UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE CONTADURÍA Y CIENCIAS ADMINISTRATIVAS

PROYECTO
(Caso Práctico)

LEGISLACIÓN DEL COMERCIO ELECTRÓNICO EN MÉXICO.

QUE PRESENTA:

ABEL PIZANO RANGEL.

PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMÁTICA ADMINISTRATIVA.

ASESOR:

M.C. ERIC ALFARO CALDERÓN.

Morelia, Mich. Febrero de 2010

PLANTEAMIENTO DEL PROBLEMA.

Problema:

Necesidad de realizar algunas de nuestras actividades por medio de los servicios que ofrece Internet como son la compra - venta de productos, pago de impuestos, transacciones con los Bancos, etc.

Problemática:

Demasiados delitos informativos existen actualmente por medio del comercio electrónico, ha surgido esta problemática por el sin numero de usuarios de Internet que han estado inmiscuidos en algún tipo de fraude, en la actualidad nuestras autoridades han estado trabajando en el desarrollo de la Legislación del Comercio Electrónico en México.

En particular me a afectado personalmente, ya que en nuestros días muchas personas, alumnos, maestros, trabajadores, empresas etc., utilizamos la WEB, de tal manera que se nos a creado la necesidad de realizar algunas de nuestras actividades por medio de los servicios que ofrece Internet como son la compra - venta de productos, pago de impuestos, transacciones con los Bancos, etc.

Esta problemática es de suma importancia para mi porque a pesar de todas las nuevas leyes que se han actualizado para regirlas se siguen realizando un sin numero de ilícitos, sin poder detectar a los infractores. Esto es algo que realmente crea una desconfianza ante las personas que utilizamos este servicio, pensando que en cualquier momento que nosotros quisiéramos utilizarlo, nos pudiera suceder algún fraude y no sepamos ni tan siquiera que hacer después de los sucedido, con quien acudir, contamos con algún respaldo legal o no, si realizamos una demanda nos apoyaran, son muchas de las incógnitas que tenemos como usuarios.

ENCUADRE PREFERENCIAL.

Justificación:

Decir que Internet ha venido a revolucionar la forma de hacer negocios en el mundo y sin duda México no es la excepción. El crecimiento exponencial del uso de Internet y de los ingresos relacionados con operaciones en línea en nuestro país, son sólo una muestra mas de esta revolución en la que estamos inmersos. Por dar una cifra (y las cifras cambian casi diariamente) según la Asociación Mexicana de Comercio Electrónico (“AMECE”) las transacciones electrónicas en

línea están creciendo en un 400% anual, superando actualmente los dos mil millones de dólares. Se espera que para finales de año, México tendrá 2.5 millones de usuarios, y este número será superior a los 10 millones para el año 2003.

De este modo la gran mayoría de los países desarrollados o en vías de desarrollo han aprobado o se encuentran en el proceso de aprobar algún tipo de regulación relacionada con el Comercio electrónico.

Hablar de Internet y comercio electrónico, sin duda el de la validez y exigibilidad de las operaciones “en línea" es uno de los fundamentales y por ello no es de extrañar que sea uno de los que han recibido mayor atención tanto a nivel nacional como internacional. Todavía dentro de este universo reducido, es el tema de las firmas electrónicas el campo donde se ha presentado, en todo el mundo, y mayor proliferación legislativa.

En mi opinión México no se encuentra en este momento tan retrasado en materia de la regulación del comercio electrónico. Las reformas del 29 de mayo de 1999, junto con las del 18 de septiembre y los acuerdos publicados el 6 de octubre del mismo año, son importantes pasos que muestran la firme decisión del gobierno por acortar la distancia entre México y los países mas avanzados en este tema. Muchos otros países, se encuentran, comparativamente, todavía en etapas previas de desarrollo.

OBJETIVOS.

Objetivos General:

Ampliar el conocimiento acerca de la legislación del comercio electrónico en México y saber hasta donde o como, realizar nuestras operaciones por Internet, con la confianza de tener un respaldo en caso de caer en algún fraude.

Objetivos específicos:

- Ampliar mi confianza en el servicio del Comercio Electrónico.
- Conocer la Legislación del Comercio Electrónico dentro y fuera del País.
- Apreciar la magnitud de los riesgos al realizar compras a través de Internet.
- Conocer los tipos de delitos informativos que existen para tener precaución.

CONTENIDO.

INTRODUCCIÓN.

La informática esta hoy presente en casi todos los campos de la vida moderna. La gran mayoría de las personas nos encontramos utilizando los sistemas computacionales y muy particularmente el uso de la Internet, ya que nos permite procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios.

En la actualidad, con el uso de este medio se puede obtener información, en segundos o minutos, este es el panorama de un nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que el Comercio Electrónico hoy en día es un medio de información utilizado por millones de personas a nivel mundial.

El objetivo principal es ampliar el conocimiento acerca de la legislación del comercio electrónico en México y que tan evolucionados están otros países.

La presente investigación cubre los aspectos mas relevantes de la legislación mexicana, con respecto al comercio electrónico, estos asuntos son principalmente la firma digital, pornografía infantil y modificación, destrucción o partida de la información. Todos ellos involucrados en el comercio electrónico.

Se verán los aspecto teórico del Comercio Electrónico, como a avanzado la tecnología en los últimos años hasta llegar a poder comunicarnos a cualquier punto del mundo, con tan sola una computadora y la red de redes.

El comercio electrónico es una herramienta de desarrollo económico del siglo XXI. El crecimiento explosivo de las redes de información, la creciente confianza de los consumidores en la tecnología, abre las puertas para los comerciantes de hoy puedan desarrollar nuevos negocios y revitalizar los existentes.

El uso del Comercio Electrónico no sólo tiene un lado ventajoso sino que plantea también problemas de legalidad, debido a esto nuestro gobierno a tenido que realizar algunas leyes para poder atacar esta problemática, en la defensa de sus usuarios de información y comunicaciones. EL análisis de las legislaciones que se han promulgado en nuestro país y algunos otros arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados los delitos informáticos.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta castigable penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos. El aumento de los delitos cibernéticos se encuentra a nivel mundial, no solo nuestro País a tenido que actualizar algunas de sus leyes sino también otros países como: los Estados Unidos, Europa Occidental, Australia, Japón etc. Algunas de las leyes más importantes de estos Países se verán en el Capitulo IV, ya que la mayoría de ellos a tenido que actualizar su legislación debido a que la mayoría de sus usuarios a sufrido algún tipo de delito cibernético.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Este tipo de fraudes serán explicados detalladamente en el capitulo II.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos.

En consecuencia, la legislación que existe en nuestro País la veremos en el Capitulo III, donde analizaremos las principales leyes que existen actualmente y con que contamos hasta hoy en día en lo que respecta a la legalidad. Ya que como la mayoría de los países nos afectado mucho el cibercrimen que nos aqueja a todos los que utilizamos el Comercio Electrónico y la Internet. Donde nos daremos cuenta con que contamos y en que estamos respaldados si tenemos necesidad de realizar algunas de nuestras actividades por este medio o si nos vemos dentro del problema saber que hacer o con quien acudir.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

La usual delincuencia tradicional, también a sido transformada a un hecho mas elevado de las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos, como se vera en el Capitulo II.

La tecnología avanza a pasos agigantados y todos alumnos, maestros, empresas, amas de casa, niños, en general casi cualquier tipo de personas nos vemos envueltos en este avance y debemos estar a la par con ella, nuestras autoridades tiene la necesidad de actualizarse también dentro de ella para que nosotros como usuarios podamos contar con un soporte Legal.

CAPITULO I.

Marco Teórico.

(Aspectos Teóricos del Comercio Electrónico).

El uso de internet se ha convertido en una herramienta indispensable para toda persona que requiera estar comunicado con el resto del mundo, ya que algunas de sus ventajas son que posibilita la conexión con todo tipo de ordenadores, desde los personales hasta los mas grandes que ocupan habitaciones enteras y muy particularmente la conexión que han tenido con las empresas para su desarrollo.se analizara como ha sido su evolución desde sus inicios hasta nuestros días.

1.1. El marco de desarrollo del comercio electrónico: Internet & la economía digital.

Al realizar referencia al comercio electrónico tenemos que tomar en cuanta previamente a Internet, pues entre ambos existe una simbiosis. Por una parte, Internet constituye el soporte sobre el cual el comercio electrónico se ha desarrollado; éste no es más que una tecnología subyacente, una aplicación que se utiliza en el entorno de aquella. Por otra parte, el comercio electrónico ha sido el propulsor fundamental para el desarrollo y expansión de Internet desde la primitiva ARPANET, hasta que adquiera la configuración que hoy tiene, incluyendo interfaces gráficos, transmisión de imagen y sonido.

A su vez el desarrollo de Internet abarca además el desarrollo de las tecnologías de la información, resultantes de la combinación entre software y comunicaciones, mismas que han tenido un impacto tan significativo en toda nuestra civilización.

1.1.1. ¿Que es Internet?.

Es un conjunto creciente de redes de computadoras que abarca todo el mundo y que conecta a organismos internacionales, instituciones gubernamentales, militares, educativas, comerciales y también a personas particulares, a una gran cantidad de servicios, recursos e información.

Algunos definen Internet como "*La Red de Redes*", y otros como "*Las Autopistas de la Información*".

Efectivamente, Internet es una *Red de Redes* porque está hecha a base de unir muchas redes locales de ordenadores, o sea de unos pocos ordenadores en un mismo edificio o empresa. Además, ésta es "La Red de Redes" porque es la más grande. Prácticamente todos los países del mundo tienen acceso a Internet. Utilizando el protocolo internet (IP) y los recursos de comunicación existentes como cables, teléfonos, satélites u ondas radioeléctricas.

Por la Red Internet circulan constantemente cantidades increíbles de información. Por este motivo se le llama también *La Autopista de la Información*. Hay 50 millones de "*Internautas*", es decir, de personas que "*navegan*" por Internet en todo el Mundo. Se dice "navegar" porque es normal el ver información que proviene de muchas partes distintas del Mundo en una sola sesión.

Una de las ventajas de Internet es que posibilita la conexión con todo tipo de ordenadores, desde los personales, hasta los más grandes que ocupan habitaciones enteras. Incluso podemos ver conectados a la Red cámaras de vídeo, robots, y máquinas de refrescos.

1.1.2. Reseña histórica de Internet.

La primera idea de lo que sería posteriormente Internet nace en los 60 tanto por la necesidad militar de comunicarse aun siendo atacadas las comunicaciones, Internet fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado DARPANET (Defense Advanced Research Project Network) iniciado en el año de 1969 y cuyo propósito principal era la investigación, desarrollo e implementación de protocolos de comunicación para redes de área amplia (WAN). Fue en ARPA donde empezó Internet. Vannevar Bush escribió además un artículo titulado *"Cómo podemos pensar"*. En este artículo, describió un dispositivo teórico de almacenamiento y extracción que llamó "memex", que utilizaría un sistema notablemente similar a lo que ahora llamamos hipertexto.

La Agencia de Proyectos avanzados de Investigación *(ARPA)* fue creada por el presidente Dwight Einsenhower. En esta época, investigadores de instituciones de reconocido prestigio como el Instituto Tecnológico de Massachusetts *(MIT)* sentaron las bases tecnológicas que facilitaron en años posteriores la creación de la red.

En 1965 la Agencia de Proyectos de Investigación para la Defensa de Estados Unidos *(DARPA, U.S. Defense Advanced Research Projects Agency),* promueve un estudio sobre *"Redes cooperativas de computadoras de tiempo compartido"*, y al año siguiente, Larry Roberts, del MIT, publica *"Hacia una red cooperativa de computadoras de tiempo compartido".* En los años sucesivos se van presentando proyectos sobre redes conmutadas por paquetes, como en el simposio sobre principios operativos de 1967.

Roberts sería el arquitecto principal de una nueva red de ordenadores que sería conocida como ARPANET. Así, los principios de Internet estaban en curso.

Con todo esto, a finales de los años sesenta, una de las preocupaciones de las Fuerzas Armadas de los Estados Unidos era conseguir una manera de que las comunicaciones estuvieran descentralizadas, que pudiera ser destruido en un eventual ataque militar con armas nucleares y que así, aún sufriendo el ataque, las comunicaciones no se bloquearan, sino que solamente se perdiera un nodo.

En 1969 la DARPA, junto con la compañía *Rand Corporation* desarrolló una red sin nodos centrales basada en conmutación de paquetes. La información se dividía en paquetes y cada paquete contenía la dirección de origen, la de destino, el número de secuencia y una cierta información. Los paquetes al llegar al destino se ordenaban según el número de secuencia y se juntaban para dar lugar a la información. Al viajar por la red paquetes, era más difícil perder datos ya que, si un paquete concreto no llegaba al destino o llegaba defectuoso, el ordenador que debía recibir la información sólo tenía que solicitar al ordenador emisor el paquete que le faltaba.

ARPANET conectó los ordenadores centrales vía ordenadores de pasarela pequeños, o *"routers"*, conocidos como *Interface Message Processors (IMPs)*.

En 1971 se creó el primer programa para enviar correo electrónico. Fue Ray Tomlinson, del BBN, y combinaba un programa interno de correo electrónico y un programa de transferencia de ficheros. También en este año presento la propuesta del primer *"Protocolo para la transmisión de archivos en Internet"*.

Los años setenta las instituciones se conectan directamente o conectando otras redes a ARPANET y con los responsables desarrollando estándares y protocolos, como Telnet, la especificación de transferencia de archivos o el protocolo de voz en redes *(NVP, Network Voice Protocol)*. Bob Metcalfe inventó Ethernet, y Douglas Englebart. Otras redes de ordenadores como la hawaiana ALOHANET y la red enlazada de satélites, SATNET, empezaron a crearse. Pronto había muchas redes diferentes alrededor del mundo, pero no podían comunicarse con otras porque utilizaban protocolos o estándares para transmisión de datos diferentes.

Entonces, en 1974, Vinton Cerf (conocido por algunos como el padre de "Internet"), junto con Bob Kahn, publican *"Protocolo para Intercomunicación de Redes por paquetes"*, donde especifican en detalle el diseño de un nuevo protocolo, el Protocolo de control de transmisión *(TCP, Transmission Control Protocol)*, que se convirtió en el estándar aceptado. La implementación de TCP

permitió a las diversas redes conectarse en una verdadera red de redes, conectarse a INTERNET.

En 1979 ARPA crea la primera comisión de control de la configuración de Internet y tras varios años de trabajo, por fin en 1981 se termina de definir el protocolo TCP/IP *(Transfer Control Protocol / Internet Protocol)* y ARPANET lo adopta como estándar en 1982, sustituyendo a NCP. Son las primeras referencias a Internet, como *"una serie de redes conectadas entre sí, específicamente aquellas que utilizan el protocolo TCP/IP".*

En 1983 ARPANET se separa de la red militar que la originó, de modo que ya sin fines militares se puede considerar esta fecha como el nacimiento de Internet. Es el momento en que el primer nodo, militar, se desliga dejando abierto el paso para todas las empresas, universidades y demás instituciones que ya por esa época poblaban la joven red.

En estos años ochenta, la expansión es enorme. Cada vez se conectan más máquinas a la red, y se van mejorando los servicios. En 1985, quince años después de la primera propuesta, se termina el desarrollo del aún vigente protocolo para la transmisión de ficheros en Internet *(FTP, File transfer protocol)*, basado en la filosofía de cliente-servidor

Un punto fundamental en el éxito fue el hecho de que ARPA distribuyera a bajo coste los protocolos, que fueron adoptados por el UNIX de BSD *(Berkeley Software Distribution)*. De esta forma se crearon una gran cantidad de servicios y se provocó un importante avance en el desarrollo de la red. Por esta época se crea el sistema de denominación de dominios *(DNS, Domain Name System)*

A partir de 1987 empezó la gran expansión, en parte debida a que el año anterior se creó la NSFNET, que estableció cinco centros de supercomputadoras para proveer un alto poder de proceso. También en ese año encontramos la primera aplicación informática de hipertexto. Fue Hypercard para Macintoch, y estaba pensada para crear y compartir *pilas* de información.

Tim Berners-Lee creó una nueva manera de interactuar con Internet en 1990: El *World Wide Web*. Su sistema hace mucho más fácil compartir y encontrar datos en Internet. El *World Wide Web* fue aumentado más a fondo por otros que crearon nuevo software y tecnologías para hacerlo más funcional.

En septiembre de 1993 se inició el primer servidor Web en español. En estos momentos se aumenta la potencia de las redes troncales de EE.UU., y en 1994 se eliminan las restricciones de uso comercial de la red y el gobierno de EE.UU. deja

de controlar la información de Internet. 1995 es el año del gran "boom" de Internet. Puede ser considerado como el nacimiento de la Internet comercial. Desde ese momento el crecimiento de la red ha superado todas las expectativas. Este hecho se produce porque es en este año cuando la www supera a *ftp-data* transformándose en el servicio más popular de la red.

Empiezan ahora a incrementarse de una manera casi exponencial el número de servicios que operan en la red. A partir de aquí la escalada de tecnología es impresionante. Como permitir la conexión con todo el mundo a precio de llamada local. Se desarrolla de una manera definitiva el comercio electrónico, para comprar productos y servicios a través de internet. Se pueden ver cientos de televisiones y escuchar radios de todo el mundo en tiempo real. Los bancos se asientan en la Red, no se puede mencionar todas las cosa que se pueden realizar. Confiando en la seguridad que ofrecen los servidores seguros.

La tecnología de telefonía movil y la de internet finalmente se unen para poder acceder desde los teléfonos móviles a la red de redes. Con la definición del conjunto de protocolos WAP *(Wireless Application Protocol)* cuando los dispositivos inalámbricos, y fundamentalmente los teléfonos móviles, se conectan a Internet.

En lo que respecta a México, la historia de Internet comienza a finales de la década de los 80's. En el año de 1987, el Instituto Tecnológico y de Estudios Superiores de Monterrey, en el campus Monterrey (ITESEM) se conectó a BITNET a través de líneas conmutadas por medio de una línea privada analógica de 4 hilos a 9600 bits por segundo, continuando un sin numero de instituciones.

Actualmente, Internet es utilizado tanto por instituciones educativas y gubernamentales, empresas privadas y personas de todo el mundo, entre quienes se llevan a cabo intercambios constantes de información dando origen a la llamada globalización de la comunicación. Hasta el día de hoy, gracias a Internet, se puede recibir información al instante de cualquier parte del mundo, agilizando y facilitando de esta forma el proceso comunicativo a distancia.

1.1.3 Desarrollo de Internet.

Internet, es producto de la relación de tres grandes áreas: la electrónica, el software y las telecomunicaciones.

Son expresiones diferentes de un mismo fenómeno; Internet se manifiesta concretamente en el fenómeno y es una revolución en si misma. El aporte de la

electrónica en el desarrollo del equipamiento de proceso de la información a un ritmo muy acelerado por la introducción del circuito integrado y el microprocesador en la informática, determinó el paso de las primeras computadoras y has las que hoy conocemos que cada vez son más pequeñas. Luego, el desarrollo del software o soporte lógico para esas maquinas ha crecido en complejidad a medida que el soporte electrónico ha evolucionado, pasando se ser especifico o de propósito general en la era de la PC y dentro de ese software las aplicaciones especificas para comunicación, permitieron crear las primeras Intranet (redes locales) en los grandes laboratorios universitarios y complejos militares.

Finalmente, las telecomunicaciones han proporcionado la capacidad de interconexión, al lograr la coexistencia y la utilización simultanea de cables de fibra de cobre, el coaxial, la fibra óptica, las transmisiones a través del satélite y las emisiones de radio de onda corta, facilitando la expansión del uso e interconexión de redes, desde los grandes laboratorios universitarios y los complejos militares a la residencia de cada usuario conectado con la Red.

Estos avances científico-tecnológicos ya se hallaban disponibles hace mas de una década, no obstante, el comienzo de la explosión del fenómeno de la Red puede situarse a mediados de la década del noventa y es recién a partir de 1997 cuando comienza a generar las características que ha adquirido en la actualidad. En estos años, Internet ha experimentado un crecimiento exponencial en el número de usuarios, al punto que hoy está consolidándose como un medio de comunicación habitual en la mayoría de países.

1.1.4. Aplicaciones de Internet.

Debido al tamaño mundial de la red y la diversidad de empresas, como organismos, instituciones gubernamentales y no gubernamentales, Instituciones educativas, investigadores y personas que se conecten dentro de esta gran telaraña de computadoras; la información ahí almacenada va desde simples paginas personales, pasando por páginas comerciales, lugares que ofrecen diversa información, hasta universidades muy prestigiadas en diversos campos de investigación que presentan.

A través de esta misma red de computadoras, se pueden intercambiar mensajes o correos electrónicos con personas tan distantes como sería al otro lado del mundo

en cuestión de minutos, con tan solo una llamada local y la dirección electrónica de la otra persona.

Esta gran red de computadoras tiene una gran variedad de usos tanto como el usuario pueda imaginar, solo falta obtener la herramienta necesaria para realizarlo.

1.1.5. La nueva economía digital.

La convergencia de los tres elementos (informática, software y comunicaciones) es también el denominador común del tejido económico de lo que se ha denominado como la "nueva economía digital". La profundidad del cambio tecnológico y el rápido avance en su aplicación al campo comercial es muy intenso, en este aspecto, las tecnologías subyacentes de Internet (tecnologías de la información) están impulsando en forma importante la creación de mercados electrónicos, situación que esta acelerando la transformación de la empresa privada y otros agentes económicos hacia varias formas de negocio digital, lo que a su vez esta cambiando la economía de los países y el origen de las fuentes de trabajo, así como al trabajo mismo y el ingreso de él derivado, y es que la esencia de la economía digital es esa, las oportunidades de negocios que son creadas en la Red, producen cambios sobre la economía física.

La economía de Internet es fundamentalmente diferente de la economía física en que prioriza tres parámetros claves: información, conocimiento y velocidad, y los relaciona con tecnología. Sin embargo, no se piense que es una simple colección o suma despersonalizada de grandes empresas de alta tecnología, por el contrario incluye a toda empresa o persona que genera ingresos en Internet (inclusive a las empresas tradicionales de telecomunicaciones y profesionales liberales), además el nuevo activo complementario al crecimiento y uso de las nuevas tecnologías de la información y de la comunicación es la inversión en capital humano e intangible.

1.1.5.1 Estructura Economía Digital.

La estructura de la nueva economía digital o de Internet que gira entorno al comercio y mercados electrónicos, comprende:

Actores de infraestructura.

Son las empresas que directamente generan todo o una parte de sus ingresos en Internet o en bienes y servicios relacionados con Internet, sus productos y servicios hacen posible la existencia de Internet (telecomunicaciones, PC.s, etc.).

Actores de aplicaciones.

Empresas cuyos productos y servicios hacen factible el uso de Internet para el comercio electrónico; por ejemplo, IBM fabrica PC.s y servidores que permiten el acceso a Internet (infraestructura) y Cisco construye ruteadores, ambos usados para el acceso a Internet.

Intermediarios electrónicos.

Empresas que funcionan como catalizadores, cuyos servicios facilitan la interacción entre compradores y vendedores, como E-Bay, E-Trade o de remate.

Los vendedores y prestadores de servicios en línea Empresas que venden productos y servicios en Internet, las hay de dos tipos:

- "Con actuación exclusiva en Internet como Amazon.
- "Empresas híbridas, trabajan en la red y en establecimientos tradicionales, esto es físicos, como L.L. Bean y Barnes and Noble, que conducen parte de sus negocios en Internet.

1.1.6. Las herramientas para la navegación en la red.

Para navegar por Internet, en primer lugar se necesita contar con una PC con Módem y una línea telefónica, en segundo lugar se debe tener una suscripción con cualquier prestador de servicio para acceso a INTERNET, por medio del cual se tiene acceso a su servidor el que sirve de plataforma para iniciar el viaje por la red.

1.1.7. La importancia de Internet en las diferentes áreas de nuestra vida.

Internet ha penetrado en nuestras vidas de una manera inmediata a pesar de que todavía no hemos alcanzado a comprender del todo para qué nos sirve y en qué medida puede ayudarnos en un futuro inmediato ya no lejano.

Es muy común a estas alturas oír hablar de Internet en cualquier momento, a cualquier hora, en cualquier lugar, al encender la radio, ver un programa de televisión, leer un diario, un anuncio publicitario o tratemos con alguna persona.

Internet lejos de ser un medio o herramienta para gente especializada en programación o sistemas de cómputo, ha abierto sus puertas a todo el mundo y a toda la gente aun cuando no todos puedan contar con una computadora personal de su propiedad; sin embargo así como los aparatos de radio y televisión fueron

introducidos en los hogares, de la misma manera es como en menos tiempo a través de las computadoras personales, Internet ha entrado en numerosos hogares convirtiéndose en una herramienta esencial para realizar trabajos de escuela o laborales.

El correo electrónico, el comercio electrónico, los chats, e incluso las video conferencias de computadora a computadora han dado una gran apertura al individuo para relacionarse con el mundo exterior de una manera real, en tiempo real.

En fin la súper carretera de la información nos trae en sí un conjunto de experiencias nuevas que ya existen, que tan sólo hay que aceptarlas y aprender a utilizar. El temor al desempleo cada vez es menor e incluso es más frecuente que la gente se interese cada día más en conocer la red de redes y en reconocer lo versátil y efectivo que resulta estar navegando y contar con una conexión, que aunado a los novedosos programas de cómputo que hasta un niño puede manejar se pueden crear nuevos sitios Web.

Mucho ofrece Internet en los diferentes aspectos de nuestras vidas. También es una fuente de empleo para la gente, que se dedican a la programación, los que ofrecen el servicio de conexión a la red, así como una multiplicidad de trabajos que se pueden realizar gracias a la red y a través de ella lo que ha venido ha cambiar la visión del trabajo. Ha empezado a modificar la concepción de oficinas gigantescas para buscar un espacio en la casa y poder manejar la mayor parte de las labores desde ahí, sin la necesidad de trasladarse grandes distancias que provocan una enorme pérdida de tiempo y esfuerzo irreversible.

Se ha convertido en un medio alterno en cuanto a la colaboración y al trabajo, ha hecho real las "oficinas virtuales", logrando de esta manera que los pendientes de trabajo se puedan resolver desde la casa y poder incluso a través de redes internas de la empresa estar enlazados con diferentes departamentos y con los empleados, pudiendo de esta forma tener un control óptimo y real del manejo de la compañía o del área requerida.

De esta manera también hay que reconocer que Internet ha influido en diferentes áreas laborales tales como la medicina, así como nuevos medicamentos y tratamientos en un tiempo real y de investigaciones recientes, brindándonos la facilidad de tener contacto con médicos especializados para poder solicitar su opinión en cualquier parte del mundo e incluso el que puedan participar en

operaciones quirúrgicas gracias a la combinación de voz e imagen a través de la red, sin tener que moverse del hospital donde trabajan.

Como es de esperarse en cualquier medio, en Internet también puede haber de todo lo bueno y todo lo malo, lo que también ha alertado a la sociedad. Por ejemplo la pornografía no ha quedado excluida sino que, al contrario, ha sido promovida por la rapidez, a través de este medio de comunicación.

Internet, es la opción más barata, fácil y universal para enlazarse y comunicarse, sobre todo a larga distancia, mediante las redes de cómputo. También permite una mejor coordinación entre las diferentes divisiones, departamentos y áreas, especialmente entre las que están distantes, pero de igual forma entre las que están cercanas. Otra ventaja es que permite el enlace con proveedores, canales de difusión y con los consumidores. De esta forma Internet es sin duda una opción para reducir costos. Cabe aclarar que el correo electrónico, el club de trabajo, el flujo de documentos o el proceso de imágenes ya existían, sin embargo eran opciones demasiado caras y difíciles lo que hacia que su uso fuera limitado y aislado, por lo que a partir de la red empezaron a crecer y ahora se han tenido que alinear a Internet, ya que ha resultado la opción más económica, efectiva, veraz y más fácil de usar con lo que se ofreció la gran oportunidad de usar una red mundial a través de la cual se puede interactuar en tiempo real y obtener una respuesta inmediata.

1.2. World Wide Web.

La historia del "World Wide Web", nació en Marzo de 1989, cuando Tim Berners-Lee del Laboratorio Europeo de Física de Partículas (conocido como CERN, un centro de investigación de física europeo de alta energía) propuso el proyecto para ser usado como medio para difundir investigaciones e ideas a lo largo de la organización y a través de la RED.

World: Mundo

Wide: A lo ancho

Web: Telaraña

Telaraña a lo ancho del Mundo

Por mucho tiempo se había soñado con la idea de tener en algún programa universal a cualquier tipo de información que fuese sencillo de manejar; en los años '60 la idea se exploró dando origen al "DOCUVERSE" el cual era un documento universal que contenía todo tipo de información a través del cual, cualquier usuario podía viajar o navegar en él para obtener todo tipo de información, revolucionando todos los aspectos de interacción humano-información.

Para fines de 1990 la primera versión del WORL WIDE WEB se presentó sobre una máquina tipo NEXT, la cual tuvo capacidad de inspeccionar y transmitir documentos en HIPERTEXTO.

Es pues que la "www", nos permite conocer toda la información que pueda ser encontrada en Internet, haciéndola accesible mediante conexiones o Hipervínculos (Ligas-Links) escritas en documentos con un formato o lenguaje especial llamado HTML (HiperText Markup Language), el cual posibilita que desde la información obtenida por un escrito o texto, uno se pueda vincular (Hiperlink) a otros documentos que se encuentren en la misma computadora o bien, en cualquier otra que se encuentre conectada a la red en otra parte del mundo, además con la posibilidad de manejar muchos recursos como textos combinados con gráficos, animaciones y sonidos.

1.3.1. Definición de Web.

Página Web: Es un espacio donde se coloca información en el WWW. Cada vez que pulsa un enlace o especifica una dirección, se carga un fichero que se le muestra en pantalla. Este fichero, llamado página, puede contener imágenes, enlaces a otras páginas, textos, etc.

WWW: World Wide Web. También conocido simplemente como el Web, es uno de los servicios más populares de Internet. Combina texto con gráficos, imágenes, animaciones e incluso música, enlazados entre sí de tal manera que facilita la navegación por la información dispersa en todo Internet. Se basa en el protocolo HTTP.

- Permite el acceso a información distribuida mediante un sistema de hipermedia.

- Permite navegar en forma secuencial o a través de índices o palabras claves : se accede a la información requerida seleccionando frases o imágenes "iluminadas" (enlace, también llamado "link") que llevan al usuario a "navegar" de un documento a otro

Al ser un sistema hipermedia incluye: texto, gráficos, sonido, animación, etc.

1.2.2. Principales Elementos del www.

http (Hypert Text Transfer Protocol).

Es el protocolo de transporte desarrollado para el WWW.

El medio de comunicación que permite que las máquinas se comuniquen entre sí, siguiendo un orden para interpretar e intercambiar información y que utilizan los servidores y clientes del World Wide Web se le conoce como (PROTOCOLO), en específico se maneja en las Páginas Electrónicas el "Protocolo de Transferencia De Hipertexto" (HTTP), siendo éste la parte medular del www.

html (Hyper Text Markup Language).

Es el lenguaje que se utiliza para diseñar documentos que serán aplicaciones WWW.

Por medio de el html, se ponen etiquetas a la información de un documento archivado en cualquier parte de la red, y estas etiquetas indican al navegador como hacer conexiones o enlaces en el documento para pasar a otra sección u otro sitio en la red en la que se encuentre documentación e información archivada en los diferentes servidores del mundo.

URL: Uniform / Universal Resource Locutor.

El www utiliza los "LOCALIZADORES DE REGISTRO UNIFORME" (URL) Uniform Resource Location, para conectarse a otros servicios de la red; es de ésta manera que el URL funciona como indicador que dice al servidor que clase de recurso de Internet.

Es pues que el URL es la columna vertebral de la red mundial en Internet del "www", ya que su función principal es la de asegurar los servidores de la red mediante un protocolo de transferencia o transporte de HIPERTEXTO mediante la localización de un recurso, un medio o una utilería de Internet especificando la dirección en donde pueda encontrarse cualquier información en particular,

añadiendo un sistema único de señalización que dice al servidor de la red acerca del recurso que se está esperando.

El comercio electrónico a tenido una enorme evolución y ha cambiado la manera tradicional del comercio con la utilización de la tecnología y el internet, teniendo alcances inimaginables.

2.1. Comercio Electrónico (E-Commerce).

Como se ve, la profundidad del cambio tecnológico y su cada vez mayor y más rápida aplicación al comercio están construyendo nuevos caminos y nuevos mercados para hacer negocios, posibilitando el surgimiento de una nueva modalidad de comercio: El comercio electrónico, cuyo sustrato es Internet, por lo que torna virtualmente posible superar las barreras del tiempo y espacio, cambiando las formas tradicionales de hacer negocios y planteándonos una nueva problemática respecto al tratamiento jurídico que este debe merecer, dada su natural vocación internacional. En ese contexto, veamos hora los aspectos teóricos fundamentales de este nuevo modo de hacer negocios.

2.2.1 El desarrollo del Comercio electrónico.

Desde su origen más primitivo, el comercio ha sido definido básicamente como un intercambio de bienes y servicios, evolucionando desde el llamado “trueque” hasta las formas contractuales más complejas existentes en la actualidad.

Antes de la aparición de las telecomunicaciones, las transacciones comerciales se realizaban siempre con limitaciones del espacio geográfico, requiriendo la cercanía física de las partes o de sus representantes. A medida que compradores y vendedores se alejaban, inventos como el teléfono, el fax y el telex facilitaron el comercio haciéndolo más ágil y dinámico al permitir la gestión de los negocios a distancia en los casos en que se podía prescindir de la presencia física.

El origen del comercio electrónico se encuentra en las décadas del setenta y ochenta, cuando las empresas extendieron su poder informático interconectándose, enviando y recibiendo órdenes de compra, notificaciones y manifiestos de embarque vía EDI (Electronic Data Interchange), iniciando el camino que pocos años más tarde se transformaría en una dimensión nueva del comercio. El EDI es un standard para compilar, transmitir e intercambiar información entre computadoras de redes privadas de comunicaciones, llamadas VANS (Value Added Networks); sin embargo, los costos privativos de las VANS pusieron a esta forma primitiva de comercio electrónico fuera del alcance de la mayoría de las pequeñas y medianas empresas, que en la generalidad de los casos se vieron relegadas al uso del teléfono, telex y fax como instrumentos de comunicaciones de negocios. Además, muchas empresas grandes tampoco

pudieron utilizar totalmente el potencial del EDI, porque gran parte de sus socios de negocios no lo usaban o no tenían posibilidad de acceso económico a él, o bien carecían de los conocimientos tecnológicos suficientes.

Con el desarrollo de Internet, el concepto de redes abiertas puso a las empresas en condiciones de participar en el comercio electrónico, no solamente dentro de los restringidos parámetros EDI, sino en formas mucho más sofisticadas permitiendo una interacción fluida con los consumidores en los mercados digitales, al facilitar la transmisión simultanea de texto, sonido e imagen en tiempo real. No obstante, recién en 1994 Internet ingresa verdaderamente en su era comercial, ya que ese año dos estudiantes de ingeniería eléctrica de Stanford fundan el primer buscador y luego portal Yahoo, que nace como un primitivo catálogo en línea de sitios Web. En 1996, cuando comienza a capitalizarse en la bolsa, provoca una verdadera fiebre entre los inversores; ese mismo año comienza a operar First Virtual, el primer banco cibernético. En 1995 un hito marca el inicio de la era del comercio electrónico, Amazon.com, el emblema del comercio en línea, vende su primer libro a través de Internet, luego paulatinamente se incrementaron los actores con la incorporación de otros portales (e-toys, e-bussines, etc.), y se amplió la oferta comerciable, que de incluir exclusivamente bienes tangibles como libros, CD.s y artículos diversos, comienza a incluir intangibles como Software, programas de radio e incluso servicios como reserva y compra de billetes de avión o pólizas de seguros. Hoy, mucha de la propiedad intelectual que es producida, envasada y almacenada en todo el mundo y físicamente despachada hacia su destino final, es susceptible de ser digitalizada y comercializada por Internet.

En el comercio electrónico estamos frente a otra revolución del mundo de los negocios y ya se habla de una nueva economía que día a día adquiere más fuerza y en la que los principales protagonistas son los organismos multinacionales, los gobiernos nacionales, los sectores representativos, los proveedores de tecnología, las empresas y los consumidores, quienes deambulan en ese gran centro comercial llamado Internet, considerada la puerta de entrada al futuro de la nueva economía global.

2.1.2. Definición de Comercio Electrónico.

El comercio electrónico se puede definir, en un sentido amplio, como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet. En este sentido,

el concepto de comercio electrónico no sólo incluye la compra y venta electrónica de bienes, información o servicios, sino también el uso de la Red para actividades anteriores o posteriores a la venta. En definitiva, el Comercio Electrónico supone comprar y/o vender productos y servicios a través de Internet como son:

- Productos físicos (coches, discos, ropa, tornillos, acero, etc.)
- Productos de servicios (viajes, consultas médicas en línea, educación a distancia, etc.).
- Productos digitales (noticias, imagen y sonido, bases de datos, software, etc.).
- Publicidad
- Búsqueda de información sobre productos, proveedores, etc.
- Negociación entre comprador y vendedor sobre precio, condiciones de entrega, etc.
- Atención al cliente antes y después de la venta
- Dar cumplimiento a trámites administrativos relacionados con la actividad comercial
- Colaboración entre empresas con negocios comunes (a largo plazo o sólo de forma coyuntural)

La comunicación. El comercio electrónico es una eficiente vía de comunicación y de marketing, que usada correctamente puede aportar un valor añadido a los clientes manteniéndoles informados de las novedades, nuevos productos y nuevas ofertas.

Esta nueva forma de comercialización directa de los productos y servicios que ofrecen las empresas a través de Internet mediante el Comercio Electrónico.

2.1.3. Cómo se realiza una operación de Comercio Electrónico.

Para comprar productos o adquirir servicios a través de Internet necesariamente hay que conectarse a la Red a través de un PC, una Televisión digital, etc. Una vez hecho esto hay diversos caminos a seguir hasta llegar al producto deseado. Directamente, si se conoce la dirección en la que encontrar el producto y servicio

concreto que se quiere adquirir (normalmente cuando se realizan compras habituales) o mediante buscadores (como Google, Yahoo, etc.) cuando únicamente se sabe lo que se quiere pero no dónde encontrarlo.

Cuando se ha localizado el producto/servicio deseado, y se está de acuerdo con sus características físicas y técnicas así como con el precio, el plazo y la forma de entrega, se pasa a formalizar el pedido. A la hora de efectuar el pago si se decide hacerlo por Internet (en ocasiones se da la oportunidad de hacerlo mediante reembolso) se efectuarán las transacciones correspondientes entre los bancos para dar conformidad a la operación de compra y se emitirá un justificante de la compra el cual, normalmente, será enviado por medio del correo electrónico. Tan solo queda esperar a recibir el producto/servicio en los términos acordados.

2.1.4. Principales Categorías del Comercio Electrónico.

Dentro del Comercio Electrónico existen diversas categorías dependiendo de quienes sean los que interactúen. Los actores principales son las Empresas, los Consumidores y las Administraciones Públicas.

- Entre empresas (B2B, Business to Business).
- Entre Empresa y consumidor (B2C, Business to Consumer).
- Entre Empresa y Administración (B2A, Business to Administration).
- Entre Empresa y Empleado (B2E, Business to Employee)
- Entre Consumidor y Administración (C2A, Citizen to Administration).
- Entre Consumidor (C2C, Citizen to Citizen).

2.1.4.1 B2B: Business to Business.

El Comercio Electrónico entre empresas, consiste en el intercambio de productos y servicios cuyo objetivo es la utilización de éstos dentro de su actividad productiva (compras de material de oficina, servicios de limpieza y seguridad, repuestos de maquinaria o pequeños equipos) o simplemente la compra-venta a gran escala. Su objetivo principal es la automatización de la gestión empresarial y la eliminación de costos asociados como la facturación, el desplazamiento, gastos en papel, comunicación, etc.

Las empresas están continuamente verificando que a partir del comercio electrónico puedan no solo generar mas oportunidades sino también mejorar su competitividad.

Las empresas pueden, contactarse con empresas de cualquier lugar del mundo. Las transacciones financieras electrónicas son seguras haciendo mas fácil el manejo de productos reduciendo los gastos y acelerando el proceso de facturación.

Licitaciones y Suministros.

Se utiliza para difundir licitaciones y recibir ofertas. En varios países este modelo esta ampliamente adoptado por organismos públicos y grandes organizaciones para el suministro de obras y servicios.

Tienda Electrónica.

Es la solución representada por la web privada de cualquier empresa y promovida por los propios comerciantes. Esta generalmente constituida por un dominio web.

Subastas.

Son el equivalente electrónico de las subastas tradicionales, pero con el atractivo que no requiere movimientos de mercancías al lugar de la subasta.

Galería Comercial (Mall).

Conjunto de tiendas que aparecen en un dominio común bajo la cobertura de un nombre comercial conocido. Las tiendas comparten gastos de galería virtual y el gestor principal de los beneficios.

Mercados gestionados por terceros.

Respecto a las galerías comerciales, la integración con el gestor es mucho mayor gestión de operaciones, ya que en el reposan responsabilidades de gestión y operación.

Suministradores de la cadena valor.

Organizaciones que se especializan en determinadas funciones de la cadena de valor, como los transportes, la logística o los medios de pago, convirtiéndose en integradores.

Infomediarios y terceras partes de confianza.

Los intermediarios de información realizan análisis de la oferta y distribución de contenidos hacia la demanda. Las terceras partes de confianza, generalmente con alto grado de tecnificación y especialización, trabajan en las areas de seguridad y legalidad del comercio electrónico.

Debe considerarse además de empresas y actividades que suministran servicios para el desarrollo del propio comercio electrónico, que contribuyen en si en un mercado creciente como suministro de plataformas, provisión de servicio de internet, creación de catálogos o alojamiento de paginas web.

2.1.4.2 B2C: Empresa y Consumido.

Las empresas que comercializan sus productos destinados al consumidor pueden ser minoristas, fabricantes de productos o proveedores de servicios.

El objeto de estas empresas es satisfacer las necesidades del consumidor aportándole productos y/o servicios para su propio beneficio. Estos pueden ser discos, software, cursos, libros, billetes de avión, ropa, etc.

En el Comercio Electrónico entre empresas y consumidores, el proveedor no es necesariamente conocido a priori. La venta se realiza mediante la introducción de los datos personales y los referentes al modo de pago.

De ahí que en este tipo de comercio electrónico utiliza las nuevas tecnologías admite, en teoría, un contacto directo entre fabricantes y consumidores. Esta es una adicional ventaja, pues permite la eliminación de intermediarios en el proceso de compra, lo que repercute enormemente en el precio final del producto favoreciendo rebajas importantes en el mismo.

2.14.3 B2A Empresa y Administrador.

La categoría "empresa-gobierno" (administración) cubre todas las transacciones entre las empresas y las organizaciones gubernamentales; en ella el comercio electrónico no tiene todavía un volumen considerable como en las precedentes, sin embargo, esta adquiriendo una creciente importancia estratégica en las compras públicas, pero sobre todo sirve para incentivar el proceso de aprendizaje del comercio electrónico en pequeñas y medianas empresas, que así se familiarizan progresivamente con las tecnologías aplicables.

2.1.4.4 B2E empresa y empleado.

Es una aplicación Intranet diseñada para que los trabajadores de una empresa puedan distribuir y compartir datos, acceder a todo tipo de proyectos y obtener información del negocio de su compañía desde cualquier lugar.

El B2E es mucho más que gestionar el conocimiento, se trata de reorganizar profundamente las relaciones con los trabajadores buscando una optimización en el uso de la información mediante el acceso permanente a la información on-line, suponiendo un considerable ahorro de tiempo, una mejora de su satisfacción y una mejora de su productividad.

Algunas de sus actividades son: Instrucciones concretas de su superior, Comunicados oficiales de la empresa, Noticias del sector que puedan incidir en su trabajo, Mensajes urgentes a responder de forma prioritaria, Reducción de costes y tiempo en actividades burocráticas, Mejora de la información interna, Comercio electrónico interno etc.

2..1.4.5 C2A Ciudadanos y Administrador.

En esta categoría participan en la transacción con las Administraciones Públicas Estas relaciones entre la administración y el consumidor originan un intercambio parecido al modelo B2A, ofreciendo al consumidor la posibilidad de pagar sus impuestos y tasas vía on-line además de acceso a toda clase de asesoramiento, devoluciones, etc.

Se trata de conseguir un acercamiento a la sociedad por medio de una serie de actuaciones:

Simplificando los procedimientos administrativos.

Instaurando la Ventanilla Única como servicio que permitirá a los ciudadanos iniciar y mantener relaciones con la Administración a través de centros situados en los lugares accesibles para ellos.

Facilitando a los ciudadanos el acceso a sus servicios mediante sencillas navegaciones Web, refinando los procedimientos de búsqueda y creando centros de información administrativa.

2.1.4.6 C2C Ciudadano.

Este tipo de relaciones son las que existen entre los mismos consumidores, como pueden ser las subastas on-line. Los productos y servicios se ofrecen y demandan

por particulares que se convierten en consumidores en el momento de la transacción.

En las subastas en línea, cualquier particular puede colocar a la ventana un producto en un sitio especial a efecto, el cual brinda una plataforma para todos los ciudadanos que deseen vender directamente sus bienes o artículos. Estos sitios no necesariamente deben ser comerciales; durante el 2000 uno de los sucesos de mayor impacto en internet fue el sitio creado por universitarios norteamericanos para el intercambio gratuito de música. En menos de un año obtuvo decenas de millones de asociados, el cual recibió una demanda de las casas discográficas, pero creo un concepto de sistema de distribución descentralizado aplicable con fines comerciales.

2.1.5 Diferencia entre Comercio y Business.

El comercio tradicional desde su aparición, se ha basado en la existencia de una relación de confianza mutua y de compromiso entre el comprador y el vendedor. Durante siglos, el comercio consistió principalmente en el intercambio de bienes. El desarrollo e implementación de la moneda supuso un gran avance sobre la economía de trueque. El riesgo que conllevaban de robo o partida aconsejó la impresión de billetes que permitían guardar su contravalor en lugar seguro: el banco. Esto nos lleva a un sin numero de diferencias entre el comercio tradicional y el comercio electrónico comenzando con que el comercio electrónico, contribuye a una muestra evidente de que estamos ante un fenómeno que supera todos los ámbitos tradicionales, específicamente en aquellos tan apegados al derecho como las nociones de cosas, espacio y tiempo.

Mejora de ingresos: el comercio electrónico le ofrece un canal de ventas adicional y la oportunidad de incrementar los ingresos y le ayuda aganar cuotas de mercado. También pueden generarse ingresos adicionales mediante la venta de espacios de publicidad en su sitio web. En particular. Si muchas de las rutinas de ventas pueden gestionarse a través de una estrategia de comercio electrónico, su fuerza de ventas queda liberada para desarrollar nuevos negocios.

Expansión de mercado. El comercio electrónico pueden permitirle vender sus productos y llevar el conocimiento de su nombre y marcar mas allá de sus limites de mercado actual a un costo inferior frente a medios alternativos, como abrir tiendas nuevas o lanzar campañas de publicidad. Mediante una estrategia de comercio electrónico a través de la web puede conseguir una presencia global

real, sin importar el tamaño de su empresa. Con un adecuando apoyo promocional, su sitio web puede convertirse en una potente fuente de negocios.

Fidelidad del cliente: La flexibilidad de internet, al permitir a los clientes conectarse en cualquier momento, hacer pedidos y realizar un seguimiento de su compra, ahorra un tiempo y esfuerzo sustancial a los propios clientes. Mejorando la experiencia del cliente, el comercio electrónico estimula la fidelidad de la repetición de la vida.

Reducción de costos: El comercio electrónico amplia las operaciones de venta y optimiza el flujo de información entre los departamentos de la empresa. Esto permite incrementar la eficiencia y productividad del personal comercial y de soporte.

CAPITULO II

DELITOS INFORMÁTICOS

Hablar acerca de la legislación en México, nos tenemos que referir sin lugar a duda a los delitos informáticos que en la actualidad suele presentársele a todos los usuarios del planta tierra que utilizan la red de redes. Las primeras bases desarrolladas por la ONU para regular el comercio electrónico en Internet, está fundamentada en el Principio de la Equivalencia Funcional. Este precepto dice que todo lo que reconoce la ley offline, también debe reconocerlo la online. Si algo es ilegal en el mundo real, también debe serlo en el virtual.

3.1 Concepto de delitos informáticos.

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos" este consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún; sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

De esta manera, el autor mexicano julio Tellez Valdez señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables. Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo". María de la Luz Lima**,** dice que el "delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin". El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".

3.2. Características principales de un delito informático.

- Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Se puede decir que el tipo de personas que cometen estos tipos de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con la facilidad de poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima.

3.3. Como instrumento o medio.

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de computo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

3.4. Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

3.5. Otros tipos de delitos.

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- **Acceso no autorizado:** Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de e-mail:** : Lectura de un mensaje electrónico ajeno.
- **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
- **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.
- **Infracción de los derechos de autor**: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.
- **Distribución de música por Internet (mp3)**: Sabido es que con relación a la música existe el conocido MP3 un formato digital de audio que permite

comprimir el tamaño de una canción digitalizada en una relación de 10 a 1 es decir que 10 MB de sonido digitalizado ocuparía solo un MB esto es lo que ha permitido un intenso tráfico de música dentro de la red que ha derivado inclusive en la venta ilegal de compactos sin intervención de las discográficas dando lugar a todo un movimiento al respecto que ha sido motivo de numerosas medidas para tratar de evitarlo.

- **Difusión de pornografía** En la mayoría de países así como en nuestro país es ilegal la comercialización de pornografía infantil o cualquier acto de pederastia. Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas scaneadas que son difundidas o comercializadas por toda la Web.
- **Manipulación informática**: es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

3.6. Delitos Mediante la RED.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- **Otros delitos:** Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

3.7. Los 10 fraudes más comunes en Internet.

La Comisión Federal de Comercio (FTC) de Estados Unidos, es el organismo que supervisa la competencia y se encarga de la protección de los consumidores. En la actualidad Internet cuenta con un decálogo de prácticas ilegales. Según la (FTC) que ha publicado una lista en la que figuran los 10 fraudes más comunes realizados al amparo de la Red.

Las subastas: Algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero puede ocurrir que reciban algo con menor valor de lo que creían, o peor todavía, que no reciban nada.

Reclamaciones de pedidos: En ocasiones se puede recibir mensajes de correo confirmando un pedido realizado en Internet. La estafa consiste en hacer que el incauto navegante llame a la empresa a través de un 906 y tras varios minutos de espera donde la operadora le hace perder el tiempo, desista de su intento, pero ya será tarde porque la llamada le ha podido costar varios pesos.

Las tarjetas de crédito: En algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El verdadero objetivo es cobrar cargos no solicitados.

Llamadas internacionales: En algunas páginas, por lo general de material para adultos, se ofrece acceso gratuito a cambio de descargar un programa que en realidad desvía el módem a un número internacional o a un 906. La factura se incrementa notablemente en beneficio del propietario de la página.

Servicios gratuitos y/ acceso a Internet: Se ofrece una página personalizada y gratuita durante un período de 30 días. Los consumidores descubren que se les ha cargado facturas a pesar de no haber pedido una prórroga en el servicio.

Ventas piramidales: Consiste en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil sólo por vender determinados productos a nuevos compradores que éstos deben buscar.

Viajes y vacaciones: Determinadas páginas de Internet ofrecen destinos maravillosos de vacaciones a precios de ganga, que a menudo encubren una realidad completamente diferente o inexistente.

Oportunidades de negocio: Convertirse en jefe de uno mismo y ganar mucho dinero es el sueño de cualquiera. En la Red abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en una estafa.

Inversiones: Las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comportan grandes riesgos para los usuarios. Como norma general, no es recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100%.

Productos y servicios milagro: Algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

3.8. Sabotaje informático.

Realizado por medio de cualquiera de estos métodos:

Virus. Los virus son un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho, y más si se utiliza Internet como vía de infección. Un virus informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de sí mismo en un fichero. Los virus se adhieren a cierta clase de archivos, normalmente EXE y COM, cuando estos ficheros infectados se transmiten a otro sistema éste también queda infectado, y así sucesivamente. Los virus entran en acción cuando se realiza una determinada actividad, como puede ser el que se ejecute un determinado fichero.

Gusanos Se fabrican de forma similar al virus con el objetivo de infiltrarlo en programas originales o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Podría decirse que es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus, es decir, un programa gusano que posteriormente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego destruirse.

Bomba ilícita o cronológica Las bombas lógicas son difíciles de detectar antes de que exploten; por eso entre todos los dispositivos informáticos criminales, la bombas lógicas son las que poseen el máximo potencial de daño. Su activación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. Puede utilizarse como material de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Acceso no autorizado La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Piratas informáticos o hackers El acceso se efectúa a menudo desde un lugar exterior, recurriendo a uno de los diversos medios como son:

Aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

Los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

3.9. Hackers, Crackers y Phreakers.

En los años 60 el término Hacker se utilizaba para una persona considerada un "autentico programador", que dominaba los sistemas informativos del momento y era capaz de manipular programas para que hicieran más cosas que para las que habías sido diseñados.

A fines de los 60 y principios de los 70, el hacking se asocio con el movimiento underground radical ("yuppie") y tomo un aire de rebeldía contra el sistema.

Las agencias policiales comenzaron a arrestar a los phreakers por entrometerse en los sistemas telefónicos. En los años 80 el FBI realizo los primeros arrestos de alto nivel entre los hackers informativos. En los 90 pusieron al día el concepto de hacker como una figura brillante y de algún modo romántica que se saltaba las leyes pero normalmente con nobles propósitos.

Llegando al año 2000, los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. Hackers Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida. También están los que se entrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones.

En todo esto hay una serie de avisos. No se quiere dar la impresión de que un individuo es un hacker, un phreaker o un Crackers exclusivamente. Estas categorías no son mutuamente excluyentes. De hecho, muchos individuos son capaces de actuar en más de uno de estos papeles.

3.9.1. Hacker.

Es un tipo de persona que es buena programando de forma rápida, que con ayuda de sus conocimientos informáticos consiguen acceder a cualquier computadora que se encuentre dentro de una red, realizan trabajo frecuentemente usando programas como UNIX. En otras palabras, un hacker es una persona que tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático.

El principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente.

Los criminólogos, describen a los Hackers en términos menos halagadores, los denominan como "violadores electrónicos" o "vándalos electrónicos".
Los *hackers* eran aficionados de la computación que “irrumpían” en los sistemas de computación gubernamentales y/o corporativos, utilizando su PC y un módem telefónico.

La ética hacker defiende la libertad absoluta de información: libre acceso y libre distribución, por lo que está emparentada estrechamente con la ética *open source*. Para muchos defender tanto la libertad es algo muy parecido a defender la rebelión contra el sistema.

Hay dos variedades de hackers dignas de destacar:

- **Samurai**. Un hacker que crackea amparado por la ley y/o la razón, normalmente es alguien contratado para investigar fallos de seguridad, que investiga casos de derechos de privacidad. Los samurais desdeñan a los crackers y a todo tipo de vándalos electrónicos.
- ***Sneaker.*** Simular en ciertos aspectos: es aquel individuo contratado para romper los sistemas de seguridad por las empresas e instituciones con la intención de subsanar dichos errores.

Otros tipos de hackers.

Wannabes. Alguien que podrá llegar a ser un hacker, pero que aún no lo es. Todos los hackers han pasado por esta etapa. Un *wannabe* adquiere el estatus de hacker cuando los veteranos deciden empezar a considerarle uno de los suyos.

Newbie. Algo muy similar a w*annabe*: un novato. Originariamente esta palabra procede de Inglaterra y se aplicaba a los recién llegados a los colegios y a las academias militares.

Estado larval. Para entrar en este comando de elite dentro de los guerreros de los bits hay que pasar por diferentes estadios de desarrollo. Uno de los periodos más frecuentes es el larval (larval stage), que oscila entre los 6 meses y los dos años y en el que el sujeto se encierra en su habitación a escribir código e ignora en mayor o menor medida la realidad que le rodea.

Bogus (farsante). Ser hacker es un honor que hay que ganar y que la comunidad hacker concede. Uno no puede empezar a proclamar que lo es sin la aquiescencia de dicha comunidad a menos que quiera ser mirado con desprecio y pasar a formar parte de la tribu de los hackers de pacotilla, los farsantes conocidos como b*ogus*.

Bigot (fanático). Una persona que es férrea partidaria de un lenguaje de programación, de un particular sistema operativo o una computadora en concreto. Aplicable a los hackers y a la familia circundante.

Spod. Alguien que reúne todos los aspectos negativos de un g*eek*, pero que no cuenta con ninguna de sus ventajas, se mueve por la Red aprovechando sus ventajas pero sin interesarse lo más mínimo es su funcionamiento o en ningún tipo de filosofía. Generalmente es despreciado.

Lurker. Un término que no es en absoluto peyorativo. Se refiere a la mayoría silenciosa que sólo participa en los foros muy de vez en cuando.

Twink. Un usuario ‘repelente’. En las partidas de rol es aquel jugador que ignora todas las reglas y convenciones sociales para hacer alarde de sus superpoderes.

Que se necesita para ser un hacker.

Los Hackers no necesitan caros equipos informáticos, tampoco una estantería rellena de manuales técnicos. Los Hacker saben cómo explorar el World Wide Web, y pueden encontrar casi cualquier información totalmente gratis. De hecho, hackear es tan fácil que si se tiene un servicio on-line y se sabe cómo enviar y leer un e-mail, se puede comenzar a hackear inmediatamente.

Los diez mandamientos del hacker.

- **I.** Nunca destroces nada intencionalmente en la Computadora que estés crackeando.
- **II.** Modifica solo los archivos que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.
- **III.** Nunca dejes tu dirección real, tu nombre o tu teléfono en ningún sistema.
- **IV.** Ten cuidado a quien le pasas información. A ser posible no pases nada a nadie que no conozcas su voz, número de teléfono y nombre real.
- **V.** Nunca dejes tus datos reales en un BBS, si no conoces al sysop, déjale un mensaje con una lista de gente que pueda responder de ti.
- **VI.** Nunca hackees en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscarte mientras que las universidades y las empresas particulares no.
- **VII.** No uses BlueBox a menos que no tengas un servicio local o un 0610 al que conectarte. Si se abusa de la bluebox, puedes ser cazado.
- **VIII.** No dejes en ningún BBS mucha información del sistema que estas crackeando. Di sencillamente "estoy trabajando en un UNIX o en un COSMOS...." pero no digas a quien pertenece ni el teléfono.
- **IX.** No te preocupes en preguntar, nadie te contestara, piensa que por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.
- **X.** Punto final. Puedes pasearte todo lo que quieras por la Web, y mil cosas mas, pero hasta que no estés realmente hackeando, no sabrás lo que es.

3.9.2. Cracker.

Cracker es un término acuñado por los hackers hacia 1985 para defenderse contra la mala utilización que hacían los periodistas de la palabra hacker y que se refiere al que rompe la seguridad de un sistema. Los crackers forman pequeños grupos, secretos y privados (se adentran en el terreno de lo ilegal), que tienen muy poco que ver con la cultura abierta que se describe en el mundo hacker.

La definición de un cracker es alguien que trata de violar el acceso a un sistema adquiriendo passwords. La mayoría de los crackers son adolescentes nada bondadosos y que buscan dar sus golpes destruyendo o alterando la data de un sistema. Tienden a unirse en grupos muy pequeños, secretos y cerrados. Tambien realizan actividades como: romper la seguridad de un sistema haciendo destrozos, robando información y utilizándola para sacar provecho.

Todos los hackers tienen habilidades de sobra para convertirse en crackers, pero han resistido la tentación y se mantienen dentro de la legalidad. Cuando un hacker responde a la llamada del lado oscuro de la fuerza se convierte un **cracker.**

Pero he aquí la gran diferencia en cuestión. Los crackers (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Esos son los crackers. Adolescentes inquietos que aprenden rápidamente este complejo oficio.

Para el cracker el invadir un sistema no requiere de misteriosos estados de iluminación mental, pero sí mucha persistencia y la testaruda repetición de trucos bien conocidos en los puntos débiles de un sistema, tratan de descubrir información clasificada hurgando al azar y con ciega persistencia. Suele decirse que los crackers son sólo hackers mediocres y que su nivel de educación e inteligencia sobre un sistema es menor.

3.9.3. Phreakers.

Son personas que utiliza la técnica de phreaking; es la técnica de como engañar a sistemas de cobro a distancia. Entiéndase no pagar, o paga menos teléfono, pagar la luz mucho mas barata, no pagar casi nada de gas, peajes gratis, tener teléfono móvil de gorra, canales gratis y todo eso. También es llamado cracker telefónico. Se puede decir también que son Aquellos que ‘rompen’ y hacen un uso ilegal de las redes telefónicas.

Los phone phreaker son los más famosos en los medios de comunicación por los desastres que han hecho a través de los años. En los años 60 ya existían los Phone Phreaks y la gran victima era AT&T.

3.9.4. Diferencia entre Hacker, Cracker, Phreakers.

Hacker se utiliza normalmente para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños, toma su actividad como un reto intelectual, no pretende producir daños, aunque su intención sea únicamente curiosear . Los **Craker** en cambio tiene como principal objetivo producir daños que en muchas casos ponen en problemas de extrema gravedad al administrador del sistema y en cuanto a los **Phrekers** es el especialista en telefonía. Se le podría llamar el cracker de los teléfonos. Sobre todo emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. Ni que decir tiene que están muy perseguidos, por la Justicia y por las compañías telefónicas.

CAPITULO IV
Legislación Internacional

Debido a la insistente problemática que se ha presentado a las empresas, usuarios, etc., ha dado motivos que den origen a las iniciativas para regular el comercio electrónico, en todos los países del mundo. En la mayoría de ellos han tenido la necesidad de comenzar a legislar las leyes referentes a la informática y muy particularmente al uso del internet. En el presente capito se presentan algunos nombres de las leyes más conocidas que existen en algunos países de América latina y los más avanzados en esta área son España y Estados Unidos.

4.1. Argentina.

Constitución de la Nación Argentina de 22 agosto 1994.

El artículo 43, tercer párrafo de la Constitución de 1994 (modificación) dice que toda persona podrá interponer el habeas para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros y bancos de datos públicos, o los privados destinados a proveer informes; y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. Agrega que no podrá efectuarse el secreto de las fuentes de información periodística.

Ley 17.711.- Reforma el art. 2311 del Código civil según el cual la energía eléctrica y magnética apropiada en forma de información contenida en un suporte digital es asimilable a una cosa. Por lo tanto, dicho bien es susceptible de ser dañado o alterado.

Ley 11.723 de Propiedad Intelectual.

Considera que la acción de borrado o destrucción de un programa de computación se encuadra perfectamente en el art. 183 del Código Penal.
Artículo 72º.a).- Son ilícitos que se cometen en violación a los derechos de autor, editar, vender o reproducir una obra musical, texto original, imágenes estáticas y en movimiento, el diseño de una página web como todo su contenido sensible y original, sin autorización.

Ley 21.173.- El que arbitrariamente se entrometiera en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieran cesado, y a pagar una indemnización que fijará equitativamente el juez...

- Ley 22.362 de Marcas
- Ley 24.481 de Patentes de Invención y Modelos de Utilidad

- Ley 24.614 modificadora de la Ley 11.672 que considera con pleno valor probatorio a la documentación de la Administración Nacional archivada en soportes electrónicos.

Ley 24.766 de Confidencialidad.

sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos. (18 diciembre 1.996)

Ley 25.036 modificadora de la Ley 11.723 de propiedad intelectual, que incluye dentro de las obras intelectuales protegidas a los programas de computación.
Decreto 62/90 otorgando exclusividad para la transmisión internacional de servicios de valor agregado –Internet-

Decreto 468/92 designación del Poder Ejecutivo Nacional de una Comisión, donde se alude a aspectos de la protección de datos personales.

Decreto 165/94 del 8 de febrero de 1.994, al igual que la Ley 11.723 protege las obras de bases de datos y de software. Dispone que tanto los programas de ordenador como las “obras de base de datos” sean incluidas dentro del artículo 1 de la Ley 11.723 como obras protegidas.

Proyecto de Código Civil y Comercial.- Decreto 685/95

Art. 974 Código Civil.- Principio de libertad de formas para la confección de documentos.

Art. 1012 Código Civil.- Establece que la firma es condición esencial para la existencia de todo acto bajo forma privada.

Art.º 1071 bis del actual Código civil.- Protección de la intimidad.

Art. 3639 Código Civil. Define la firma como el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad.

Resolución 45/97 de la Secretaría de la función Pública sobre firma digital

Resolución 125/97 de la Secretaría de la Función Pública que crea la Unidad Ejecutora 2.000 a fin de controlar el impacto del problema del año 2.000 en la administración pública.

Decreto 554/97 declarando de interés nacional el acceso a Internet
Decreto 555/97 sobre firma digital

Resolución 555/97 del Ministerio de Trabajo y Seguridad Social

Decreto 1279/97 declarando comprendida a la Internet en la garantía constitucional de libertad de expresión

Ley 104 de acceso a la información de la Ciudad Autónoma de Buenos Aires
Modificación del Código Aduanero (1998)
Resolución 212/98 de la Secretaría de la Función Pública

Resolución 1616/98 Anexo de la Secretaría de Comunicaciones; Resolución 145/99 del Ministerio de Salud y Acción Social

Decreto 427/98 del 16 de abril de 1.998.

Por el cual se aprueba la infraestructura de Firma Digital para el Sector Público Nacional. Subsecretaría de la Gestión Pública de la Jefatura del Gabinete de Ministros 16/IV/1998. Autoriza por el plazo de dos años, el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa. Otorga a la firma digital similares efectos que la firma manuscrita para los actos internos de la Administración.

Ley 25.868 (Boletín 11.11.1998) introduce como objeto de protección de los derechos de autor a los programas de computación fuente y objeto y las compilaciones de datos

Resolución 1636/98 CNC sobre el efecto 2.000

Resolución 173/99 sobre lealtad comercial de la Secretaría de Industria, Comercio y Minería, que obliga a quienes comercialicen equipos de computación o programas que dependan de una variable temporal que incluya el dato “año” a colocar una identificación sobre el carácter compatible o no con el año 2.000.

Resolución 462/99 del sistema de información de la AFIP

Resolución 4536/99 de la Secretaría de Comunicaciones sobre autoridad de aplicación de la firma digital

Resolución 474/99 de la AFIP sobre obligaciones impositivas y previsionales

Resolución 512/99 de la Comisión Nacional de Comunicaciones que intima a los prestadores de servicios de telecomunicaciones y correo postales a presentar informes sobre la actividad del año 2.000.

Resolución 976/99 CNC sobre el efecto 2.000

Decreto 3345/99 de la Comisión Nacional de Valores

Decreto 412/99 de recomendaciones sobre comercio electrónico del Ministerio de Economía, Obras y Servicios Públicos

Código Procesal Constitucional de 8 de marzo de 1.999

Art.º 67.- Amparo informativo (corpus data). "Cualquier personas física puede reclamar por vía del amparo, una orden judicial para conocer las informaciones relativas a su persona, que consten en registros o bancos de datos de entidades públicas o privadas, destinadas a proveer informes; es destino, uso o finalidad dado a esa información, para actualizar dichas informaciones o rectificar sus errores; para imposibilitar su uso con fines discriminatorios, para asegurar su confidencialidad, para exigir su supresión o para impedir el registro de datos relativos a sus convicciones ideológicas, religiosas o políticas, a su afiliación partidaria o sindical, o a su honor, vida privada, condición social o racial o intimidad familiar y personal. Será competente para conocer en esta acción el juez en lo civil y comercial común.

Decreto de Necesidad y Urgencia.- Decreto 1004/99 publicado en el boletín del 22.9.1999 declara el estado de alerta de todos los Sistemas informáticos, y aun a aquellos no informáticos pero cuyas prestaciones dependan de dispositivos electrónicos que puedan verse afectados en su funcionamiento a causa de la llamada crisis del 2.000.

Decreto 252/00 Programa Nacional para la Sociedad de la Información

Resolución 354/00 de la Comisión Nacional de Valores sobre comercialización de cuotas parte de Fondos Comunes de Inversión por Internet

Proyecto del Grupo de Investigación y Virus Informáticos de la Universidad de Belgrano, que propone reformar el Código Penal en el capítulo relativo a falsificaciones, incluyendo un concepto amplio de documento electrónico o digital, tomando como base la reforma española de 1.995, que sería el Art. 297 bis del Código Penal: "A los fines de este artículo (sobre falsedades en documentos) se considerará documento a todo soporte magnético, óptico o electrónico que exprese o incorpore datos, hechos o declaraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Anteproyecto de Ley formato digital de los actos jurídicos. Comercio electrónico.

Se presentó un proyecto de ley para regular la firma digital. El Jefe del Gabinete, Rodolfo Terragno

Resolución nº 1/2000 de la Cámara Laboral reglamentando diversos aspectos de la notificación electrónica.

Resolución 2226/2000 del Ministerio de Relaciones Exteriores y Culto de la Nación, sobre registro de denominaciones para su uso en páginas de Internet (Boletín Oficial de la República Argentina de 29.8.2000)

Ley 25.326 de Protección de Datos (Habeas Data) (2 noviembre de 2.000).

Decreto 995/2000, de 30 de octubre de 2000.
Reglamentación de la ley de Protección de Datos.

Reglamento Nombre de Dominio.

Decreto 96/2001 de Creación de la Unidad Administradora del Sistema Unificado de Base de Datos. 25 de enero de 2.001. Publicado en el Boletín Oficial del 30 de enero 2.001.

4.2. Venezuela.

Constitución de la República Bolivariana de Venezuela. (Deroga Constitución de 1971).

Decreto nº 825 del 10 de mayo de 2000.

Decreto sobre Internet como prioridad de la república Bolivariana de Venezuela de la Presidencia de la República Bolivariana de Venezuela. Publicado en Gaceta Oficial de la República Bolivariana de Venezuela nº 36.955 del 22 de mayo de 2000.

Decreto con Fuerza de Ley sobre **Mensajes de datos y Firmas Electrónicas** del 10 de febrero de 2001. Publicado en Gaceta Oficial de la República Bolivariana de Venezuela nº 37.148 del 28 de febrero de 2001)

Ley Especial contra Delitos Informáticos (Gaceta Oficial nº 37.313 de 30 de octubre 2001).

4.3. Brasil.

Decreto de Ley Nº 2848, de 07 de diciembre de 1940 Código Penal.

Constitución de la República Federativa de 1988.

La Constitución brasileña de 1988 recoge la protección de datos.

En su artículo 5, LXXII, se crea un recurso especial de “habeas Data”, en la instancia constitucional. “Se concede el habeas data: a) para asegurar el conocimiento de las informaciones relativas a la persona del impetrante que constaran en registros o bancos de datos de entidades gubernamentales o de carácter público”.

El código de Protección y Defensa del Consumidor Ley no. 8078/90. Actualizado hasta que las alteraciones introdujeran por la ley 9870, de 23.11.1999,

Decreto no. 2181/1997 sanciones para el inobservancia de las normas del consumo.

Ley Proyecto en la creación, archivo la utilización de y de electrónicos de los documentos.

La ley no. 9.507 del 12 de noviembre de 1997. - Regula el derecho de acceso a informaciones y disciplina el rito procesal del las "Fechas de Hábeas"

La ley no. 9.755, del 16 de diciembre de 1998. Dispone sobre la creación del "homepage" en la "Internet" para el Tribunal de Facturas de la Unión, para la divulgación de los datos e información que especifica, y el he/she da otro usted hace los arreglos. Publicado en mí DÉ him/it de 17.12.1998

La ley no. 9800 de 26 de mayo1999. Permite el uso de sistema de transmisión de datos la práctica de acciones procesales a las partes. Publicado en mí DÉ him/it de 27.05.1999

La ley en el software libre del mundo, aprovada en Recife (Pernambuco) el 22 de marzo de 2.000

Proyecto de ley no. 3.016, de 2.000. – Relativo a Internet

El proyecto De Ley (Comercio electrónico)

Decreto nº 3.587, de 5 de septiembre de 2.000, por el que se establecen normas sobre infraestructura de claves públicas del Poder Ejecutivo Federal

La ley no. 10.176, de 11enero del 2001. Ley en los 8.248, del 23 de octubre de 1991, la Ley en los 8.387, del 30 de diciembre de 1991, y el decreto de Ley no. 288, del 28 de febrero de 1967, que dispone sobre el entrenamiento y competitividad de la sección de tecnología de la información.

La ley no. 16.639/2001 utiliza preferenciales de software libre para el distrito municipal de arrecife de 16 abril de 2001

Medida Provisoria No. 2200, de 27 de junio de 2001.

Crea la Infraestructura de Clave Pública del Brasil (ICP-Brasil). La norma establece que la Autoridad Certificante Raíz estará constituida en el Instituto Nacional de Tecnologías de la Información.
Proyecto de Ley del Senado no. 367, del 28 de agosto de 2003. Bill de Spam. el tiene como objetivo al refrenamiento el uso de mensajes electrónicos ningún pidió a través de la Internet y para garantizar la protección del derecho fundamental al retiro

Decreto no. 4.829, del 3 de septiembre de 2003. En el se dispone sobre la creación de un comité Gestor del Internet en Brasil. CGIbr, en el modelo de provincias de la Internet en Brasil.

Proyecto de Ley 5460/01 del Senado: establece como el crimen la divulgación de la imagen de los niños y adolescentes en las escenas de sexo explícito o la simulación sexual en la Internet, en revistas o en cualquier otro medio visual.

Proyecto de Ley 757/03. Prohíbe las prestadoras de los servicios de celular y mobiliario móvil personal de ellos, usen el servicio del mensaje para la verificación de propaganda comercial.

4.4. Chile.

Constitución de la Republica de Chile 1980.

Modificada en el plebiscito de 30 de julio de 1989 .

Art.º 20.- Ante actos u omisiones en materia de procesamiento de datos que causen privación, perturbación o amenaza en el ejercicio de garantías como la vida privada, el honor, la imagen pública, la igualdad ante la ley, el derecho al trabajo, etc., se puede accionar directa y judicialmente el recurso o la acción de protección.

Ley de Protección de Datos de 1988.

Código de Comercio.

Artículo 913.- Nos indica que las anotaciones en el diario de navegación pueden estamparse por medios mecánicos o electrónicos que garanticen la fidelidad y permanencia de los datos.

Artículo 913. “El libro bitácora o diario de navegación tiene el valor de un instrumento público, siempre que las anotaciones en él estampadas lleven la firma del oficial de guardia y estén visadas por el capitán de la nave. Estas anotaciones no deben tener espacios en blanco, ni enmendaduras o alteraciones”

Artículo 1014.- Nos indica que la firma en el conocimiento de embarque puede ser registrada por cualquier medio mecánico o electrónico.

Artículo 1014. “Cuando el transportador o el transportador efectivo se hagan cargo de las mercancías, el primero deberá emitir un conocimiento de embarque al cargador, si éste lo solicita.

El conocimiento de embarque podrá ser firmado por una persona autorizada al efecto por el transportador. Se entenderá que el conocimiento de embarque suscrito por el capitán de la nave que transporte las mercancías, lo ha sido en nombre del transportador. La firma en el conocimiento de embarque podrá ser manuscrita, impresa en facsímil, perforada, estampada en símbolos o registrada por cualquier otro medio mecánico o electrónico.

Ley nº 17.336 de Propiedad Intelectual.

Ley 18.857.

Que reforma el Código de Procedimiento Penal en 1989, se mejoró esta situación en el proceso penal, en lo que se refiere a los documentos admitiendo como elementos de prueba, en su Art. 113.b. “las películas cinematográficas, fotografías, fonografías, y otros sistemas de reproducción de la imagen y del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe ser alterados los originales de estas pruebas”
Ley 19.052 de 14 de abril de 1991 que consagró explícitamente el carácter de instrumento público de los certificados que el Servicio del Registro Civil e identificación expide mecanizadamente, a través del procesamiento electrónico de datos, sin intervención del hombre y sin firma manuscrita.

Ley 19.223 Relativa a Delitos Informáticos.

Fecha de publicación 7 de junio de 1.993. Fecha de promulgación 28 de mayo de 1.993. Fecha de entrada en vigor junio de 1993

Ley 19.496 sobre protección de los consumidores.

Ley 19.628 sobre protección de la vida privada en Chile Agosto 1.999.

Ley 19.628 sobre la protección de datos personales, del 28 de agosto de 1.999, que entrará en vigor el 27.10.1999. Ministerio Secretaría General de la Presidencia:

Los responsables de los bancos de datos deberán indemnizar el daño patrimonial y moral que cause el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los antecedentes de acuerdo a lo requerido por el titular o, en su caso lo ordenado por el tribunal.

No se podrá llevar un archivo de las recetas médicas o exámenes de laboratorios clínicos, ya que son datos reservados

Decreto nº 81/1999, del Ministerio Secretaría General de la Presidencia.

Que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado.

Proyecto de ley sobre documentos electrónicos.

Que regula la utilización de la firma y el funcionamiento de los certificadores de clave pública.

Circular nº 1493 de la Superintendencia de Valores y Seguros, de 10 de agosto de 2000.

Decreto Supremo nº 779.

Que aprueba el Reglamento del Registro de Banco de Datos Personales a cargo de Organismos Públicos (Diario Oficial de Chile 11 noviembre 2.000).

Moción parlamentaria que modifica la Ley Nº 19.628.

Sobre protección de la vida privada, para favorecer la reinserción laboral de las personas desempleadas.

Resolución nº 9 de 15 febrero 2.001.

Establece normas que regulan el uso de la firma electrónica en el ámbito tributario.

Proyecto de Ley sobre Firmas Electrónicas de 23 marzo 2001.

Informe de la Comisión de Hacienda sobre proyecto que modifica la Ley Nº 19.628

Sobre protección de la vida privada, para favorecer la reinserción laboral de las personas desempleadas. (10 de julio de 2001).

Informe complementario de la Comisión de Hacienda sobre proyecto que modifica la Ley Nº 19.628.

Sobre protección de la vida privada, para favorecer la reinserción laboral de las personas desempleadas. (1 de agosto de 2001)

Ley 19.799 sobre Documentos Electrónicos, firma electrónica y los servicios de certificación de dicha firma de 26 de marzo 2002.

4.5. España.

4.5.1. Datos de carácter personal.

Ley 230/1963, de 28 de diciembre.

Ley General Tributaria (Modificada por LOR 15/1999) (B.O.E. 313/18248 del 31 de diciembre de 1963).

Ley Orgánica 3/1985, de 29 de mayo.

sobre modificación de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Ley 12/1989, de 9 de mayo.

Sobre la Función Estadística Pública (B.O.E. nº 10.767 de 11 de mayo de 1989, y nº 18.332 de 31 de julio de 1990.) Capitulo II de la recogida de datos. Capitulo III del secreto estadístico y Capitulo IV sobre la difusión y conservación de la información estadística. Se establece la posibilidad de la obligación de proporcionar datos, tanto por parte de los ciudadanos hacia la administración como entre administraciones públicas, así como la previsión del secreto estadístico y el carácter finalista de los datos.

Ley 17/1989 del Régimen del Personal Militar Profesional sobre los datos contenidos en los informes personales.

Ley Orgánica 5/1992, de 29 de octubre.

De Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD: B.O.E. nº 262, de 31 de octubre de 1.992).

Ley 13/1995, de 21 de abril,

De regulación del uso de informática en el tratamiento de datos personales por la Comunidad de Madrid. (Boletín Oficial de la Comunidad de Madrid, 4 de mayo de 1995).

Ley 13/1997 de 16 de junio.

Por la que se introducen modificaciones en la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid (BOCM nº 148, de 24 de junio de 1997)

Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

Transposición de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997. (B.O.E. nº 99, de 25 de abril de 1998)

En su artículo 50 nos habla de la protección de los datos de carácter personal y de la garantía de los mismos por los operadores que presten servicios de telecomunicaciones.

Ley Orgánica 15/1999, de 13 de diciembre.

de Protección de Datos de Carácter Personal. (B.O.E nº 298, martes 14 de diciembre de 1999)

Ley 8/2001, de 13 de julio.

De Protección de Datos de Carácter Personal en la Comunidad de Madrid

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley 47/2002, de 19 de diciembre.

De reforma de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, para la transposición al ordenamiento jurídico español de la Directiva 97/7/CE en materia de contrato a distancia, y para la adaptación de la ley a diversas Directivas Comunitarias (B.O.E. 304/44759 de 20 de diciembre de 2002)

Ley 12/2003, de 21 de mayo.

De prevención y bloqueo de la financiación del terrorismo (B.O.E. 122/19490 de 22 de mayo de 2003)

Ley 62/2003, de 30 de diciembre.

De medidas fiscales, administrativas y del orden social (B.O.E. 313/46874 del 31 de diciembre de 2003)

4.5.2. Delitos informáticos.

Ley Orgánica 10/1995, de 23 de noviembre.

Del Código Penal (B.O.E. nº 281, de 24 de noviembre de 1995; corrección de errores en B.O.E. nº 54, de 2 de marzo de 1996)

4.5.3. Dinero Electrónico.

Ley 44/2002, de 22 de noviembre.

De Medidas de Reforma del Sistema Financiero (B.O.E. num. 281 del 23 de noviembre de 2002)

Ley 16/1985 del Patrimonio Histórico Español.

Art. 49.- Define documento como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos.

Ley del Patrimonio Histórico de 25 de junio de 1988, en la que se define en su artículo 49 el documento como “toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos”.

Ley 24/1988 de Mercado de Valores de 28 de Julio de 1988 que permite las anotaciones en cuenta por procedimientos electrónicos para la representación de valores. (B.O.E. 29 de julio de 1988).

Ley 19/1989, de 25 de julio que modifica el artículo 38 de la Ley de Sociedades Anónimas, permite las anotaciones en cuenta.

Ley Orgánica 7/1992, de 20 de noviembre (B.O.E. nº 280 de 21-11-1992) de Modificaciones de la Ley del Registro Civil, en su Art. 33 indica que "las referencias a los libros y asientos regístrales, podrán entenderse referidas a los ficheros automatizados de datos regístrales y al tratamiento de estos"

Ley 37/1992 de 28 de diciembre de 1992 del I.V.A., abre la posibilidad a la admisión de la factura electrónica a efectos fiscales. En su artículo 88 admite y reconoce la factura electrónica por vía telemática a efectos fiscales, al decir que "la repercusión del impuesto deberá efectuarse mediante factura o documento análogo, que podrán emitirse por vía telemática, en las condiciones y con los requisitos que se determinen reglamentariamente".

Ley General Tributaria 25/1995 de 20 de julio , en su artículo 142 indica que, los libros y la documentación del sujeto pasivo, incluidos los programas informáticos y archivos con soporte magnético que estén relacionados con el hecho imponible, serán examinados por la inspección, pudiendo incautarse de los archivos y equipos electrónicos que puedan contener la información pertinente. (B.O.E. de 22 de julio de 1995)

Ley 66/1997 de 30 de diciembre.

De Medidas Fiscales, Administrativas y del Orden Social, que autoriza al Ministerio de Economía y Hacienda para que determine mediante Orden los supuestos y condiciones en que las grandes empresas habrán de presentar por medios telemáticos sus declaraciones, declaraciones-liquidaciones, autoliquidaciones o cualesquiera otros documentos exigidos por la normativa tributaria. Establece que la Fábrica Nacional de Moneda y Timbre (FNMT) cumplirá la función de "Servicio de Certificación" para las Administraciones Públicas. En su artículo 81 faculta a la Fabrica Nacional de Moneda y Timbre para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos entre las Administraciones y entre éstas y los particulares.

Ley 4/1999 de 13 de enero, que modifica a la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Dispone que los Registros de las Administraciones deberán llevarse en soportes informáticos

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley 44/2002, de 22 de noviembre.

De Medidas de Reforma del Sistema Financiero (B.O.E. num. 281 del 23 de noviembre de 2002)

Ley 53/2002, de 30 de diciembre.

De Medidas Fiscales, Administrativas y del Orden Social (B.O.E. de 31 de diciembre de 2002)

4.5.4. Firma Electrónica.

Ley 66/1997 de 30 de diciembre.

De Medidas Fiscales, Administrativas y del Orden Social, que autoriza al Ministerio de Economía y Hacienda para que determine mediante Orden los supuestos y condiciones en que las grandes empresas habrán de presentar por medios telemáticos sus declaraciones, declaraciones-liquidaciones, autoliquidaciones o cualesquiera otros documentos exigidos por la normativa tributaria. Establece que la Fábrica Nacional de Moneda y Timbre (FNMT) cumplirá la función de "Servicio de Certificación" para las Administraciones Públicas. En su artículo 81 faculta a la Fabrica Nacional de Moneda y Timbre para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos entre las Administraciones y entre éstas y los particulares.

Ley 55/1999, de 29 de diciembre.

De medidas fiscales, administrativas y del orden social (B.O.E. 312/46095 del 30 de diciembre de 1999).

Ley 34/2002, de 11 de julio.

De servicios de la sociedad de la información y de comercio electrónico.

Ley 53/2002, de 30 de diciembre.

De medidas fiscales, administrativa y del orden social (B.O.E. 313/46086 del 31 de diciembre de 2002).

Ley 59/2003, de 19 de diciembre, de firma electrónica. (B.O.E. 304/45329)

4.5.5. Medidas de seguridad.

Ley Orgánica 15/1999, de 13 de diciembre.

De Protección de Datos de Carácter Personal. (B.O.E nº 298, martes 14 de diciembre de 1999)

PROTECCIÓN JURÍDICA DEL SOFTWARE Y DE LAS BASES DE DATOS.

Ley 11/1986, de 20 de marzo, sobre Patentes.

Art. 42. No se considerarán invenciones, en particular:....c) Los planes, reglas y métodos para el ejercicio de actividades intelectuales para juegos o para actividades económico-comerciales, así como los programas de ordenadores.
Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual, artículos 95, 96, 97, 98, 99 y 100. (B.O.E. nº 275, de 17 de noviembre de 1987)

Ley 11/1988, de 3 de mayo.

De protección jurídica de topografías de productos semiconductores. (B.O.E. nº 11.074 de 5 de mayo de 1988).

Ley 16/1993, de 23 de diciembre sobre la protección jurídica de programas de ordenador; objeto, titularidad, beneficiarios, restricciones, excepciones, duración de la protección, infractores, acciones de protección.

Ley 27/1995, de 11 de octubre, de incorporación al Derecho español de la Directiva 93/98/CE, del Parlamento y del Consejo, relativa a la armonización del plazo de protección del derecho de autor.

Ley Orgánica 10/1995, de 23 de noviembre.

Del Código Penal (B.O.E. nº 281, de 24 de noviembre de 1995; corrección de errores en B.O.E. nº 54, de 2 de marzo de 1996).

Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

4.5.6. Telecomunicaciones y protección de datos de carácter personal en dicho sector.

Ley 31/1987 de 18 de diciembre de 1.987 de Ordenación de las telecomunicaciones. (L.O.T.).

Ley 42/1995, de 22 de diciembre, de Telecomunicaciones por Cable.

Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

Transposición de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997. (B.O.E. nº 99, de 25 de abril de 1998). En su artículo 50 nos habla de la protección de los datos de carácter personal y de la garantía de los mismos por los operadores que presten servicios de telecomunicaciones.

Ley Orgánica 15/1999, de 13 de diciembre.

De Protección de Datos de Carácter Personal. (B.O.E nº 298, martes 14 de diciembre de 1999).

Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social: Procedimiento de asignación de nombres y direcciones de dominio de Internet bajo el código de país correspondiente a España. Modificación de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, entidad pública empresarial Redes.

Ley 32/2003, de 3 de noviembre.

General de Telecomunicaciones (B.O.E. del 4 de noviembre de 2003)

4.6. Estados Unidos.

Estados un idos es un país que actualmente lleva el liderazgo de transacciones de comercio electrónico y se puede obtener con facilidad los medios necesarios para cometer irregularidades en internet, las personas con diversas motivaciones se han aprovechado de sus conocimientos u habilidades informáticas para cometer las faltas; ante esta situación en EEUU se han elaborado leyes, normativas y reglamentos que permiten regular el uso de internet son a nivel país y de cada estado. Cabe mencionar que con los hechos del 11 de septiembre del 2001, las medidas de seguridad se incrementan y ahora las sanciones son mas estratégicas.

A continuación se mencionan algunas leyes que regulan los delitos informaticos, dentro de este país.

UTAH.

En mayo de 1995 fue emitida la primera ley sobre firmas digitales por el estado de Uthah, y es conocida como Utah Digital Signature Act.

ABA.

El comité de seguridad del la información, de la división del comercio electrónico, de las American Bar Asociation, emitió, en agosto de 1996, la Gía de Firmas Digitales.

4.6.1. Electronic Communications Privacy Act (ECPA).

Ley de privacidad en las comunicaciones electrónicas, vigente desde 1986.

El código de EE.UU. define a las comunidades electrónicas como “cualquier transferencia de muestras, de señales, de la escritura, de imágenes, de sonidos, de datos, o de la inteligencia de cualquier naturaleza transmitida en entero o en parte por un alambre, un radio, foto electrónica o el sistema óptico de la foto que afecta comercio de un estado a otro o extranjero.

La ECPA prohíbe el acceso ilegal y ciertos accesos del contenido de la comunicación, además evita que las entidades del gobierno requieran el acceso de comunicaciones electrónicas sin procedimiento apropiado.

4.6.2. Acta Federal de Abuso Computacional.

Ley federal de abuso computacional de 1994, modifico la ley vigente de 1986.

Tiene la finalidad de eliminar a los argumentos hiper-tecnicos acerca de que es y que no es un virus, un gusano, un caballo de Troya y en el que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas.

Especifica la diferencia del contagio del virus realizado con intención y sin intención.

La ley constituye un acercamiento mas responsable al creciente problema de los virus informáticos, describe la forma en que se comete el delito de tal forma deja abierto para la nueva era de los ataques tecnológicos a los sistemas informáticos.

Diferencia los niveles de delito: estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos del acceso a sistemas informáticos.

4.6.3. Childre`s Oline Privacy Protection Act (COPPA).

Vigente desde 28 de octubre de 1998.

Un operador del web site o de un servicio en línea con información dirigida a los niños tiene la responsabilidad de lo que publica si sabe que los visitantes son niños menores de 13 años.

Si el web site recoge información del menor, deberá indicarse el uso de la información, permitir mecanismos para que los padres conozcan lo que el menor ha ingresado, y a su vez dar la posibilidad de realizar mantenimiento a dicha información.

4.6.4. Anty-Cybersquating Consumer Protection Act (ACCPA).

Ley de protección al consumidor Anty-Cybersquating vigente desde el 29 de noviembre de 1999.

Los dueños legítimos de marcas registradas pueden tomar acciones contra cualquier persona que, con un intento de mala fe y de beneficiarse registren o utilicen un nombre de dominio idéntico o similiar a la marca registrada.

La lley se aplica a todos los nombres de dominio a partir de la fecha de vigencia de la ley.

4.6.5 Gramm Leach Biley.

Vigente desde el 12 de noviembre de 1999.

Establecen nuevas obligaciones con respecto al a privacidad financiera.

La ley permite a los clientes de bancos, corredores de bolsas, compañías de tarjetas de crédito, compañías de seguros que se notifique, si no desean que la información sobre su historial financiera sea vendida a terceros.

La ley estableció la reserva federal como el supervisor de las actividades financieras.

4.6.6. Electronic Signature in Global and National Commerce (ESGNC)

Ley de firmas electrónicas en el comercio global y nacional, vigente desde el 11 de octubre del 2000.

Es una ley que reconoce el E-Commerce como transacciones legales y el uso de las firmas electrónicas al igual que las firmas manuscritas.

La ley proporciona solamente un marco jurídico para los contratos electrónicos, se evito detallar lo que constituye la firma electrónica, por que no se podía predecir la

tecnología con la que se publicaría. Solo se define en teoría, la firma digital es "cualquier tipo de señales electrónicas", esto permite libertad en las leyes de los diferentes estados de EE.UU.

4.6.7. USA Patriot Act (UPA).

Ley patriota de estados unidos vigente desde octubre 24 del 2001.

Es una ley antiterrorista la cual fue promovida por el presidente Geoge Bush, esta facilita a las autoridades federales la intervención del correo electrónico las conversaciones telefónicas, los mensajes de voz y hasta el espionaje de las rutas de navegación seguidas en internet.

Condena el acceso no autorizado a las computadoras con penas de hasta cinco años de prisión.

4.6.8. Cyber Securuty enhancement Act (CSEA).

Ley de perfeccionamiento del a cyber Seguridad vigente desde diciembre 13 del 2001.

Es una ley de seguridad la cual tratará de clasificar los puntos de la Patriot Act, en donde otorga al gobierno la potestad de incrementar las penas para los crímenes relacionados con hacking, fraudes informáticos y la publicidad de dispositivos ilegales.

Proporciona directrices para determinar las sentencias, diferenciando los delitos cometidos para lucro personal de aquellos que puedan afectar a la defensa y la seguridad nacional.

Amplia el poder de la policía para intervenir telecomunicaciones sin necesidad de contar con una orden judicial y obliga a los ISPs a facilitar información sobre la navegación o el contenido de los correos electrónicos en caso de investigaciones policiacas.

4.6.9.. Cyber Security Reseach and Developmet Act (CSRDA).

Ley sobre investigacion y desarrollo de la seguridadcibernetica vigente desde abril 17 del 2002.

Ley que destina 880 millones para que las empresas privadas junto con las universidades se dediquen a la investigación de la seguridad informática. Nacional Sciencie foundation creará nuestros centros de investigación que conbatan el problema de seguridad de las computadoras del gobierno y privadas, además

otorgar becas y subsidios a instituciones educativas de grado e instituciones universitarias locales.

4.6.10. Controling Assault of Non-Solicted Pornography and Marketing (Can-Spam Act).

Vigente desde el 17 de mayo del 2002.

La ley establece estándares para controlar los envíos macivos, define al Spam como el e-mail que no incluye la dirección del remitente y no ofrece la posibilidad de darse de baja.

Lal ley obliga a los mensajeros no solicitados a estar bien etiquetados (remitentes, asuntos y encabezados correctos) e incluir instrucciones para darse de baja fácilmente, y permitir a los ISPs emprender acciones legales contra los infractores.

CAPITULO 5

COMERCIO ELECTRÓNICO

LEGISLACIÓN EN MÉXICO

Luego de haber tocado los principales aspectos contextuales y teóricos relacionados con el comercio electrónico, los delitos informáticas que mas lo envuelven, nos enfocaremos al diagnostico del estado legislativo del mismo. Comenzando con el Derecho en cual surge como un medio efectivo para regular la conducta del hombre en sociedad. Pero la sociedad no es la misma en cada uno de los lugares del planeta ni es la misma en cada momento de la historia. La sociedad evoluciona y cambia a través del avance de la ciencia y la tecnología.

El Derecho regula la conducta y los fenómenos sociales a través de leyes. El proceso de creación e inserción de las leyes a la vida de una comunidad jurídica determinada ya sea en un municipio, estado o país, suele ser lento, sobre todo en el sistema jurídico latino y particularmente en nuestro país México.

En los últimos años, las tecnologías de la Información y la Comunicación han revolucionado la vida social en muchos aspectos: científicos, comerciales, laborales, profesionales, escolares e incluso han cambiado los hábitos de entretenimiento y de interrelación de las personas al interior de nuestra vida familiar.

Es por ello que las leyes de nuestro país deben también ir a par con la tecnología regulando cada fenómeno o conducta lícita o ilícita en el ámbito jurídico existente, empezando porque los fenómenos y/o conductas tienen que manifestarse primero, ya que las leyes no pueden regular lo que aún no existe.

El desarrollo de la regulación sobre comercio electrónico ha tenido un importante avance en México. En los últimos años se han realizado reformas y adecuaciones a importantes ordenamientos en materia comercial y tecnológica.

5.1. Primeros antecedentes de las leyes en México.

1.- El día veintinueve de abril de mil novecientos noventa y nueve, según sesión celebrada por la H. Cámara de Diputados los secretarios dieron cuenta al Pleno de la Iniciativa de Decreto que reforma del Código de Comercio.

2.- El día quince de diciembre de mil novecientos noventa y nueve, los secretarios continuaron en el Pleno con la Iniciativa de Decreto que reforma y adiciona diversas disposiciones del Código Civil para el Distrito Federal en Materia

del Fuero Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles y del Código de Comercio, en materia de contratos electrónicos.

3.- El día veintidós de marzo del 2000, se continuo con los trabajos dando cuenta al Pleno de la Iniciativa de Decreto de reformas y adiciones a 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.

4.- Los miembros integrantes de las Comisiones de Justicia y de Comercio de la LVII Legislatura procedieron al estudio de las iniciativas aludidas, habiendo efectuado múltiples razonamientos sobre la aplicación de los conceptos contenidos en las iniciativas que se discuten, en los que se concluyó que deberían adoptarse los principios de la Ley Modelo de la Comisión de Naciones Unidas sobre el Derecho Mercantil Internacional y deberían realizarse algunas modificaciones en el Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal.

5.- En sesión celebrada el 22 de marzo del 2000, por la Cámara de Diputados, el Diputado Rafael Oceguera Ramos, del partido el PRI, presentó la Iniciativa de reformas y adiciones a diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código de Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor en Materia de Comercio Electrónico.

En esa misma fecha, la Presidencia de la Cámara de Diputados turnó esta iniciativa a las Comisiones de Justicia y de Comercio, para que dictaminaran, y a la Comisión de Distribución y Manejo de Bienes de Consumo y Servicios, para que rindiera opinión.

La Comisión de Distribución y Manejo de Bienes de Consumo y Servicios citó a reunión plenaria de comisión el día 29 de marzo del 2000, con el fin de dar a conocer la iniciativa y de efectuar la discusión respectiva.

La Iniciativa manifiesta la necesidad de adecuar el marco jurídico mexicano, para dar seguridad jurídica en el uso de medios electrónicos; para facilitar las transacciones por éstos, y para lograr la interacción global e integral de los campos en que se utilizan dichos medios.

5.2. Ley Modelo sobre Comercio Electrónico (UNCITRAL).

Las Naciones Unidas desde a partir de los años 60 ha estado dedicada a *facilitar* los procedimientos del comercio internacional, que desde comienzo de los años 90 se haya estado preocupado del llamado Intercambio Electrónico de Datos, conocido como "EDI" por su acrónimo en ingles, a través de la *CNUDM*I, mejor

conocida por su también acrónimo en ingles *UNCITRAL*, la cual Constituyó un Grupo de Trabajo (conocido como el Working Group en Comercio Electrónico) a fin de elaborar leyes modelos que den soporte legal a los mensajes electrónicos. Este esfuerzo ha producido la Ley Modelo de UNCITRAL sobre el Comercio Electrónico.

Para la redacción de esa Ley Modelo, UNCITRAL, tomó en cuenta las Reglas de 1990 sobre Conocimientos de Embarque Electrónico del Comité Marítimo Internacional, los programas de computación (software) especialmente diseñados para los *EDI,* hecho por la Conferencia Marítima y del Báltico y el proyecto de conocimiento de embarque para Europa, llamado proyecto BOLERO.

Posteriormente, el Proyecto de la Ley Modelo, se remitió para el examen de la Comisión en su sesión 29 en Nueva York., habiéndose previamente completado la redacción del resto de sus artículos generales y renombrado el mismo como Proyecto de Ley Modelo sobre "***COMERCIO ELECTRÓNICO***", a modo de ampliar su ámbito de aplicación no solo a los *EDI* sino a todas las formas de transmisión de mensajes electrónicos comerciales.

Por otra parte, habiéndose completado los primeros 17 artículos de la ley modelo, la Secretaría de UNCITRAL, a estado trabajando en el tema de las firmas digitales, donde actualmente ya cuenta con la ley que rige esta problemática.

5.2.1. Breve análisis de la ley modelo de UNCITRAL sobre comercio electrónico.

En la primera parte de la Ley Modelo, se establecen principios generales con el fin de dar el soporte legal al comercio electrónico en aquellos países que promulguen las leyes modelos. Estas serían extremadamente sobre Conocimientos de Embarques Electrónicos. Sin embargo, tales artículos no tienen aplicación directa al comercio marítimo, pero son esenciales si el comercio marítimo se realiza en un ambiente electrónico.

En la segunda parte del proyecto de ley, compuesto de dos artículos (16 y 17) referidos a los contratos de transporte de mercancías, se provee la base legal para la negociabilidad de los documentos de transporte electrónicos, redactados de forma tal que sean aplicables a cualquier tipo de transporte.

El Capítulo I, contiene las provisiones generales: ámbito de aplicación (artículo 1), definiciones (artículo 2), interpretación (artículo 3) y modificación mediante acuerdo (artículo 4).

La característica única de este capítulo es la creación del término *"mensaje de datos*" usado para diferenciar el cruce de comunicación con las otras formas de aviso, información y mensajes tradicionales.

El Capítulo II, se refiere a la aplicación de los requisitos legales de los ***"mensajes de datos"***, comenzando con su reconocimiento jurídico, al señalar que no se le negará efectos jurídicos, validez o fuerza probatoria por la sola razón de esté en forma de *mensaje de datos*. Este reconocimiento es necesario, esencial y de sentido común, por la razón de que el comercio electrónico es un concepto nuevo, lo que probablemente causara resistencia a su aceptación en lugar de las formas tradicionales, siendo de invalorable ayuda para la implementación de los conocimientos de embarque electrónicos.

Los artículos 6 al 8, sobre escrito, firma y original, respectivamente, proporcionan la llamada "***equivalencia funcional"***. Si hay un requerimiento legal para una de esas categorías, esos requerimientos pueden ser satisfechos por el *equivalente funcional* del mensaje de datos.

El problema de la admisibilidad y la fuerza probatoria de los "***mensajes de datos",*** está solucionado en aquellas jurisdicciones donde se ha adoptado la llamada ***"regla de la mejor prueba"***, conforme a la cual no se dará aplicación a regla alguna de la prueba un *mensaje de datos* por razón de no haber sido presentado en su forma original, de ser ese mensaje *la mejor prueba* que quepa razonablemente esperar de la persona que la presenta.

Es importante, sin embargo, señalar que, tal como se mencionara durante las deliberaciones del Grupo de Trabajo, probablemente habrán casos, especialmente en los países de derecho continental o civil, en donde su derecho procesal no ha admitido esa regla de prueba, por lo que sus tribunales se encontrarán en dificultad en admitir el valor probatorio de los *mensajes de datos* generados por computadoras, en lugar de los documentos escritos en papel, tradicionalmente admitidos.

El artículo restante en este capítulo, señala los requisitos para la conservación o el archivo de los mensajes de datos. Para que el mensaje de datos, sea confiable, es esencial que sean conservados o archivados sin que se le pueda hacer modificación alguna durante largos períodos de tiempo. Igualmente, es importante que, durante ese largo período de tiempo, puedan ser accesibles.

El capítulo III prevé los protocolos de comunicación de los mensajes de datos; esto es la formación y validez de los contratos a través de los *"mensajes de datos",* su reconocimiento por las partes, su atribución, su acuse de recibo y su tiempo y lugar del envío y recepción. Mientras que estos artículos no establecen normas directa y necesariamente aplicables a los conocimientos de embarque electrónico, podrían ser útiles para definir los derechos y responsabilidades que nacen de los *mensajes de datos*, a los efectos de la aplicación voluntaria de las Reglas de París del CMI.

La **segunda parte** de la Ley Modelo, está dirigido a la regulación del comercio electrónico en áreas específicas, la primera de las cuales es el transporte de mercancías. En el artículo 16, (Actos relacionados con el Transporte de Mercancías), se describen y especifican los diversos actos regulados, que pudieran haber sido registrados en fragmentos separados de documentos escritos a medida que la mercancía es procesada para su transporte. Esto es necesario para asegurar un tratamiento similar a todos los *mensajes de datos* relacionado con el transporte, en lugar de sólo darle aceptación a los mensajes de actos importantes, teniendo que acudir a documentos escritos para los actos circunstanciales. Los actos se entienden aplicables a cualquier modo de transporte, y no sólo al marítimo.

El Artículo 17, (Documentos de Transporte), establece *la singularidad* del *mensaje de datos, a*l señalar que cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más *mensajes de datos,* siempre que se emplee un método fiable para garantizar la *singularidad* de *ese mensaje o esos mensajes de datos*.

Con sujeción a ese requisito de la *singularidad,* en los casos que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más *mensajes de datos*.

En consecuencia, el requisito de la *singularidad* del *mensaje de datos,* es esencial para la transferibilidad de derechos a través de *mensajes de datos*, sin lo cual, las Reglas de París del CMI, o cualquier otro esquema voluntario para transferir derechos sobre las mercaderías no podría funcionar.

El párrafo 17 hace referencia a la manera de valorar del nivel de *fiabilidad* requerido para el reconocimiento de tales *mensajes de datos*, mientras el párrafo 17 reconoce que, mientras existen instancias donde las partes tienen que volver a

los conocimientos de embarque por escrito o que consten en un papel, ambos sistemas no pueden ser usados al mismo tiempo, de lo contrario la ***singularidad*** podría ser destruida. Consecuentemente, antes de que un conocimiento de embarque por escrito o que consten de papel pueda ser emitido, el uso de los *mensajes de datos* debe ser terminado y tal hecho registrado en el conocimiento de embarque escrito en papel que se emita.

El párrafo 17 asegura que si una convención sobre responsabilidad del transportista de mercaderías por agua, como las Reglas de La Haya, rige obligatoriamente un conocimientos de embarque por escrito o que consten de papel, al contrato de transporte creado por el *mensaje de datos,* no dejará de aplicarse dicha convención.

Actualmente han realizado la ley que regula la firma digital ya que esta 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.

Basándose en 12 artículos los cuales en resumen dicen lo siguiente:

Que esta ley será aplicable a todos los casos que utilicen firmas electrónicas, Se presentan las definiciones de Firma Electrónica, Certificado, Mensaje de datos, firmante, prestador de servicios de certificación y Parte que confía. Tendrá igualdad de tratamiento de las tecnológicas para la firma, Se tendrá en cuenta el origen internacional, Modificación mediante un acuerdo, Cumplimiento del requisito de firmas; donde tendrá que ser cumplido por medio de mensaje de datos que sea fiable. Proceder del firmante, Fiabilidad, Reconocimiento de certificados y de firmas electrónicas extranjeras.

5.3. Reforma al código de comercio.

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.

"El congreso de los estados unidos mexicanos, decreta”:

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 180.- Se describe los actos mercantiles o de comercio, la cual la Secretaria de Comercio será quien 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. Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral.

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.

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

I.- Aplicar las disposiciones 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, según 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.

Artículo 21.- Existirá un folio electrónico por cada comerciante o sociedad.

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:

a) Recepción, física o electrónica de una forma precodificada, acompañada con la inscripción, pago de los derechos, generación de una boleta de ingreso y del número de control progresivo.

b) Análisis 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.

c) Autorización de la inscripción en la base de datos mediante la firma electrónica del servidor, con lo cual se generará o adicionará el folio mercantil electrónico correspondiente.

d) Emisión de una boleta de inscripción que será entregada física o electrónicamente.

Artículo 21 bis 1.- La preferencia 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.

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.

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.

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, según los lineamientos que emita la Secretaría.

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.

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, el monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal.

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

I. El acto o contrato que en ellos se contenga no sea de los que deben inscribirse.

II. Esté en manifiesta contradicción con los contenidos de los asientos registrales preexistentes, o

III. 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.

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.

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.

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.

5.3.1. Comercio en General (Libro Segundo).

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.

5.3.2. Comercio Electrónico (Titulo II).

Artículo 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.

Artículo 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.

II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Artículo 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.

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.

Artículo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un comprobante 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 comprobante respectivo.

Artículo 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 accesibles 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 consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 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."

5.3.4 Firma Electrónica.

Viernes 29 de agosto de 2003 DIARIO OFICIAL 1.

Secretaria de Economía decreto, por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica.

Artículo Único: Se reforman los artículos 89, 90, 91, 92, 93, 94, 95, 96, 97, 98,99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113 y 114. Se adicionan los artículos 89 bis, 90 bis, 91 bis, 93 bis. Se adicionan los Capítulos Primero, Segundo, Tercero y Cuarto al Título Segundo, denominado del Comercio Electrónico, correspondiente al Libro Segundo, todos del Código de Comercio, para quedar de la siguiente manera:

Título Segundo del Comercio Electrónico.

Capítulo I (De los Mensajes de Datos).

Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en

relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:

Certificado: Todo Mensaje de Datos u otro registró que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Secretaría: Se entenderá la Secretaría de Economía.

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

Artículo 89 bis.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Artículo 90.- Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:

I. Por el propio Emisor;

II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos.

III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.

Artículo 90 bis.- Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por lo tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia, cuando:

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste.

II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía, resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio.

Lo dispuesto en el presente artículo no se aplicará:

I. A partir del momento en que el Destinatario o la Parte que Confía, haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia.

II. A partir del momento en que el Destinatario o la Parte que Confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor.

La identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas.

Artículo 91.- Salvo pacto en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará como sigue:

I. Si el Destinatario ha designado un Sistema de Información para la recepción de Mensajes de Datos, ésta tendrá lugar en el momento en que ingrese en dicho Sistema de Información.

II. De enviarse el Mensaje de Datos a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario recupere el Mensaje de Datos.

III. Si el Destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el Mensaje de Datos ingrese a un Sistema de Información del Destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el Sistema de Información esté ubicado en un lugar distinto de donde se tenga por recibido el Mensaje de Datos conforme al artículo 94.

Artículo 91 bis.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del Emisor o del Intermediario.

Artículo 92.- En lo referente a acuse de recibo de Mensajes de Datos, se estará a lo siguiente:

I. Si al enviar o antes de enviar un Mensaje de Datos, el Emisor solicita o acuerda con el Destinatario que se acuse recibo del Mensaje de Datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del Destinatario, automatizada o no, o

b) Todo acto del Destinatario, que baste para indicar al Emisor que se ha recibido el

Mensaje de Datos.

II. Cuando el Emisor haya indicado que los efectos del Mensaje de Datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el Mensaje de Datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el Emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del Mensaje de Datos;

III. Cuando el Emisor haya solicitado o acordado con el Destinatario que se acuse recibo del Mensaje de Datos, independientemente de la forma o método determinado para efectuarlo, salvo que:

a) El Emisor no haya indicado expresamente que los efectos del Mensaje de Datos estén condicionados a la recepción del acuse de recibo, y

b) No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio.

El Emisor podrá dar aviso al Destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el Emisor reciba acuse de recibo del

Destinatario, se presumirá que éste ha recibido el Mensaje de Datos correspondiente;

IV. Cuando en el acuse de recibo se indique que el Mensaje de Datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

Artículo 93.- Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.

Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.

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.

Artículo 93 bis.- Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos:

I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y

II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado

de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 94.- Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:

I. Si el Emisor o el Destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y

II. Si el Emisor o el Destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

Artículo 95.- Conforme al artículo 90, siempre que se entienda que el Mensaje de Datos proviene del Emisor, o que el Destinatario tenga derecho a actuar con arreglo a este supuesto, dicho Destinatario tendrá derecho a considerar que el Mensaje de Datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El Destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el Mensaje de Datos recibido.

Se presume que cada Mensaje de Datos recibido es un Mensaje de Datos diferente, salvo que el Destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo Mensaje de Datos era un duplicado.

Capítulo II de Las Firmas

Artículo 96.- Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho

requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante.

II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante.

III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma.

IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

Artículo 98.- Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables

que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 99.- El Firmante deberá:

I. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;

II. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;

III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones q ue

haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas.

El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y

IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

CAPÍTULO III

De Los Prestadores De Servicios De Certificación

Artículo 100.- Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría:

I. Los notarios públicos y corredores públicos;

II. Las personas morales de carácter privado, y

III. Las instituciones públicas, conforme a las leyes que les son aplicables.

La facultad de expedir Certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o

no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

Artículo 101.- Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;

II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación;

III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado, y

IV. Cualquier otra actividad no incompatible con las anteriores.

Artículo 102.- Los Prestadores de Servicios de Certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 100 puedan ser Prestadores de Servicios de Certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los Prestadores de Servicios de Certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación; **II.** Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;

III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;

IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de

la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;

VI. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y

VII. Registrar su Certificado ante la Secretaría.

B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Artículo 103.- Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.

Artículo 104.- Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:

I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;

II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;

III. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;

IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo

autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;

V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;

VI. En el caso de cesar en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;

VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;

VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y

IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:

a) La identidad del Prestador de Servicios de Certificación;

b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;

c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;

d) El método utilizado para identificar al Firmante;

e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;

f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;

g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y

h) Si se ofrece un servicio de terminación de vigencia del Certificado.

Artículo 105.- La Secretaría coordinará y actuará como autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en este Capítulo.

Artículo 106.- Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores, se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras.

Artículo 107.- Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:

I. Verificar la fiabilidad de la Firma Electrónica, o

II. Cuando la Firma Electrónica esté sustentada por un Certificado:

a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y

b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

Artículo 108.- Los Certificados, para ser considerados válidos, deberán contener:

I. La indicación de que se expiden como tales;

II. El código de identificación único del Certificado;

III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;

IV. Nombre del titular del Certificado;

V. Periodo de vigencia del Certificado;

VI. La fecha y hora de la emisión, suspensión, y renovación del Certificado;

VII. El alcance de las responsabilidades que asume el Prestador de Servicios de

Certificación, y

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Artículo 109.- Un Certificado dejará de surtir efectos para el futuro, en los siguientes casos:

I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del Certificado podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación;

II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado;

III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado;

IV. Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe, y

V. Resolución judicial o de autoridad competente que lo ordene.

Artículo 110.- El Prestador de Servicios de Certificación que incumpla con las

obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 111.- Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Artículo 112.- Las autoridades competentes harán uso de las medidas legales necesarias, incluyendo el auxilio de la fuerza pública, para lograr la ejecución de las sanciones y medidas de seguridad que procedan conforme a esta Ley. Incluso, en los procedimientos instaurados se podrá solicitar a los órganos competentes la adopción de las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 113.- En el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los Certificados que haya expedido pasarán, para su administración, a otro Prestador de Servicios de Certificación, que para tal efecto señale la Secretaría mediante reglas generales.

CAPÍTULO IV.

Reconocimiento de certificados y firmas electrónicas extranjeros

Artículo 114.- Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica.

II. El lugar en que se encuentre el establecimiento del Prestador de Servicios de Certificación o del Firmante.

Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.

A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de Firmas Electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

TRANSITORIOS.

Primero. El presente Decreto comenzará su vigencia 90 días después de su publicación en el Diario Oficial de la Federación.

Segundo. Dentro del plazo de 90 días posteriores a la entrada en vigor del presente Decreto, el Ejecutivo emitirá las reglas generales a que se refieren las presentes disposiciones.

Tercero. En lo que se refiere al artículo 102, dentro de los doce meses siguientes a la entrada en vigor de las reglas generales a que se refiere el artículo anterior, el plazo de 45 días a que se refiere el mismo, será de 90 días.

Cuarto. Por lo que se refiere al artículo 106, el Banco de México, en el ámbito de su competencia, regulará y coordinará a la autoridad registradora central, registradora y certificadora, de las instituciones financieras y de las empresas mencionadas que presten servicios de certificación.

México, D.F., a 8 de abril de 2003.- Dip. Armando Salinas Torre, Presidente.- Sen. Enrique Jackson Ramírez, Presidente.- Dip. Adela Cerezo Bautista, Secretaria.- Sen. Sara I. Castellanos Cortés, Secretaria.- Rúbricas".

En cumplimiento de lo dispuesto por la fracción I del Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos, y para su debida publicación y observancia,

5.4. Reforma al código civil federal.

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.

"El congreso de los estados unidos mexicanos, decreta:

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:

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.

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 accesibles 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."

5.5. Reforma a la Ley Federal de Protección al Consumidor.

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.

"El congreso de los estados unidos mexicanos, decreta:

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.- Fracción 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.- Fracción 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;

Capitulo VIII BIS.

De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología

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:

I. 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.

II. 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.

III. 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.

IV. 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.

V. 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.

VI. 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.

VII. 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.

5.6. Reforma al Código Federal de Procedimientos Civiles.

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.

El congreso de los estados unidos mexicanos, decreta:

Artículo 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."

5.7. Acuerdo que establece los lineamientos para la operación del Registro Público de Comercio. Sistema Integral de Gestión Registral.

Herminio Blanco Mendoza, Secretario de Comercio y Fomento Industrial, con fundamento en los artículos 18, 20 bis, 30 bis y 32 bis del Código de Comercio; 34 fracción XIV de la Ley Orgánica de la Administración Pública Federal, y 5 fracción XVI del Reglamento Interior de la Secretaría de Comercio y Fomento Industrial, y

Considerando:

Que el Plan Nacional de Desarrollo 1995-2000 establece entre sus objetivos la reforma de gobierno y la modernización de la administración pública, y la consolidación de un régimen de seguridad jurídica sobre la propiedad y posesión de los bienes y las transacciones de los particulares.

Acuerdo que establece los lineamientos para la operación del registro publico de comercio.

Artículo 1.- El presente Acuerdo tiene por objeto establecer los lineamientos para la adecuada operación del Registro Público de Comercio, a que se refieren los artículos 18, 20 bis, 30 bis y 32 bis del Código de Comercio.

Artículo 2.- Para los efectos del presente Acuerdo se entenderá por:

I. Secretaría, a la Secretaría de Comercio y Fomento Industrial;

II. Registro, al Registro Público de Comercio;

III. Oficina de la entidad, la que integra una base de datos con la información registral de toda una entidad federativa, a la que estarán interconectadas las oficinas distritales, en caso de que éstas existan, y que generalmente se encuentra en la capital y está interconectada a la base de datos central.

IV. Oficinas distritales, también llamadas regionales, delegaciones o subdelegacionales o cualquier otra denominación que prevea la normatividad local, a las que prestan el servicio de Registro Público de Comercio en el interior de la entidad federativa e interconectadas a la base de datos de la oficina de la entidad;

V. Sistema, al programa informático establecido por la Secretaría, en términos del artículo 20 del Código de Comercio, para la operación del Registro Público de Comercio denominado Sistema Integral de Gestión Registral (SIGER).

VI. Código, al Código de Comercio.

VII. Reglamento, al Reglamento del Registro Público de Comercio.

VIII. Manuales del Sistema, los manuales de instalación, del usuario, técnico, de instalación del Web, de operación del Web, y de estrategias de instrumentación, mismos que se entregan al gobierno de cada entidad federativa conjuntamente con el Sistema, así como las actualizaciones que realice a los mismos la Dirección General de Normatividad Mercantil.

Articulo 3.- El equipo de Computo y los programas informáticos necesarios para la prestación del servicio registral a través del Sistema serán determinados en los convenios de coordinación que se suscriban en términos del artículo 18 del Código de Comercio, de acuerdo a los volúmenes de operaciones que maneje, el número

de personal y a la planeación para la implementación del procedimiento registral automatizado.

Articulo 4.- El Sistema se compone de los subsistemas siguientes:

Subsistema de Registro, Subsistema de Consulta, Subsistema de Certificación, Subsistema de Control de Gestión y Subsistema de Captura del Acervo Histórico.

El sistema cuenta con un módulo Web, a través del cual se operan vía remota los subsistemas de registro y de consulta, el cual podrá ser utilizado por los fedatarios públicos autorizados para tal efecto.

Artículo 5.- La operación de los subsistemas de Registro, Consulta y Certificación, en sus distintas fases estará a cargo del número de usuarios necesarios, previa autorización del responsable de la oficina del Registro, los cuales serán identificados por su nombre, clave, contraseña y especificación de sus derechos dentro del Sistema de acuerdo a la función que desempeñen en el proceso registral.

Los usuarios del sistema deberán desempeñar alguna de las funciones siguientes: Recepcionista, Analista, Calificador, Archivista y Responsable de entrega.

Artículo 6.- El responsable de la oficina del Registro verificará que se lleve a cabo la función de administración del sistema, a través de la cual se realizará el respaldo de la información y la replicación diaria a la base de datos central, en términos de los manuales del Sistema; deberá además encargarse de la seguridad física e informática del sistema, así como la ejecución de las actividades y funciones de los usuarios en los términos autorizados por el propio responsable.

Artículo 7.- Las consultas de los asientos registrales resguardados en la base de datos de la entidad, se llevará a cabo de acuerdo a las modalidades siguientes:

I. Consulta local, la que se realiza en la oficina registral a través de las terminales que para tal efecto sean habilitadas.

II. Consulta remota, la que podrán efectuar los usuarios autorizados para acceder vía Internet a la base de datos ubicada en la entidad federativa de que se trate a través del módulo Web.

Artículo 8.- El Sistema para su correcta operación requiere de diversos catálogos. Los correspondientes a fedatarios, giros, formas, municipios, estados y monedas, se rigen por los criterios establecidos en los manuales del Sistema y por los que,

en su caso, defina la Secretaría a través de la Dirección General de Normatividad Mercantil.

Artículo 9.- Para los casos de error material o de concepto, previstos en el artículo 32 del Código, el proceso de rectificación a que se refiere su artículo 32 bis, se efectuará cuando proceda mediante el uso de una forma precodificada para tal efecto, la que una vez firmada electrónicamente, pasará a formar parte del folio mercantil correspondiente e inscrito en la base de datos del Registro, se tendrá por rectificado el error del que se trate. Fuera de esos supuestos los asientos registrales de las bases de datos del Registro realizados en términos de lo dispuesto por el Código, no pueden ser modificados.

Artículo 10.- Para efecto de lo dispuesto en el artículo 30 bis del Código de Comercio, la certificación de los medios de identificación electrónica lo hará la Secretaría, por conducto de la Dirección General de Normatividad Mercantil. Dicha certificación se hará a través de la expedición de certificados digitales u otros medios de identificación que determine dicha Dirección General. Tratándose de certificados digitales, deberán contener al menos lo siguiente:

Nombre del titular, Dirección, Vigencia, que no será mayor a un año a partir de su expedición, Clave pública, Nombre de la autoridad expedidora y Los demás que determine la Secretaría, por conducto de la Dirección General de Normatividad Mercantil.

El certificado digital raíz lo tendrá la Dirección General de Normatividad Mercantil de la Secretaría, la que expedirá los certificados digitales u otros medios de identificación a cada uno de los responsables de las oficinas del Registro en las entidades federativas, y éstos a los registradores de la oficina a su cargo que le auxilien en términos de la fracción II del artículo 20 bis del Código de Comercio.

La Dirección General de Normatividad Mercantil habilitará a las autoridades certificadoras para emitir los certificados digitales u otros medios de identificación de los notarios y corredores públicos.

Dicha unidad administrativa tendrá a su cargo la revocación, registro, administración y publicidad de los certificados digitales u otros medios de identificación a que se refiere el presente artículo, asimismo decidirá sobre la

autorización a que se refiere el artículo 30 bis cuando se trate de personas distintas a las anteriormente señaladas.

Artículo 11.- Los responsables de las oficinas del Registro en las entidades federativas proporcionarán a los notarios y corredores públicos, que cuenten con certificado digital expedido en términos de lo dispuesto por el artículo anterior, su usuario y su clave de acceso a la base de datos de la entidad de que se trate.

Artículo 12.- Será causa de cancelación de la autorización del notario o corredor público para acceder a la base de datos del Registro el hacerlo con fines distintos a los autorizados o si el notario o corredor público ha revelado la clave privada para el uso de su firma electrónica, independientemente de las responsabilidades en que pudieran incurrir.

En el caso de los servidores públicos de los registros públicos de la propiedad, la cancelación se hará a solicitud de los responsables de las oficinas del Registro en cada entidad.

Artículo 13.- El certificado digital y los demás medios de identificación podrán ser revocados a solicitud expresa del usuario, de la autoridad certificadora que lo emitió o de un tercero que demuestre tener interés jurídico para ello.

Artículo 14.- El monto de la fianza prevista en el artículo 30-bis 1 del Código de Comercio, se aplicará en el orden determinado por la autoridad competente, cuando se deba cubrir a un particular el monto fijado en la resolución correspondiente por responsabilidad en contra de un notario o corredor público.

5.8. **Reforma de Ley de Protección de Datos.**

Martes 4 de junio de 2002 Diario Oficial.

Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales- Requisitos que deben observarse para la conservación de mensajes de datos.

Considerando:

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, cual se realizó en el Diario Oficial de la Federación el 16 de noviembre del mismo año. Que durante el plazo de 60 días 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. 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 conservación de mensajes de datos.

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.

Su Campo de aplicación 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.

Disposiciones generales.

Los comerciantes deberán conservar los mensajes de datos de acuerdo al método establecido en la presente Norma Oficial Mexicana.

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

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.

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.

Elementos que intervienen en la conservación de mensajes de datos:

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.

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.

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.

Vigilancia:

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

5.9. Dictamen sobre delitos cibernéticos.

CC. PRESIDENTE Y SECRETARIO DEL A MESA DIRECTIVA DE LAH. CÁMARA DE SENADORES.

PRESENTE:

Con base en las referidas actividades, esta comisión sometió a la consideración de esta honorable asamblea el siguiente dictamen:

DICTAMEN:

Con fundamento en lo anterior se emiten los siguientes considerandos:

CONSIDERANDOS:

PRIMERO.- Los delitos cibernéticos se presentan cuando a las computadoras se les proporcionan nuevos métodos para cometer delitos tradicionales, como fraude, hurto, amenazas, distribución de pornografía infantil. Sin embargo las leyes, preparadas para los delitos tradicionales pueden no ser adecuadas para cubrir adecuadamente los delitos cibernéticos.

Existen tres categorías de delitos cibernéticos.

1. **Computadora como arma:** (verdadero delito cibernético) Uso de sistema para atacar, dañar a un sistema y robar información estratégica: clasificada o militar, de valor económico: industrial o financiera., datos personales: archivos de crédito o médicos

2. **Computadora como herramienta**: (Delitos tradicionales) Fraudes; Juegos de dinero; Explotación de niños; Piratería; Robo de identidad.

3. **Computadora como centro de datos:** Deposito de comunicaciones

SEGUNDO.- En razón de la proliferación de la pornografía infantil a través del internet se han realizado adecuaciones al código penal federal para combatir la promoción electrónica de las mencionadas actividades ilícitas. De esta forma el libro segundo, titulo 9no denominado Revelación de los Secretos y Acceso Ilesito a Sistemas de equipo de informática dispone lo siguiente:

Articulo 201 bis: Al que procure o facilite por cualquier medio el que uno o mas menores de 18 años, con o sin su consentimiento lo o los obliguen o induzcan a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de video grabarlos, fotografiarlos o exhibirlos mediante anuncios impresos o

electrónico, con o sin el fin de obtener un lucro, se le impondrán de 5 a 10 años de prisión y de 1000 a 2000 días de multa.

Al que fije, grabe, imprima actos de exhibicionismo corporal, lascivos o sexuales, en que participen uno o mas menores de 18 años, se le impondrá la pena de 10 o 14 años de prisión, y de 500 a 3000 días de multa. La misma pena se impondrá a quien con fines de lucro o sin el, elabore reproduzca, venda, arriende, exponga, publicite, o trasmita el material que se refieren las acciones anteriores.

Se impondrá prisión de 8 a 16 años y de 3000 a 10000 días de multa, así como el decomiso de los objetos, instrumentos y productos del delito, a quien por si o a través de terceros, dirija, administre o supervise cualquier tipo de asociación delictuosa con el propósito de que se realicen las conductas previstas en los dos párrafos anteriores con menores de 18 años.

Para los efectos de este articulo se entiende por pornografía infantil, la representación sexualmente explicita de imágenes de mores de 18 años.

TERCERO.- De igual forma, para combatir y castigar nuevas problemáticas que han surgido con nuevas tecnologías, se han tipificado nuevos delitos en el código penal federal.

Artc. 211 bis. 1: al que sin autorización modifique destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de 6 meses a 2 años de prisión, y de 100 a 300 días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de 3 meses a 1 año de prisión, y de 50 a 150 días de multa.

Articulo 211 bis 2: al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipo de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrá de 1 a 4 años de prisión, y de 200 a 600 días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegido por algún mecanismo de seguridad se le impondrán de 6 meses a 2 años de prisión y de 100 a 300 días de multa.

Articulo 211 bis 3: Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida

de información que contengan, se le impondrán de 2 a 8 años de prisión y de 300ª 900 días de multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de 1 a 4 años de prisión y de 150 a 400 días de multa.

Artículo 211 bit 4: Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de información de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de 6 a 4 años de prisión y de 100 a 600 dias de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de 3 meses a dos años de prisión y de 50 a 300 días de multa.

Articulo 211 bis 5: El que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente, modifique, destruya o provoque perdida de información que contengan, se le impondrán de 6 meses a 4 años de prisión y de 100 a 600 días de multa.

Al que estando autorizado para acceder a sistemas o equipos de informática de las instituciones de sistemas financieros, indebidamente copie información, que contengan, se le impondrán de 3 meses a 2 años de prisión y de 50 a 300 dias de multa.

Las penas previstas en este articulo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Articulo 211 bis 7: Las penas previstas en este articulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

CUARTO.- El código de comercio contiene un capitulo completo referente a comercio electrónico, en donde establece, entre otros conceptos, definiciones exactas de aspectos técnicos como: certificado, datos de creación de firma electrónica, firma electrónica, firma electrónica avanzada o fiable. Intermediario, mensaje de datos, prestador de servicios de certificación, sistemas de información; así mismo, menciona el proceso de creación y funcionamiento de la firma

electrónica; las personas o instituciones que puedan fungir como prestadores de servicios de certificación y las obligaciones que tienen como tale; y las consideraciones que deben tomarse para determinar si un certificado o una firma electrónica de extranjeros produce efectos jurídicos.

QUINTO.- La ley federal de protección del consumidor también se ha adecuado en el mismo sentido del código del comercio, pues ya contempla en sus principios básicos la real y efectiva protección al consumidor en las transacciones efectuadas, a través del uso de medios electrónicos, así como la atribución de la procuraduría federal del consumidor (PROFECO) de promover en coordinación con la secretaria de economía, la formulación, difusión y uso de código de ética, por parte de promover que incorporen los principios previstos por la ley; respecto de las transacciones que celebren con consumidores, a través de uso de medios electrónicos.

SEXTO.- A nivel internacional, destacan varios proyectos exitosos, siendo el mas conocido la convención sobre delincuencia cibernética del consejo de Europa, celebrada en el 2001, la cual tiene como objetivo unificar criterios y avanzar hacia un cómbate mas coordinado contra delitos cibernéticos.

SÉPTIMO.- La ley de servicios de la sociedad de la información y comercio electrónico de España, incluye aspectos de servicios como suministro de información, actividades de intermediación, transmisión de datos por redes de telecomunicaciones, y alojamiento de información en servidores; reglamenta la contratación de bienes y servicios por vía electrónica; establece actos de cesación en materia de protección de los intereses de los consumidores, pretende generar la confianza necesaria para el empleo de este nuevo medio; y busca cubrir aspectos que no están contemplados por la regulación existente.

OCTAVO.- Se considera que en virtud de que el internet cambio la forma de comunicación y hacer negocios, tenemos que proteger a los usuarios y a los sitios de internet que trabajan en forma legitima y honesta, por lo que es impredecible contar con un marco legal que establezca sanciones para aquellos que hoy se aprovechan del vacio legal para cometer, actos delictivos utilizando internet y los sistemas informáticos.

Los temas que deberían ser prioritarios desde nuestra perspectiva son:

- Propiedad intelectual.
- Privacidad.
- Spam.
- Fraude.
- Hacking, DOS, Attacks, Piratería Informática.

5.10. Decreto contra la delincuencia organizada.

Decreto que reforma y adiciona diversos artículos de código penal federal, del código federal de procedimientos penales, de la ley de instituciones de crédito y de la ley federal contra la delincuencia organizada, en materia de delitos informáticos.

Artículo Primero.- Se reforma el Titulo Decimotercero para adicionar un capitulo Segundo Bis que se denominara "falsificación electrónica" con los artículos 240 Ter Y 240 Qatar, se adicionaran los artículos 211 Bis 6 211 Bis 7, recorriéndose los demás en su orden; se adicionaran los artículos 168 Ter 389 Ter; y se reformara la fracción II del articulo 424 Bis, del código penal federal, para quedar como sigue:

Artículo 168 Ter.- Se impondrá de 1 a 3 años de prisión y de 200 a 2000 días de multa al que por medio de dispositivos o elementos electrónicos, o por cualquier otro medio, obtenga ilícitamente servicios de telecomunicaciones para obtener un beneficio propio o ajeno.

Articulo 211 Biis 6.- Al que sin autorización o excediendo la que hubiere obtenido acceda a la totalidad o parte de un sistema informático o equipo informático se le impondrá una pena de 3 meses a 1 año de prisión y de 50 a 150 días de multa. Cuando se acceda a sistemas informatices o equipo sin formaticos protegidos por algún mecanismo de seguridad, o a sistemas o equipos informatices del estado de las instituciones que integran el sistema financiero, la pena que se refiere al párrafo anterior se aumentara en su mitad.

Artículo 211 Bis 7.- Al que sin autorización intercepte por medios técnicos, datos informáticos comunicados en transmisiones no publicas efectuadas en un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos se le impondrá una pena de 2 a 4 años de prisión y de 300 a 600 días de multa.

Artículo 211 Bis 8.- Para los efectos de los artículos 211 Bis 4, 211 Bis 5 y 211 Bis 6 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este código.

Artículo 211 Bis 9.- las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida utilice en provecho propio o ajeno.

Titulo Decimo Tercero

Falsedad.

Capítulo I

Falsificación, alteración y destrucción de moneda.

Articulo 234. – a Articulo 238.-…….

Capítulo II

Falsificación y utilización indebida de títulos al portador, documentos de crédito público y documentos relativos al crédito.

Articulo 239.- a Articulo 240Bis.-……..

Falsificación Electrónica.

Articulo 240 Ter.- Se impondrá de 5 a 10 años de prisión y de 400 a 600 días de multa al que introduzca datos a sistemas o equipos informáticos protegidos por algún mecanismo de seguridad, o a los sistemas o equipos de información sean del estado o de las instituciones que integran el sistema financiero, con el fin de que utilicen para efectos legales como si se tratara de datos auténticos. La misma pena se impondrá a quien introduzca datos informáticos para crear documentos electrónicos falsos con el mismo fin.

Artículo 240 Quater - Para los efectos de los artículos 211 Bis 4, 211 Bis 5 y 211 Bis 6 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este código.

Articulo 398 Ter.- Comete el delito de fraude informático el que introduzca, altere, borre o suprima datos informáticos o realice otra interferencia en el curso de procedimiento de datos, con la intención de obtener ilícitamente alguna cosa o lucro indebido para sí mismo o para otra persona.

Este delito se sancionara con penas previstas en el artículo 386 de este código.

Capítulo III a VIII…

Artículo 424 Bis.-

I.

II. A quien fabrique, almacene, transporte, distribuya, con fin de lucro, o venda un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo Segundo.- Se adicionan las fracciones IV, V, VI, recorriéndose las demás en su orden, al artículo 112 Bis de la ley de instituciones de crédito, para quedar como lo siguiente:

I a III.-…

IV. Aceda sin la autorización correspondiente a los sistemas o equipos informáticos del sistema bancario e introduzca datos para usar tarjetas de crédito, debito o en general instrumentos de pago utilizados por el sistema bancario con el fin de disponer de recursos financieros.

V. Por cualquier medio capture, grabe, copie, altere, duplique o elimine la información contenida en una tarjeta de crédito o de debito u otros instrumentos similares provistos de banda magnética| o dispositivos técnicos de almacenamiento de datos, para obtener un lucro indebido.

VI. Atreves de sistemas o equipos de informática o cualquier tecnología de la información acceda al sistema bancario para crear, captura, duplicar o alterar la información con el fin de incorporar usuarios, cuantas, registros o modificar la cuenta de consumos en la adquisición de productos o servicios de cualquier naturaleza.

VII. Obtenga o use indebidamente la información sobre los clientes u operaciones del sistema bancario, y sin contar la autorización correspondiente.

Artículo Tercero.- Se adiciona un inciso 17) Bis a la fracción I del articulo 194 del código Federal de procedimientos penales, para quedar como sigue:

I.

1) a 17) …

17) Bis.- La falsificación electrónica de datos en sistemas o equipos informaticos de las instituciones que integran el sistema financiero, previsto en el articulo 240Ter.

18) a 34)…

II a VII…

VIII. De la ley de instituciones de crédito, los previstos en los artículos 111, 112n en el supuesto del cuarto párrafo ; excepto la fracción V; 112 Bis Fracciones V y VI, y 113 Bis en el supuesto del cuarto párrafo del artículo 112 Bis.

Los delitos señalados den la fracción IV de dicho Articulo lo serán únicamente si, además de cometerse por un miembro de la delincuencia organizada, el ministerio publico de la federación ejerce la facultad de atracción. En este caso, el ministerio publico de la federación y las autoridades jurídicas federales serán las competentes para conocer tales delitos. Bajo ninguna circunstancia se agravaran las penas previstas en las legislaciones de las federativas.

Transitorios.

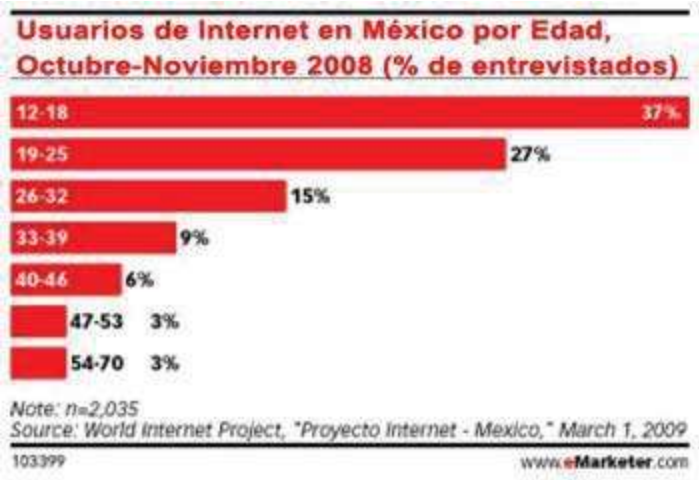
UNICO.- el presente decreto entrara en vigor al día siguiente de su publicación en el diario oficial de la federación.

INVESTIGACIONES.

El uso de internet en México

Referencia año 2009

Una sólida mayoría de usuarios de Internet son jóvenes y muchos viven en áreas urbanas. De acuerdo a un estudio del World Internet Project, el 64% de los usuarios mexicanos de Internet tenían entre 12 y 25 años en el 2008. Adicionalmente, el estudio encontró que cerca del 26.2% del total de usuarios de Internet en México residen en el Distrito Federal. En otras palabras, esa sola ciudad aporta más de una cuarta parte de todos los usuarios de Internet en todo el país.



Los usuarios Web más jóvenes tienden a adoptar más rápidamente las más nuevas y la más amplia gama de actividades en línea. comScore World Metrix reportó un incremento de 10% en la audiencia en Internet en Marzo 2009 comparado con el mismo mes del año anterior. Adicionalmente, al menos cuatro de los 15 Sitios Web más populares en el país contienen elementos de medios sociales, con un crecimiento en visitantes únicos en Facebook, WordPress, Batanga, y hi5 de 220%, 61%, 60% y 35% respectivamente.

Los 15 Websites más Populares en México, por Visitantes Únicos, Mar/08 -Mar/09 (miles de visitantes y % de cambio)

	March 2008	March 2009	% change
1. Microsoft sites	9,288	11,084	19%
2. Google sites	8,905	10,738	21%
3. Yahoo! sites	6,135	7,311	19%
4. MercadoLibre	5,472	6,154	12%
5. Wikimedia Foundation sites	4,189	5,427	30%
6. Batanga	2,817	4,508	60%
7. hi5	3,045	4,100	35%
8. WordPress	2,241	3,606	61%
9. Fox Interactive media	2,722	3,085	13%
10. Orange sites	3,267	2,944	-10%
11. Terra-Telefonica	2,385	2,747	15%
12. Facebook	841	2,696	220%
13. Televisa Digital sites	1,851	2,687	45%
14. NetShelter Technology Media	-	2,609	-
15. Apple Inc.	2,024	2,478	22%
Audiencia Total de Internet en México	**11,687**	**12,914**	**10%**

Nota: edad 15+; uso en hogar y trabajo; excluye tráfico desde computadoras públicas y acceso desde teléfonos celulares y PDAss

Source: comScore World Metrix as cited in press release, April 27, 2009

103477 www.eMarketer.com

Unos de los Sitios con mayor crecimiento, Batanga, es un popular sitio bilingüe, español e inglés, con contenido de medios con acceso en tiempo real (streaming media). El sitio implementó nuevas funciones de tipo social en marzo 2009 y reportó un incremento de 38% en registros de nuevos usuarios, y un incremento de 28% en actividades de consumidores en la semana siguiente al lanzamiento. Aún cuando Batanga es un Sitio que reside en los EEUU, su atractivo, basado en una combinación de contenido en tiempo real y medios sociales, definitivamente ha cruzado la frontera.

CONCLUCIONES.

En los últimos años los usuarios del comercio electrónico en nuestro país, se han visto dentro de la problemática de los delitos informáticos y como ya es un numero considerable de casos es importante su legislación.

Los principales obstáculos para que la legislación se desarrolle legalmente esta muy marcada y solo los países muy desarrollados han legislado mas ampliamente, por que son los mas susceptibles a los ataques, mientras que en los países menos desarrollados no han trabajado lo suficiente. La situación de la legislación en mexico se puede decir que en los últimos años ha tenido un importante avance en nuestro país. Ya que se han realizado reformas y adecuaciones a importantes ordenamientos en materia comercial y tecnológica, teniendo como base para su desarrollo la ley modelo sobre comercio electrónico (UNCITRAL) de las Naciones Unidas.

Se puede concluir que la incompetencia o pasividad de las autoridades por combatir acciones delictivas o fraudulentas, junto con una actitud similar por parte de la sociedad por denunciarlas, nos lleva a considerar el marco legal del entorno y de las organizaciones creadas por velar por su cumplimiento. La impunidad, la ausencia de sanciones, el aumento de absoluciones, o la falta de castigos solo llevara a perpetrar este modo de vida.

El fracaso del comercio electrónico en lo que se refiere a legalidad, no ha estado en la tecnología empleada sino en la equivocada asunción de que el modo seria adoptado sin importar los cambios en los procesos o actividades ya establecidas.

Se considero que el costo de su adopción seria absorbido por las ganancias que produciría en corto tiempo pero nadie previo que este requería mas tiempo para vencer no los problemas tecnológicos si no los sociales, políticos y económicos.

Se puede decir que en la forma en que esta haciendo regulada esta problemática en mexico, donde evidente el incremento de esta situación y considero necesario a pesar de que en nuestro país el delito informático no ha alcanzado el grado de peligrosidad, se debe de tomar en cuenta los grandes avances de las leyes que existen en otros países desarrollados que regulan penalmente las conductas ilícitas derivadas del uso de la computadora y para que nosotros como mexicanos podamos contar con mejores reformas acerca de la legislación del comercio electrónico en México y tengamos la confianza suficiente de realizar cualquier tipo de operación dentro de el.

BIBLIOGRAFIA.

Debra Little Zinder, Prevencion Y Detención de Delitos Informaticos, Anaya S.A. 2

Francisco Javier García, Marco Jesús Tramillas Sanz, World Wide Web, - Ra –Ma.

Eva Fernández Gómez, Comercio Electrónico. Mc Graw Hill,

Valte, Fundamentos de Comercio Electrónico, Mc Graw Hill

Karanjit Siyan Ph. D. Internet y Seguridad en Redes, Prentice Hall – Mexico

Alan Freedman, Diccionario de Computacion, Mc Graw Hill.

Titulo Segundo de Comercio Electronico,

http://www.diariooficial.com.mx/2003/agosto/dof_29-08-03.pdf. Poder Ejecutivo Federal.

Norma Oficial Mexicana NOM-151-SCFI. Politicas Comerciales- Requisitos que deben observarse para la conservación de mensajes de datos.

http://www.diariooficial.com.mx/2003/agosto/dof_04-06-02.pdf.Poder Ejecutivo Federal.

Proyecto de la Norma Oficial Mexicana PROM-NOM-151-SCFI-conversacion de los mensajes de datos.

http://www.diariooficial.com.mx/2003/agosto/dof_16-11-01.pdf.Poder Ejecutivo Federal.

Legislación del Derecho Informático.

http://www.informatica-juridica.com/legislacion/mexico.asp Ivonne V. Muños Torres.

Ley de Modelo sobre Comercio Electrónico, Comisión de las Naciones Unidas.

http://www.uncitral.org/sp-index.html. Asamblea General.

Internet como un Nuevo Medio de Comunicación.

http://www.unlz.edu.ar/biblioteca/tutores/histoweb/medios.htm#* Biblioteca Central de la Universidad Nacional de las Lomas de Zamora.

¿Qué es un hacker?
Hhttp://groups.msn.com/best/informacionhackerycracker.msnw, Ester Martinez.

Legislación del Comercio Electrónico en España,

http://usm.edu.ec/eticainformatica/validacion/cap%20v%20v-%20legislacion%20España.PDF, Veronica Vauerizo Arosemena, Ma. De Lourdes Plaza.

Precaución: Fraudes por Internet,

http://www.tvazteca.com/hechos/especiales/finanzas/nf38.shtml, Samuel Prieto Rodríguez.

Comercio Electrónico,

http://.profeco.com.mx/html/comercio_lineamientos.html,

Dictamen sobre Delitos Informáticos

http://www.senado.gob.mx/sgsp/gaceta/?sesion&documento=56, Senado de la República.

Delitos Informáticos, http://unifr.ch/derehopenal/articulos/PDF/DELITOS.pdf,

Miguel Estrada Garavilla.