov/cia/publications/95fact/index.html
Los registros de votación de los miembros del Congreso de Estados Unidos son registrados y evaluados por la League of Conservation Voters
http://www.lev.org

YAHOO DE ESTADÍSTICAS
http://www.yahoo.com/Computers_and_Internet/Internet/Statistics_and_Demographics/

MÉXICO
http://www.nmsu.edu/~bri/mexico.html

INTERNET
ACM Brings You the World of Computing http://www.acm.org/

EMPRESAS QUE OFRECEN SEGURIDAD PARA INTERNET

Entrust	www.entrust.com
RSA	www.rsasecurity.com
Verifone	www.verifone.com
Baltimore	www.baltimore.com
Verisign	www.verisign.com
CyberCash	www.cybercash.com
DigiCash	www.digicash.com
MasterCard	www.mastercard.com
Mondex	www.mondex.com
Visa	www.visa.com
NetCheque	www.netcheque.com
UPS	www.ups.com

TESIS CON
FALLA DE ORIGEN

ORGANISMOS INTERNACIONALES PARA EL CUMPLIMIENTO DE ESTÁNDARES

El Open Group (formalmente OSF y X/Open)	http://www.opengroup.org
ISO/IEC JTC1/SC21/WG4 y ITU-T SG7 Directory	http://www.iso.org
ANSI X9F1 Cryptographic Algorithms for the Financial Industry	http://www.ansi.org
IEEE P1363	http://grouper.ieee.org/groups/1363/index.html
Federal PKI Technical Working Group (TWG)	http://csrc.nist.gov/pki/twg
PKCS Technical Working Groups	http://www.rsasecurity.com/rsalabs/pkcs
Secure Digital Music Initiative (SDMI)	http://www.sdmiorg
The Wireless Application Protocol (WAP)	http://www.wapforum.org
Several Internet Engineering Task Force (IETF)	http://www.ietg.org

GLOSARIO A

TERMINOS Y ABREVIATURAS

NOMBRE	DESCRIPCIÓN EN INGLES	DESCRIPCIÓN EN ESPAÑOL
3DES o 3-DES	*Triple Data Encryption Standard*	Triple Encripción de datos estándar
ACL	*Access control list*	Lista de control de acceso
AES	*Advanced Encryption standard*	Encripción de datos Avanzado
ANSI	*American National Standars Institute*	Instituto Nacional americano de Estándares
ANX	*Automotive Network eXchange*	Intercambio automotriz de redes
API	*Application Programming Interface*	Interfase de Programación de aplicaciones
ARL	*Authority Revocation List*	Lista de revocación de autoridad
B2B	*Business-to-Business*	Negocio a Negocio
B2C	*Business-to-Consumers*	Negocio a Consumidores
BCA	*Bridge Certification Authority*	Autoridad de certificación de puente
CA	*Certification Authority*	Autoridad Certificadora
CAST	*Symmetric Cipher named after the inventors Carlisle Adams and Stafford Tavares*	Cifrado simétrico llamado así por sus inventores: Carlisle Adams and Stafford Tavares
CBC	*Cipeher Block Chaining*	Cifrado de bloque cambiante
CCITSE	*Common Criteria for Information Technology Security Evaluation*	Criterio común para información de evaluación de tecnología
CEN / ISSS	*European Committeee for Standardisation/Information Society Standarisation System*	Comité Europeo para estandarización / sociedad de información de sistemas de estandarización
CDSA	*Common Data Security Architecture*	Arquitectura de seguridad común de datos
CMP	*Certificate Management Protocols*	Protocolos de administración de certificados
CMS	*Cryptographic Message Syntax*	Sintaxis de mensajes criptográficos
CP	*Certificate Policy*	Políticas de certificado
CPS	*Certification Practice Statement*	Enunciado de Practicas de certificación
CRL	*Certificate Revocation List*	Lista de revocación de certificados
CRT	*Certificate Revocation Tree*	Árbol de revocación de certificados
CSP	*Certificate Service Provider*	Proveedor de servicios certificado
CTL	*Certificate True List*	Lista verdadera de certificados
DAP	*Directory Access Protocol*	Protocolo de directorio de acceso
DB	*Database*	Base de datos
DCE	*Distributed Computing Environment*	Ambiente distribuido de computación
DEA	*Data Encryption Algorithm*	Algoritmo de encriptación de datos
DES	*Data Encryption Standard*	Estándar de encriptación de datos
DH o D-H	*Diffie-Hellman*	Diffie-Hellman
DISP	*Directory Information Shadowing Protocol*	Protocolo de información de directorios de sombra
DIT	*Directory Information Tree*	Árbol de información de directorios
DN	*Distinguished Name*	Nombre distintivo
DoS	*Denial of Service*	Servicio Denial u fuera de servicio (ocupado)
DSA	*Digital Signature Algorithm*	Algoritmo de firma digital
DSA	*Directory System Agent*	Agente de sistemas de directorios
DSP	*Directory System Protocol*	Protocolo de sistemas de directorios

TESIS CON
FALLA DE ORIGEN

DSS	*Digital Signature Standard*	Estándar digital de firma
DVCS	*Data Validation and Certification Server (Protocols)*	Servidor de Validación y certificación de datos (protocolos)
EC	*Elliptic Curve*	Curva elíptica
ECC	*Elliptic Curve Cryptography*	Curva elíptica criptográfica
EDC	*Elliptic Curve Diffie-Hellman*	Curva elíptica Diffie-Hellman
ECDL	*Elliptic Curve Discrete Logarithm*	Curva elíptica con logaritmo discreto
ECDSA	*Elliptic Curve Digital Signature Algorithm*	Curva elíptica con firma digital
EDI	*Electronic Data Interchange*	Intercambio electrónico de datos
EE	*End-Entity*	Termino de la entidad
EESSI	*European Electronic Signature Standardisation Initiative*	Iniciativa de Estándares de la Firma electrónica europea
ERP	*Entreprise Resource Planning*	Planeación de recursos de la empresa
E-SIGN	*Electronic Sitnatures in Global and National Comerce Act*	Firma electrónica en actos comerciales nacionales y globales
ETSI	*European Telecomunications Standards Institute*	Instituto de Estándares europeo de telecomunicaciones
EU	*European Union*	Unión europea
FBCA	*Federal Bridge Certification Authority*	Autoridad de certificación federal de puentes
FIPS	*Federal Information Processing Standard*	Estándar de proceso federal de información
FTP	*File Transfer Protocol*	Protocolo de transferencia de archivos
G2B	*Government-to-Business*	Gobierno a negocio
G2C	*Government-to-Consumer*	Gobierno a consumidor
GNFS	*General Number Field Sieve*	Número general de campo sieve
GSS API	*Generic Security Service Application Programming Interface*	Aplicación de interfase de programación de servicios de seguridad genérica
HR	*Human Resources*	Recursos humanos
HTTP	*Hyper-Text-Transfer Protocol*	Protocolo de transferencia de hipertexto
ID	*Identification or Identifier*	Identificación o indentificador
IDEA	*International Data Encryption Algorithm*	Algoritmo internacional de encriptación de datos
IDS	*Instrusion Detection Software*	Software de detección de intrusos
IDUP	*Independent Data Unit Protection*	Protección independiente de unidad de datos
IEEE	*Institute of Electrical and Electronics Engineers*	Instituto de ingenieros eléctricos y electrónicos
IESG	*Internet Engineering Steering Group*	Grupo de ingenieros de Internet steering
IETF	*Internet Engineering Task Force*	Tareas de fuerza de ingeniería en Internet
IKE	*Internet Key Exchange*	Intercambio de llaves por Internet
IP	*Internet Protocol*	Protocolo de Internet
IPSec o Ipsec	*Internet Protocol Security*	Seguridad de protocolos de Internet
ISAKMP	*Internet Security Association and Key Management Protocol*	Asociación de seguridad en Internet y administración de protocolo de llaves
ISO	*International Organization for Standardization*	Organización internacional de Estandarización
ITU	*International Telecomunications Union*	Unión internacional de telecomunicaciones
KeyGen	*Key Generator*	Generador de llaves
LAN	*Local Area Network*	Red de área local
LDAP	*Lightweight Directory Access Protocol*	Protocolo de acceso a directorios Lightweight

TESIS CON
FALLA DE ORIGEN

LDUP	*LDAP Duplication/Replication/Update/ Protocols*	Protocolos de Duplicación, replicación y de actualización LDAP
MAC	*Message Authentication Code*	Código de autentificación de mensaje
MD	*Message Digest*	Mensaje de resumen
MD5	*Message Digest Algorithm 5*	Mensaje de resumen Algoritmo 5
MIME	*Multipurpose Internet Mail Extensions*	Extensiones de correo para Internet con multipropósitos
MISPC	*Minimum Interoperability Specifications for PKI Components*	Interoperatibilidad mínima para los componentes de especificaciones para PKI
NACHA	*National Automated Clearing House Association*	Asociación nacional automatizada de casas claras
NCCUSL	*National Conference of Commissioners on Uniform State Law*	Conferencia nacional de comisionados de leyes uniformes del estado
NIST	*National Institute of Standards & Technology (US)*	Instituto nacional de estándares y tecnología (US)
O/S o OS	*Operating System*	Sistema operativo
OCSP	*On-line Certificate Status Protocol*	Protocolo de estatus de certificación en línea
OCSP-X	*On-line Certificate Status Protocol Extensions*	Extensiones de protocolo de certificación en línea
OOB	*Out-of-Band*	Fuera de la banda
PC	*Personal Computer*	Computadora personal
PCMCIA	*Personal Computer Memory Card International Association*	Asociación internacional para Tarjeta de Memoria para la Computadora personal
PDA	*Personal Digital Assistant*	Asistente personal digital
PEM	*Privacy Enhanced Mail*	Correo privado Realzado
PK	*Public Key*	Llave pública
PKCS	*Public Key Cryptography Standards*	Estándares de criptografía de Llaves públicas
PKCS#1	*RSA Encryption Standard*	Estándar de encriptación RSA
PKCS#2	*No longer User, folded into PKCS#1*	No se utiliza
PKCS#3	*Diffie Hellman Key Agreement Standard*	Acuerdo de estandarización de llaves Diffie Hellman
PKCS#4	*No longer User, folded into PKCS#1*	No se utiliza
PKCS#5	*Password Based Encryption Standard*	Estándar basado en encripción de passwords
PKCS#6	*Extended Certificate Syntax Standard*	Estándar de certificados extensión de sintaxis
PKCS#7	*Cryptographic Message Syntax Standard*	Estándar de sintaxis de Mensaje criptográfico
PKCS#8	*Private Key Information Syntax Standard*	Estándar de sintaxis de información de llave privada
PKCS#9	*Select Attibute Types*	Tipos de atributos selectivos
PKCS#10	*Certification Request Syntax Standard*	Estándar de peticiones de certificación
PKCS#11	*Cryptographic Token Interface Standard*	Estándar criptográfico de interface token
PKCS#12	*Personal Information Exchange Syntax Standard*	Estándar de sintaxis de intercambio personal de información
PKCS#15	*An ICC File Structure Recommendation*	Una recomendación de estructura de archivo ICC
PKI	*Public Key Infrastructure*	Infraestructura de llave pública
PKIX	*Public Key Infrastructure (based on) X.509*	Infraestructura de llave pública basada en X.509
PMI	*Privilege Management Infraestructure*	Infraestructura de administración de

		privilegios
RA	*Registration Authority*	Autoridad Registradora
RC2	*Rivest Cipher Algorithm 2*	Algoritmo de cifrado Rivest 2
RC5	*Rivest Cipher Algorithm 5*	Algoritmo de cifrado Rivest 5
RDN	*Relative Distinguished name*	Nombre relativo distinguido
RFC	*Request for Comment*	Petición para comentarios
RIPEMD	*RACE Integrity Primitives Evaluation Message Digest*	Resumen de mensaje para evaluación de integridad primitiva RACE
RL	*Revocation List*	Lista de revocación
RNG	*Random Number Generator*	Generador de números aleatorio
RSA	*Rivest-Shamir-Adleman (Public Key Algorithm)*	Rivest-Shamir-Adleman (Algoritmo de llave pública)
S/MIME	*Secure MIME*	MIME seguro
SCVP	*Simple Certificate Validation Protocol*	Protocolo simple de validación de certificados
SET	*Secure Electronic Transaction*	Transacción electrónica segura
SHA	*Signature Hash Algorithm*	Firma de algoritmo de Hash
SHA-1	*Signature Hash Algorithm Number One*	Firma de algoritmo de Hash número uno
SIRCA	*Securities Industry Root Certification Authority*	Certificación de ruta para la autoridad de la industria segura
SPKM	*Simple Public Key Mechanism*	Mecanismo simple de llave pública
SSL	*Secure Sockets Layer*	Capa Segura de los sockets
SSO	*Single Sign-On*	Simple firma o entrada al sistema
TCO	*Total Cost of Ownership*	Total de costos de Propiedad
TCP	*Transmission Control Protocol*	Protocolo de transmisión de control
TLM	*Trust List Manager*	Administrador de lista de confianza
TLS	*Transport Layer Security*	Seguridad de transporte de la capa
UCC	*Uniform Comercial Code*	Código comercial uniforme
UETA	*Uniform Electronic Transactions Act*	Acto uniforme de transacciones electrónicas
UNCITRAL	*United Nations Commission on International Trade Law*	Comisión de las naciones unidas en el intercambio de leyes
URL	*Uniform Resource Locator*	Localizador uniforme de recursos
V1	*Version 1*	Versión 1
V2	*Version 2*	Versión 2
V3	*Version 3*	Versión 3
VPN	*Virtual Private Network*	Red privada virtual
WAP	*Wireless Application Protocol*	Protocolo de aplicación de radio
X 509	*Collaborative ITU-T (X.509) ISO/IEC (9594-8) international standard that defines frameworks for public-key and attribute certificates*	Collaborative ITU-T (X.509) ISO/IEC (9594-8) Estándar internacional que define a los armazones de llave pública y atributos de certificados.
XTR	*Efficient Compact Subgroup Trace Representation*	Representación eficiente compacta de subgrupos de intercambio

TESIS CON
FALLA DE ORIGEN

GLOSARIO B

INTERNET Y FIRMA DIGITAL

Una de las principales barreras para poder entender correctamente el concepto de Internet, son los términos que se emplean para hablar de la red. Desarrollado este glosario facilita el uso de esta maravillosa forma de comunicación. Parte de este glosario fue tomado del site Glosario de Términos y Recursos de Internet http://www.geocities.com/Athens/7014/Glosario1.htm#LetraA

A

Accesos Dedicados — Conexión tipo E0 de fibra óptica de 64 Kbps o DS0 cable coaxial de cobre a 64 Kbps. Para los usuarios de empresas que deseen accesar todos los servicios de Internet y poder tener identidad y acceso propio a sus servidores, ya sea que estén ubicados en sus instalaciones o en SuperNet.

@ Arroba — Carácter que significa "que tiene su buzón en". Por Ejemplo: smmartinez@abchospital.com

Acceso conmutado — Es una conexión de red que se puede crear y desechar según se requiera. Los enlaces de marcado por línea telefónica son la forma mas sencilla de conexiones con acceso conmutado. SLIP y PPP son protocolos generalmente utilizados en este tipo de conexiones. Vea Línea conmutada, módem, Acceso directo.

Acceso directo — Es una conexión de red que esta integrada a una red de área local (LAN), que ya sea por conexión directa o a través de una red de área metropolitana (MAN) forma parte de Internet.

Aceptación de autoría — A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente

Acnet — Es la línea principal o backbone para América Latina con más de 45MB por segundo de capacidad de transmisión y es además un sistema a prueba de intrusos.

Active X — Un lenguaje de programación apoyado en controles OLE, Visual Basic y Librerías del entorno Windows (OCX) de Microsoft (http://www.microsoft.com), Active X permite que interactuen aplicaciones Windows con el World Wide Web. Actualmente solo es soportado por el Internet Explorer, aunque existen planes para integrarlo a plataformas Macintosh y UNIX. Vea Java.

Recursos:
Microsoft:http://www.microsoft.com/activex/
The ActiveX Working Group:http:\\www.activex.org
Activex de CNET: http://www.activex.com

TESIS CON
FALLA DE ORIGEN

Acto de comercio	A todo acto que la legislación vigente considera como tal.
Address	(Dirección). Vea Dirección Electrónica, Dirección IP
administrador	El responsable de mantener en operación continua los recursos de cómputo con los que cuenta un sitio.
Advanced Research Projects Agency Network	Vea ARPANET
Agente Electrónico	El término de Agente Electrónico se refiere a los programas de computadora o electrónicos o cualquiera que sea automatizado independientemente de que inicie una acción que responda a un registro electrónico o rendimiento en todo o en parte sin revisión o intervención de un individuo al tiempo que sucede dicha acción o respuesta.
Altavista	Herramienta de Búsqueda del World Wide Web desarrollada por DIGITAL. Contiene uno de los índices más completos del Web. Se localiza en http://www.altavista.com. Vea Operadores Booleanos, Yahoo!
Ancho de banda	Cantidad de bits que pueden viajar por el medio físico (cable coaxial, par trenzado, fibra óptica, etc.). Entre mayor sea el ancho de banda obtenemos más rápido la información. Se mide en millones de bits por segundo (Mbps).Las velocidades típicas hoy en día son de 10 Mbps a 100 Mbps.
Anonymous	Utilizado para designar a los usuarios en general. Admitido en la mayoría de los servidores FTP para todos los visitantes. Generalmente como password se debe dar la dirección electrónica del visitante.
Anonymous FTP	Vea FTP
AOL	(American Online) Es una red que ofrece servicio electrónico de información (BBS) y es independiente de Internet.
API	(Application Program Interface). Conjunto de reglas de programación que determinan como una aplicación debe acceder a un servicio. Vea: Cliente, Servidor.
Aplicación	Software que realiza una función útil. Los programas que se utilizan para realizar alguna función (como correo electrónico, FTP, etc.) son las aplicaciones Cliente. Existe una gran número de sistemas, programas, juegos, datos, etc. dentro de internet. Desarrolladas para propósitos específicos. Estas se encuentran instaladas en los diferentes servidores, cada uno con especialidades distintas para ser utilizados a través de la infraestructura de la red. Pudiendo así, tanto usuarios como empresas tener el acceso a estas aplicaciones, ya sean propias o de terceros, cuando está permitido.

TESIS CON
FALLA DE ORIGEN

Applets	Vea Java.
Archie	Es una aplicación que permite realizar búsquedas de archivos en FTP y una vez localizados, podrán ser transferidos a nuestra PC o a otras cuentas (hosts). Un sistema para la localización de archivos que están disponibles públicamente por FTP anónimo. Es necesario conocer el nombre del archivo o una subcadena del mismo para utiliar archie. Recursos: RED UNAM: telnet://condor.dgsca.unam.mx con Login: archie Gopher: Gopher://servidor.dgsca.unam.mx. World Wide Web: http://hoohoo.ncsa.uiuc.edu/archie.html. NEXOR (Lista de servidores archie en el mundo): http://web.nexor.co.uk/public/archie/servers.html
Archivo binario	Vea Binario.
Archivo de Texto	Archivo que utiliza solamente caracteres del estandar ASCII y por lo tanto que puede ser enviado por correo electrónico sin ningún tipo de modificación. Vea Binario, UUENCODE, UUDECODE.
Archivo parcial	Al mensaje de datos representado en formato ASN.1, conforme al apéndice de la presente Norma Oficial Mexicana.
Archivos Compactados	Los archivos compactados permiten la compresión de los datos al eliminar datos redundantes, de esta manera permiten un mayor almacenamiento de archivos, aumentar la velocidad de transferencia de los mismos, etc. Vea ZIP. Entre los formatos de archivos compactados se encuentran: Para PC arc, arj, lha, zip. Utilería:Winzip: http://www.winzip.com zip. Utilería PKZIP, PKUNZIP PARA MACINTOSH HQX, BIN, SIT UTILERÍAS: STUFFIT Para UNIX gzip Utileria Gzip Z Utileria compress/uncompresstar Utilera Tar
Archivos de dominio público	Son los archivos que se pueden obtener de Internet y que han sido puestos a disposición de los usuarios por compañías, dependencias y personas. Pueden ser Freeware o Shareware. Recursos: Stroud's CWSApps List Version 16 Bits(Con liga a la de 32) http://cwsapps.fibr.net/cwsa.html Download: http://www.download.com/ Jumbo: http://www.jumbo.com Shareware.Com: http://www.shareware.com The Oak Software Repository: Vía FTP ftp://oak.oakland.edu o vía WWW http://oak.oakland.edu

TESIS CON
FALLA DE ORIGEN

Tucows http://www.tucows.com
Yahoo!: http://headlines.yahoo.com/download/Internet/

ARCNET — Red de computadoras con recursos asignados (*Attached Resource Computer Network*). Red de area local (LAN) desarrollada por Datapoint Corporation que utilizaba una tecnología de acceso llamada Token Passing y que tiene un Ancho de Banda de 2.5 Mbps. El diseño original de las redes ARCNET se apoyaba en la topología de estrella.

Arpanet — (Advanced Research Projects Agency) Red creada por el gobierno de los Estados Unidos de Norteamérica en 1969, para la investigación de proyectos avanzados. Con financiamiento de DARPA (Defense Advanced Research Projects Agency) y que diera origen a Internet. Al principio, su objetivo era estudiar técnicas necesarias para construir un sistema que pudiera conectar redes por conmutación de paquetes que ya existían, pero que estaban aisladas por resultar incompatibles.

Fue la base de Internet y se inició conectando universidades y a sus investigadores, uniendo así sus proyectos e ideas. Cada uno de los investigadores contaba con dos conexiones en Arpanet, una para comunicarse y la otra para experimentar con ideas nuevas. En enero de 1973, DARPA propone TCP, centrando los primeros usos del protocolo TCP/IP en los servicios como correo electrónico, transferencia de archivos y login (acceso) remoto.

Red experimental con fines militares establecida en los setenta, en la cual se probaron las teorías y el software en los que esta basado Internet. ARPANET era una red experimental que apoyaba la investigación militar, en particular la investigación sobre cómo construir redes que pudieran soportar fallas parciales (como las producidas por los bombardeos) y aún así funcionar. La red fue diseñada para requerir un mínimo de información de las computadoras que forman parte de ella. La filosofía era que cada computadora en la red se pudiese comunicar, como un elemento particular con cualquier computadora.

ASCII — (*American Standard Code for Information Interchange*). Es de facto el estándar del World Wide Web para el código utilizado por computadoras para representar todas las letras (mayúsculas, minúsculas, letras latinas, números, signos de puntuación, etc.). El código estándar ASCII es de 128 letras representadas por un digito binario de 7 posiciones (7bits), de 0000000 a 1111111. Vea Archivo de Texto, Binario,UUENCODE, UUDECODE.

ASN.1 — A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis).

Ataque — Un incidente cuyo objetivo es causar daño a un sistema, robar información del mismo, o utilizar sus recursos de forma no autorizada.

Auditoria — Deben conocerse en cada momento las actividades de los usuarios dentro del sistema.

TESIS CON FALLA DE ORIGEN

Autenticación — Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.

Autentificado — Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.

TESIS CON
FALLA DE ORIGEN

B

Bauds — Medida de la velocidad de modulación entre los módem, que es expresada en unidades por segundos. Continuamente tanto bauds como bps son utilizados como sinónimos, sin ser esto correcto.

Backbone — Llamada así a la columna vertebral de Internet, ya que se concentran las redes en América , haciendo posible que la mayor parte de la información pase por ésta columna.
Línea de transmisión de información de alta velocidad o una serie de conexiones que juntas forman una via con gran ancho de banda. Un backbone conecta dos puntos o redes distanciados geográficamente, a altas velocidades.

Bancos De Informacion — Diversos lugares donde se encuentra información clasificada para ser utilizada según se requiera y se adapte al usuario. Pudiendo este "navegar" a través de los archivos jerarquizados y dependiendo de las necesidades y privilegios, puede hacer uso de estos y transmitir los archivos hacia la computadora, imprimirlos o enviarlos por correo hacia una dirección específica, para su conveniente explotación. Existe dentro de internet una gran cantidad de bancos de información disponibles.

Bases de datos distribuidas — Bases de datos que se pueden encontrar en diversas partes del planeta y que se presentan ante el usuario como una base de datos única. Un ejemplo de ello es el DNS (Domain Name Service) en que se basa Internet, donde las direcciones de las computadoras se encuentran en diversas computadoras (cada una encargada de un dominio), y que se presentan ante el usuario como una base de datos única con todos los dominios del planeta.

Bauds por segundo — Vea Bps.

BBS — (Bulletin Board Service) Son sistemas propios de cómputo que permiten a sus usuarios conectarse por medio de los módem y usar los servicios instalados en estos. Se pueden bajar archivos, consultas, dejar información, áreas de discusión, etc.
(*Bulletin Board System*). Servicio que proporcionan desde grandes compañias (Compuserve, America On Line, etc) hasta pequeños proveedores, que consiste en intercambiar información con otros usuarios, descargar archivos etc., sin estar conectados a Internet por lo que actualmente estan cayendo en desuso. Las BBS se cuentan por miles (¿o

millones?) en el mundo, corriendo desde una simple PC con una o dos líneas telefónicas. La tendencia actual es que las BBS se vayan convirtiendo en proveedores de servicio de Internet.

Binario — Archivo que contiene códigos y caracteres que sólo pueden ser utilizados por tipo específico de software. Los más comunes son los archivos ejecutables, gráficos y documentos con formato. Vea Archivo de Texto, BinHex., UUENCODE, UUDECODE.

BinHex — (*BINary HEXadecimal*) Método para convertir archivos no ASCII o binarios al formato de siete bits ASCII. Este método es utilizado principalmente por computadora Macintosch. Esto es necesario porque el correoen Internet solo puede utilizar el ASCII. En 7 bits. Vea Mime,UUENCODE, UUDECODE.

Bit — (*Binary DigIT*). Unidad mínima de almacenamiento de la información. Su valor puede ser 0 ó 1 ó verdadero o falso. Vea bps, Bps, Byte, Paquete. A la unidad mínima de información que puede ser procesada por una computadora.

BITNET — (*Because It's Time NETwork* ó *Because It's There NETwork*). Red de sitios educativos (investigación y universitarios) separada de Internet, pero el correo electrónico es libremente intercambiado entre BITNET e Internet. Los Listservs son la forma mas popular de los grupos de noticias originados en BITNET. Las computadoras de BITNET son usualmente mainframes corriendo el sistema operativo VMS (variante de UNIX).

bits por segundo — Vea bps.

Bps — (*Bits-Per-Second*) Bits por segundo. Corresponde a la velocidad de intercambio de información entre computadoras, de los módem o enlaces. Es el número de cambios que sufre la señal por segundo y es indicativo de la cantidad de bits por segundo que se están transmitiendo. Un puede aumentar la velocidad de enlace si utiliza compresión de datos. Para aprovechar la máxima velocidad de un módem, tanto el proveedor como el usuario deben de tener módems que operen a la máxima velocidad y utilizar ambos la compresión de datos. Vea bit. Es la velocidad a la que se transmiten los bits en un medio de comunicación. Vea ASCII, Bps.

Bridge — Vea Puente.

Browser — Programa navegador o visor es una herramienta que nos permite conectarnos con los diferentes servidores de internet para obtener información de manera sencilla y agradable ya que, opera de manera gráfica, por ejemplo: Internet Explorer, Netscape, Mosaic, Chamaleon, etc. Vea Visualizador.

Busqueda — Vea: Herramientas de Búsqueda.

Byte — Conjunto de 8 bits. A la secuencia de 8 bits.Suele representar un valor asignado a un carácter.

TESIS CON FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

Vea Kilobyte.

C

Cc (Carbon copy o Courtesy copy) Con copia para. (Se usa en el encabezado del correo electrónico).

C, C++ Lenguajes de programación (orientado a objetos en el caso de C++) utilizados en el World Wide Web a través de un CGI, principalmente para realizar consultas a bases de datos como Oracle, SQL-Server, SyBase, etc, o a herramientas locales como WAIS. Generalmente el servidor donde se encuentra el programa funciona en ambiente UNIX.

Recursos:
news:comp.lang.c
news:comp.lang.c++
Nota: Puede consultar los grupos de noticias en WWW desde DejaNews (http://www.dejanews.com).

Cable Coaxial Núcleo de cobre, aislado por plástico de un recubrimiento metálico y este a su vez envuelto en otra capa de plástico. Suelen emplearse dos tipos de cable coaxial para las redes locales: cable de 50 Ohms, para señales digitales, y cable de 75 Ohms, para señales analógicas y para señales de alta velocidad. Es el medio físico por medio del cual se pueden conectar varias computadoras.
Vea cableado, Fibra Optica, Par Trenzado.

Cableado Columna vertebral de una red que utiliza un medio físico de cable, casi siempre del tipo de red de area local (LAN), que lleva la información de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.
Vea Cable Coaxial, fibra óptica, par trenzado, topología de red.

CCITT Consultative Committee for International Telephony and Telegraphy.

Cello Visualizador descontinuado del World Wide Web.

CERN Laboratorio Europeo para Física de Partículas Creadores del HTTP y HTML.
Laboratorio Europeo de Física de Partículas. Fue el desarrollador inical del World Wide Web. Actualmente los estándares del Web son desarrollados por la World Wide Web Organization (3W). El web site del CERN se encuentra en http://www.cern.ch

CERT Equipo de Respuesta para Emergencias Informáticas *(Computer Emergency Response Team)*. Fue creado en 1988 como respuesta a las carencias mostradas durante el incidente del gusano de ese mismo año que afecto a más de 6000 computadoras enlazadas a Internet. Entre los objetivos del CERT se encuentran:

a) Trabajar junto a la comunidad Internet para facilitar su respuesta a problemas de seguridad. informática que afecten la operación de

Internet.

b) Dar soporte a los administradores y usuarios para elevar la conciencia colectiva sobre temas de seguridad informática.
c) Realizar tareas de investigación que tengan como finalidad mejorar la seguridad de las redes existentes.
d) Brindar asistencia 24 horas al día para responder a incidencias sobre seguridad informática, asistencia sobre vulnerabilidad de productos, documentos técnicos y cursos de formación.
e) Adicionalmente, el CERT mantiene numerosas listas de correo y ofrece un servidor de FTP anónimo, en ftp://cert.org donde se archivan documentos y herramientas sobre temas de seguridad informática. El CERT brinda asistencia técnica vía correo electrónico en cert@cert.org
Vea Cracker, Hacker, ISOC, Virus.

Recursos:
ASC (Area de Seguridad en Computo) de la UNAM (México): http://www.super.unam.mx/seguridad/
Forum of Incident Response and Security Teams.(FIRT): http://www.first.org/
FAQ del esCERT-UPC http://escert.upc.es/castella/cert_faq.html
Administración, operación y seguridad en Internet:
http://info.isoc.org:80/adopsec/index.html

El CERT® Equipo de Respuesta para Emergencias Informáticas de sus siglas en ingles; (Computer Emergency Response Teams). es un centro de seguridad informática especializada localizada en el Instituto de Ingeniería de Software (Software Engineering Institute), operado por la universidad de Carnegie Mellon University bajo un fondo federal de investigación y desarrollo de los EEUU.

Certificado Registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.

Certificado digital Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública.

CGI (Common Gateway Interface). Una interfaz escrita en un lenguaje de programación (perl, C, C++, visual basic, etc) y posteriormente ejecutada o interpretada por una computadora servidor para contestar a pedidos del usuario desde una computadora con una aplicación cliente; casi siempre desde el World Wide Web. Esta interfaz permite obtener los resultados pedidos, como los que resultan al consultar una base de datos.

TESIS CON
FALLA DE ORIGEN

Recursos:
The common Gateway Interface:
http://www.ug.bcc.bilkent.edu.tr/WWW/hoohoo/cgi/overview.html
A CGI Programmer's Reference: http://www.best.com/~hedlund/cgi-faq

Chat — Sistema multiusuario de discusión en Internet.
Termino utilizado para describir la comunicación de ususarios en tiempo real.
Vea IRC

Cix — (Commercial Internet eXchange) Primera y más grande industria de proveedores de acceso a internet

Clave privada — A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos

Clave pública — A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada

Cliente — En el ambiente de cómputo es muy conocido el término Cliente/Servidor, que nos permite conceptualizar la unión entre las terminales de una red con su servidor "en línea" ; esto es en el mismo instante y observando todo mundo la misma información ya que es actualizada por los mismos clientes al momento.

Cuando accesamos Internet desde nuestra PC lo hacemos mediante una serie de programas "clientes" que son capaces de comunicarse con un servidor de su clase y que se encargan de contactar al servidor localizado en algún lugar remoto y extraer de él la información necesaria.

a) Una aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red.
b) Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio.

Vea Modelo Cliente-Servidor.

CMOS — Es un tipo de circuito integrado ampliamente utilizado para procesadores y memorias.

TESIS CON
FALLA DE ORIGEN

Código — Al Código de Comercio

Código de error — Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 35. A la clave indicativa de un suceso incorrecto

Com — Extensión que tiene en el nombre del servidor, que indica que es de tipo Comercial. (por ejemplo : http://www.ibm.com)

Comerciantes — A las personas físicas o morales a los que la legislación les otorga tal carácter

Compromiso — A cualquier acto jurídico diferente del contrato o del convenio, que genere derechos y obligaciones

Compuserve — Red independiente que provee de servicio electrónico de información.

TESIS CON
FALLA DE ORIGEN

Confidencial	La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.
Confidencialidad	Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada
Consistente	El sistema, al igual que los datos, debe comportarse como uno espera que lo haga
Constancia del prestador de servicios de certificación	Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana
CONSUMIDOR	El término consumidor se refiere al individuo que obtiene, por medio de una transacción, productos o servicios los cuales son utilizados de manera personal, familiar o con propósitos de posesión, igualmente aplica al representante legal del individuo.
Contraseña	Vea Password.
Contrato	Al acuerdo de voluntades que crea o transfiere derechos y obligaciones
Control de acceso	Debe conocerse en todo momento quién entra al sistema y de dónde procede
Convenio	Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones
Cookie	Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para sus posterior recuperación.(proceso realizado por el Internet Explorer cuando utiliza Microsoft Network (http://www.msn.com)). En la práctica la información es proporcionada desde el visualizador al servidor del World Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se acede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio. Vea *CGI*.
Correo Electrónico	Es el medio de comunicación más eficiente que ha desarrollado el ser humano. Con él, se puede mandar mensajes de texto a cualquier otro usuario de internet o red comercial, enviar archivos binarios, enviar mensajes a uno o más usuarios simultáneamente, contestar los mensajes que son recibidos, suscribirse a listas de correo o discusión, etc. El *e-mail* permite el intercambio de mensajes entre personas conectadas a una red de manera similar al correo tradicional. Entre las aplicaciones cliente de correo electrónico tenemos a Eudora, Mail , Pine, Pegasus, etc. La definición acerca del correo electrónico fue especificada en el RFC # 822. Para más información consulte http://www.internic.net/rfc/rfc822.txt Vea Dirección Electrónica, Firma, finger, IMAP, InterNIC, Listas de correo, MIME, MTA, MUA, POP, Smiley, SMTP, UUDENCODE, UUDECODE.
Cracker	Persona que trata de introducirse a un sistema sin autorización y con la

intención de realizar algún tipo de daño u obtener un beneficio. Vea CERT, Hacker.

Criptografía Al conjunto de técnicas matemáticas para cifrar información

Criptosistema asimétrico algoritmo o serie de algoritmos que brindan un par de claves confiable

Cuenta Shell Es la forma más sencilla de conectarse a Internet. La información que se accesa está en forma de texto, no se emplean imágenes, sonidos o gráficos y para poder utilizar este tipo de conexión es necesario que el usuario tenga conocimiento de UNIX.

Cyberspace Termino originado por William Gibson en su novelo Neuromancer. La palabra Cyberspace es ampliamente usada para descrubir los recursos de información disponibles a través de Internet.

D

Dial Up Acceso a Internet vía red pública telefónica, con ambientes gráficos Windows, Windows 95, Macintosh, OS/2 y Unix. Vea Línea Conmutada

DejaNews Uno de los índices más completos acerca de los grupos de noticias en el World Wide Web. Excelente recurso para buscar información en los NEWS.
Vea: Herramientas de búsqueda.

TESIS CON
FALLA DE ORIGEN

Destinatario A aquella entidad a quien va dirigido un mensaje de datos.

Dirección electrónica (address). Dirección de un usuario en Internet. Por medio de ella es posible enviar correo electrónico a un usuario. Esta es única para cada usuario y se compone por el login de un usuario, arroba y el nombre del servidor de correo electrónico. p.e. usuario@computadora.com.

Dirección IP La dirección del protocolo de Internet (IP) es la dirección numérica de una computadora en Internet. Cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como 132.248.53.10 Vea IANA.

Direcciones Número único que se le asigna a cada máquina y que es brindado por Network Information Center, en los Estados Unidos (por ejemplo: 200.45.15.9).

Disponible La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos

DNS Sistema de nomenclatura de dominios (*Domain Name System*) Es un sistema que se establece en un servidor (que se encarga de un dominio) que traduce nombres de computadoras (como servidor.dgsca.unam.mx) a domicilios numéricos de Internet (direcciones IP) (como 132.248.10.1). Vea Bases de datos distribuidas, IANA, InterNIC.

Por este método, las direcciones de Internet se convierten en direcciones que reconoce el protocolo de internet. (IP), para que puedan ser localizados e identificadas las computadoras.

Domain Ver DNS.

Dominio Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. Vea Bases de datos distribuidas, DNS, Jughead, InterNIC

Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Ejemplo:

.comComercial
.edu educación (USA),
.gob gobierno (USA)
.mx México
.es España, etc,

Los dominios a su vez se van dividiendo en otros dominios:
.gob.mx Gobierno de México
.com.mx Comercio en México

Download Electrónicas Es copiar un archivo de un servidor remoto a nuestra PC, a través de Internet y por medio del FTP.

TESIS CON
FALLA DE ORIGEN

E

E-Mail ver "correo electrónico"

Electrónico El término electrónico se refiere a la tecnología ya sea, eléctrica, digital, magnética, óptica, electromagnética, inalámbrica o alguna con características similares.

Emisor A aquella entidad que genera y transmite un mensaje de datos.

Encriptado o Encriptyon Codificación (forma de modificar los datos de manera confidencial) y compresión de alguna información que viaja en Internet. Esto se realiza por motivos de seguridad.

Enrutador Elemento que determinan la trayectoria más eficiente de datos entre dos segmentos de red. Operan en la capa superior del modelo OSI a la de los puentes -la capa de red- no están limitado por protocolos de acceso o medio.
Vea Gateway, Puente.

Entidad	A las personas físicas o morales.
Estacionamiento De Equipos	Se denomina de esta manera, al ubicar uno o más equipos de cómputo dedicado en un ISP para el uso exclusivo de la empresa que lo contrata, aprovechando la infraestructura de los servicios del nodo, además del mantenimiento profesional por parte del personal del ISP.
Ethernet	Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de Bus. Y que tiene un ancho de banda de10 Mbps. Vea Enrutador, Token Ring.
Etiqueta	Reglas de comportamiento para facilitar la comunicación entre los miembros de Internet, por ejemplo: El correo electrónico que se envíe debe ser compacto. No deberán enviarse mensajes masivos a personas que no han solicitado información. Tampoco se deberán escribir los mensajes en mayúscula ya que da la impresión de que se está gritando.
Eudora	Aplicación que permite el manejo del "CORREO ELECTRÓNICO", así como el envío y consulta de mensajes través de Internet. Recursos: Eudora: http://www.qualcomm.com
Expediente electrónico	Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente norma oficial mexicana.

TESIS CON
FALLA DE ORIGEN

F

FAQ	(Frecuently Asked Questions) Compendio de las preguntas más comunes, relacionadas con el tema en cuestión. Se refiere a una pregunta o preguntas más frecuentes y a sus respuestas. Para obtener una lista de las FAQ consulte: http://insti.physics.sunysb.edu/faq/index.html
Fibra óptica	Combinación de vidrio y materiales plásticos. A diferencia del cable coaxial y del par trenzado no se apoya en los impulsos eléctricos, sino que transmite por medio de impulsos luminosos. Es el medio físico por medio del cual se pueden conectar varias computadoras. Vea cableado, cable coaxial, part trenzado.
File Transfer Protocol	Vea FTP.
Finger	Herramienta de software que informa acerca de usuarios (Nombre completo, Dirección postal, etc.), utilizada para saber si cierto usuario está conectado a Internet.
Finger	Programa que le permite determinar si un usuario específico está en un

momento determinado en línea, o bien, qué usuarios se encuentre en ese momento en línea en un escenario específico. Este comando es implementado en programas de correo electrónico como Eudora. Vea Correo Electrónico.

Firewall

Un dispositivo de hardware y software que actúa como una barrera protectora entre una red privada y el mundo exterior; se usa para proteger el acceso a los recursos internos desde el exterior, así como para controlar los recursos externos que son accedidos desde la red privada

Llamado también filtro de acceso, todo el tráfico de información debe pasar por éste en ambos sentidos. Estos filtros deben de ser inviolables con lo cual se incrementa el nivel de seguridad.
Una combinación de hardware y software que separa una red de área local (LAN) en dos o mas partes con propósitos de seguridad. Para obtener más información consulte
http://www.dma.state.mn.us/website/imac/inet_firewall_FAQ.htm

Firma

(*signature*). Es un archivo de aproximadamente cinco líneas que los usuarios anexan al final de un mensaje de correo. Contiene cuando menos un nombre y un domicilio de correo electrónico.

Firma digital

Ver Firma Electrónica.

Firma Electrónica

A la firma electrónica que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital es una especie de firma electrónica que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.

A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre los datos y la identidad del firmante.

Es la información creada o utilizada que permite determinar su autenticidad y ser atribuida a su autor. El término de Firma Electrónica se refiere al símbolo o proceso electrónico agregado o lógicamente asociado a un contrato u otro registro y atribuido o adoptado por una persona que firma un registro.

Son los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre

los datos y la identidad del firmante.

La utilización de un criptosistema asimétrico basado en el uso de un par de claves, una pública y una privada relacionadas entre sí, es fundamental debido a que, si una persona posee el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante y si el mensaje ha sido modificado desde que se efectuó la transformación.

Flame o vociferar — Ser grosero o insultante en la red; normalmente se trata de una respuesta a un correo electrónico o mensaje del grupo de noticias que no es del gusto del insultante. Por lo general no es recomendable.

Flops — (FLOating point operations Per Second) Unidad de medida de cálculos de operaciones con punto flotante por segundo.

Formato — A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información.

Foros De Discusion — Existen más de 3,500 temas de discusión y para ingresar a los foros se requiere de tener un "servidor" de noticias que periódicamente realiza el intercambio de "posts" o mensajes con los demás servidores, así como un programa "cliente" para que facilite el intercambio de ideas entre los usuarios.
Otro nombre dado a las listas de correo.

Foros de discusión interactivos — Permite el intercambio entre dos o mas personas a través de una conversación escrita simultánea, realizada por conducto de algún programa. Vea IRC.

Freeware — Nombre que se le da al software que se puede usar y copiar sin ninguna obligación. Aplicaciones que pueden obtenerse directamente de Internet y que no es necesario pagar por su utilización. Vea archivos de dominio público, Shareware.

Ftp — (File Transfer Protocol) Es el programa para transferencias de archivos en Internet.

Cumple además con la función de facilitar el intercambio de archivos por medio de la instalación de servidores públicos o privados que contienen en forma ordenada y jerarquizada los archivos y dependiendo de los privilegios del usuario, le permiten transmitirlos hacia su computadora.

El uso más importante de FTP se conoce como FTP anónimo.

FTP Anónimo : Permite accesar bases de información o de software sin tener una cuenta en la computadora remota. Mediante este servicio es posible obtener imágenes, fotografías, programas de todo tipo, textos e incluso videos y animaciones.

TESIS CON
FALLA DE ORIGEN

a) Protocolo de transferencia de archivos (*File transfer Protocol*).
b) Aplicación que desplaza archivos utilizando el Protocolo de transferencia de archivos. FTP anónimo. Procedimiento que se utiliza para descargar archivos públicos de una computadora remota a un local. Es aveces necesario introducir un password que puede ser la palabra guest (huésped), o nuestra dirección electrónica.

Recursos:
Cute FTP: http://www.cuteftp.com
FTP Icon Connectión: http://www.jtec.com
WS-FTP: http://www.csra.net/junodj

Full Duplex

Característica de algunas tarjetas de sonido que permite que estas transmitan información audible al mismo tiempo que la reciben, de manera similar a un teléfono convencional. Para saber si su tarjeta de sonido soporta full duplex consulte al fabricante de la misma.
Vea Telefonía en Internet.

TESIS CON
FALLA DE ORIGEN

G

Gateway, Puente o Compuerta

Computadora que permite interconectar dos distintas redes con diferentes protocolos. Es un tipo de enlace entre redes que pueden ser de distinto tipo o utilizar diferentes protocolos.

Gif

(Graphics Interchange Format) Es un formato para el almacenamiento de imágenes comprimidas, desarrollado por Compuserve que maneja color de 8 bits y utiliza proporciones de comprensión aproximadamente de uno a dos.

Gopher

Información a través de menús. Programa que permite revisar directorios y obtener archivos mediante un sencillo sistema de menús, de manera rápida y fácil, además, permite el acceso a catálogos de universidades. Un buen inicio para entrar al gopherspace es hacer un telnet a gopher.micro.umn.edu que es, históricamente hablando, el padre de todos los gophers en Internet.

H

Hardware

Lo integran los cables y todos los componentes electrónicos, o sea que es la parte física de los computadores.

Hacker

Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un craker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.Vea CERT.

Hdlc

Protocolo de la capa de enlace de datos.

Herramientas de búsqueda

Aplicaciones que nos sirven para encontrar archivos en diferentes servidores como lo son Archie y Verónica. Archie permite encontrar

archivos en diversos servidores de FTP mientras que Verónica hace lo mismo, pero en servidores de gopher.

Programas que permiten a los usuarios definir criterios o palabras relacionadas con una información requerida, siendo otras computadoras de la red las que efectúan la búsqueda indicando los sitios donde se encuentran los datos.
Vea: Busqueda de archivos: Archie, Archivos de dominio público, Verónica, Jughead, Gopher, grupos de noticias, Operadores Booleanos, Robots, World Wide Web, Búsqueda de Personas: White pages.

Recursos:
Búsquedas en Internet: Todo en uno http://serpiente.dgsca.unam.mx
Lista de servidores de WWW en el Mundo:
http://www.w3.org/pub/DataSources/WWW/Servers.html
Dejanews: Indice de grupos de noticias:(NEWS)
http://www.dejanews.com
Education world: Recursos sobre educacion http://www.education-world.com
Microsoft: http://www.microsoft.com/latam/busqueda/default.htm
Archivos:
Sahreware.com: http://www.shareware.com
World Wide Web:
Herramientas Internacionales:
Altavista: http://www.altavista.com
Excite: http://www.excite.com
HotBot: http://www.hotbot.com
InfoSeek: http://www.infoseek.com
Buscar recursos de Internet
http://www.infoseek.com/Internet?tid=502&sv=A2
http://www.infoseek.com/Internet?tid=502&sv=A2
Lycos http://www.lycos.com
Magellan: http://www.mckinley.com
Yahoo!: http://www.yahoo.com
WebCrawler: http://webcrawler.com
Herramientas de búsqueda en Español:
Indica: http://www.m3w3.com.mx/INDICA
Mexmaster: http://www.mexmaster.com/
Mexico Web Guide: http://mexico.web.com.mx
Yellow Pages México: http://www.yellow.com.mx

TESIS CON
FALLA DE ORIGEN

herramientas de Seguridad

Programas que nos permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas, casi todas de libre distribución. Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son:
Para el manejo de contraseñas: anipasswd, passwd+, crack, John The Ripper, S/Key
Para el manejo de autenticación: Kerberos, SecureRPC
Para el monitoreo de redes: Satan, ISS
Para auditoria interna: COPS, Tiger, Tripwire
Para control de acceso: TCP-Wrapper, PortSentry

herramientas de Seguridad

Programas que nos permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas, casi todas de libre distribución. Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son:
Para el manejo de contraseñas: anipasswd, passwd+, crack, John The Ripper, S/Key
Para el manejo de autenticación: Kerberos, SecureRPC
Para el monitoreo de redes: Satan, ISS
Para auditoria interna: COPS, Tiger, Tripwire
Para control de acceso: TCP-Wrapper, PortSentry

Hipermedia

Combinación de texto y multimedia. Actualmente es un recurso ampliamente explotado en el World Wide Web.

Hipertexto

Documentos que contienen vínculos con otros documentos, al seleccionar un vinculo automáticamente se despliega el segundo documento. Vea HTML, HTTP, Página Web, World Wide Web.

Son documentos que se despliegan y que contienen ligas o encadenamientos a otros documentos dentro del mismo servidor u otros, si así fuera el caso. Permite la organización de la información a los usuarios.

Home Page

Página Principal: es el documento que se despliega cuando con un visor nos ligamos a cualquier servidor de Internet.
(Página inicial). Es la página web de entrada a un lugar del World Wide Web. Es considerada la página principal.

Host

(Anfitrión) Computadora a la que tenemos acceso de diversas formas (telnet, FTP, World Wide Web, etc). Es el servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente. Un host es la computadora (anfitriona) que desempeña funciones centralizadas, y que tiene disponibles programas o información para las computadoras (invitadas) que se conecten. Vea Guest.

HTML

(Hyper Text Markup Language) Lenguaje de programación utilizando www y que contienen las reglas que gobiernan la creación de documentos que se pueden ver con un browser. La inmensa mayoría de los documentos que aparecen en Mosaic y Netscape son documentos HTML.

Lenguaje de marcado de hipertexto, (*Hiper-Text Markup Language*) es el lenguaje con que se escriben los documentos en el World Wide Web. A la fecha existen tres versiones de HTML. HTML 1, donde se sientan las bases para la disposición del texto y las gráficas, HTML 2 donde se agregan formas y HTML 3 (llamado también extensiones Netscape) donde se añaden tablas, mapas,etc. Vea HTTP.
Recursos:
A beginner's guide to HTML http://dmi.uib.es/info/Beginners.html
Webmaster's Tool Chest http://www.hometeam.com/tools/

TESIS CON
FALLA DE ORIGEN

HTTP — (Hyper Text Transport Protocol) Protocolo de Transferencia de Hipertextos (*Hiper-Text Transfer Protocol).* Es el protocolo usado por el World Wide Web para transmitir páginas HTML. El protocolo de comunicación empleado por los servidores de WWW.

Hub — Concentrador, es un término usado generalmente para describir un dispositivo que sirve para conectar una red.

I

IAB — (Internet Architecture Board) Es el grupo dedicado a todos los aspectos técnicos de Internet. Consejo de Arquitectura de Internet (*Internet Architecture Board* http://www.iab.org/iab/). Es el consejo reglamentador que toma decisiones sobre estándares que regirán a Internet. Determina las necesidades técnicas a medio y largo plazo, y toma las decisiones sobre la orientación tecnológica de la Internet. Aprueba las recomendaciones y estándares de la Internet a través de una serie de documentos denominados RFC Consulte: http://info.isoc.org:80/standards/index.html Vea IESG, IETF, ISOC.

IANA — (*Internet Assigned Numbers Authority*). Es el organismo de la ISOC (Internet Society http://info.isoc.org) de la administración de las direcciones Internet (Direcciones IP) así como de la creación de nuevos dominios (DNS) (Actualmente se encuentra en estudio la creación de nuevos dominios como inc, co etc). La IANA delega la asignación de dominios ya creados a la InterNIC. Para conocer más de la IANA consulte: http://www.iana.org/iana/ o la definición por la ISOC en http://info.isoc.org:80/adopsec/index.html.

ICMP — (Internet Control Message Protocol) Protocolo de Internet de la capa de red que provee de paquetes de mensajes para reportar errores y otra información relevante al procesamiento de los paquetes de IP.

TESIS CON
FALLA DE ORIGEN

IE	Vea Internet Explorer.
IESG	Grupo de Dirección de Ingeniería de Internet. (Internet Engineering Steering Group http://www.ietf.org/iesg.html). Grupo voluntario que se encarga de considerar los estándares propuestos por el Internet Engineering Task Force (IETF) que posteriormente serán establecidos por el IAB. Consulte: http://info.isoc.org:80/standards/index.html Vea ISOC.
IETF	Internet (*Internet Engineering Task Force http://www.ietf.org/).* Es el grupo que se encarga de regular los estándares técnicos en los que se basa Internet. Grupo de Trabajo de Ingeniería voluntario que investiga y desarrolla estándares que posteriormente son considerados por el Internet Engineering Steering Group (IESG).Consulte: http://info.isoc.org:80/standards/index.html Vea IAB, ISOC
IMAP	Protocolo de Acceso a Mensajes de Internet (Internet Message Access Protocol). Protocolo diseñado para permitir la manipulación de buzones remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el buzón y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el buzón hasta que el usuario confirma su eliminación. Un programa característico es Pine. Vea Correo Electrónico, POP.
Incidente	**Un evento que pone en riesgo la seguridad de un sistema de cómputo.**
Información	**El término de Información se refiere al dato, texto, imágenes, sonidos, código, programas de computadora, software, bases de datos o lo similar.**
In-Line Image	Una imagen desplegada en un documento HTML.
Integrated Services Digital Network	Vea ISDN
Íntegro	**La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo.**

TESIS CON
FALLA DE ORIGEN

Internet

Red de redes, un gran recipiente de conocimientos que no tiene fin. Internet está formada por miles de redes independientes que cuentan con sus propias reglas, sistemas de administración y criterios de información.

A través de Internet, se puede tener acceso a todas las fuentes de información que se quieran utilizar, ya que se puede obtener el conocimiento de las bibliotecas más prestigiadas del mundo y la búsqueda se realiza en cuestión de segundos, los 365 días del año. Es importante señalar que el usuario de Internet no solo puede recibir información sino también enviarla a donde él desee. Por otro lado, las empresas multinacionales han comenzado a usar Internet como un gran escaparate para dar a conocer sus productos y servicios. Internet se encuentra constituido por: El hardware, aplicaciones, protocolo y por los usuarios.

Es una red de cómputo a nivel mundial que agrupa a distintos tipos de redes usando un mismo protocolo de comunicación. Los usuarios en Internet pueden compartir datos, recursos y servicios. Internet se apoya en el conjunto de Protocoloes TCP/IP. De forma más especifica, Internet es la WAN más grande que hay en el planeta, e incluye decenas de MAN´s y miles de LAN´s. Las computadoras que lo integran van desde modestos equipos personales, minicomputadoras, estaciones de trabajo, mainframes hasta supercomputadoras. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión.El organismo que se encarga de regular, establecer estándares, administrar y hacer operacional a Internet es la ISOC (Internet Society). Vea ARPANET.

Recursos
Internet Society(ISOC): http://info.isoc.org
ISOC MEXICO http://www.isocmex.org.mx/
Numero de usuarios de Internet: Network Wizards http://www.nw.com
Perfil de los usuarios: All five GVU WWW UserSurveys:http://www.cc.gatech.edu/gvu
Administración, operación y seguridad en Internet: http://info.isoc.org:80/adopsec/index.html. Vea CERT.
Servicios de Información: http://info.isoc.org:80/infosvc/index.html
Mapa Global de Internet http://info.isoc.org:80/images/mapv15.gif

TESIS CON
FALLA DE ORIGEN

Internet address	(Dirección internet) Vea dirección IP.
Internet explorer	Programa Visualizador del World Wide Web. Disponible gratuitamente desde http://www.microsoft.com/ie. La versión 3 de este programa soporta Java y controles Active X.
InterNIC	Es el comité que se encarga de administrar las direcciones de Internet. (NIC= Network Information Center) Es el nombre que se le da al conjunto de proveedores de servicios de registro. El InterNIC define los nombres de dominio a nivel mundial. El sitio de la Internic (http://www.internic.net) es mantenido además por la Nacional Science Fundation (NSF http://www.nsf.gov) y la compañía de telecomunicaciones ATT (http://www.att.com). Vea DNS, Dominio, RFC, IANA.
Intranet	Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno. Por ejemplo, muchas compañías tienen servidores World Wide Web disponibles solo para sus empleados.
Intrusos	Vea CERT, Cracker, Hacker.
IP	(Internet Protocol) Es el protocolo o estándar utilizado por las computadoras para transmitir información a través de Internet. Protocolo Internet. Permite a un paquete de datos viajar a través de múltiples redes hasta alcanzar su destino. Se encarga de la capa de red del modelo OSI Vea Dirección IP, TCP.
IRTF	(Internet Research Task Force) la parte correspondiente exclusivamente a la investigación de los aspectos técnicos de Internet.
IP-Address	Es una dirección única en Internet en donde se puede localizar un servidor, que consta de 32 bits y se separa en 4 grupos de 8 bits cada uno, expresados como decimales. Por ejemplo :200.15.17.252.

TESIS CON
FALLA DE ORIGEN

IRC

(Internet Relay Chat) Es un software que hace posible conversaciones simultáneas en línea por medio del teclado con otros usuarios dentro de Internet. Si quieres hacer amigos, usa IRC, y podrás establecer conversaciones en tiempo real con usuarios de todo el mundo, unidos a través de conversaciones escritas que se llevan a cabo con la ayuda de esta herramienta, que sirve además para mantener informado a los individuos.

Programa basado en el modelo cliente servidor que permite conversar con múltiples usuarios en red sobre un tema común. b) Protocolo mundial para conversaciones simultáneas que permite comunicarse por escrito entre sí a través de ordenador a varias personas en tiempo real. El servicio IRC está estructurado mediante una red de servidores, cada uno de los cuales acepta conexiones de programas cliente, uno por cada usuario. Vea Foros de discusión Intereactivos.

Recursos
Comic Chat para Windows
http://www.microsoft.com/ie/comichat/advan.htm
The Palace http://www.thepalace.com/

ISDN

Red Digital de Servicios Integrados.(RDSI) (*Integrated Services Digital Network*). En español se abrevia RDSI. En el servicio de ISDN las líneas telefónicas transportan señales digitales en lugar de señales analógicas, lo que aumenta considerablemente la velocidad de transferencia de datos a la computadora. Si se cuenta con el equipo y el software necesarios, y si la central telefónica local ofrece ISDN y el proveedor de servicios lo soporta, el ISDN es posible utilizarlo. La velocidad de transferencia que puede alcanzar ISDN es de 128,000 bps, aunque en la práctica las velocidades comunes son de 56,000 o 64,000. Es una red digital de servicios integrados, especializados en la transmisión de datos sin empleo de los módem, utilizando protocolos de comunicación que permiten a las redes telefónicas transportar voz, datos y otro tipo de fuentes.

ISO

(International Standard Organization) es la Organización Internacional para la Estandarización. Esta Organización es responsable de la definición y publicación de los más altos estándares de calidad.

Organización Internacional para la Estandarización (*Internacional Organization for Standarización*). Es una organización que ha definido un conjunto de protocolos diferentes, llamados protocolos ISO/OSI. Esta organización de carácter voluntario fue fundada en 1946 y es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática, las ecológicas y las comunicaciones. Está formada por las organizaciones de normalización de sus 89 países miembros.

ISOC

(Internet SOCiety) Es el grupo voluntario más importante, que ayuda al desarrollo de Internet.

Sociedad Internet (Internet Society). Es una organización cuyos miembros dan el soporte y regulan a Interent. La Internet Society (http://info.isoc.org)fue creada en 1992 como una organización profesional

TESIS CON
FALLA DE ORIGEN

sin ánimo de lucro que facilita y da soporte a la evolución técnica de Internet, estimula el interés y forma a las comunidades científica y docente, a las empresas y a la opinión pública acerca de la tecnología, usos y aplicaciones de Internet y promueve el desarrollo de nuevas aplicaciones para el sistema. Esta sociedad ofrece un foro para la discusión y la colaboración en el funcionamiento y uso de la infraestructura global. La ISOC esta presente en muchos países conformando comites llamados capítulos. En México se localiza en http://www.isocmex.org.mx/ Los organismos que componen la ISOC son los siguientes:

Estándares de Internet
IETF (*Internet Engineering Task Force*)
IESG (*Internet Engineering Steering Group*)
IAB (*Internet Architecture Board*)

Administración de Internet:
IANA (*Internet Assigned Number Authority*).
Operación de Internet
IEPG -(*Internet Engineering Planning Group*) Consulte:
http://info.aarnet.edu.au:80/iepg/ y
http://info.isoc.org:80/adopsec/index.html
Seguridad en Internet.
CERT (*Computer Emergency Response Teams*). Exiten varios CERT´s en el planeta y se encuentran coordinados por Forum of Incident Response and Security Teams.(FIRT) en http://www.first.org/. Vea también http://info.isoc.org:80/adopsec/index.html

Recursos
ISOC http://info.isoc.org
ISOC MEXICO http://www.isocmex.org.mx/
Administración, operación y seguridad en Internet:
http://info.isoc.org:80/adopsec/index.html.
Estándares de Internet: http://info.isoc.org:80/standards/index.html
Servicios de Información: http://info.isoc.org:80/infosvc/index.html
FAQ de la ISOC: http://info.isoc.org:80/infosvc/allabout.html

ISP (*Internet Service Provider*). Vea Proveedor de Servicios de Internet.

TESIS CON
FALLA DE ORIGEN

J

Java

Un lenguaje de programación que permite ejecutar programas escritos en un lenguaje muy parecido al C++, llamados applets, a través del World Wide Web. La diferencia contra un CGI es que la ejecución se realiza totalmente en la computadora cliente, en lugar del servidor. Java fue originalmente desarrollado por Sun Microsystems (http://www.sun.com). El principal objetivo de JAVA fue hacer un lenguaje que fuera capaz de ser ejecutado de una forma segura a traves de Internet. Esta característica requiere la eliminación de muchas contrucciones y usos de C y C++. El más importante, es que no existen punteros. Java no puede acceder arbitrariamente a direcciones de memoria. Java es un lenguaje compilado en un código llamado "codigo-byte" (byte-code). Este código es interpretado "en vuelo" por el interprete Java.

Recursos:
El situo JAVA de sun: http://java.sun.com/ o Javasoft:
http://www.javasoft.com
Java FAQ list and Tutorial: a work in progress
http://sunsite.unc.edu/javafaq/javafaq.html
Java(tm): Programming for the Internet
http://sunsite.doc.ic.ac.uk/packages/java-http/
Java World http://www.javaworld.com/
Recursos: http://www.gamelan.com/index.shtml
Sunsite en la UNAM: http://sunsite.unam.mx/
Where can I read about it http://java.sun.com/nav/read/index.html

JPG o JPEG

(Joint Photographic Expert Group) Un formato para guardar imágenes que las hace ocupar poco espacio en la memoria de la computadora y en disco. Por esta razón son más rapidas de transmitir a través del web. A diferencia del formato GIF, este formato no es aceptado por todos los Visualizadores del World Wide Web. Es un método de comprensión de imágenes en forma digital. JPG. Es un tipo de archivo de acuerdo a la norma de comprensión JPEG.

Jughead

Herramienta de localización que permite realizar búsquedas basadas en palabras clave en directorios y dominios de gopher. La búsqueda se reduce a un dominio. Vea Gopher, herramientas de búsqueda, Veronica

TESIS CON
FALLA DE ORIGEN

K

Kbps

(Kilobits por segundo) Velocidad en la transmisión de miles de bits por segundo.

Kermit

Programa que ofrece un ambiente interactivo para transferir archivos de un servidor a una computadora conectada vía acceso conmutado. Utilizado principalmente para extraer archivos de una BBS. Vea Xmodem

Kilobyte

Mil bytes. Actualmente es usado como 1024 (dos elevado a la 10) bytes.

L

LAN

(Local Area Network) Es una red de computadoras dentro de un mismo lugar.
Red de área local (*local area network*). Red cuyas dimensiones no exceden 10 km. Puede tratarse de computadoras conectadas en una oficina, en un edificio o en varios. Vea MAN, WAN.

Legislación

A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo.

Línea conmutada

Conexión múltiple bajo una línea conmutada. Es un servicio que permite conectar redes locales (LAN) a través de una línea conmutada a Internet, y como éste servicio no es el de una línea dedicada, su costo es inferior. Sus principales características son: Que el tráfico comercial está permitido y puede correr el protocolo PPP, así como establecer conexiones múltiples bajo una línea conmutada.
Se refiere al tipo de conexión que se establece usando un emulador de terminal y un módem. Vea acceso conmutado, proveedor de servicios de Internet.

Línea dedicada

Es un servicio que proporcionan las compañías telefónicas a quien lo solicite, permitiendo que se mantengan conectadas los dos extremos permanentemente. Y son utilizadas para diferentes servicios como telefonía, transmisión de datos, conexión a Internet, etc.
Línea privada que se utiliza para conectar redes de área local de tamaño moderado a un proveedor de servicios de Internet. Se caracteriza por ser una conexión permanente.

Link

Vea Vinculo.

Linux

Sistema operativo (apoyado en las normas de la GNU), similar al UNIX. Linux tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitarea real, memoria virtual, librerías compartidas, dirección y manejo propio de memoria y TCP/IP. Usa las características hardware de la familia de procesadores 386.

Recursos:
Linux en México. http://www.linux.org.mx
Linux Documentation Proyect http://sunsite.unc.edu/mdw
Pagina relacionada a Linux en México http://www.lsl.com.mx/

TESIS CON
FALLA DE ORIGEN

Lista de discusión

Otro nombre dado a las listas de correo.

Listas de correo o listas de discusión o foros de discusión

Servicio automatizado de mensajes, a menudo moderado por un propietario en el que los suscriptores reciben mensajes dejados por otros suscriptores por un tema dado. Los mensajes se envían por correo electrónico. Vea Listserv, Mayordomo, Moderador, USENET.

Recursos:

Foros Interplanet: http://www.interplanet.com.mx/foros/

Listserv

Programa que permite la creación y distribución de listas de correo. La comunicación con el programa es vía correo electrónico. La ventaja de Listserv frente a Mayordomo es que conociendo el nombre de un servidor listserv es posible obtener copia de todas las listas de correo de todo el mundo. La comunicación con Listserv es enviando en el cuerpo del mensaje (no en el subject) la instrucción deseada. El servidor mas conocido es mailto:LISTSERV@LISTSERV.NET.

Por ejemplo: Para obtener una relación de todas las listas de correo existentes:

To LISTSERV@LISTSERV.NET
Subject [Vacio]
list Global
Para suscribirse a una lista, por ejemplo aVirtual Tour of Cyberspace
To LISTSERV@LISTSERV.NET
Subject VacioU
suscribe TOURBUS
Para cancelar la subscripción a una lista, por ejemplo aVirtual Tour of Cyberspace
To LISTSERV@LISTSERV.NET
Subject VacioU
unsuscribe TOURBUS
Para pedir ayuda acerca de los comandos disponibles:
To LISTSERV@LISTSERV.NET
Subject VacioU
help

LLC

(Control Lógico de Enlace) Maneja el control de flujo y errores.

Login

Clave de acceso que se le asigna a un usuario para que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de internet junto con la dirección electrónica de la computadora que utiliza.
Vea password

Lynx

Visualizador en modo texto del World Wide Web, desarrollado por la Universidad de Kansas (http://www.cc.ukans.edu), y es del dominio público para usos no comerciales.

Recursos:
Lynx: ftp://ftp2.cc.ukans.edu/pub/lynx

TESIS CON
FALLA DE ORIGEN

M

MAC	(Media Access Control) Dirección física en redes locales tipo ethernet en seis bytes y expresados en hexadecimal y separados por dos puntos y es el mecanismo a través del cual los dispositivos conectados a una red, pueden accesar el medio de transmisión.
Macintosh	Serie de computadoras de Apple Computer (http://www.apple.com). Su sistema operativo fue el primero totalmente gráfico y basado en ventanas. El entorno es intuitivo, eliminando el teclado de los comandos del sistema. A todos los objetos se le asigna una representación gráfica (iconos). Recursos Lista de sitios Apple http://www.share.com/peterlewis/applesites.html
Mail	Programa en ambiente UNIX para la edición lectura y respuesta de correo electrónico. Vea MUA.
Majordomo	Programa administrador de listas de correo. La manera de pedir ayuda es mandando un mensaje. Por ejemplo, a la UNAM a majordomo@servidor.unam.mx con la palabra clave "ayuda" (sin comillas) en el cuerpo del mensaje, de manera similar a como se realiza con Listserv, con la diferencia que en este caso son comandos en español (p.e. ayuda, listas, etc).
Maling Lists	Grandes listas para comunicarte de manera electrónica con gente interesante.
MAN	Red de área metropolitana (*Metropolitan area Network*). Red que no va más allá de los 100 km. Equipos de computo y sus periféricos conectados en una ciudad o en varias forman una MAN. Vea LAN, WAN.
Marcado	Conexión que se realiza cuando una computadora llama a otra vía telefónica. Vea módem, script.
Mbps	(Megabits por segundo) Velocidad de transmisión millones de bits por segundo.
Medio	Término que se refiere al canal de comunicación.
Mensaje de datos	**Martes 4 de junio de 2002 DIARIO OFICIAL (Primera Sección) 36. A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.**
México Web guide	Herramienta de búsqueda en español que dispone además de un catalogo de recursos en http://mexico.web.com.mx. Puede realizar búsquedas utilizando operadores booleanos en: http://mexico.web.com.mx/buscar.html. Vea Herramientas de búsqueda.

MIB	Más conocido como variables MIB. Bases de datos de información.
Microsoft	Compañía creadora del sistema operativo Windows 95, Windows NT, de los controles Active X, desarrolladora del Navegador del World Wide Web Internet Explorer, entre otros recursos. Recursos: Microsoft México: http://www.microsoft.com/mexico/ Busqueda de recursos: http://www.microsoft.com/latam/busqueda/default.htm Microsoft http://www.microsoft.com Microsoft network http://www.msn.com
MIME	Extensiones de Correo de Internet de Múltiples propósitos (*Multipurpose Internet Mail Extensions*) Técnica para codificar archivos y anexarlos a un mensaje de correo electrónico. Permite principalmente enviar archivos binarios como parte de un mensaje. Método para codificar y decodificar de manera automática la información y se utilizado para mandar correo a través de diferentes plataformas. Vea BinHex, UUENCODE, UUDECODE.
Mirror	(espejo). Término usado en Internet para hacer referencia a un servidor FTP, Página Web o cualquier otro recurso que es espejo de otro. Estos mirrors se realizan automáticamente y en una frecuencia determinada, y pretenden tener una copia exacta del lugar del que hacen mirror.
MLID	Manejador de la interfaz de enlace múltiple.
MNP	(Microcom Network Protocol) Protocolo para corregir errores o comprimir la información en los enlaces con los módem, y que va de 1 a 5.
MNP5	Protocolo de comprensión de datos que puede mejorar el enlace de datos vía módem hasta un 200n.
Modelo Cliente-Servidor	El modelo cliente-servidor se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor). De esta manera los clientes son los elementos que necesitan servicios del recurso y el servidor es la entidad que poseen el recurso. Los clientes sin embargo no dependen totalmente del servidor. Ellos pueden realizar los procesamientos para desplegar la información (por ejemplo en forma gráfica). El servidor los provee únicamente de la información sin hacerse cargo de otros procesos. El tráfico en la red de esta forma se ve aligerado y las comunicaciones entre las computadoras se realizan más rapido.
Módem	(MOdulador / DEModulador) Equipo electrónico que sirve para enlazar computadoras a través de las líneas telefónicas o equipos de radio. Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados (ISDN), mediante un proceso denominado de modulación (para transmitir información) y demodulación (para recibir información), de ahí su nombre. La velocidad máxima que puede alcanzar un módem para línea telefónica es de 33 kBps.

TESIS CON
FALLA DE ORIGEN

sin embargo los más comerciales actualmente son los de 28 kBps. Un módem debe cumplir con los estándares de MNP5 y V42.bis para considerar su adquisición. Los módems se dividen en *internos* (los que se colocan en una ranura de la computadora) y en *externos* (que se conectan a un puerto serial de la computadora). Instalacion: Modems Internos. Estos deben ser configurados antes de ser instalados. Es necesario mover los puentes (jumpers) para indicar un puerto (COM) y una interrupción (IRQ). Modem Externos. La instalación requiere de un cable (DB25 o de 25 agujas macho a 25 agujas hembra o a 9 agujas hembra) que conecte directamente al puerto serial de la computadora. Es necesario asegurarse que no se esta utilizando un puerto compartido con otro elemento de hardware (p.e. un mouse). Para ello debe instalarse en COM2 o COM4 si el mouse esta instalado en COM1 o en COM1 o COM3 si el mouse esta instalado en COM2. La interrupción (IRQ) depende del puerto donde este instalado. Vea Acceso conmutado, Script, SLIP, PPP.

Moderador — Persona que se dedican a moderar listas de correo y grupos de noticias y son responsables de decidir qué mensajes de correo electrónico pueden incorporarse a dichos grupos y listas.

Mosaic — Programa gráfico (visor) que le permite navegar en Internet para explorar el World Wide Web. Fue el primer browser en Internet. Navegador o Visualizador para el World Wide Web. Fue el primer visualizador para los ambientes Macintosh, UNIX y Windows, desarrollado por la NCSA (http://www.ncsa.uiuc.edu/).

MPEG — (*Moving Pictures Expert Group*). MPEG es un estándar de compresión de vídeo. Se adhiere a los visualizadores por medio de un Plug in. La versión 3 del Internet Explorer lo trae ya integrado.

MTA — Agente para el transporte de correo electrónico (*Mail Transport Agent*) son programas que se encargan de distribuir los mensajes generados en el sistema. El más popular es el llamado sendmail, distribuido con sistemas UNIX.

Mtud — Unidad máxima de transmisión.

MUA — Agente usuario de Correo electrónico (*Mail User Agent*). Son todo auquellos programas que permiten la edición, lectura y respuesta de correo electrónico.
Vea Eudora, Mail, Pine.

MUD — Diálogo o dimensión multiusuario (*Multiuser Dungeon o Dimension*). Es un juego interactivo de actuación que se juega en Internet. los jugadores entran em el juego desde cualquier parte de Internet; solo tienen que conectarse por medio de la red al sistema donde se guarda el juego y, posteriormente interactuar de manera recíproca uno con otro. Programa que simula un lugar en el que es posible conversar con otros usuarios, interactuando con el ambiente.

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

N

Name Server	ver DNS
Navegador	Es un programa gráfico (visor) que le permite navegar en Internet para explorar el World Wide Web. Ver BROWSER
NC	Vea Network Computer.
NCSA	Centro Nacional de Aplicaciones de Supercómputo (National Center for Supercomputing Applications). Se localiza en la Universidad de Ilinois en Urbana-Champaign Creadores de Mosaic, entre otras muchas aplicaciones para el Internet. Desarrolladores del visualizador Mosaic para el World Wide Web. Localizado en. http://www.ncsa.uiuc.edu/
Net PC	Vea Network Computer.
NETbios	(NET Basic Input Output System)Protocolo de transporte comunmente usado para redes de área local de PC.
Netiqueta	Etiqueta de Internet que consiste en buenos hábitos. Pequeño manual de Netiqueta E-Mail y Listas de correo : No contestar a todos los miembros de una lista de correos o grupo de discusión, cuando lo que se tiene que decir es para uno solo. Hacer referencia sólo al párrafo que se esta contestando en un mensaje y no enviarlo todo nuevamente al responder. Contestar un mensaje de correo electrónico con mayúsculas equivale a alzar la voz . FTP obtener los archivos de la ubicación más cercana para no obstruir el paso en la red. Transferir archivos en las horas de menor demanda (horas no hábiles) Generales No insultar a otros usuarios en la red. No enviar a ningún usuario información no solicitada. Comportarse de una manera cortes con otros usuarios. No ejecutar procesos innecesarios
Netnews	Son los grupos que se concentran en servidores que forman una red de información, de tal manera, que las noticias viajan más rápido en Internet que en cualquier otro medio.
Netscape Navigator	Es un programa gráfico (visor) que le permite navegar en Internet para explorar el World Wide Web. Visualizador para el World Wide Web. Disponible desde http://www.netscape.com, en las siguientes plataformas X-Windows (UNIX), Macintosh y Windows. Ver BROWSER
Network	Es la manera en que dos o más computadoras se comunican entre sí. Vea RED.
Network Computer	(NC- Computadora de Red). También llamada NET PC, Web Pc, Web TV Sistema capaz de sintonizar canales de TV e Internet a través de un módem y utilizando el World Wide Web. Se espera que su utilización se

	extienda más a futuro conforme vayan aumentando las prestaciones y se reduzca su precio.
Network Information Center	Vea NIC
Network News	Dentro de Network News se organizan grupos de discusión (newsgroups). Un programa despachador de artículos (NewsReaders) se encarga de presentar tales pláticas de manera ordenada.
Network Operation Center	Vea NOC.
Newgroups	Grupos de discusión bajo un conjunto de amplios apartados que son conocidos como grupos de noticias. Todos estos Newgroups juntos, son llamados Usenet. Y tratan por lo general diversos temas específicos.
NEWS	Vea USENET, Grupos de noticias.
NIC	Centro de Información de red (*Network Information Center*). Organización responsable de proporcionar información de una red a los usuarios. En México se encuentra en http://nic.mx y en RED UNAM en http://www.unam.mx/nicUNAM. Vea NOC.
No Carrier	No hay portadora. Mensaje del módem que notifica, que no logra la conexión con la frecuencia para la transmisión de una señal. Indica que es un desperfecto o falla.
No Dialtone	Mensaje que indica que no hay tono de línea y por lo tanto no se puede marcar.
NOC	Centro de Operaciones de la Red (*Network Operation Center*). Es un grupo responsable de la operación diaria de la red. Cada proveedor de servicios tiene su propio NOC, por lo que es importante saber a cual llamar en caso de Emergencia. Vea NIC.
Nodo	Computador integrado a Internet con su propia dirección IP que es única. Computadora conectada a una red de area local por un medio físico.
NSFNET	Red de la Fundación Nacional de la Ciencia (*National Science Foundation* (NSF) http:// www.nsf.gov). Fue de las primeras redes académicas en hacerse cargo de Internet y es actualmente eje central de la misma. Vea Internic.
Ñ ñ	Letra característica del idioma español. Debido a que su código ASCII (164 minúscula, 165 mayúscula) se encuentra encima del tope de 7 bits (156) , no es posible su inclusión en el correo electrónico, abreviándose como (ni) .Por ejemplo Anio (Año).

TESIS CON
FALLA DE ORIGEN

O

Octeto (*octect*). Termino para referirse a los ocho bits que conforman un byte. Vea dirección IP.

Objetos A las definiciones del lenguaje ASN.1

Operadores Booleanos Son operadores lógicos que permiten realizar búsquedas complejas. Cada herramienta de búsqueda tiene distintos operadores, aunque existen unos cuantos que tratan de ser universales como el AND (Y) el OR (o) y el NOT (no). La mayoría de las veces se puede encontrar los operadores que utiliza una herramienta de búsqueda en la opción tips. A continuación se mencionan algunos ejemplo de como se utilizan los operadores booleanos en Excite (http://www.excite.com)

1. Todos los operadores lógicos deberán ir con mayúsculas (AND, OR, NOT, etc)
2. Para buscar por ejemplo las referencias de la película el Mago de Oz se puede utilizar la siguiente pregunta wizard AND or AND movie.
3. La busqueda de palabras compuestas se hará utilizando la primera letra como mayuscula: ejemplo: Apple Computer

Organización Auto-Reguladora El término de Organización Auto-Reguladora se refiere a la organización o entidad que no es una agencia reguladora federal o estado, pero que se encuentra bajo la supervisión de la ley federal para adoptar y administrar reglas aplicables a sus miembros los cuales son reconocidos por dicha organización u entidad, por la agencia federal reguladora o por otra organización de auto-regulación.

Original A la información contenida en un mensaje de datos que se ha mantenido íntegra e inalterada desde el momento en que se generó por primera vez en su forma definitiva.

OSI (Open System Interconnection) Norma de ISO para organización de los programas para intercambio de datos y además ayuda a facilitar el trabajo conjunto entre programas de diferentes fabricantes. Las 7 capas del modelo OSI son :

- Aplicación
- Presentación
- Sesión
- Transporte
- Red
- Enlace de Datos
- Física

TESIS CON
FALLA DE ORIGEN

P

Página Electrónica	Ver Home Page.
Packet	Conjunto de bytes que viaja de una computadora a otra, en orden definido.
Página web	Es el resultado en hipertexto e hipermedia que proporciona un visualizador de World Wide Web después de obtener la información solicitada. Vea Home Page, Web site.
Paquete	(*packet*) .La unidad de datos que se envía a través de una red. Un paquete se compone de un conjunto de bits que viajan juntos.
Par trenzado	Parecido al cable utilizado para teléfonos, pero con una cantidad mayor de cables dentro. Es el medio físico por medio del cual se pueden conectar varias computadoras. Vea cableado, cable coaxial, fibra óptica.
Password	Palabra clave que se le asigna a un usuario -además de su login- como contraseña para la utilización de los recursos de una computadora. El password no es visible en la pantalla al momento de teclearlo.
Pegasus Mail	Cliente de correo electrónico para plataformas DOS, Macintosh, Windows y UNIX. Existen dos versiones las Shareware y la Freeware. Consulte http://www.pegasus.usa.com. Vea Eudora, Pine.
Perl	Lenguaje de programación utilizado en el World Wide Web a través de un CGI, principalmente para realizar consultas a bases de datos como Oracle, SQL-Server, SyBase, etc, o a herramientas locales como WAIS. Perl es un lenguaje para manipular textos, archivos y procesos, proporciona una forma fácil y legible para realizar trabajos que normalmente se realizarían en C o en un shell. Perl nació y se ha difundido bajo el sistema operativo UNIX, aunque existe para otras plataformas. Perl fue desarrollado por Larry Wall, y está distribuido libremente bajo la filosofía de la GNU. Recursos: FTP anonymous: ftp://jpl-devvax.jpl.nasa.gov/pub
PINE	Programa de correo electrónico organizado por medio de menus mediante los cuales se pueden leer, enviar y administrar mensajes electrónico. Vea Eudora, IMAP, Pegasus.
Ping	Prueba básica de conectividad. Es un comando que prueba si podemos conectarnos a una computadora remota. Esta simple función es extremadamente valiosa para la prueba de interconexión, ya que verifica enlaces y conexiones por eco.
Plugins	Programas que se agregan a un visualizador del Word Wide Web que realizan funciones determinadas. Estas pueden ser visualización de archivos multimedia, soporte a archivos graficos no estándares con el visualizador, etc. Vea Real Audio, Shockwave.

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

POP	Protocolo de Oficina de Correos (*Post Office Protocol*) Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita la entre de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta. Los mensajes enviados a la aplicación cliente son inmediatamente eliminados del servidor, sin embargo las aplicaciones modernas pueden omitir este paso. Entre los programas que utilizan dicho protocolo se encuentra Eudora. Vea IMAP.
POP-3	Versión 3 del Protocolo de Oficina de correos.
Postscript	Un lenguaje para describir páginas ideado por Adobe Systems. Software que proporciona una salida capaz de imprimir texto y gráficos en la mayoría de las impresoras o componedores gráficos.
PPP	(Point to Point Protocol) Protocolo de comunicación punto a punto, es un método confiable para conectar computadoras a Internet. Ver SLIP.
PPP	Protocolo Punto a Punto (*Point to Point Protocol).* Implementación de TCP/IP por líneas seriales (como en el caso del módem). Es mas reciente y complejo que SLIP. Recursos: FreePPP 2.5 para Macintosh http://www.macworld.com/cgi-bin/software.pl/NewUploads/Software.647.html Para windows http://www.cris.com/~beers/here/
Prompt	Carácter o palabra que indica que la computadora está lista para recibir comandos (órdenes) del usuario.
Protocolo	Reglas formales de comportamiento. Son reglas acordadas en común, que son difundidas y conocidas ampliamente para su observancia. Es la definición de como deben comunicarse dos computadoras, sus reglas de comportamiento, etc
Proveedor de Servicios de Internet	(*Internet Service Provider*) Organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Vea BBS. Los factores que se deben considerar para elegir un proveedor de Internet son: a) Ancho de banda: Velocidad que ofrece el proveedor para transmitir los datos. b) Tipo de conexión, En forma directa o en forma conmutada. c) Costo por hora, mes o año; tanto de la conexión como del registro del correo electrónico en un servidor. d) Numero de usuarios. En importante conocer el numero de usuarios por línea disponible. e) Seguridad. Confianza en la ética del proveedor para respetar los datos

de los usuarios.

Puente	(*bridge*). Los puentes son dispositivos que tienen usos definidos. Primero, pueden interconectar segmentos de red a través de medios físicos diferentes; por ejemplo, no es poco común ver puentes entre cable coaxial y de fibra óptica. Además, pueden adaptar diferentes protocolos de bajo nivel (capa de enlace de datos y física de modelo OSI). Vea Enrutador, Gateway.
Puerto	Es un numero que identifica a una aplicación particular de Internet. Uno de los canales de entrada/salida de una computadora. Vea Módem.
Pulsos	Es un modo de marcar un numero telefónico en el cual cada dígito se representa por tantos números consecutivos como el número. Es el modo más común en las líneas telefónicas de México. Vea Módem, Script, Tonos
Persona	El término de Persona se refiere al individuo, corporación, negociación, estado, confiable, asociación, fusión, agencia gubernamental, corporación pública o cualquier otra entidad comercial.
Prestador de servicios de certificación	A la entidad que presta los servicios de certificación a que se refiere la presente Norma Oficial Mexicana.

Q

Quicktime	Un método para almacenar video y audio en formato digital, desarrollado por Apple.
Quick Cam	Cámara de video digital que se conecta al puerto paralelo de la computadora y permite la realización de *Video-conferencia* utilizando Internet. Recursos: QUICK CAM: *http://www.connectix.com* FLEXCAM *http://www.flexcam.com*
Quick Search	Búsqueda Rápida

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

R

Real Audio	*Plugin* que se agrega al *visualizador* para poder sintonizar mensajes enviados a traves de la *red* en tiempo real con formato audible. Disponible en *www.realaudio.com* Vea *Telefonía en Internet*
Realidad Virtual	Vea *VRML*
RED	Al sistema de telecomunicaciones entre computadoras. Agrupación tanto de equipos como de programas que comparten recursos entre sí, observando "reglas de comportamiento" a partir del uso de un lenguaje y medios de transmisión comunes, sin importar -en lo esencial- la naturaleza de cada elemento dentro de la red. Vea *Backbone, LAN, MAN, WAN*
Red Digital de Servicios Integrados	Vea *ISDN.*
Red Inalámbrica	Red que no utiliza como medio físico el cableado sino el aire, utilizando generalmente microondas, o rayos infrarojos.
Registro	El término de Registro se refiere a la información la cual está inscrita en un medio tangible el cual es almacenado en un medio electrónico u otro medio el cual es recuperable y posee una forma perceptible.
Registro Electrónico	El término de Registro Electrónico se refiere al contrato u otro registro creado, generado, enviado, comunicado, recibido o almacenado bajo medios electrónicos.
Repositorio	Sistema para almacenar y recuperar certificados y demás información pertinente a las firmas digitales.
Requiremento	El término de Requerimiento incluye prohibición.
Resumen O Compendio	Al resultado de aplicarle a un mensaje de datos una función de criptografía del tipo hash.
RFC	Solicitud para comentarios (Request for Comments). Es un conjunto de documentos en los cuales los estándares de *Internet*, los estándares propuestos y, generalmente las ideas en proceso de aceptación son documentados y publicados. Los documentos pueden ser consultandos en *Internic* en *http://www.internic.net/rfc*. Vea *IAB*.
Robots	Los robots en el contexto del *World Wide Web* son programas que viajan en el Web, indexando páginas, localizando errores, etc. Estos programas son enviados y mantenidos por varias *herramientas de búsqueda*.
Router	Dispositivo que selecciona un recorrido adecuado de la información, en las redes que tienen múltiples vías de comunicación entre los usuarios y estas.
Rpg	Generador de informes de programas introducido en 1964 por IBM.

Rs-232	(Recomended Satandard 232 del EIA) Interfaz de 25 cables que sirve para unir una computadora y un periférico, tal como módem, mouse, impresora, etc. Emplea conectores DB-25, DB-9 u otros.
RSDI	(Red Digital de Servicios Integrados) Ver ISDN.

S

Server	Poderosa máquina de gran rapidez y con gran capacidad de almacenamiento, que funciona como el equipo principal de una red de cómputo y que permite los accesos a los usuarios registrados a través de sus terminales respectivas.
Script	Secuencia de comandos que se le dan a un *módem*. Esta secuencia puede ser por ejemplo para asignar una configuración al módem (velocidad, compresión de datos, etc) o para realizar tareas específicas (llamar al proveedor, colgar, etc). A veces es necesario modificar un script o cadena de inicio que le establece al módem las condiciones iniciales (por ejemplo cambiar ATDT que establece una línea telefónica por *tonos* a ATDP que indica una línea telefónico por *pulsos*, etc.) Vea *marcado*.
Secretaría	A la Secretaría de Economía.
Seguridad	Vea *CERT*.
seguridad en cómputo	Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoria.
Sendmail	Vea *MTA*
Sello del prestador de servicios de certificación	Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.

TESIS CON
FALLA DE ORIGEN

Servidor	Computadora dedicada a gestionar el uso de la red por otras computadoras llamadas *clientes*. Contiene archivos y recursos que pueden ser accesados desde otras computadoras (terminales). Vea *Modelo cliente-servidor*.
Sesión remota	Uso de los recursos de una computadora desde una terminal que no precisamente se encuentra cercana a ella. Vea *telnet*
Shareware	Es software registrado que se puede copiar y usar por un período de prueba, en caso de aceptarlo se deberá pagar al autor o compañía representante, el importe del mismo, al término del período indicado. En caso contrario, deberá desinstalar el programa y eliminar la copia hecha, bajo su propia responsabilidad. Programas que pueden ser obtenidos por Internet de computadoras con *archivos públicos*. La regla de utilización es que se paguen después de un periodo de evaluación (por lo regular 30 dias). Vea *Freeware*
Shareware.Com	(*http://www.shareware.com*) *Herramienta de búsqueda* para localizar archivos shareware de cdnet (*http://www.cnet.com*). Actualmente mantiene un indice de 170,000 archivos para la mayoria de las plataformas existentes. Vea: *Archivos de dominio público.*
Shell	Es la forma más sencilla de conectarse a Internet, accesando toda la información en modo de texto, no emplea gráficos y se necesitan conocimientos de Unix.
Shockwave	Un programa para *Netscape* que permite hacer presentaciones de multimedia (con audio, video, etc) a través del web. Disponible en *www.shocker.com*. Vea *Plugins*.
Signature	Vea *Firma*
Sistema de Nomenclatura de dominios	Vea *DNS*
Sitio (Site)	Cualquier organización (militar, gubernamental, comercial, académica, etc.) que posea recursos relativos a redes y computadoras.

TESIS CON
FALLA DE ORIGEN

Slip — *Serial Line Internet Protocol.* Es una implementación de TCP/IP por líneas seriales. Para conectar un *módem* a Internet es necesario establecer un protocolo SLIP o *PPP.* En el caso de *RED* UNAM la conexión se realiza por SLIP y por un programa que realiza la conexión y establece los sockets o canales de comunicación de las aplicaciones, de esta manera se permite la transferencia de paquetes a la computadora local. El protocolo SLIP define un mecanismo sencillo de transmisión de paquetes a través de líneas seriales. Con lo cual permite el acceso a todos los servicios de Internet y cuenta con grandes beneficios en su forma de enlace, ya que no se hacen cargos extra por usar los módem rápidos y se dispone de acceso completo a Internet, incluyendo los servicios: E-mail, Telnet, FTP, Gopher, Archie, Talk, WWW, Finger, Ping y Usenet News.

Slip + Pop3 — Es una gran ayuda para atraer el correo electrónico y leerlo en la PC.

Smiley — Caras sonrientes empleadas en el *correo* y en los artículos de *USENET* para indicar algún sentimiento.

Pequeño diccionario no oficial de smileys (*The Unofficial Smilie Dictionary*) (tomado de *gopher://condor.dgsca.unam.mx*, donde se encuentra el diccionario mayor)

:-) = Sonrisa básica. Indica un comentario gracioso o sarcástico
;-) = Sonrisa con un guiño
:-(= El emisor del mensaje esta triste
:-I = Indiferencia
---e--l(@ = Rosa.

SMTP — (Simple Mail Transfer Protocol). Protocolo usado en redes TCP/IP para definir el flujo de correo electrónico en la misma. *Protocolo* que se usa para transferir *correo electrónico* entre servidores de correo. Como sólo transfiere mensajes entre servidores, el *usuario* debe utilizar otro protocolo para acceder los mensajes como *POP* o *IMAP*

Software — Programas de cómputo.

SOHO — (Small Office-Home Office) Se refiere a las pequeñas empresas o instalaciones domiciliarias de computación.

SSL — Capa de conexiones Seguras. (Secure Sockets Layer) Utiliza una llave de 40 bits para encriptar la información proporcionada de manera confidencial, ya sea a un proveedor, una base de datos, etc.

TESIS CON
FALLA DE ORIGEN

T

Talk

Permite que un usuario puede tener una conversación interactiva con cualquier otra persona conectada a Internet. Conversación. Protocolo que permite a dos personas conectadas a terminales situadas en dos lugares distintos comunicar por escrito entre sí en tiempo real. Vea: IRC

TCP

(Transmission Control Protocol) Es una conexión orientada a transmitir información en paquetes y cuando usa el estándar IP, es entonces cuando se le conoce como el protocolo TCP/IP. El Protocolo de control de transmisión es el protocolo que se encarga de la transferencia de los paquetes a través de Internet y de que los paquetes lleguen al destino sin ningún error o pide su reenvío. Se encarga de la capa de transporte del modelo OSI
Vea IP, UDP.

Telefonía en Internet

La telefonía en Internet se caracteriza por establecer comunicación auditiva entre dos usuarios utilizando micrófonos y tarjetas de sonido Full Duplex.
Vea UDP, Video-Conferencia.

TESIS CON
FALLA DE ORIGEN

Recursos:
Internet Phone: http://www.vocaltec.com
Net2Phone: http://www.net2phone.com
Webphone: http://www.netspeak.com

Telnet

(Network Terminal Protocol) Es un programa que permite accesar una computadora remota y utilizarla a través de la red. Permitiendo a una computadora actuar como terminal tipo multiusuario.

Protocolo de emulación de terminal que permite establecer una sesión remota a otra computadora en Internet. Vea Sesión Remota, Telnet no estándar.
Recursos:
Biblioteca central de la UNAM: telnet://132.248.67:23, login opac
Biblioteca del Congreso de los E.U.: telnet://dra.com

Telnet no estándar

Uso de telnet para ejecutar una aplicación en párticular. Para ello es necesario conocer el puerto en particular. P.E. telnet://debra.dgbt.doc.ca:3000, donde 3000 es el número del puerto en la computadora donde se ejecuta el programa.

TIFF

(Tag Image File Format) Formato de archivo de imágenes elaboradas por scanner.

Token Passing

(Paso de ficha). Protocolo que se utiliza en redes Arcnet y Token Ring, y que se basa en un esquema libre de colisiones, dado que la señal (token) se pasa de un nodo o estación al siguiente nodo. Con esto se garantiza que todas las estaciones tendrán la misma oportunidad de transmitir y que un sólo paquete viajará a la vez en la red.

Token Ring	Red local desarrollada por IBM que utiliza el protocolo de acceso Token Passing y que utiliza un ancho de banda de 4 y 16 Mbps. Utiliza la topología de anillo. Vea Ethernet.
Tonos	Es una forma de marcar un número telefónico en el cual cada numero tiene asignado un cierto tono audible (tono). Vea módem, pulsos, script
Topología de bus	Topología en donde todas las estaciones se conectan a un cable central llamado "bus". Este tipo de topología es fácil de instalar y requiere menos cable que la topología de estrella. Vea Ethernet.
Topología de estrella	Topología donde cada estación se conecta con su propio cable a un dispositivo de conexión central, bien sea un servidor de archivo o un concentrador o repetidor. Vea Arcnet.
Topología de red	Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Tres de las topologías principales de red son la topología de bus, de estrella, y de anillo.
Topologías de anillo	Topología en donde las estaciones de trabajo se conectan físicamente en un anillo, terminando el cable en la misma estación de donde se originó. Vea Token Ring.
Transferencia de Archivos	Vea FTP.
Transacción	El término de TRANSACCIÓN se refiere a la acción o al conjunto de acciones relativas al negocio, consumidor o relaciones comerciales entre dos o mas personas incluyendo cualquier otro tipo de las siguientes conductas: 1. La venta, intercambio, licenciamiento o cualquier otra disposición de: i. Propiedad personal, incluyendo bienes e intangibles ii. Servicios iii. Cualquier combinación entre ellas. 2. La venta, intercambio, licenciamiento o cualquier otra disposición de cualquier interés de una propiedad real o cualquier combinación sobre la misma
Transferencia Electrónica	Es un registro electrónico que: d) El usuario de los registros electrónicos expresados como un acuerdo de registros transferibles e) Relativos a adquirir una como una propiedad real. f) Una transferencia electrónica puede ser ejecutado usando una

firma electrónica

U

UNIX

Sistema operativo especializado en capacidades de multiusuario y multitarea. Fue la base inicial de Internet. Entre sus características más importantes se encuentran:

Redireccionamiento de Entrada/Salida
Alta portabilidad al estar escrito en lenguaje *C*, lo que lo hace independiente del hardware
Interface simple e interactivo con el usuario

Sus componentes básicos son:

Kernel Parte del sistema operativo que reside permanentemente en memoria. Dirige los recursos del sistema, memoria, E/S de archivos y procesos.
Shell Intérprete de comandos. Interpreta y activa los comandos o utilidades introducidos por el usuario. Es un programa ordinario (ejecutable) cuya particularidad es que sirve de interface entre el Kernel y el usuario. Es también un lenguaje de programación (similar al *C*), y como tal permite el usar variables, estructuras sintácticas, entradas/salidas etc.

Programas La shell es un caso especial de programa. Son programas que son partes estándar de Unix (comandos de sistema, utilidades, etc), programas de usuario (compilados) y shell scripts (comandos y sentencias interpretadas por una shell).

Sistema operativo multiusuario, de multitarea, desarrollado por los laboratorios Bell (AT&T) y es el sistema operativo más común para servidores de Internet.

UDP

Protocolo de Datagramas de usuario (User Datagram Protocol). Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP esta diseñado para satisfacer necesidades concretas de ancho de banda, como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada, pues un paquete perdido no afecta la calidad del sonido. Entre las aplicaciones que utilizan este protocolo encontramos a Real Audio. Vea: TCP, Telefonía en Internet, Video-Conferencia.

Upload

Es enviar un archivo a una computadora remota desde la nuestra.

TESIS CON
FALLA DE ORIGEN

UPS — (Uninterumpible Power Supply) Es una fuente continua de energía, que proporciona seguridad a un sistema de computación.

URL — (Uniform Resource Locator) Corresponde a la dirección de una fuente de información y consta de cuatro partes siendo la primera el tipo de protocolo (http, ftp, gopher), seguida del nombre de la máquina, la ruta del directorio y el nombre del archivo.

URL — Localizador Uniforme de recursos (*Uniform Resorce Locator*). Sistema de direccionamiento estandar para archivos y funciones de Internet, especialmente en el World Wide Web. El url esta conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.unam.mx) más el directorio y el archivo referido.

Usenet — La información de Usenet se organiza de tal manera que los usuarios tengan acceso a los tópicos de su interés. Para que un grupo sea "auténtico", debe ser primero aprobado por los demás usuarios o demostrada su importancia mediante el uso frecuente, cada uno tiene su propia estructura (ver newsgroups). Existe una jerarquía principal de grupos, formada por las siguientes categorías:
alt. Grupos "alternativos"

bit. Duplicaciones de listas de correo.
biz. Negocios.
comp. Computadoras y redes.
K12. Educación.
misc. Temas que no entran en las otras categorías.
news. Discusión sobre Usenet mismo.
talk. Todo tipo de charla.
soc. Sociales y culturales.
sci. Ciencia y medicina .
rec. Recreativos y deportes.

Cada una de estas categorías cuenta con diversas subcategorías, que a su vez tienen varias divisiones. Para conocer el nombre de un grupo, se toma la categoría principal y se le agregan los nombres de las subcategorías, separándolos con un punto, hasta llegar al tema de discusión en sí. Hay más de 10,000 grupos, donde es posible entablar discusiones sobre miles de temas. Usenet es un servicio muy popular porque permite una gran diversidad y completa libertad de expresión.

USENET — (*USEr NETwork*). Sistema de redes que contiene articulos llamados NEWS que pueden ser consultados sin necesidad de estar inscrito. Vea listas de correo, Grupos de noticias.

Recursos:
Free Agent http://www.freeagent.com.
WinVN http://www.ksc.nasa.gov/software/winvn/winvn.html

Usuario — Un usuario es la persona que tiene una cuenta en una determinada computadora por medio de la cual puede acceder a los recursos y servicios que ofrece una red. Un usuario que reside en una determinada computadora tiene una dirección electrónica única. Vea Correo electrónico. Cualquier persona que hace uso de alguno de los recursos de cómputo con los que cuenta una organización.

UUCP — (Unix to Unix Copy) Método común de comunicación para computadoras que se conectan a Internet temporalmente y que además permite el uso de correo, Usenet y transferencia de archivos.

UUDECODE — (Unix to Unix Decoding). Metódo para convertir archivos enviados por correo electrónico (codificados con UUENCODE), a un formato binario Vea Mime, UUENCODE.

UUENCODE — (Unix to Unix Encoding). Método para convertir archivos binarios a formato ASCII (Archivo de Texto), para que puedan ser enviados vía correo electrónico. Vea Mime, UUDECODE.

TESIS CON
FALLA DE ORIGEN

V

Verónica — Indice de Red Amplia muy fácil Orientado hacia Roedores para Archivos Computarizados(*Very.Easy Rodent-Oriented Net-Wide Index to Computerized Archives*) Herramienta de localización que permite realizar búsquedas basadas en palabras clave en directorios y dominios de Gopher, Herramientas de búsqueda, Jughead. Instrumento de ayuda para localizar archivos en otros Gophers. Por lo general Verónica se encuentra como una opción en el menú de "Otros Gophers", lo único que hay que indicar es la palabra o el tema a buscar y en unos segundos Verónica da la respuesta.

V42.bis — Protocolo de detección de errores y comprensión de datos que puede mejorar la velocidad de un enlace vía módem hasta en un 400n.

Video Conferencia — Sistema que permite la transmisión en tiempo real de video sonido y texto a través de una red, ya sea de área local (LAN) o global (WAN). El hardware necesario es tarjeta de sonido y video, video cámara, micrófono y bocinas. La velocidad de transmisión lograda actualmente es de 10 cuadros por segundo. Actualmente ya se incluye soporte vía módem. Vea Quick Cam

Recursos:
En español. VidCall: http://www.neurosys.com.mx/vidcall1.htm

CU SeeMe: http://www.cu-seeme.com/iw.htm
Cinecom: http://www.cinecom.com

Vínculo (link) es un indicador de texto o una imagen que sirve como enlace a otro documento. Vea Hipertexto.

Virus Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras como son:

a) Solamente advertir al usuario de su presencia, sin causar daño aparente

b) Tratar de pasar desapercibidos para causar el mayor daño posible

c) Adueñarse de las funciones principales (infectar los archivos de sistema).

El CERT es un organismo que proporciona soporte a los administradores de sistemas en situaciones semejantes.

Virus en correo electrónico: Los virus no pueden viajar en mensajes de correo electrónico, ya que únicamente utilizan el formato de 7 bits para transferir texto. La única manera en que pueden viajar es por archivos binarios que se envían ligados (attachment) al mensaje de texto (y que el MIME convierte automáticamente). Es recomendable revisar estos archivos con un antivirus antes de su lectura.

Macro-Virus. Es la última presentación de los virus. Viajan en plantillas de archivos de aplicación (Word, Excel, etc) y no en archivos binarios (como lo hacen los virus tradicionales). Se puede encontrar soporte para este tipo de virus en Microsoft (http://www.microsoft.com) Vea Gusano

Recursos:
Mcafee: ftp://ftp.mcafee.com, http://www.mcafee.com
Norton Antivirus: http://www.nav.com

Visual Basic Lenguaje de programación de Microsoft orientado a eventos, utilizado principalmente en el World Wide Web para realizar consultas a bases de datos de Microsoft como Fox Pro, SQL-Server, etc., que funciona en servidores de Windows NT. Vea CGI

TESIS CON
FALLA DE ORIGEN

Recursos:
Microsoft http://www.microsoft.com
Microsoft network http://www.msn.com
Lista de discusión de Visual Basic VISBAS-L
Lista de discusion de Visual Basic y Bases de datos: VBDATA-L
Para suscribirse a la lista de discusión (listserv)mandar en el cuerpo del mensaje (no en el subject)
subscribe nombre-de-la lista a mailto:LISTSERV@LISTSERV.NET

Visualizador (Browser). Programa que despliega la información almacenada en páginas

HTML que se encuentran disponibles en servidores del World Wide Web. Como ejemplo de visualizadores tenemos Cello, Internet Explorer, Mosaic, Netscape, Plugins, etc.

VMS — (Virtual Memory System) Sistema de memoria virtual.

VRML — (*Virtual Reality Modeling Language antes Virtual Reality Markup Language*) Lenguage de programación utilizado para hacer presentaciones de realidad virtual en el Word Wide Web. Puede ser un visualizador propio o integrado a los visualizadores WWW a través de un Plugin. En agosto de 1995 se anuncio la especificación 2.0 como un nuevo estandar. VRML 1.0 permite crear mundo estáticos en 3-D, que contienen objetos que pueden girar libremente alrededor de su eje, pero sin ningún movimiento interactivo real. VRML 2.0 por su parte permite manipular los objetos, cuenta con sensores de proximidad, sonido etc.

Recursos
Nescape http://home.netscape.com/eng/live3d
Intervista Inc. http://www.intervista.com
RealSpace Inc. http://www.rlspace.com
Comumunity Place 2.0 http://http://vs.sony.co.jp/VS-E/vstop.html Demos en
http://vs.spiw.com/vs/archive.html
Cosmo Player 2.0 http://vrml.sgi.com/cosmoplayer
Macromedia http://www.macromedia.com
VREAM http://www.vream.com

VT-100 — Tipo de terminal de uso muy generalizado y reconocido por la mayoría de los Hosts.
V-22 bis: Norma CCITT para los módem; 600 y 1200 bps.
V-32 bis: Norma CCITT para los módem; 2400, 4800, 9600 y 14400 bps.
V-34 bis: Norma CCITT para los módem hasta 28800 bps.
V-42 bis: Norma CCITT para corregir errores y comprimir información, clase 2 a 4 nmp.

TESIS CON
FALLA DE ORIGEN

W

Wais — (Wide Area Information Server) Método para buscar en una base de datos indexada dentro de Internet.

WAN — (Wide Area Network) Red de computadoras con grandes distancias, conectadas a través de líneas telefónicas, satélites u otras soluciones en telecomunicaciones.

Write — Es una herramienta útil para enviar mensajes sencillos directamente a la pantalla de otro usuario.

World Wide Web — El concepto WWW fue desarrollado en Suiza en el año 1989 por Tim Berners-Lee y está compuesto por un conjunto de software, protocolos y estándares de comunicación que permite accesar información en diversos

formatos, como gráficas, audio, hipertexto y video.

Es además la mejor herramienta para navegar en Internet y accesa a casi todos los recursos. Es sencilla de utilizar y además tiene capacidad de multimedia y ofrece el concepto de hipertexto.

El hipertexto no es otra cosa que un texto común donde algunas palabras o frases se destacan de las demás. Estas palabras se llaman "lazos" (links). Un lazo (o liga) es entonces una palabra, frase o elemento gráfico destacado en un texto, que contiene información sobre un recurso determinado en cualquier lugar de Internet. Si se presiona el botón del mouse sobre uno de estos lazos, esta información es utilizada para accesar el recurso en cuestión. De esta misma manera funciona, por ejemplo, el sistema de ayuda de Windoms o de las Macintosh.

Los usos de la WWW son los siguientes:

- Entretenimiento.
- Catálogos y tiendas en línea.
- Librerías virtuales.
- Servicios informativos.
- Publicación a bajo costo.
- Cursos y aplicaciones interactivas.

TESIS CON
FALLA DE ORIGEN

WORLD WIDE WEB = WWW = W3 = The Web

Winsock — (Interfase de Programa de Aplicación) Diseñada para que algunas aplicaciones nativas de Windows corran sobre una red TCP/IP.
X-25: Norma internacional de comunicación de paquetes de uso muy difundido.
X-400: Protocolo Internacional para Correo Electrónico.
X,Y,Z Modem: Protocolos de corrección de errores para transferencia de archivos vía módem.

W30 — (World Wide Web Organization). Es la organización decicada al desarrollo e implementación de nuevos estandares para el Word Wide Web. Localizada en http://www.3w.org. Vea CERN.

WAIS — Servicio de Información de Area Amplia (*Wide Area Information Service*). Es una herramienta que permite encontrar información almacenada en archivos o en bases de datos a través de Internet.

WAN — Red de área mundial (World Area Network). Puede extenderse a todo un país o a muchos a través del mundo. Vea LAN, MAN.

Web — Vea World Wide Web.

Web PC ó Web TV — Vea Network Computer.

Website — Conjunto de páginas web que comparten un mismo tema e intención y que generalmente se encuentra en un sólo servidor, aunque esto no es forzoso.

Windows 95 — Sistema operativo gráfico de 32 bits desarrollado por microsoft (http://www.microsoft.com) y diseñado especificamente para computadoras con procesadores compatibles con Intel. Vea Windows NT.

Recursos:
Microsoft http://www.microsoft.com
Microsoft network http://www.msn.com
Windows 95 http://www.windows95.com
Ayuda: http://www.creativelement.com/win95ann/
En español: http://veracruz.infosel.com.mx/arturo/home.htm

Windows NT — Sistema operativo gráfico de 32 bits desarrollado por Microsoft muy similar al Windows, pero con más prestaciones. Vea Windows 95

World Wide Web — Sistema basado en hipertextos cuya función es buscar y tener acceso a documentos a través de la red. Vea Altavista, CGI, Hipertexto, Herramientas de búsqueda, HTML, HTTP, Internet explorer, Java, Mosaic, Netscape,Plugins, Visualizador, Yahoo!.

World Wide Web Organization — Vea W3O

White Pages — Listas de usuarios de internet. Existen varios lugares donde los usuarios pueden registrarse y realizar búsquedas de personas.

Recursos:
UNAM: sistema Sabueso: http://www.unam.mx
WhoWhere http://www.whowhere.com
Bigfoot.http://www.bigfoot.com

WWW — Vea World Wide Web

X

Xmodem — Programa utilizado para transferir archivos de un servidor a una computadora conectada vía acceso conmutado. Utilizado principalmente para extraer archivos de una BBS. Vea Kermit.

Y

Yahoo! — Herramienta pública de búsqueda del World Wide Web disponible en http://www.yahoo.com, la búsqueda se realiza a partir de los títulos de los documentos de HTML. Yahoo! Se distingue por tener un gran índice de documentos ordenados por categorías. Vea Altavista., Operadores Booleanos.

Ytalk — Programa en ambiente UNIX similar al IRC. Permite la comunicación en tiempo real entre varios usuarios.

Z

ZIP

Formato de compresión de archivos para el sistema MS-DOS. Los archivos contienen la extensión .zip. La utilería que maneja este tipo de archivos es PKZIP/PKUNZIP. Vea archivos compactados.
Recursos: Winzip: http://www.winzip.com

Programa de Posgrado en Ciencias de la Administración
Oficio: PPCA/EG/2001
Asunto: Envío oficio de nombramiento de jurado de Maestría.

Ing. Leopoldo Silva Gutiérrez
Director General de Administración Escolar
De esta Universidad
P r e s e n t e.

At'n.: Biol. Francisco Javier Incera Ugalde
Jefe de la Unidad de Administración del Posgrado

Me permito hacer de su conocimiento, que el alumno **Sergio Mauricio Martínez Monterrubio** presentará Examen de Grado dentro del Plan de Maestría Administración (Negocios Internacionales), toda vez que ha concluido el Plan de Estudios respectivo y su tesis, por lo que el Subcomité de Nombramiento de Jurado del Programa, tuvo a bien designar el siguiente jurado:

Dr. Marco Antonio Murray Lasso	Presidente
M. en I. Graciela Briebiesca Correa	Vocal
M.A. Arturo David Motta Martínez	Secretario
Dr. Hugo Rodas Morales	Suplente
M.A. Francisco Juan Carlos Rodríguez Ramírez	Suplente

Por su atención le doy las gracias y aprovecho la oportunidad para enviarle un cordial saludo.

A t e n t a m e n t e
"Por mi raza hablará el espíritu"
Ciudad. Universitaria, D.F., 27 de noviembre del 2002.
El Coordinador del Programa

Dr. Sergio Javier Jasso Villazul

MFB

205