UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE DERECHO Y CRIMINOLOGIA

DIVISION DE ESTUDIOS DE POSGRADO

TESIS

"AVANCES DE LA FIRMA ELECTRONICA EN EL DERECHO MEXICANO".

PRESENTA

LA LIC. ROSA GPE. ESPARZA MACIAS

PARA OBTENER EL GRADO DE

MAESTRIA EN DERECHO PUBLICO

DIRIGIDA POR

EL LIC. RENE BARRERA PEREZ

CD. UNIVERSITARIA FEBRERO DE 2003

TESIS

"AVANCES DE LA FIRMA ELECTRONICA EN EL DERECHO MEXICANO".

UNIVERSIDAD AUTONOMA DE NUEVO LEÓN

FACULTAD DE DERECHO Y CRIMINOLOGÍA

DIVISIÓN DE ESTUDIOS DE POSGRADO

TESIS

"AVANCES DE LA FIRMA ELECTRONICA EN EL DERECHO MEXICANO".

QUE PRESENTA

LA LIC. ROSA GPE. ESPARZA MACÍAS

PARA OBTENER EL GRADO DE

MAESTRÍA EN DERECHO PÚBLICO

DIRIGIDA POR

EL LIC. RENE BARRERA PEREZ

CD. UNIVERSITARIA

FEBRERO DE 2003

A DIOS:

Por darme la fortaleza para afrontar mis retos,

la sabiduría para dar lo mejor de mí

y por la enorme capacidad de amar y soñar

A MIS PADRES;

SR. JOSÉ PEDRO ESPARZA TREVIÑO

Y SRA. ROSA MA. MACÍAS GAYTÁN:

Con mi mayor gratitud y amor por ser mi guía,

Mi apoyo y mi aliento

A MIS HERMANOS; PEDRO, ALEJANDRO Y CARLOS:

Por ser mis tres pilares y enriquecer mi vida

A GRISELDA, PEDRO EMILIO Y MARISOL:

Por dejarme aprender de ellos y formar parte importante de mi vida

MUY ESPECIALMENTE:

A mis grandes alientos y apoyo,

Lic. Pedro Quezada Bautista

Lic. Rosa Isela Moreno González

Lic. Héctor Mario Domínguez Rivera

C.P. Rafael Serna Sánchez

Lic. Karla Castillo

Lic. Karla Zuñiga

Lic. José de Jesús Regis García

Lic. Gerardo Regis García

... GRACIAS

DEDICATORIA ESPECIAL

AL LICENCIADO RENE BARRERA PEREZ

Con mi respeto, admiración y reconocimiento

INDICE

PROLOGO

El único procedimiento posible para la transformación de bienes y servicios en bienestar general, es la tecnología. Es este producto, tal vez, la expresión máxima de la cultura de un país, puesto que por su intermedio se satisfacen las demandas indispensables de sus ciudadanos.

Por tratarse de un vocablo de aparición reciente, en el terreno del pensamiento económico y social, y más aún, en el campo publicitario, no es necesario aferrarse a una lógica de "Real Academia" ni defender con tenacidad una u otra definición, pero, en el caso de documentos conceptuales o doctrinarios, o de carácter político, debería precisarse cuidadosamente el valor de la palabra.

Es más o menos evidente que el término tecnología se asocia al adelanto y a la innovación. En nuestra definición de tecnología, entonces, consideraremos, implícitamente que aquélla debe tener valor propio para serlo y que la que habiendo sido superado, y por lo tanto su valor de cambio desaparecido, aun puede tener valor de uso en un marco social y económico adecuado.

Otro aspecto importante de la cuestión tecnológica es que la tecnología no es única para la solución de un problema productivo. Cada

sociedad puede encontrar una solución diferente acorde con sus posibilidades científico - técnicas y con el perfil de su demanda.

Además, es preciso decir que en tanto el avance del conocimiento científico exige la originalidad como valor de legitimación, en el campo del desarrollo tecnológico la originalidad no es demasiado importante y la copia, pecado capital del científico, se acepta como un medio válido para la fabricación y la obtención de un paquete tecnológico o de una tecnología.

Términos tales como "incorporación de tecnología administrativa o informática" que poseen significado simbólico para mucha gente, no parecen ser categorías útiles para el desarrollo de pensamiento de base y cuando se termina de explicar, resulta que aquella expresión pretenciosa se puede reemplazar por "compramos algunas PC's".

La trascendencia de los medios de producción es tan obvia que no es necesario profundizar en los efectos sociales de su existencia y la consiguiente magnitud de conflictos que los acompañan en toda la gama de materias.

Algunos conceptos que se manejan en el tratamiento serio de esta cuestión no encuentran significado en el manejo social cotidiano y, sin embargo, son representativos del fenómeno tecnológico. Algunos de ellos:

transferencia de datos, registro de tecnología, investigación aplicada, know how, empresa de tecnología, firma electrónica, entre otras.

El ocasiones el uso común de la palabra tecnología no pasa de un sinónimo de, entre otras palabras, herramienta, método, técnica, informática, computadora, software, hardware y otras cosas por el estilo.

El presente nos coloca frente al desmesurado desafío de encontrar respuestas a problemas de naturaleza prácticamente desconocida en los diversos terrenos del devenir social. El derecho no escapa a esa demanda, complicado adicionalmente por la lentitud con que la nave de su doctrina responde al timón. Y aun por las dificultades naturales, culturales y políticas que representa poner en vigencia una norma novedosa sobre un asunto especializado de cierta complejidad.

Es curioso comprobar que los abogados, que asignamos particular importancia a las opiniones autorizadas y escuchamos con respeto las pericias técnicas en el contexto de una causa judicial, que tenemos notoria influencia sobre los planteos y las decisiones, no consideramos ni valoramos de igual manera las observaciones que hacen esos mismos especialistas cuando se refieren a temas que se consideran privativos del derecho.

El progreso científico y técnico tiene interacciones con una gran cantidad de factores que inciden en la vida de una comunidad, y acarrea cambios radicales en los procesos productivos y en los servicios.

Resulta posible pensar, en consecuencia, en una concepción integrada y coherente entre el campo tecnológico y la organización, donde la dinámica esté dada por la existencia de información rigurosa donde apoyar toda reconceptualización del producto o del servicio que se habrá de ofrecer.

Se ha sostenido que muchos de los problemas contemporáneos provienen de dos factores: la exclusión de la ciencia y de la técnica de la cultura general, y la costumbre de estudiar las situaciones fragmentándolas en problemas parciales, creyendo poder resolverlos independientemente unos de otros y analizándolos preferentemente de manera monodisciplinaria.

La introducción de una computadora en el ámbito de la justicia, en cambio, es capaz de replantear inmediatamente los modelos de realizar el trabajo y este cuestionamiento extenderse a la organización; la suma de ambos puede dar elementos imprescindibles para las reformas normativas, todo lo cual crea nuevas necesidades de formación de recursos humanos, así como de espacios físicos.

El futuro ya no será, parafraseando a Bertrand Rusell, lo que podría haber sido. Este tema es un buen ejemplo de este aserto.

INTRODUCCIÓN

En este trabajo se intenta mostrar la situación en la que se halla el derecho en el marco de esta nueva sociedad de la información, en donde las distancias no existen, las fronteras se desdibujan y las culturas se fusionan, *todo ello al ritmo de la vertiginosidad y agilidad que posee el ciclo del* conocimiento.

Asistimos a un cambio de paradigma en el derecho, pudiendo afirmar que su generación no proviene exclusivamente de incorporar a la disciplina cada logro o avance de la interminable e incesante producción científico – tecnológica, sino del proceso universal de globalización que abarca todas las actividades humanas.

La dispersión de las redes digitales a través de todo el planeta ha puesto en evidencia que los sistemas jurídicos de las naciones, considerados aisladamente, son ineficaces para dar respuesta a las situaciones que plantea esta fenomenología: la humanidad transita el camino hacia la aldea global, que se presenta como inevitable e ineludible en una profecía determinista.

A partir de las nuevas tecnologías digitales, el hombre se encuentra frente a la exigencia de hacerlas converger y, por ello, está comenzando a desenvolverse en la interfaz entre lo físico y lo virtual, en un metamundo en el que es incapaz de escindirse de los artefactos que crea.

El mundo virtual y globalizado que generaron las redes ofrece posibilidades casi tan inagotables como la imaginación humana, y a medida que nos internemos en ese mundo, todavía casi inexplorado, se presentarán situaciones que deberán ser analizadas a la luz del derecho.

El objetivo que se pretende con el trabajo que expondremos es introducirnos dentro del tema del documento informático, haciendo un breve repaso de su aceptación internacional e internacional.

Sin lugar a dudas, es un tema extenso y complejo del cual resta mucho por conocer, pero estamos ciertos de que siempre un camino de mil leguas ha comenzado con un paso y que, según enseñaba Aristóteles, aquello que debamos aprender lo aprenderemos haciendo.

III. EL NUEVO PARADIGMA

3.1. Metamorfosis del caos.

Durante las últimas décadas se ha abierto camino a un concepto nuevo: la noción de inestabilidad dinámica asociada al caos. La palabra caos hace pensar en desorden, imposibilidad de previsión.

La actividad creadora de esa inestabilidad dinámica hace que nos encontremos en presencia del camino cualitativo más importante que jamás haya habido en la *historia de la humanidad. Esta abrumadora transformación* científica y tecnológica, que puede ser considerada esperanzadora o *apocalíptica*, ha sido más evidente en los últimos sesenta años y nos presenta un mundo en el que no podemos desdeñar su fundamental influencia en la comprensión y explicación de cualquier disciplina que tenga por objeto el análisis del hombre en su contexto social y temporal.

A los seres humanos nos gusta rotular las épocas y los períodos de la historia, y muchos ya han sugerido que la Edad Contemporánea, que comenzó en 1789 con la Revolución Francesa, debe ceder paso a otras denominaciones, debido a la aceleración de sucesos, para permitir nombres acordes a la época en la que vivimos.

Así, muchos han rotulado a nuestra época como la Era Nuclear o Era Atómica, en virtud de la disposición de esa increíblemente dual tecnología; otros, como la Era Espacial, por los avances en el conocimiento del espacio exterior y otros cuerpos celestes.

Por otro lado, se le ha dado una denominación más orientada a la política internacional, primero como la Era de la Guerra Fría y luego, con la caída del comunismo en la ex Unión de Repúblicas Socialistas Soviéticas, como la Era de la Posguerra Fría, que desemboco en una única potencia dominante y que otros, en una interpretación sociopolítica, quieren denominarla como la Era del Poscomunismo o como la Era de la Sociedad Poscapitalista.

Finalmente, otros prefieren calificarla como la era Genética, por las significativas revoluciones en ese campo a partir del hallazgo de la clave genética del ADN, tal vez el descubrimiento científico mas importante del siglo. Otras en cambio, la designan como la Era del Orden al Caos.

También podemos decir, según el autor que consultamos, que nos encontramos en la Era de la Información o de la Postinformación o en la era del Conocimiento, las que ofrecen posibilidades de explosiones creativas a `partir de la información disponible, merced a la inmediatez y rapidez de

interacción en las redes que permiten el acceso masivo a ese conocimiento, entendido éste más allá del mejor conocimiento asequible o conocimiento científico que, por supuesto, no es el único posible.[1]

Podríamos alegar que estamos viviendo la era del Aprendizaje debido a la enorme cantidad de coas que se aprenden en poco tiempo, al punto de la exacerbación de la cuestión, pues se puede afirmar que un alto porcentaje de la población esta actualmente en oficios que no existían cuando nacieron.

O quizás se pueda decir, por ejemplo, que estamos en presencia de la Era del Fin del Trabajo, en vista de que se ha afirmado que en los próximos años nuevas y más sofisticadas tecnologías informáticas basadas en la información y en el empleo de los ordenadores llevarán a la civilización a situaciones cada vez más próximas a la desaparición del trabajo.

En realidad, no importa como denominemos a este particular tiempo que nos toca vivir, ni tampoco interesa si su impronta es negativa o positiva, lo importante es visualizar de que manera el desarrollo científico y tecnológico influye en la transfiguración acelerada de nuestra civilización.

Las telecomunicaciones, las computadoras y el mundo digital que éstas han generado, están creciendo a un ritmo tan veloz como el de la

1 Poper, In search of a better world. Lectures and essays from thirty years. P. 9 a 75.

vertiginosidad del cambio del conocimiento humano, y es difícil establecer cual de ellos dos es la génesis del otro.

Nunca en tan corto lapso, la humanidad estuvo tan expuesta a cambios tan contundentes como los que vivimos desde la mitad del siglo XX, pareciendo incluso que hasta el mismo cambio, cambia.

Si bien es cierto; la tecnología es esencialmente pragmática, dado que no constituye un instrumento para investigar la realidad ni es su fin la búsqueda del conocimiento y la verdad, ésta aún restringiéndonos al rasgo epistemológico de considerarla investigación acerca de la validez de determinado conocimiento, así como de la interrelación con otros saberes, crea nuevas realidades y modifica al mundo, al extremo de concebir nuevos universos; como por ejemplo, pueden considerarse la realidad virtual o las comunidades virtuales.

En sí misma, la tecnología es sólo una herramienta, un instrumento, pero como toda nueva herramienta nos fuerza a cambiar el que hacemos y no únicamente como lo hacemos.

Bajo la denominación de "tecnología de la información" se abarca todo aquello que implique la creación, procesamiento y transmisión de señales digitales y está conformada por hardware, software, cibernética, sistemas de

información, redes, chips inteligentes, criptografía, robótica, inteligencia artificial y realidad virtual.

3.2. Sociedad y Tecnología de la Información.

En el último medio siglo se han producido avances tecnológicos de tal magnitud que provocaron cambios sociales y culturales que pueden ser considerados como el advenimiento de una era posterior a la "Era Industrial".

Si bien suele asociarse el nacimiento de la "Era de la Información" o de la "Sociedad de la Información", con la dispersión de las redes de computadoras en forma relativamente masiva, puede decirse que la transformación comienza cuando la manufactura deja de ser el pilar económico de los países industrializados.

De hecho, esta transformación augura nuevas formas de concebir el poder. Al adquirir un papel preponderantemente en las sociedades, la información (y su control) se torna una fuente dominante de poder en la evolución sociopolítica del hombre. Las tecnologías de la información y las telecomunicaciones están afectando las formas de gobierno y su organización, así como la estructuración de las sociedades, al tiempo que se producen variaciones en la constitución de las elites de poder.

Del mismo modo en que los valores sociales se van moldeando bajo la presión de los avances tecnológicos y la valoración que las sociedades asignan a la información y a las actividades intelectuales, se va modificando la apreciación del poder y el modo de ejercerlo.

El poder político, en su forma actual, también tiende a resentirse. Las tecnologías digitales pueden proveer las herramientas para una ciudadanía más comprometida que tenga la posibilidad de una participación más directa en las decisiones de gobierno y pueda de ese modo llegar a prescindir de sus representantes parlamentarios. Asimismo, estas tecnologías pueden constituirse en una poderosa herramienta que permita la descentralización del poder en unidades cada vez más pequeñas.

3.3. El Derecho y el Paradigma de lo Digital.

A menudo oímos hablar de digital o digitalizar, e incluso mencionamos estos términos con frecuencia; es probable que en esas ocasiones no sepamos con exactitud a que nos estamos refiriendo. El vocablo "Digital" hace referencia a dígito o número y es la manera de representar información numéricamente, en notación binaria, es decir, mediante ceros y unos.

Digitalizar significa traducir señales de texto, imágenes, sonido o video a lenguaje binario o bits, que cuando se reproducen a gran velocidad, se obtiene una réplica, en apariencia, exacta al original.

La digitalización permite la comprensión y transmisión de gran cantidad de información a muy bajo costo, con alta fidelidad y a una gran velocidad.

Los especialistas en megatendencias, como Toffler, Naisbitt o Negroponte, sugieren un mundo distinto, desigual y cambiante a partir de la incorporación del concepto de digitalización y pronostican cambios fundamentales en la concepción de la sociedad. Han dicho que la "tecnología digital es la llave de la culminación exitosa de la infraestructura de la información y también es la tecnología que reinventará la manera en que la gente vivirá, trabajará y se divertirá".[2]

En este presente en que la hiperconexión, la hipercomunicación y el conocimiento aparecen como fundamentos, pareciera que uno de los mayores beneficios que ofrece la tecnología es la libertad relativa que pueden tener las personas, porque en un mundo telecomunicado digitalmente los individuos serán libres de trabajar en cualquier lugar del

---

2 Naisbitt, *Global paradox*. P. 61.
Toffler. Las guerras del futuro. P. 338.
Negroponte. Being digital. P. 232 y 233.

planeta, dado que sus computadoras y sus recursos de interconexión personal les permitirán estar en contacto con su estudio, oficina, fábrica o negocio, cualquiera que sea el lugar en donde estén.

La posibilidad que ofrece el mundo digital de permitir diferentes elaboraciones o exposiciones y profundizaciones de los temas, de acuerdo con el criterio personal de cada lector, ha sido denominada interactividad digital y es la piedra angular de la comunicación del futuro, en donde la actitud de quien se informa dejará de ser pasiva. Los usuarios podrán seleccionar la información conforme a sus necesidades y evitarán así ser cargados con una enorme cantidad de datos inútiles e innecesarios.

Otra vertiente de la digitalización es la acumulación de la información y del conocimiento. Nunca antes la humanidad se ha encontrado en esta situación, en la que millones de personas pueden acceder a tanto conocimiento acumulado.

Es indudable que la digitalización permite esta nueva manera de acceso al conocimiento, pero también debemos reconocer que esto conlleva un impacto social negativo al provocar la vulneración de derechos. Toda la estructura social se resiente ante las asimetrías evidentes entre quienes poseen acceso a la infraestructura de la información y quienes no. Estas

situaciones de desigualdad se generan tanto entre distintas naciones del mundo como dentro de un mismo país.

La digitalización esta cambiando al mundo y no podemos ser indiferentes a este proceso, lo llamativo es que la digitalización no estará limitada solamente a la información, sino que se hará extensiva, también a objetos de todo tipo, como la ropa, las edificaciones u otros objetos.

3.4. La visión autopoiética de la Teoría Pura.

Es menester aclarar que en la utilización de la metáfora autopoiética no se intenta revisar ni cuestionar la teoría de Kelsen. Sólo se pretende comprender sus procesos con el auxilio de un mecanismo de conocimiento, sin hacer juicios de valor respecto de su categoría formal.

Dada la trascendencia universal de la teoría pura del derecho de Kelsen, utilizaremos la metáfora autopoiética con el doble propósito de interpretar y comprender esta teoría y justificar la utilización eficiente de la teoría sistemática en la disciplina.

Se debe tener presente que el derecho no es un sistema ni tampoco un fenómeno autopoiético, sino que utilizamos estas metáforas para comprender su fenomenología.

Es en tal sentido que visualizaremos a la teoría pura como un sistema cerrado en acople estructural con la sociedad y con el contexto y que el derecho puede reconocerse a sí mismo asemejando entornos.

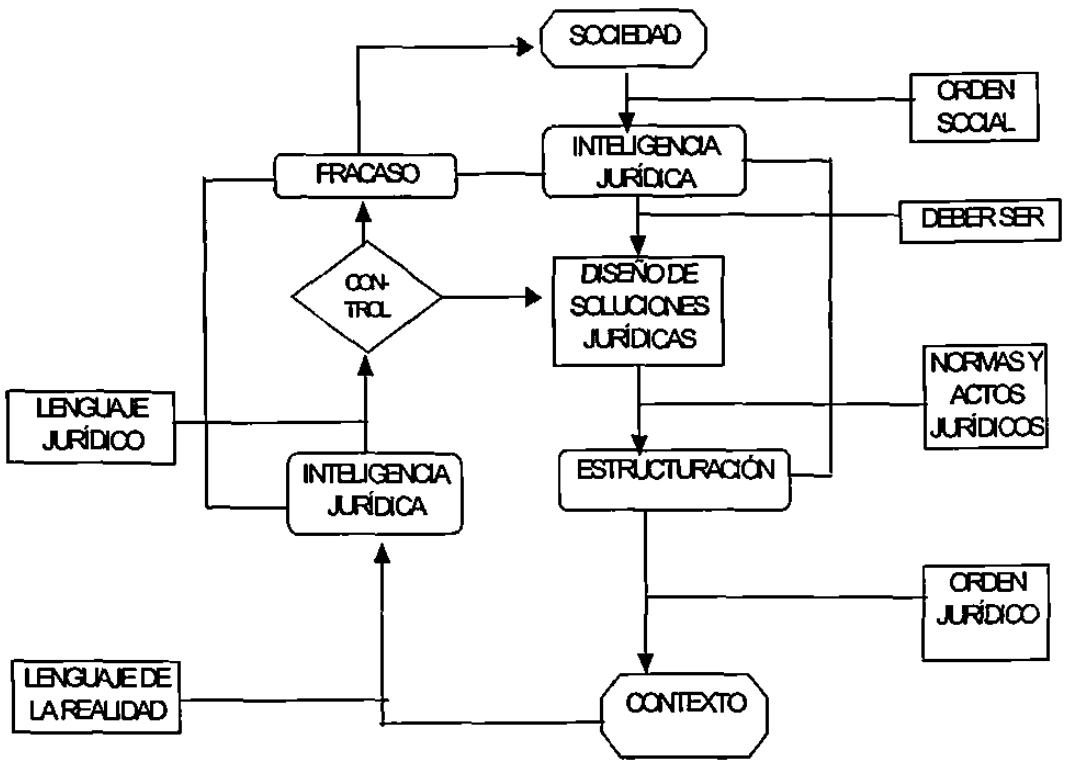
Kelsen ha dicho que el derecho "tiene la particularidad de que regula su propia creación y aplicación. La constitución regula la legislación, o sea la creación de normas jurídicas generales bajo la forma de leyes. Las leyes regulan a su vez, los actos creadores de normas jurídicas particulares. Por último, los actos por los cuales las sanciones son ejecutadas, aplican las normas jurídicas sin crear otras nuevas". [3]

Esto nos permite reconocer a la teoría pura como un proceso auterreferencial a través del cual el derecho intenta mantener y reproducir su propia identidad. Al autorreferenciarse con la sociedad, el derecho logra el fin que es necesario para ello: reproducirse a sí mismo en su propia imagen.

Intentaremos ahora, explicar la teoría pura, siguiendo la siguiente figura; pues si bien, el derecho es la interfaz entre la sociedad y su contexto, el derecho ya no es más considerado como una categoría eterna y absoluta. Se reconoce que su contexto varía según las épocas y que el derecho

[3] Kelsen. Teoría pura del derecho. P. 43 y 44.

positivo es un fenómeno condicionado por las circunstancias del tiempo y de lugar.



Lo que interesa a los fines de este análisis es, en realidad, la salida de la sociedad constituida por su orden social. Sin los valores el mundo carecer de sentido, y para evitar la eterna discusión acerca de ellos se admitirá su diversidad y se aceptará que constituyen términos primitivos que se acuerda no discutir.

El orden social es el lenguaje propio de la sociedad (lenguaje de valores, en términos de medios – fines) y constituye el lenguaje (input) objeto de la teoría pura del derecho, que lo transforma en metalenguaje (lenguaje *jurídico).*

En el análisis sistemático (visión autopoiética) de la teoría pura, en el input de I sistema operante se debe encontrara un proceso que formule aquella transformación de lenguajes. En otras palabras, un mecanismo que traduzca el lenguaje del orden social en lenguaje jurídico, o lo que es lo mismo, el lenguaje de la realidad social en un tiempo y lugar determinados, al de la realidad jurídica. Si no se inventara la realidad jurídica, es decir, si no hubiera una traducción *del lenguaje de la naturaleza y del orden social* (producto de la sociedad) se tendría una *única realidad y no habría una* distinción entre orden social y orden jurídico: la única realidad, el único objeto posible del conocimiento *científico sería la naturaleza, o sea, en este campo,* los fenómenos psicofisiologicos, sometidos a la causalidad.

Así en términos kantianos, la noción de causalidad no aparece como *una idea trascendente y en* ello se fundamenta Kelsen para formular la traducción de la causalidad natural a las categorías lógicas de la teoría pura en el deber ser, como un concepto genérico: el deber ser considerado como idea trascendente.

El lenguaje jurídico de interpretación del orden social genera un lenguaje en términos de deber ser, mientras que el lenguaje de interpretación de la realidad debe transformarse en términos jurídicos auterreferenciados a la teoría pura. La determinación del deber ser constituye un procedimiento de creación intelectual teórico, es decir, un modelo de representación del mundo social, externo al derecho. Esto significa pasar del ser al deber ser: "la expresión debe ser que figura en la regla del derecho indica solamente el sentido especifico de la relación establecida `por toda ley social entre una condición y su consecuencia: esta relación tiene el carácter de imputación. En otros términos el debe ser, tiene aquí un sentido puramente lógico y está desprovisto de toda significación moral o jurídica, ya que la imputación es una categoría y no una noción moral o jurídica".[4]

Como el deber ser constituye un modelo de representación de los conflictos de intereses de la sociedad en lenguaje jurídico, la teoría pura del derecho prevé un proceso de creación de soluciones. Es pues, el punto de partida de un procedimiento y su carácter es esencialmente formal y dinámico. Sólo la validez< de las normas de un orden jurídico puede ser deducida de su norma fundamental. Su contenido está determinado en cada caso por un acto particular que no es una operación mental, sino un acto de voluntad, costumbre o procedimiento legislativo, si se trata de normas

[4] Kelsen. Teoría pura del derecho. P. 85 y 86.

generales; decisión judicial, acto administrativo o acto jurídico de derecho privado, si se trata de normas individuales.

La salida de este proceso lo constituyen, entonces, las normas jurídicas, los fallos, los actos administrativos, para ser considerados válidos deben derivar de la norma fundamental.

El orden jurídico es el resultado de aplicar el derecho al orden social. Es el lenguaje de salida del derecho, pero no se debe de confundir la configuración con las normas que lo conforman, para evitar que cualquier modificación de éstas se traduzcan en una modificación estructural del orden jurídico.

La visión autopoiética permite corroborar las afirmaciones de la teoría pura, en el sentido de que el derecho es la interfaz entre una sociedad y el su contexto y tiene por fin inducir la conducta de los hombres. El derecho, de este modo, se autorreferencia, se autoclausura y traduce un orden social a un orden jurídico y se constituye así en un medio de la sociedad en un tiempo y un lugar.

IV. LA SEGURIDAD EN LAS REDES ABIERTAS

4.1. El paradigma vigente.

Las nuevas tecnologías digitales, que han irrumpido en redes abiertas de telecomunicaciones, han permitido el desarrollo y rápido crecimiento de Internet, como ícono representativo de esas redes y de numerosos servicios disponibles a través de ellas.

El crecimiento de Internet fue constante al principio, pero pronto se desarrollo sin control; por ende, es fácil advertir que actualmente Internet experimenta un crecimiento exponencial. Esta circunstancias puede ser abalizada mediante la imagen del *bucle de retroacción positiva.*

Esta red de comunicación inició con unos pocos investigadores que habían interconectado sus ordenadores entre sí, a ellos se les unieron, más tarde, un grupo de aficionados. Así la red, fue tornándose un ámbito sumamente útil y atractivo para el desarrollo de telecomunicaciones fidedignas y a bajo costo, lo cual favoreció el incremento de computadoras interconectadas. Actualmente, es casi impensable el no estar conectado a internet.

El impacto sociojurídico y cultural de este fenómeno es un tema complejo en virtud de sus implicaciones, por su magnitud y masividad, y por las proyecciones que se prevén para el desarrollo de esa red a corto plazo.

Su consecuencia fundamental es la de reconfigurar la topología de un planeta que se está modificando y comienza a desdibujar fronteras.

Todas la servicios y prestaciones que ofrecen las tecnologías digitales han transformado los hábitos y la forma de vida de las personas, pero si bien, por un lado, han abierto una brecha que posibilita la vulneración de derechos, garantías y libertades fundamentales, por otra parte posibilitan el surgimiento de nuevos horizontes para el conocimiento y la comunicación entre los pueblos, a la vez que permiten el crecimiento de pequeñas comunidades acotadas y limitadas a un determinado mercado. Pero para que esto sea posible, se debe otorgar protección a estos medios para que puedan ser considerados confiables.

4.2. La necesidad de protección jurídica.

Es innegable que Internet se ha transformado en una inmensa fuente de información de acceso universal que ejercer una importante influencia en la educación y en el ámbito sociocultural, a la vez que presenta buenas perspectivas en el ámbito del comercio.

Se trata de un importante foro donde se desarrollan numerosas actividades, la mayoría de las cuales son realizadas con fines legítimos y provechosos; pero, obviamente, también se llevan a cabo actividades ilícitas y conductas socialmente no aceptables. Por ello, el tema de la seguridad en las redes es un tópico fundamental en los ámbitos académicos internacionales, tanto tecnológicos como jurídicos.

Como se ha puntualizado anteriormente, la primera respuesta a la necesidad de protección en las redes fueron las técnicas criptográficas que permiten proteger la información e impiden que los sistemas sean utilizados o accedidos por personas no autorizadas o con fines ilícitos. Pero, por otra parte, ello facilita las actividades delictivas en las redes al transformar las comunicaciones en inexpugnables. No se debe perder de vista que, en todos los casos, está presente el interés legítimo de los Estados de velar por la seguridad y el orden públicos y el resguardo de las naciones.

Básicamente, el problema de la seguridad en las redes es un tema que, por la magnitud de sus consecuencias y las proyecciones que se prevén en el futuro desarrollo de ellas, se ha tornado estratégico para los gobiernos en todo el mundo.

Con este último objetivo los Estados, han tomado decisiones estratégicas para otorgar mayor seguridad a las redes, fundamentalmente tratando de delinear un marco normativo adecuado que brinde seguridad jurídica con el fin de fomentar el desarrollo de actividades a través de la red.

Uno de los aspectos fundamentales de la seguridad en la red, es el de aquellas cuestiones que comportan atentados contra la seguridad y el orden públicos y la consecuente posibilidad de hacer efectivo o no el cumplimiento de la ley, en materia de extradición o persecución de los responsables.

En la comunidad ciberespacial no existen valores constantes, puesto que la diversidad de culturas que las componen hace imposible la determinación de estándares. En consecuencia, los valores mutan permanentemente y se generan, en forma cíclica y continua, crisis y caos regulatorios propios de esa comunidad virtual global que propician formas especiales de autorregulación.

Indudablemente los hechos que más alertan respecto del potencial de internet como foro de actividades ilícitas con aquellos en que, además de reproducirse escritos o imágenes obscenas se utilizan los chats o los grupos de debate para tomar contacto con menores.

Normalmente lo usuarios de internet están identificados electrónicamente, ya sea por la dirección de identificación de la página de la WWW (URL) o mediante la dirección de correo electrónico o un mensaje de grupo de debate, pero la tecnología ha posibilitado, además, la utilización del correo electrónico o de los grupos de debate de manera absolutamente anónima.

En realidad, si bien es conveniente el anonimato para que las personas puedan expresar libremente sus ideas, es importante tener en cuenta que quien es libre de expresar sus ideas debe ser, asimismo, responsable por sus acciones. En este sentido, entonces, adquiere importancia la localización jurídica.

Para el caso de la utilización del correo electrónico, y en orden a conciliar el anonimato con la necesidad de identificación del emisor para posibilitar la localización de cualquier presunto delincuente en los casos de actividades ilícitas o contenidos nocivos, existen algunas propuestas.

Una de ellas es la reglamentación de la utilización de seudónimos que hagan posible una ulterior reconstrucción de la verdadera identidad del emisor y que, de ese modo, hagan posible su localización jurídica. Otra de las propuestas es que los remitentes anónimos hagan constar detalles sobre

su identidad al proveedor de servicios de internet, quien deberá de resguardarlos.

Para el caso de los chats y de los grupos de debate, las soluciones propuestas se encaminan a exigir a los proveedores de estos servicios que aseguren, en todo momento, la intervención de un moderador; el cual sería el encargado de monitorear el contenido de ese grupo de conversación, para cerciorarse de que no se viertan contenidos ilícitos.

V. FIRMA ELECTRONICA

5.1. Antecedentes.

El concepto histórico de firma y, a la vez, el más amplio y genérico, ha sido el de cualquier rasgo hecho con la intención de expresar el consentimiento a la manifestación de voluntad vertida en el instrumento.

Ahora bien, desde el punto de vista del derecho, se le ha otorgado valor jurídico a las distintas representaciones de esa autenticación o confirmación de la identidad de la persona, de acuerdo con las sociedades y con los diversos momentos históricos.

Básicamente, la firma sirve a los siguientes propósitos, los que, por supuesto, no se agotan en esta enumeración:

a) Consentimiento. La firma expresa el *consentimiento sobre lo escruto o la* intención de asignarle efectos jurídicos.
b) Solemnidad. El hecho de firmar un documento llama a la reflexión al firmante respecto del significado jurídico del acto que realiza y en consecuencia, esta solemnidad tiende a evitar la asunción de compromisos de manera inconsciente.
c) Prueba. Una firma autentica el cuerpo de escritura que le precede al identificar a su signatario. Cuando el signatario coloca al pie de un

Las presentaciones tecnológicas que brinda la firma electrónica la constituyen en un medio idóneo para cumplir con el fin propuesto:

a) Autenticidad del signatario. Con la utilización de la criptografía de clave pública (que funciona sobre la base de un par de claves), se garantiza la autenticidad del signatario; es decir, se asegura de que el emisor es quien dice ser.
b) No es un acto por omisión. El proceso tecnológico de firmar electrónicamente un mensaje es un acto afirmativo. Por lo tanto, se garantiza que quien firme es consciente de sus consecuencias, a la vez que permite reflejar la voluntad del firmante.
c) No repudio. Además de garantizar la identidad del emisor y la integridad del instrumento, estos métodos brindan el servicios de no repudio que es utilizado entre emisor y receptor. Es un medio de prueba que permite repeler la negativa tanto de haber recibido como de haber enviado el mensaje.

Tales consideraciones ponen de manifiesto que estos métodos aportan la confiabilidad necesaria como para ser utilizados en el tráfico jurídico.

5.2. Criptografía.

La creciente expansión y difusión de las redes de comunicaciones evidenció que debía protegerse toda la información personal que fluía por

ellas, porque ante la falta de esa protección se veía amenazada la privacidad de los individuos.

Las redes informáticas son especialmente vulnerables, debido a ciertas características en su estructura: en primer lugar, no existe una conexión física directa entre el emisor y el receptor; en segundo lugar, no se puede asegurar la inmediata transmisión entre ambos, y, por último, no se puede garantizar que ésta llegue a producirse.

Para que tal protección pudiera hacerse efectiva fue necesario recurrir a la criptografía que es, actualmente, la herramienta más promisoria para lograr la seguridad y confiabilidad en las comunicaciones electrónicas y, de este modo, favorecer el pleno desarrollo del potencial de las redes abiertas.

Las técnicas criptográficas, necesarias para brindar seguridad a los sistemas, son utilizadas, entre otros, para los siguientes propósitos fundamentales:

1. Mantener la confidencialidad del mensaje, es decir, hacer que la información transmitida a través de una red o almacenada en un sistema informático sea totalmente ilegible para quien no posea la clave para hacerla legible.

2. Garantizar la autenticidad del emisor/receptor, es decir, permitir al destinatario asegurarse de que el mensaje fue enviado realmente por *quien dice ser.*
3. Asegurar la integridad de la información, de manera que ésta no pueda ser modificada o alterada, intencional o accidentalmente. El mensaje debe llegar a destino sin alteraciones *en* su contenido o en el orden de la recepción de las unidades.
4. Permitir el no *repudio*, para poder probar fehacientemente que el usuario ha enviado o recibido un mensaje, de modo que ninguna de las dos partes pueda alegar que no efectuó la transmisión de datos.
5. Posibilitar el *control* de acceso, de modo que solo los usuarios autorizados y debidamente identificados puedan obtener permiso de acceso al sistema y a determinado datos.
6. Garantizar las disponibilidad, es decir, asegurar que la información y los sistemas se encuentren disponibles cuando sean requeridos. El objetivo es asegurar la continuidad operativa de los sistemas.

La criptografía clásica se ocupaba sólo de la confidencialidad, pero no ofrecía garantías de que el mensaje recibido era el que realmente había sido enviado y que emisor y receptor eran quienes decían ser.

En 1976, Diffie y Hellman introdujeron la criptografía de clave público, que se ocupo también de los otros dos aspectos.

La diferencia entre la criptografía clásica y la de clave pública radica en la seguridad. La primera goza de una seguridad probable, mientras que la segunda debe contar con una seguridad matemáticamente demostrable.

El objetivo de la seguridad en las redes no debe de ser únicamente el de proteger los datos transmitidos sino, también, evitar el acceso a los diversos elementos de la red que pudieran ser atacados.

En cuanto a las clasificaciones de los métodos criptográficos, una de ellas es la que se basa en las claves utilizadas y se desglosa en métodos simétricos y asimétricos.

El criptosistema (o familia de funciones) de cifrado asimétrico o de clave pública, utiliza un par de claves. Una es pública y la otra es secreta o privada. Cada clave efectúa una transformación unívoca sobre el mensaje y es función inversa de la otra, de modo que cada par de claves puede *descifrar sólo lo que su par correspondiente cifró.*

Para implementar un criptosistema de clave pública, dada una familia de funciones unidireccionales tramposas, cada usuario elige una clave pública, mientras que la trampa necesaria para invertirla es su clave privada.

La criptografía de clave pública es la utilizada para firmar electrónicamente y posibilita que cada mensaje enviado lleve la firma electrónica del usuario (análoga a la ológrafa), para permitir que el receptor tenga certeza sobre la identidad del emisor y la integridad del mensaje. Las firmas electrónicas deben ser fáciles de hacer y fáciles de verificar, per difíciles de falsificar.

Los esquemas de firma electrónica suelen ser muy lentos en su transmisión y, en ocasiones, la longitud de la firma suele ser similar o mayor al mensaje mismo; por ende, en la práctica se utiliza la función *hash* antes de firmar un mensaje. Esta función consiste en aplicar a un mensaje de longitud variable, una representación de longitud fija del propio mensaje, que se denomina *valor hash.* La función también se utiliza para realizar un digesto o resumen de un documento y poder hacer público ese resumen, sin revelar el contenido del documento del que procede el mensaje. De este modo, el problema de la longitud se soluciona si en lugar de firmar el mensaje completo, se firma sólo su resumen.

El procedimiento de firmar electrónicamente, en términos muy sencillos, es el siguiente.-

1. Un usuario A calcula su rúbrica cifrando el mensaje que desea enviar con su clave privada.

2. Luego, A determina su firma para ese mensaje sólo con encriptar, con la clave pública de B, la rúbrica que acaba de determinar.
3. B, recupera el mensaje y para verificar la firma electrónica de A, calcula la rúbrica de éste por medio de su clave privada.

El procedimiento de firmar electrónicamente un mensaje utilizando la función *hash* consiste en que si un usuario A desea enviar un mensaje al usuario B, junto con su firma, lo que hará es enviar el mensaje encriptado, y como firma enviará la rúbrica encriptada.

En suma, cada clavé efectúa una transformación unívoca sobre los datos y es función inversa de la otra, por lo que una clave sólo puede descifrar lo que su par encriptó y a la inversa, esa decir, que la clave puede ser utilizada en ambas direcciones.

En otras palabras, el mensaje encriptado se transforma en un documento que ninguna otra persona pudo haber generado. Asimismo, podemos afirmar que la firma electrónica es más segura que la ológrafa, puesto que además de asegurar que el mensaje fue realmente generado por quien lo envía, garantiza que ninguna parte de él ha sido modificada.

Las técnicas de encriptación requieren la realización de operaciones matemáticas complejas que demandan un gran procesamiento. Con objeto

de optimizar los tiempos de codificación y de decodificación de mensaje, se han desarrollado dispositivos de *hardware especiales.* Se trata de chips ubicados dentro de la computadora, que tiene funciones especificas.

Es interesante mencionar el modo en que funciona el sistema. La clave individual está depositada por partes, en dos fideicomisos, junto con el número de serie. En cualquier momento, el gobierno puede reclamar a los fideicomisos, con los recaudos legales pertinentes, las claves que tienen en *clipper chip.* Cada vez que se entabla una comunicación, se establece una clave de sesión con la que se cifra la información; pero, al mismo tiempo, se transmite una campo de acceso de defensa de la ley, con la identificación del chip y la clave de sesión cifrada bajo la clave individual y la estructural.

Las diferentes técnicas criptográficas pueden ser utilizadas en situaciones jurídicamente relevantes, como la firma simultanea de un contrato bilateral, el correo con acuso de recibo o la protección del *software.*

El protocolo de intercambio de secretos se utiliza cuando dos personas quieren intercambiar dos secretos, los cuales han sido previamente encriptados, mediante la utilización del criptosistema RSA. De este modo, si cada uno de ellos llega a conocer la factorización de la clave del otro, ambos pueden recuperar el secreto de la otra parte.

La firma simultánea de un contrato permite que ambas partes puedan firmar un contrato en el mismo momento en una red, de modo que ninguna de las pueda romper el protocolo y disponer de la firma de la otra parte sin haber firmado el contrato previamente.

Por su parte el correo con acuso de recibo, constituye otra codificación del protocolo de intercambio de secretos.

En conclusión, como ya hemos señalado, desde el punto de vista tecnológico, la criptografía, como disciplina, aporta las técnicas para lograr que la información transmitida por las redes sea confiable, para lo cual transforma el mensaje a enviar, de legible a ilegible. A su vez, permite averiguar si el mensaje recibido fue realmente el enviado y si quien lo envía es quien dice ser. Desde el punto de vista jurídico – político, estas dos posibilidades que ofrece la criptografía, es decir, la firma electrónica y la encriptación, presentan dos aristas bien definidas que han sido analizadas independientemente, debido a que una de ellas tiene implicaciones jurídicas y políticas polémicas, puesto que en la intervienen valores, mientras que la otra favorece la coacciono de la ley, en virtud de que su uso posibilita conocer las identidades del emisor y del receptor del mensaje.

Otra de las aplicaciones prácticas de la criptografía es la utilizada por el correo electrónico que, actualmente, la aplicación de mayor difusión y de mayor utilidad en las redes para diversos propósitos.

Asimismo, cabe mencionar la importancia de la criptografía en aplicaciones bancarias y financieras, en la mayor parte de las cuales es sustancial poder identificar perfectamente al emisor y al receptor, aunque no es imprescindible mantener la confidencialidad de los datos transmitidos.

5.3. Trabajo legislativo realizado sobre la materia.

A continuación se mencionan una serie de iniciativas internacionales sobre la materia, que ponen de relieve la preocupación de la mayoría de las naciones por brindar un marco normativo adecuado a la creciente utilización de las redes digitales para la realización de negocios y otorgar así seguridad jurídica a un medio ampliamente difundido.

La necesidad de hacerlo confiable se ve reflejada en las numerosas legislaciones, proyectos de leyes o enunciación de pautas que han comenzado a elaborarse en todo el mundo, los cuales versan, en forma genérica, sobre autenticación, integridad y confidencialidad de la información.

Todos estos son objetivos esenciales para la implementación y utilización de la firma electrónica y encriptación.

a) Unión Europea. Los lineamientos generales en torno de los cuales se enmarcan los proyectos normativos sobre firma electrónica, encriptación y promoción del comercio electrónico; están contenidos en diversas Directivas, Resoluciones y Comunicaciones del Parlamento y del Consejo Europeo.

   Entre estos podemos citar a los siguientes.- Resolución del Parlamento Europeo de 1996, la cual se dirige a encuadrar en un marco normativo adecuado la seguridad de la información, la confidencialidad, la firma electrónica y la protección de la privacidad; la Resolución del Consejo de Ministros de la Unión Europea, las cuales son una serie de medidas para asegurar la integridad y autenticación de instrumentos transmitidos electrónicamente; la Comunicación del Comité Económico y Social y del Comité de las Regiones al Parlamento Europeo y al Consejo Europeo, que consiste en establecer la política encaminada a garantizar la libre circulación de las tecnologías y los productos de encriptación e instó al desarrollo de un marco político al efecto.

b) Organización para la Economía, Cooperación y Desarrollo. El 27 de marzo de 1997, se establecieron los principios que sirvieron de base a los

países miembros para la formulación de sus propias políticas relacionadas con el uso de la criptografía. Estos lineamientos, si bien no son obligatorios, constituyen el primer intento a escala internacional de aportar políticas orientadas en varios aspectos de la criptografía.

c) Naciones Unidas. Destacan los trabajos realizados por la Comisión de las Naciones Unidas en la Ley Comercial Internacional, en la Cámara de Comercio Internacional, la Cooperación Económica de Asia – Pacífico.

d) Alemania. El 20 de diciembre de 1996, el gobierno alemán presentó al Parlamento una legislación sobre firma electrónica. Ella contiene los detalles técnicos del uso de firmas electrónicas en Alemania, así como las normas para el funcionamiento de las autoridades de certificación, la validez de los certificados, los componentes técnicos utilizados para firmas electrónicas y otros asuntos similares.

La ley de firma electrónica regula los certificados de las claves y la autoridad certificadora. Permite el seudónimo, pero prevé su identificación real por orden judicial. A la firma electrónica se le define como sello digital, con una clave privada asociada a la clave pública certificada por un certificador.

e) Australia. En octubre de 1997, el gobierno lanzó un proyecto destinado al análisis y desarrollo de un marco jurídico para la autenticación de usuarios online. Las conclusiones al respecto fueron plasmadas en informes y estudios posteriores.

f) Austria. En 1997 un grupo de expertos se reunió con el objeto de preparar un proyecto de ley sobre firma electrónica, el reporte se dio a conocer en 1998 bajo la denominación "Reporte del proyecto austríaco de ley sobre firma electrónica, ley de computadoras y seguridad", que ha sido la base de todas las discusiones sobre la materia en ese país.

g) Bélgica. En mayo de 1997 el Consejo de Ministros de Bélgica estableció la necesidad de una adaptación de la legislación belga a los desafíos de la nueva sociedad de la información.

h) Brasil. Este país aún no cuenta con la legislación especifica sobre firma electrónica, aunque un grupo de expertos del Colegio de Abogados de Brasil ha preparado un anteproyecto de ley sobre documentos electrónicos y firma electrónica.

i) Canadá. Varias son las iniciativas sobre la materia en este país; entre ellas se han realizado diversos estudios sobre aspectos legales relativos a la seguridad de la información electrónica. Se ha desarrollado la

infraestructura para un adecuado funcionamiento de la firma electrónica, mediante la provisión de los servicios de confidencialidad a los administrados y la utilización del comercio electrónico.

j) Colombia. En este país es incipiente la legislación en materia de comercio electrónico o implementación de firma electrónica, las propuestas al respecto han sido elaboradas sobre la base de la ley modelo en comercio electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

k) Corea del Sur. Se evidencia aquí un activo trabajo en la promoción del comercio electrónico. Así existe una serie de proyectos de ley que tienen por fin la consecución de ese objetivo y ya se han sancionado normas en ese sentido. El 1 de julio de 1999 entró en vigencia la ley básica de comercio electrónico que tiene por objeto otorgar efectos jurídicos a las transacciones hechas por medios electrónicos, al tiempo que brinda un entorno seguro y confiable. Para ello se ha establecido el Programa para la Promoción del Comercio Electrónico.

l) Dinamarca. El anteproyecto de ley sobre firma electrónica tiende a regular tanto a ésta como al funcionamiento de las autoridades certificadoras en las comunicaciones públicas y privadas. Se adopta la tecnología de la

criptografía como la más adecuada para firmar mensajes electrónicamente.

m) España. El 29 de febrero de 2000 entró en vigencia el real decreto 1906/1999, aprobado el 17 de diciembre de 1999. La norma reglamenta la contratación electrónica bajo la modalidad de contrato de adhesión. Así mismo, el 17 de septiembre de 1999 se aprobó el real decreto ley 14/1999 por medio del cual se regula la firma electrónica y el régimen al cual deben de ajustarse las autoridades de certificación.

n) Estados Unidos de América. La ley federal sobre la seguridad de datos electrónicos dictada en marzo de 1997, cuenta con una normativa tendiente a posibilitar el desarrollo de la infraestructura necesaria para la utilización de los productos de encriptación basados en clave pública que aseguren a los individuos y al comercio la transmisión digital de información confidencial, a la vez que prevé su autenticidad e integridad.

Estados Unidos es el país en donde está más avanzada la legislación sobre firma electrónica. El valor probatorio de la firma electrónica ya ha sido admitido en Utah, en donde su uso se basa en un criptosistema asimétrico, definido como un algoritmo que proporciona una pareja de claves segura. Sus objetivos, son facilitar el comercio por medio de

mensajes electrónicos fiables, minimizar las incidencias de la falsificación de firmas digitales y el fraude en el comercio electrónico.

o) Finlandia. En líneas generales, puede decirse que los intentos de legislación en Finlandia corresponden al tipo de normativas de configuración simple. En ellos solo se prevé la autorización genérica para la utilización de la firma electrónica, a la que se le otorga iguales efectos que la afirma ológrafa.

p) Francia. En septiembre de 1998 el Consejo de Estado emitió un informe por medio del cual se reconoce la necesidad de adaptación de la legislación francesa en orden a otorgar efectos jurídicos a la firma electrónica y se insta al reconocimiento de las autoridades certificantes tanto nacionales como del resto de la Unión Europea.

q) India. En diciembre de 1998 se sancionó en este país la ley sobre tecnología de la información que contiene previsiones relacionadas con el comercio y firmas electrónicas.

r) Italia. El avance normativo sobre este tema ha llevado a este país a la implementación de estándares técnicos en firma electrónica, publicados el 15 de abril de 1999 en un boletín oficial.

s) Japón. El Consejo para la Promoción del Comercio Electrónico de Japón, elaboró el 7 de abril de 1997 un anteproyecto que establece estándares provisionales para cada uno de los ítems que generalmente se consideran lineamientos formales. Se trata de pautas sobre autoridades de certificación, certificados, servicios de criptografía para la generación de las claves públicas y privadas, generación y validación de la firma electrónica, encriptación para la confidencialidad de la información, generación y validación de claves de confidencialidad, etc.

t) Malasia. En 1997, por medio de la ley 562 se incorporó al ordenamiento jurídico la firma electrónica y se reguló la actividad de las autoridades de certificación y su licenciamiento.

u) Perú. A partir de mayo de 2000 está en vigencia la ley 27.269 de firmas y certificados digitales, que equipara los efectos de aquéllas a los de la firma manuscrita. Considera que una firma electrónica es cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento y que cumple todas o algunas de las funciones características de una firma manuscrita.

v) Singapur. En junio de 1998 se aprobó la ley de firmas electrónicas y digitales, registros electrónicas y comercio electrónico.

5.4. Trabajo Legislativo en México.

El 7 de junio de 2000 entró en vigencia el decreto por el cual se reforma el Código Civil, el Código Federal de Procedimientos Civiles, el Código de Comercio y la Ley Federal de Protección al Consumidor. Con estas modificaciones se regula la oferta por medios electrónicos y ópticos y se prevé la utilización de cualquier otra tecnología.

Autoriza el otorgamiento de instrumentos públicos por medios digitales, siempre que el fedetario público haga constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información y conserve bajo su resguardo una versión íntegra del instrumento.

La reforma al Código de Procedimientos Civiles tiene por objeto, incorporar los medios digitales como medios de prueba.

Con relación al Código de Comercio, establece que los contratos celebrados por medios electrónicos u ópticos se considerarán perfeccionados desde el momento en que se reciba la aceptación de la propuesta.

Resulta también de profundo interés la Norma Oficial Mexicana NOM-151-SCFI-2002, publicada en el Diario Oficial de la Federación el 4 de junio de 2002, que se refiere a las prácticas comerciales y los requisitos que deben de observarse para la conservación de mensajes de datos; dada su importancia para el tema en estudio me permito transcribirla:

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

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

La Secretaría de Economía, por conducto de la Dirección General de Normas, con fundamento en los artículos 34 fracciones XIII y XXX de la Ley Orgánica de la Administración Pública Federal; 39 fracción V, 40 fracciones III y XVIII, 47 fracción IV de la Ley Federal sobre Metrología y Normalización, y 23 fracciones I y XV del Reglamento Interior de esta Secretaría, y

CONSIDERANDO

Que es responsabilidad del Gobierno Federal procurar las medidas que sean necesarias para garantizar que los servicios que se comercialicen en territorio

nacional contengan los requisitos necesarios, con el fin de garantizar los aspectos de información para lograr una efectiva protección del consumidor;

Que con fecha 28 de septiembre de 2001 el Comité Consultivo Nacional de Normalización de Seguridad al Usuario, Información Comercial y Prácticas de Comercio aprobó la publicación del proyecto de Norma Oficial Mexicana PROY-NOM-151-SCFI-2002, Prácticas comerciales - Requisitos que deben observarse para la conservación de mensajes de datos, lo cual se realizó en el ***Diario Oficial de la Federación*** *el 16 de noviembre del mismo año, con objeto de que los interesados presentaran sus comentarios;*

Que durante el plazo de 60 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; y que dentro del mismo plazo, los interesados presentaron sus comentarios al proyecto de norma, los cuales fueron analizados por el citado Comité Consultivo, realizándose las modificaciones procedentes;

Que con fecha 20 de marzo de 2002 el Comité Consultivo Nacional de Normalización de Seguridad al Usuario, Información Comercial y Prácticas de Comercio, aprobó por unanimidad la norma referida;

Que la Ley Federal sobre Metrología y Normalización establece que las Normas

Oficiales Mexicanas se constituyen como el instrumento idóneo para la protección de los intereses del consumidor, se expide la siguiente Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales - Requisitos que deben observarse para la conservación de mensajes de datos.

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

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

PREFACIO

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

- *ACERTIA NETWORKS, S.A. DE C.V.*
- *ALESTRA, S. DE R.L. DE C.V.*
- *ASOCIACION MEXICANA DE ESTANDARES PARA EL COMERCIO ELECTRONICO, A.C.*
- *ASOCIACION MEXICANA DE LA INDUSTRIA DE TECNOLOGIAS DE INFORMACION, A.C.*

- *ASOCIACION NACIONAL DE TIENDAS DE AUTOSERVICIO Y DEPARTAMENTALES, A.C.*
- *BANCO DE MEXICO.*
- *BANCO INTERNACIONAL, S.A.*
- *BANCO NACIONAL DE MEXICO, S.A.*
- *BBVA BANCOMER, S.A.*
- *CAMARA NACIONAL DE COMERCIO DE LA CIUDAD DE MEXICO.*
- *CAMARA NACIONAL DE LA INDUSTRIA ELECTRONICA, DE TELECOMUNICACIONES E INFORMATICA.*
- *CECOBAN, S.A. DE C.V.*
- *CONSEJO MEXICANO DE LA INDUSTRIA DE PRODUCTOS DE CONSUMO, A.C.*
- *COMISION FEDERAL DE TELECOMUNICACIONES.*
- *COMPAÑIA PROCTER & GAMBLE MEXICO, S. DE R.L. DE C.V.*
- *HEWLETT PACKARD DE MEXICO, S.A. DE C.V.*
- *IBM DE MEXICO, S.A. DE C.V.*
- *INSTITUTO NACIONAL DE ESTADISTICA, GEOGRAFIA E INFORMATICA.*
  DIRECCIÓN GENERAL DE POLÍTICAS Y NORMAS EN INFORMÁTICA.
- *KPMG CARDENAS DOSAL, S.C.*
- *PEGASO COMUNICACIONES Y SISTEMAS, S.A. DE C.V.*

- *PETROLEOS MEXICANOS.*
  GERENCIA DE INFORMÁTICA Y SISTEMAS FINANCIEROS.
- *PODER JUDICIAL FEDERAL.*
  INSTITUTO FEDERAL DE ESPECIALISTAS DE CONCURSOS MERCANTILES.
- *PROMOCION Y OPERACION, S.A. DE C.V.*
- *SECRETARIA DE ECONOMIA.*
  -DIRECCIÓN GENERAL DE NORMAS.
  -DIRECCIÓN GENERAL DE FOMENTO AL COMERCIO INTERIOR.
  -DIRECCIÓN GENERAL DE POLÍTICA DE COMERCIO INTERIOR Y ABASTO.
- *SEGURIDATA PRIVADA, S.A. DE C.V.*
- *SERVICIO DE ADMINISTRACION TRIBUTARIA.*
  ADMINISTRACIÓN GENERAL DE GRANDES CONTRIBUYENTES.
  ADMINISTRACIÓN GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN.
- *SOFTWARE AG, S.A. DE C.V.*
- *VERA ABOGADOS, S.C.*
- *WAL-MART DE MEXICO, S.A. DE C.V.*
- *XEROX MEXICANA, S.A. DE C.V.*
- *X WEB ADOBE, S.A. DE C.V.*

INDICE

De conformidad con lo dispuesto por los artículos 40 de la Ley Federal sobre Metrología y Normalización en relación con el 49 del Código de Comercio, la Secretaría de Economía deberá emitir una Norma Oficial Mexicana que permita el cumplimiento de la obligación, a cargo de los comerciantes que utilicen mensajes de datos para realizar actos de comercio, de conservar por el plazo establecido en dicho Código, el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones; y cuyo contenido debe mantenerse

íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta.

1. Objetivo

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

2. Campo de aplicación

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

3. Definiciones

3.1 *Aceptación de autoría*

A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente.

3.2 *Acto de comercio*

A todo acto que la legislación vigente considera como tal.

3.3 *Autenticación*

Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.

3.4 *Archivo parcial*

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

3.5 *ASN.1*

A la versión 1 de Abstracts Sintax Notation (Notación Abstracta de Sintaxis).

***3.6** Bits*

A la unidad mínima de información que puede ser procesada por una computadora.

***3.7** Bytes*

A la secuencia de 8 bits.

***3.8** Clave pública*

A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada.

***3.9** Clave privada*

A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.

3.10 Certificado digital

Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública.

3.11 Código

Al Código de Comercio.

3.12 Código de error

A la clave indicativa de un suceso incorrecto.

3.13 Comerciantes

A las personas físicas o morales a los que la legislación les otorga tal carácter.

3.14 Compromiso

A cualquier acto jurídico diferente del contrato o del convenio, que genere derechos y obligaciones.

3.15 Confidencialidad

Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada.

3.16 Contrato

Al acuerdo de voluntades que crea o transfiere derechos y obligaciones.

3.17 Convenio

Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones.

3.18 *Constancia del prestador de servicios de certificación*

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

3.19 *Criptografía*

Al conjunto de técnicas matemáticas para cifrar información.

3.20 *Destinatario*

A aquella entidad a quien va dirigido un mensaje de datos.

3.21 *Emisor*

A aquella entidad que genera y transmite un mensaje de datos.

3.22 *Entidad*

A las personas físicas o morales.

3.23 Expediente electrónico

Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente norma oficial mexicana.

3.24 Firma digital

A la firma electrónica que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital es una especie de firma electrónica que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.

3.25 Firma electrónica

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

firma electrónica establece la relación entre los datos y la identidad del firmante.

3.26 *Formato*

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

3.27 *Legislación*

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

3.28 *Mensaje de datos*

A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

3.29 *Objetos*

A las definiciones del lenguaje ASN.1

3.30 *Original*

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

3.31 *Prestador de servicios de certificación*

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

3.32 *Red*

Al sistema de telecomunicaciones entre computadoras.

3.33 *Resumen o compendio*

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

3.34 *Sello del prestador de servicios de certificación*

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

3.35 *Secretaría*

A la Secretaría de Economía.

4. Disposiciones generales

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

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

4.3 *Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto*

de comercio, que se encuentre soportada en un medio físico similar o distinto a aquéllos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana. La migración de la información deberá ser cotejada por un tercero legalmente autorizado, que constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente autorizado deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente y cumpla con los requisitos legales aplicables.

4.4 *Los programas de cómputo (software) para la conservación de los mensajes de datos deberán dar cumplimiento a lo establecido por la presente Norma Oficial Mexicana.*

5. Elementos que intervienen en la conservación de mensajes de datos

5.1 *Para la emisión de la firma electrónica y/o digital, así como el prestador de servicios de certificación, deberán observar los requisitos que la normatividad aplicable señale para su operación.*

5.2 *La constancia emitida por el prestador de servicios de certificación deberá observar los términos establecidos en el Apéndice de la presente Norma Oficial Mexicana.*

5.3 *Los programas informáticos en y con los que se almacenen los mensajes de datos a los que se refiere la presente Norma Oficial Mexicana, utilizarán los formatos para mensajes de datos en los términos establecidos en el Apéndice del mismo.*

6. Vigilancia

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

7. Apéndice Normativo

INTRODUCCION

En este Apéndice normativo se presentan los elementos necesarios para la implantación de la presente Norma Oficial Mexicana; la descripción del

algoritmo de conservación de información y la definición ASN.1 de los objetos usados.

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

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

FORMACION DE ARCHIVOS PARCIALES

Para formar un archivo parcial se crea un mensaje en formato ASN.1 que contiene (I) el nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo, (II) el tipo del archivo, y (III) el

contenido del mismo; con el objetivo de guardar la relación lógica que existe entre estos tres elementos.

OBTENCION DE LOS COMPENDIOS O RESUMENES DIGITALES

Se calcula el compendio o resumen digital del archivo o archivos parciales resultado del proceso anterior, usando el algoritmo MD5.

INTEGRACION DEL EXPEDIENTE ELECTRONICO

Para conformar un expediente electrónico se creará un mensaje ASN.1 que contiene (I) el nombre del expediente, que debe de coincidir con el nombre con el que se identifica en el sistema de información en donde está o estuvo almacenado, (II) un índice, que contiene el nombre y el compendio de cada archivo parcial que integra el expediente, (III) la identificación del operador del sistema de conservación, y (IV) su firma digital de acuerdo a la definición correspondiente en la presente Norma Oficial Mexicana.

OBTENCION DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACION

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

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

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

```
<form action="url del    ama generador de constancias "
                        -data">
    Expediente: <input type="file"
    <input type="submit" value="Obtener
</form>
```

La constancia deberá regresar al cliente como un archivo de tipo mime application/octet-stream[1].

---

[1] Los MIME Types (Multipupose Internet Mail Extensions) son la manera estándar de mandar contenido a través de la red.
Los tipos MIME especifican tipos de datos, como por ejemplo texto, imagen, audio, etc.

El prestador de servicios de certificación podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes.

FORMACION DE LA CONSTANCIA

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

METODO DE VERIFICACION DE AUTENTICIDAD

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

I. verificar la firma digital del prestador de servicios de certificación en la constancia;

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

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

Definición ASN.1

```
================================================================
NCI-NOM-000-SECOFI DEFINITIONS ::=
BEGIN

NombreOP ::= PrintableString

TipoOP ::= OBJECT IDENTIFIER

EmisorOP ::= IdentificadorUsuario

IdUsuarioOP ::= IdentificadorUsuario

md5                  OBJECT IDENTIFIER ::= { 1 2 840 113549 2 5}
rsaEncryption        OBJECT IDENTIFIER ::= { 1 2 840 113549 1 1 1}
md5WithRSAEncryption OBJECT IDENTIFIER ::= { 1 2 840 113549 1 1 4}
    --
    -- Identificador de objeto a utilizar para las Normas Oficiales Mexicanas
    --

    mex OBJECT IDENTIFIER ::= { 2 37  137 }

    nom OBJECT IDENTIFIER ::= { mex 179 }

    --
    -- Identificadores de objeto a utilizar para tipos de archivos
    --

    nomArchivos OBJECT IDENTIFIER ::= {nom 197}

    nomABinario OBJECT IDENTIFIER ::= {nomArchivos 1}
```

```
nomATexto    OBJECT IDENTIFIER ::=          vos 2} -- Extensiones
nomAT-TXT    OBJECT IDENTIFIER ::= {nomATexto 1} -- .txt
nomAT-TEX    OBJECT IDENTIFIER ::= {nomATexto 2} -- .tex
nomAT-PS     OBJECT IDENTIFIER ::= {nomATexto 3} -- .ps
nomAT-HTML   OBJECT IDENTIFIER ::= {nomATexto 4} -- .htm .html

nomAAudio    OBJECT IDENTIFIER ::= {nomArchivos  -- Extensiones
nomAA-AU     OBJECT IDENTIFIER ::= {nomAAudio 1} -- .au
nomAA-WAV    OBJECT IDENTIFIER ::= {nomAAudio 2} -- .wav
nomAA-MP3    OBJECT IDENTIFIER ::= {nomAAudio 3} -- .mp3
nomAA-RAM    OBJECT IDENTIFIER ::= {nomAAudio 4} -- .ram


nomAVideo    OBJECT IDENTIFIER ::= {nomArchivos 4} Extensiones
nomAV-MPEG   OBJECT IDENTIFIER ::= {nomAVideo 1} -- .mpg .mpeg
nomAV-DVD    OBJECT IDENTIFIER ::= {nomAVideo 2} -- PENDIENTE
nomAV-MOV    OBJECT IDENTIFIER ::= {nomAVideo 3}  -- .mov .qt .movie .moov

nomAImagen   OBJECT IDENTIFIER ::= {nomArchivos 5} Extensiones
nomAI-JPEG   OBJECT IDENTIFIER ::= {nomAImagen 1}-- .jpeg .jpg
nomAI-GIF    OBJECT IDENTIFIER ::= {nomAImagen 2}-- .gif
nomAI-BMP    OBJECT IDENTIFIER ::= {nomAImagen 3}-- .bmp

nomAMicrosoft OBJECT IDENTIFIER ::= {nomArchivos 6}-- Extensiones
nomAM-WORD     OBJECT IDENTIFIER ::= {nomAMicrosoft 1} .doc
nomAM-W6       OBJECT IDENTIFIER ::=      -WORD 1}
nomAM-W97      OBJECT IDENTIFIER ::= {nomAMWORD 2}
nomAM-W2000    OBJECT IDENTIFIER ::=      -WORD 3}
nomAM-PPT      OBJECT IDENTIFIER ::= {nomAMicrosoft 2} .ppt
nomAM-EXCEL    OBJECT IDENTIFIER ::= {nomAMicrosoft 3} .xls
nomAM-OUTLOOK OBJECT IDENTIFIER ::= {nomAMicrosoft 4} .pst
nomAM-ACCESS   OBJECT IDENTIFIER ::= {nomAMicrosoft 5} .mdb


--
-- Identificadores de objeto a utilizar para identificacion de
--
```

nomIdentificacion OBJECT IDENTIFIER ::= {nom 373}

nomIPersonaFisica OBJECT IDENTIFIER ::= {nomIdentificacion 1}

nomIF-NOMBRE OBJECT IDENTIFIER ::= {nomIPersonaFisica 1}

nomIF-IFE OBJECT IDENTIFIER ::= {nomIPersonaFisica 2}

```
nomIF-CURP        OBJECT IDENTIFIER ::= {nomIPersonaFisica 3}
nomIF-PASAPORTE   OBJECT IDENTIFIER ::= {nomIPersonaFisica 4}
nomIF-CEDULAFISCAL OBJECT IDENTIFIER ::= {nomIPersonaFisica 5}

nomIPersonaMoral  OBJECT IDENTIFIER ::= {nomIdentificacion 2}
nomIM-NOMBRE      OBJECT IDENTIFIER ::= {nomIPersonaMoral 1}
nomIM-CURP        OBJECT IDENTIFIER ::= {nomIPersonaMoral 2}
nomIM-CEDULAFISCAL OBJECT IDENTIFIER ::= {nomIPersonaMoral 3}

NombrePersonaFisica ::= SEQUENCE { nombreIdP       PrintableString,
  apellido1IdP    PrintableString,
  apellido2IdP    PrintableString}

IdentificadorPersona ::= SEQUENCE { nombreIdP
ombrePersonaFisica, tipoIdP        OBJECT IDENTIFIER, contenidoIdP
PrintableString}

NumeroCertificado ::= PrintableString

IdentificadorUsuario ::= SEQUENCE { personaFisicaMoral  OBJECT
IDENTIFIER, nombreRazonSocialIdU CHOICE {NombrePersonaFisica,
PrintableString},
  tipoIdU          OBJECT IDENTIFIER, contenidoIdU      PrintableString,
```

Expediente ::= SEQUENCE { nombre-expediente PrintableString, indice SET OF Entrada-al-Indice, id-usuario IdUsuarioOP, firma-usuario FirmaUsuarioOP}

Sello ::= SEQUENCE { estampa-de-tiempo UTCTime, emisor EmisorOP, folio-usuario Folio-UsuarioOP}

Constancia ::= SEQUENCE {nombre-de-la constanciaNombreConstanciaOP, expediente Expediente, marca-de-tiempo Sello, firma-constancia FirmaConstanciaOP}

END

==========

En el programa ASN.1 se definen primeramente los identificadores de objeto necesarios para identificar los tipos de archivo que se podrán almacenar observando la presente Norma Oficial Mexicana; estas definiciones podrían ser objeto de revisiones periódicas para incluir nuevos formatos, luego los objetos necesarios para almacenar los archivos o mensajes de datos que serán conservados.

A lo largo del programa se definen diferentes objetos ASN.1 cuyo uso dentro del programa aclara su función.

El campo firma-usuario del objeto expediente es la firma digital de los campos nombre-expediente, índice e id-usuario concatenados en ese orden, vistos como una secuencia de bytes.

En el objeto sello, el campo estampa-de-tiempo es la fecha y hora en formato GMT o IMT con la cual se creó el sello, emisor es el representante del prestador de servicios de certificación que está creando el sello y folio-usuario es un número secuencial ascendente para cada usuario registrado del prestador de servicios de certificación. Es decir, cada usuario llevará un registro numerado consecutivamente de cada operación que registra el prestador de servicios de certificación.

El objeto Constancia contiene un campo nombre-de-la-constancia que almacena el nombre del archivo de computadora donde se guardará dicha constancia en el sistema de información del prestador de servicios de certificación, expediente que es de tipo Expediente y es la información que se registra con el prestador de servicios de certificación con un sello emitido por ella, este sello contiene la fecha y la hora del momento en que se crea la Constancia. El campo firma-constancia es la firma digital de los campos nombre-de-la-constancia,

expediente, marca-de-tiempo concatenados en ese orden y vistos como una secuencia de bytes.

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

Enseguida se presenta el contenido de los objetos ASN.1 correspondientes. La línea "==========" representa el principio y el fin del archivo respectivamente y no forma parte del archivo.

Los objetos ASN.1 que se presentan están en formato BER y se muestra un vaciado hexadecimal comentado.

Archivo "mensaje.txt"

==========

Archivo de texto utilizado para ejemplificar la creacion de documentos de usuario y constancias de la Oficialia de Partes. Este es uno de dos archivos que se utilizaran en dicho ejemplo.

==========

Archivo "mensaje1.txt"

==========

Segundo archivo de texto que se utilizara en la creacion de un ejemplos para mostrar un documento usuario y una constancia de la oficialia de partes.==========

Archivo parcial "arp1.ber"

```
==========================================
30 81 d7 /*ArchivoParcial*/
   13 0b 6d 65 6e 73 61 6a 65 2e 74 78   74 /*titulo:mensaje.txt*/
   06 09 75 81 09 81 33 81 45 02 01 /*tipo:nomAT   -TXT*/
   03 81 bc /*contenido*/
      00 41 72 63 68 69 76 6f 20 64 65 20 74 65 78 74 6f 20 75 74 69 6c 69
7a 61 64 6f 20 70 61 72 61 20 65 6a 65 6d 70 6c 69 66 69 63 61 72 20 6c     61
20 63 72 65 61 63 69 6f 6e 20 64 65 20 64 6f 63 75 6d 65 6e 74 6f 73 20 64
65 0a 75 73 75 61 72 69 6f 20 79 20 63 6f 6e 73 74 61 6e 63 69 61 73 20 64
65 20 6c 61 20 4f 66 69 63 69 61 6c 69 61 20 64 65 20 50 61 72 74 65 73 2e
20 45 73 74 65 20 65 73   20 75 6e 6f 20 64 65 20 64 6f 73 20 61 72 63 68 69
76 6f 73 0a 71 75 65 20 73 65 20 75 74 69 6c 69 7a 61 72 61 6e 20 65 6e 20
64 69 63 68 6f 20 65 6a 65 6d 70 6c 6f 2e 0a
==========================================
```

Archivo parcial "arp2.ber"

```
======== ==================================
30 81 b3 /*ArchivoParcial*/
   13 0c 6d 65 6e 73 61 6a 65 31 2e 74 78 74 /*titulo:mensaje1.txt*/
   06 09 75 81 09 81 33 81 45 04 01 /*tipo:nomAV   -MPEG*/
   03 81 97 /*contenido*/
      00 53 65 67 75 6e 64 6f 20 61 72 6   3 68 69 76 6f 20 64 65 20 74 65 78
74 6f 20 71 75 65 20 73 65 20 75 74 69 6c 69 7a 61 72 61 20 65 6e 20 6c 61
20 63 72 65 61 63 69 6f 6e 20 64 65 20 75 6e 20 65 6a 65 70 6d 6c 6f 73 0a
70 61 72 61 20 6d 6f 73 74 72 61 72 20 75 6e 20 64 6f 63 75 6d 65 6e     74 6f
20 75 73 75 61 72 69 6f 20 79 20 75 6e 61 20 63 6f 6e 73 74 61 6e 63 69 61
20 64 65 20 6c 61 20 6f 66 69 63 69 61 6c 69 61 20 64 65 20 70 61 72 74 65
73 2e 0a
==========================================
```

Expediente "docusuario.ber"

El *expediente* en formato BER correspondiente a los *archivos parciales* que aparecen arriba es:

```
==========================================
30 82 01 4b /*expediente electrónicousuario:*/
   13 0f 64 6f 63 75 6d 65 6e 74 6f 20 23 20 34 35 36 /*nombre      -expediente
electrónico:documento # 456*/
   31 5e /*indice:*/
      30 2d /*Entradaal-Indice:*/
         13 08 61 72 70 31 2e 62 65 72 /*titulo:arp1.ber*/
         30 21 /*resumen:*/
            30 0c /*algoritmoresumen:*/
               06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*/
              05 00 /*NULL*/
            03 11 00 23 e7 4a 8a be d5 60 dd ec 07 5c 66 44 29 71 c2 /*resumen
      30 2d /*Entrada-al-Indice:*/
```

```
         13 08 61 72 70 32 2e 62 65 72 /*titulo:arp2.ber*/
         30 21 /*resumen:*/
            30 0c /*algoritmoresumen:*/
               06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*/
               05 00 /*NULL*/
            03 11 00 8c c0 81 b0 ce 66 e9 b7 90 5a 96 05 e8 38 13 20 /*resumer
   30 64 /*idusuario*/
      06 08 75 81 09 81 33 82 75 01 /*peronaMoralFisica: nomIPersonaFisica*/
      30 1c /*nombreRazonSocialIdU:*/
         13 08 52 61 79 6d 75 6e 64 6f /*Raymundo*/
         13 07 50 65 72 61 6c 74 61 /*Peralta*/
         13 07 48 65 72 72 65 72 61*/Herrera*/
      06 09 75 81 09 81 33 82 75 01 03 /*tipopIdU: nomCURP*/
      13 2f 41 71 75 69 20 76 61 20 6c 61 20 43 6c 61 76 65 20 55 6e 69
63 61 20 64 65 20 52 65 67 69 73 74 72 6f 20 64 65 20 50 6f 62 6c 61 63 69
6f 6e /*contenidoIdU:Aqui va la Clave Unica de Registro de Poblacion*/
         30 72 /*firmausuario:*/
            30 0d /*algoritmoFirma:*/
               06 09 2a 86 48 86 f7 0d 01 01 04 /*Identificador de Objeto:
md5WithRSAEncryption*/
               05 00 /*NULL*/
            03 61/*firma:*/
               00 6f 06 26 71 0e 7a 2a 55 33 f2 e1 cc 1b 44 de 3a 40 e9 b3
0d 87 ee 32 5d 90 5b 7c b2 29 72 56 d8 57 88 6d e4 37 c2 7b 95 2f 32 f8 72
15 87 ce 95 71 39 66 3c b2 d7 25 76 08 15 49 07 cf 2c 87 04 87 f5 f3 d6 31
c3 d0 13 16 1b 2b fc f2 6b 73 63 2c 37 e1 ce d6 0a a7 b4 30 57 df 96 c5 6d
30 98
=======================================
```

Constancia "recibo.ber"

Finalmente la *constancia* del *prestador de servicios* de certificación contiene u
copia del *expediente* más la *estampa de tiempo* y la identificación del prestado
de servicios de certificación que la generó.

```
==========================================
30 82 02 f0 /*Constancia de la Oficialia de Partes*/
   13 0a 72 65 63 69 62 6f 2e 62 65 72 /*nombre-de-la-constancia:recibo.ber*/
   30 82 01 4b /*expediente electrónico usuario:*/
      13 0f 64 6f 63 75 6d 65 6e 74 6f 20 23 20 34 35 36 /*nombre  -expedient
electrónico:documento # 456*/
      31 5e /*indice:*/
         30 2d /*Entrada al-Indice:*/
            13 08 61 72 70 31 2e 62 65 72 /*titulo:arp1.ber*/
            30 21 /*resumen:*/
               30 0c /*algoritmo resumen:*/
                  06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5
                  05 00 /*NULL*/
               03 11 00 23 e7 4a  8a be d5 60 dd ec 07 5c 66 44 29 71 c2
/*resumen*/
         30 2d /*Entrada al-Indice:*/
            13 08 61 72 70 32 2e 62 65 72 /*titulo:arp2.ber*/
            30 21 /*resumen:*/
               30 0c /*algoritmo resumen:*/
                  06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*
                  05 00 /*NULL*/
```

```
         03 81 81 /*firma:*/
            00 94 c1 94 4a 8c 32 59 5d 5f b8 2c f8 6c fc f4 d7 b    0 1f 24 81
b9 ad ba 2d db 7e c8 43 f4 25 5e cf d6 40 a9 2e f8 d0 02 59 1a b2 99 95 76
5e 56 ee f6 e8 4b ee 0b 45 3d 3f 50 86 12 f4 74 f4 17 59 2f e5 45 d2 d9 d6
d6 ec f7 e6 58 54 f8 da c2 8e a8 6b 9f d3 0f e1 cd 87 de 2d 38 85 ee 56 cd
03 53 c9 c6 49 f 3 36 b3 a6 d9 03 3a d6 e7 16 db 6d 82 89 54 93 8d 92 f9 2b
5f 63 10 1e e6 bb 94 78
==========================================
```

Claves privadas usadas para firmar

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

Clave privada de usuario:

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

Introducción

El FEC es un programa desarrollado para manejar las comunicaciones en aplicaciones con arquitectura cliente/servidor, fue diseñado pensando

en aplicaciones que requieran intercambiar mensajes en tiempo real. Se puede usar la definición de este sistema para especificar el protocolo de comunicación entre los clientes del prestador de servicios de certificación y los sistemas que se indican en la presente Norma Oficial Mexicana. La Secretaría de Economía deberá contar con un sistema de referencia para que el o los prestadores de servicios de certificación tengan un estándar contra el cual verificar que la implantación de la norma es correcta.

Los objetivos del FEC son:

- *Simplificar la programación de los sistemas con arquitectura cliente/servidor, de tal manera que al desarrollar un sistema se dejen a un lado los detalles relacionados al manejo de las comunicaciones y el esfuerzo se centre en los detalles propios del sistema.*
- *Lograr un ambiente de operación flexible que permita la interacción de programas desarrollados en distintas plataformas, sistemas operativos y lenguajes.*
- *Optimar el uso de los recursos y permitir que los sistemas que lo usen operen en tiempo real.*

El FEC se encarga de realizar algunas tareas que, en la arquitectura cliente/servidor tradicional, serían realizadas por el servidor, por ejemplo:

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

Es por ello que su uso proporciona las siguientes ventajas:

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

Esquema de operación

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

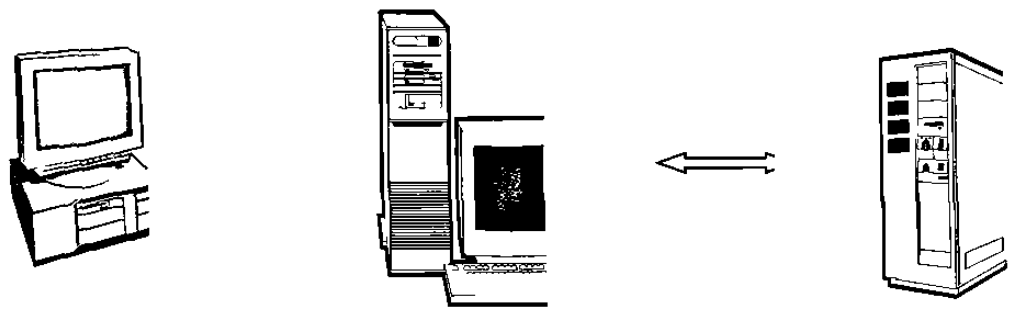
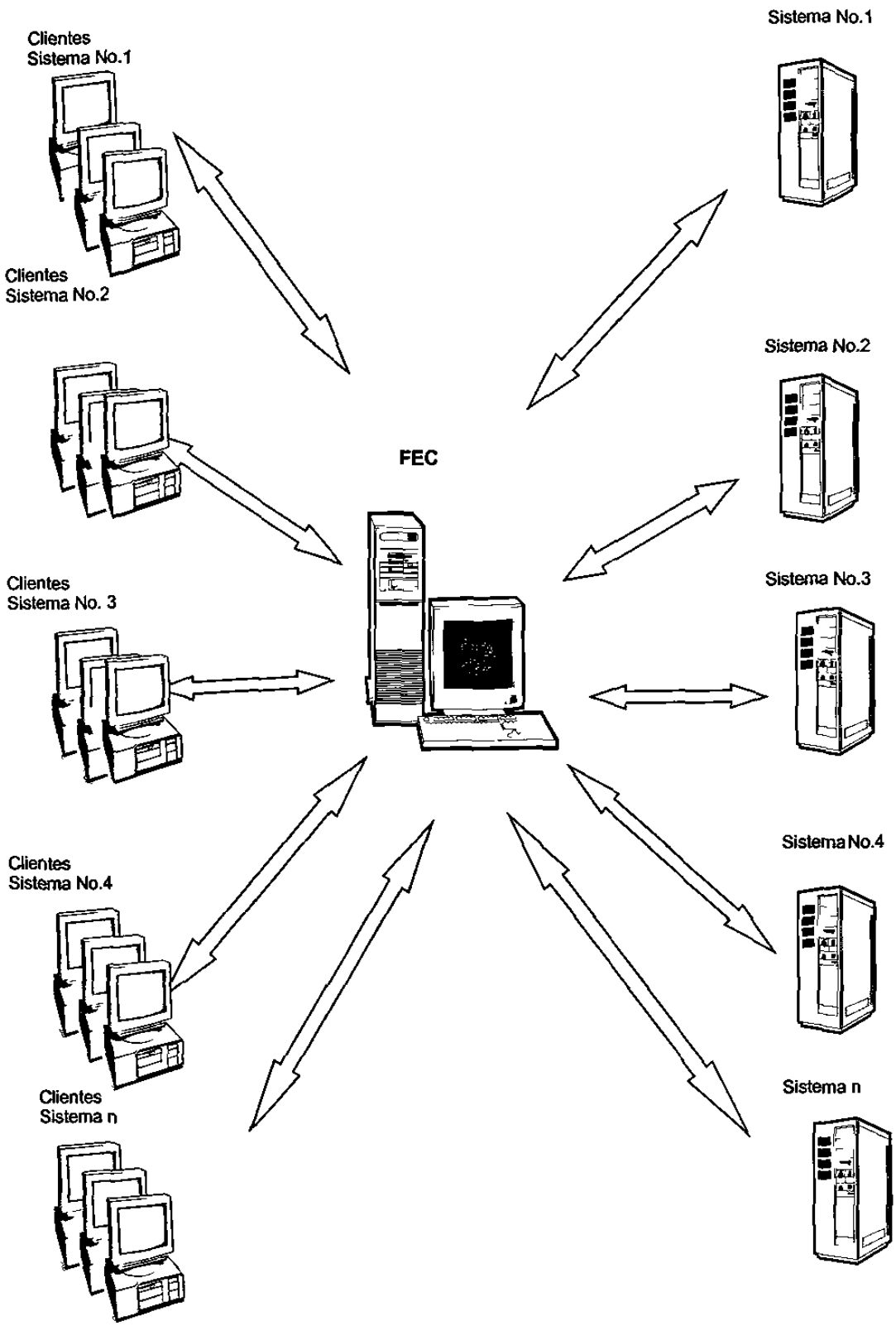


Figura 1. Esquema básico de operación del FEC

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

Del mismo modo, el FEC recibe los mensajes del servidor y los entrega al cliente indicado por éste.

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


Clientes
Sistema No.1
Clientes
Sistema No.2
Clientes
Sistema No. 3
Clientes
Sistema No.4
Clientes
Sistema n
FEC
Sistema No.1
Sistema No.2
Sistema No.3
Sistema No.4
Sistema n

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

Comunicaciones en el FEC

Manejo de Comunicaciones en el FEC

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

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

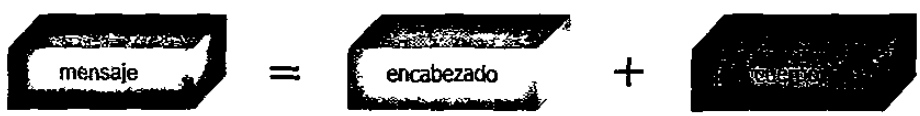


Figura 3. Todos los mensajes están formados por encabezado y cuerpo

Tanto el encabezado como el cuerpo de los mensajes se construyen con los tipos de datos básicos de todos los lenguajes de programación: char, int, short, string.

Es importante mencionar que el protocolo utilizado permite, a partir de los tipos de datos mencionados y respetando ciertas reglas (similares a las de las expresiones regulares), construir cualquier tipo de mensaje. La única restricción para que los programas intercambien información

es que acuerden de antemano el "formato" de los mensajes que se enviarán durante la operación.

Encabezado de los Mensajes

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

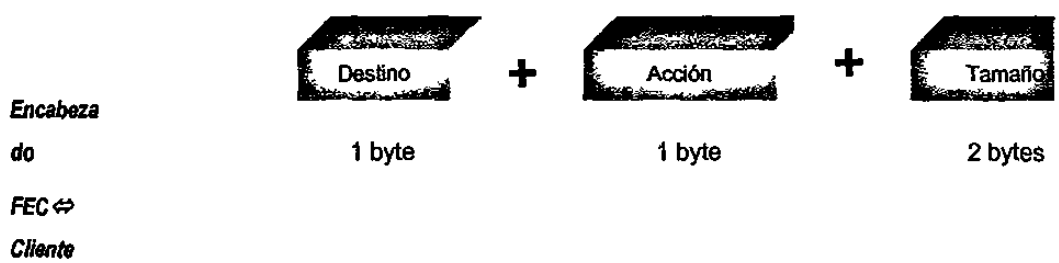


Figura 4. Encabezado de un mensaje FEC Cliente

A continuación se explican los campos que lo forman:

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

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

Los elementos que conforman este encabezado son:

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

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

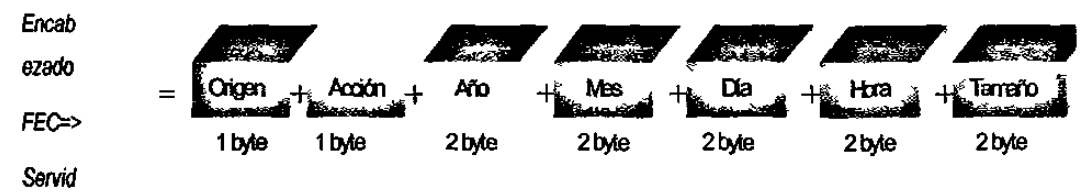


Figura 5. Encabezado de un mensaje FEC => Servidor

Cuerpo de los mensajes

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

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

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

El "formato" de un mensaje es una secuencia de tipos de datos básicos que describe su contenido. Para facilitar la lectura e interpretación de

estas secuencias, a cada tipo de dato se le ha asignado un símbolo, el cual se muestra a continuación[2] :

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

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

Interpretación del formato de un mensaje

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

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

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

el primer y segundo bytes de la trama respectivamente.
El valor del tercer dato debe obtenerse de los dos últimos bytes de la trama.
Lo anterior puede deducirse de la tabla donde se muestra la longitud de los elementos que conforman los mensajes[3] *.*

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

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

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

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

[3] Tome en cuenta las longitudes de los tipos de datos mostrados en la tabla de la sección anterior y además recuerde que los

longitud se desconoce y después una serie de "n" elementos, este número "n" es un valor de 4 bytes. A continuación vienen "n" elementos de un byte, "n" elementos de 2 bytes,"n" elementos de 4 bytes y finalmente "n" cadenas.

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

Construcción de mensajes

Dado que el campo Acción en el encabezado de un mensaje tiene una longitud de 1 byte, existen únicamente 255 acciones válidas en la operación de un sistema.

Aunque cada aplicación es la encargada de determinar el número de acciones que requiere y la información que debería incluirse en el cuerpo de los mensajes a enviar, resulta evidente que existe un conjunto de acciones comunes a todos los sistemas que interactúen con el FEC (por ejemplo los mensajes para establecer o terminar la conexión con el FEC); es por ello que algunos de los 255 posibles

---

datos viajan en formato de red, es decir, una vez obtenidos deberán transformarse al formato de la computadora receptora.

mensajes están reservados a estas acciones comunes a todos los sistemas. En esta sección se indican cuáles son estos mensajes reservados y se dan ejemplos de su construcción.

Mensajes reservados

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

Mensajes reservados para el FEC

Acción	Nombre	Formato	Descripción
236	CONFPASSWD		Confirma a un cliente que su contraseña fue cambiada exitosamente
243	DEADSRVR		Avisa a un cliente que el servidor ha dejado de operar
244	BYE		Avisa a un servidor que un cliente se desconectó
245	AREYOUALIVE		Pregunta a un cliente/servidor si opera correctamente

247	GREETING	%s%l	Avisa a un servidor de la conexión de un cliente. Incluye nombre y clave del cliente
249	CHPSWDFAIL		Avisa a un cliente que su contraseña no pudo ser cambiada
251	LOGINFAIL		Avisa a un cliente que su conexión fue rechazada
252	NOSERVICE		El servidor al que desea conectarse está fuera de servicio
253	LOGGED	%d	Avisa a un cliente que su conexión fue aceptada
254	LOGINREQ		Solicita a un cliente su clave de usuario para autenticarlo
255	PASSWREQ		Solicita a un cliente su contraseña para autenticarla

Mensajes comunes a todos los clientes

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

2 1 2	CHANGEPAS S	%s	Solicita cambio de contraseña, envía nueva contraseña al FEC

Ejemplos de construcción de mensajes

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

En algunos casos la dirección más baja de memoria contiene el byte menos significativo del entero (formato Little Endian). En otros, la dirección más baja de memoria contiene el byte más significativo del entero (Formato Big Endian). Estas dos maneras de almacenar datos se ilustran en la figura 6[4] *.*

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

Internet resuelve el problema del orden de los bytes al definir un estándar de red que debe utilizarse para intercambiar datos. Las computadoras que intercambian información deben convertir sus datos de la representación local a la representación estándar de red antes de enviarlos. Al recibir datos deben convertirlos de la representación estándar de red a la representación local.

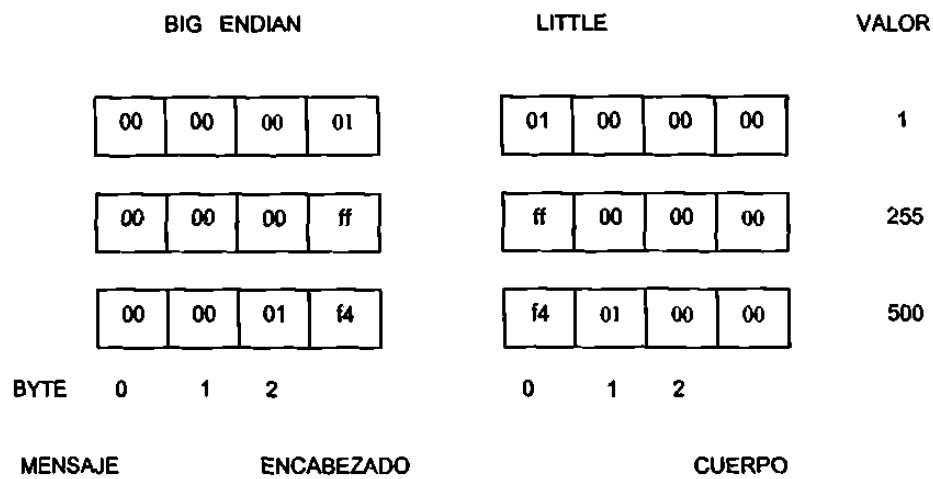


Figura 6. Diferentes Representaciones de Datos

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

Nuestro protocolo utiliza el estándar de red de Internet para intercambiar información. En la figura 7 representamos los mensajes necesarios para que un cliente establezca comunicación con el FEC siguiendo el estándar antes mencionado[5] . No olvide que los valores deben enviarse en formato de red.

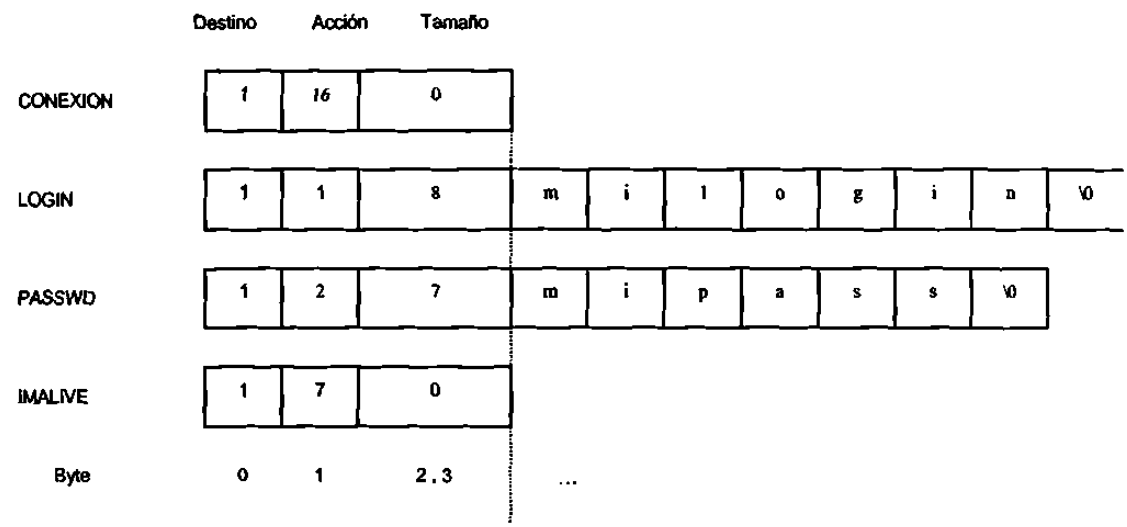


Figura 7. Construcción de Mensajes para Conectarse al FEC

Secuencia de Conexión

Recepción y transmisión de mensajes en el FEC

La secuencia de recepción y transmisión de mensajes en el FEC se muestra en la figura 8.

El mecanismo es el siguiente:

---

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

1. *El cliente C envía al FEC un mensaje destinado al servidor S, este mensaje tiene un encabezado de 4 bytes.*

2. *El FEC recibe el mensaje y analiza el encabezado para determinar a quién debe transferirlo, incluye en el encabezado original una estampa de tiempo y lo envía al destinatario adecuado.*

3. *El servidor S recibe un mensaje del FEC cuyo encabezado es de 12 bytes, en él se indica quien lo originó y a que hora se recibió en el FEC.*

4. *El servidor S envía un mensaje dirigido al cliente C, este mensaje tiene un encabezado de 4 bytes.*

5. *El FEC recibe el mensaje del Servidor S, analiza el encabezado, determina a quién debe transferirlo y lo envía.*

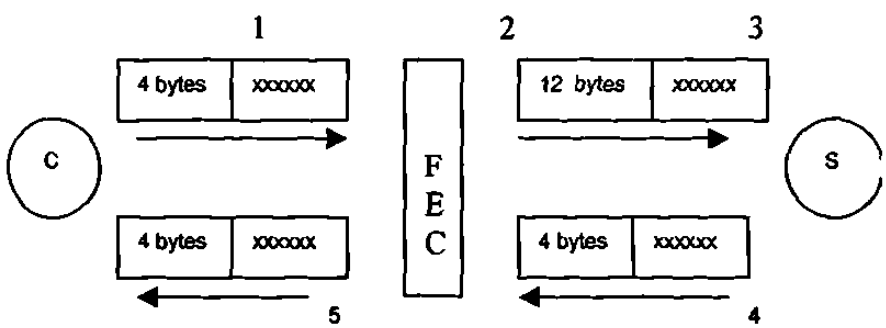
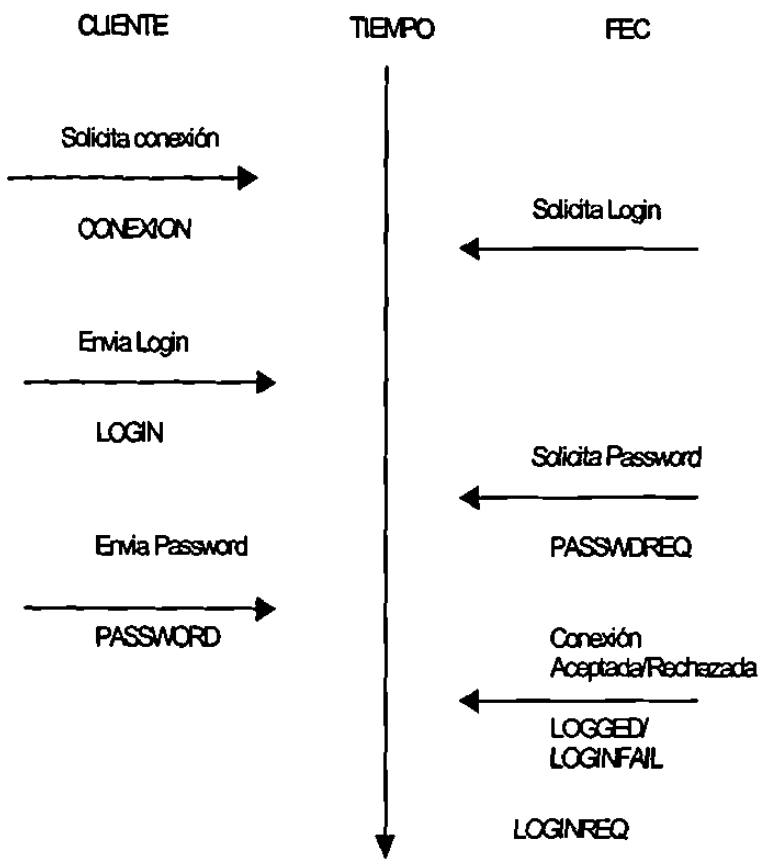


Figura 8. Secuencia de transmisión y recepción de Mensajes en el FEC

Conexión entre un Cliente y el FEC

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



MENSAJES PARTICULARES DE LA APLICACION

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

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

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

1. *El usuario genera, a partir de sus mensajes de datos los archivos parciales necesarios para hacer con ellos un expediente el cual enviará al*

prestador de servicios de certificación. Solicitud de conexión por parte del usuario ante el prestador de servicios de certificación e identificación entre ellos usando un esquema seguro de identificación con certificados digitales (este proceso puede darse mediante un esquema de clave de usuario y contraseña en una primera etapa).

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

3. El usuario almacena su Constancia como considere conveniente.

MENSAJES TIPO FEC

Mensajes del usuario al prestador de servicios de certificación.

Nombre		***Formato***	***Descripción***	***Posible respuesta***

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

Mensajes del prestador de servicios de certificación al usuario

Nomb re		***Form ato***	***Descripción***

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

Juego de caracteres ISO 8859-1 (Latín 1)

Char	Code (código) (en decimal)	Name (nombre)	Description (descripción)
	32	-	Normal space
!	33	-	Exclamation
"	34	quot	Double quote
#	35	-	Hash or pound
$	36	-	Dollar

%	37	-	Percent
&	38	-	Ampersand
'	39	-	Apostrophe
(	40	-	Open bracket
)	41	-	Close bracket
*	42	-	Asterik
+	43	-	Plus sign
,	44	-	Comma
-	45	-	Minus sign
.	46	-	Period
/	47	-	Forward slash
0	48	-	Digit 0
1	49	-	Digit 1
2	50	-	Digit 2
3	51	-	Digit 3
4	52	-	Digit 4
5	53	-	Digit 5
6	54	-	Digit 6
7	55	-	Digit 7
8	56	-	Digit 8
9	57	-	Digit 9
:	58	-	Colon
;	59	-	Semicolon
<	60	lt	Less than
=	61	-	Equals
>	62	gt	Greather than
?	63	-	Question mark
@	64	-	At sign
A	65	-	A

B	66	-	B
C	67	-	C
D	68	-	D
E	69	-	E
F	70	-	F
G	71	-	G
H	72	-	H
I	73	-	I
J	74	-	J
K	75	-	K
L	76	-	L
M	77	-	M
N	78	-	N
O	79	-	O
P	80	-	P
Q	81	-	Q
R	82	-	R
S	83	-	S
T	84	-	T
U	85	-	U
V	86	-	V
W	87	-	W
X	88	-	X
Y	89	-	Y
Z	90	-	Z
[	91	-	Open square bracket
\	92	-	Backslash
]	93	-	Close square bracket
^	94	-	Pointer

_	95	-	Underscore
`	96	-	Grave accent
a	97	-	a
b	98	-	b
c	99	-	c
d	100	-	d
e	101	-	e
f	102	-	f
g	103	-	g
h	104	-	h
i	105	-	i
j	106	-	j
k	107	-	k
l	108	-	l
m	109	-	m
n	110	-	n
o	111	-	o
p	112	-	p
q	113	-	q
r	114	-	r
s	115	-	s
t	116	-	t
u	117	-	u
v	118	-	v
w	119	-	w
x	120	-	x
y	121	-	y
z	122	-	z
{	123	-	Left brace

|	124	-	Vertical bar
}	125	-	Right brace
~	126	-	Tilde
	160	nbsp	Non-breaking space
¡	161	iexcl	Inverted exclamation
¢	162	cent	Cent sign
£	163	pound	Pound sign
¤	164	curren	Currency sign
¥	165	yen	Yen sign
¦	166	brvbar	Broken bar
§	167	sect	Section sign
¨	168	uml	Umlaut or diaeresis
©	169	copy	Copyright sign
ª	170	ordf	Feminine ordinal
«	171	laquo	Left angle quotes
¬	172	not	Logical not sign
-	173	shy	Soft hyphen
®	174	reg	Registered trademark
¯	175	macr	Spacing macron
°	176	deg	Degree sign
±	177	plusmn	Plus-minus sign
²	178	sup2	Superscript 2
³	179	sup3	Superscript 3
´	180	acute	Spacing acute
µ	181	micro	Micro sign
¶	182	para	Paragraph sign
·	183	middot	Middle dot
¸	184	cedil	Spacing cedilla
¹	185	sup1	Superscript 1

º	186	ordm	Masculine ordinal
»	187	raquo	Right angle quotes
¼	188	frac14	One quarter
½	189	frac12	One half
¾	190	frac34	Three quarters
¿	191	iquest	Inverted question mark
À	192	Agrave	A grave
Á	193	Aacute	A acute
Â	194	Acirc	A circumflex
Ã	195	Atilde	A tilde
Ä	196	Auml	A umlaut
Å	197	Aring	A ring
Æ	198	AElig	AE ligature
Ç	199	Ccedil	C cedilla
È	200	Egrave	E grave
É	201	Eacute	E acute
Ê	202	Ecirc	E circumflex
Ë	203	Euml	E umlaut
Ì	204	Igrave	I grave
Í	205	Iacute	I acute
Î	206	Icirc	I circumflex
Ï	207	Iuml	I umlaut
Ð	208	ETH	ETH
Ñ	209	Ntilde	N tilde
Ò	210	Ograve	O grave
Ó	211	Oacute	O acute
Ô	212	Ocirc	O circumflex
Õ	213	Otilde	O tilde
Ö	214	Ouml	O umlaut

×	215	times	Multiplication sign
Ø	216	Oslash	O slash
Ù	217	Ugrave	U grave
Ú	218	Uacute	U acute
Û	219	Ucirc	U circumflex
Ü	220	Uuml	U umlaut
Ý	221	Yacute	Y acute
Þ	222	THORN	THORN
ß	223	szlig	sharp s
à	224	agrave	a grave
á	225	aacute	a acute
â	226	acirc	a circumflex
ã	227	atilde	a tilde
ä	228	auml	a umlaut
å	229	aring	a ring
æ	230	aelig	ae ligature
ç	231	ccedil	c cedilla
è	232	egrave	e grave
é	233	eacute	e acute
ê	234	ecirc	e circumflex
ë	235	euml	e umlaut
ì	236	igrave	i grave
í	237	iacute	i acute
î	238	icirc	i circumflex
ï	239	iuml	i umlaut
ð	240	eth	eth
ñ	241	ntilde	n tilde
ò	242	ograve	o grave
ó	243	oacute	o acute

ô	244	ocirc	o circumflex
õ	245	otilde	o tilde
ö	246	ouml	o umlaut
÷	247	divide	division sign
ø	248	oslash	o slash
ù	249	ugrave	u grave
ú	250	uacute	u acute
û	251	ucirc	U circumflex
ü	252	uuml	u umlaut
ý	253	yacute	y acute
þ	254	thorn	thorn
ÿ	255	yuml	y umlaut

7. Bibliografía

- *Código de Comercio.*
- *Ley Federal sobre Metrología y Normalización.*
- *Reglamento de la Ley Federal sobre Metrología y Normalización.*
- *NMX-Z-13-1997, Guía para la redacción, estructuración y presentación de las normas oficiales mexicanas.*
- *Schneier, Bruce. Applied Cryptography.*
- *Leyes Modelo de la CNUDMI sobre las Firmas Electrónicas y sobre Comercio Electrónico en General.*
- *ISO/IEC 8859-1:1998 Information technology-8bit single-byte coded graphic character sets-Part 1: Latin alphabet No. 1.*

8. Concordancia con normas internacionales

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

TRANSITORIO

UNICO.- *La presente Norma Oficial Mexicana entrará en vigor una vez que la Secretaría de Economía por conducto de la Dirección General de Normas, publique en el* ***Diario Oficial de la Federación*** *el aviso mediante el cual dé a conocer la existencia de infraestructura para llevar a cabo la evaluación de la conformidad en los términos de la Ley Federal sobre Metrología y Normalización y su Reglamento.*

México, D.F., a 20 de marzo de 2002.- El Director General, ***Miguel Aguilar Romo.-*** *Rúbrica."*[5]

5.5. Implicaciones jurídicas.

Como puede observarse, la firma electrónica está comenzando a ser utilizada en muchos países del mundo. La práctica demuestra que éste es un medio seguro y poco costoso de autenticar mensajes y asegurar su integridad y confidencialidad. Ello prueba que puede reemplazar de modo confiable a la firma ológrafa y generar así un entorno favorable para la promoción del comercio electrónico.

Existen sustanciales ventajas tales como:

a) Su disponibilidad instantánea en la cantidad deseada para ser trabajada directamente por el receptor.
b) La rapidez de su envío.
c) Los costos prácticamente insignificantes de su transmisión.

Existen diversas denominaciones para este tipo de firma electrónica, como firma digital y autenticación electrónica. Estas expresiones tienen, en realidad, diferentes significados y suelen ser definidas del siguiente modo:

a) Firma electrónica. Por su parte este concepto se refiere, usualmente, al identificador que va adosado (atachado) o lógicamente asociado a un mensaje electrónico, documento o datos, y los propósitos para los cuales fue incluido implican el concepto jurídico de firma. Un ejemplo de firma electrónica es el nombre tipeado al final de un mensaje de correo electrónico, a pesar de sus deficiencias e seguridad. Esta no requiere, necesariamente, ratificar ninguna porción de información; simplemente indica la intención del signatario. [6]

b) Firma digital. Puede ser definida como una firma electrónica realizada mediante la transformación de un registro electrónico utilizando criptosistemas asimétricos y función hash, de modo que la persona que tiene el mensaje de origen y la clave pública el signatario puede

---

[5] Diario Oficial de la Federación.
[6] Viviana Sarra, Andrea. Comercio electrónico y derecho. P. 389.

determinar si la transformación se efectuó por medio de la clave privada que se corresponde con la clave pública que él tiene y si el mensaje original fue alterado desde que se hizo la transformación.[7]

c) Autenticación electrónica. Esta expresión se refiere al método tecnológico utilizado para confirmar una porción de información.[8]

Cabe destacar que actualmente se están estudiando los denominados "métodos de autenticación biométrica". La biometría se refiere a la identificación de una persona en entornos digitales por medio de los caracteres humanos congénitos, como la escritura, las huellas dactilares, el timbre de la voz o la retina del ojo. Las tecnologías biométricas requieren de una infraestructura similar a la utilizada para la firma digital, de modo de correlacionar de manera segura las características físicas con la persona.

Por el momento, uno de los métodos más seguros de firmar electrónicamente es el de la criptografía de clave pública, denominada usualmente firma electrónica. En los países que cuentan con legislaciones sobre la materia, ésta tiene una amplia gama de aplicaciones, algunas de las cuales enumeramos a continuación:

---

[7] Idem.
[8] Idem.

a) Comunicaciones oficiales; por ejemplo, para llamados a licitaciones públicas, declaración de impuestos o transmisión de documentos con implicaciones jurídicas.
b) Relaciones contractuales en redes informáticas abiertas; por ejemplo, transacciones financieras o compraventa por medios electrónicos.
c) Identificación y autorización; por ejemplo, autorización para conectarse a un determinado sistema de computadoras o identificación de servidores.
d) Utilización dentro de sistemas o redes cerradas; por ejemplo, intranet.
e) Utilización con propósitos personales.

5.6. Infraestructura de la firma electrónica en los ordenamientos jurídicos.

Aunque a primera vista pueda parecer suficiente la existencia de un directorio de claves públicas y un ente que fiscalice que su composición no sea alterada, se requiere, en realidad, de todo un sistema de controles que ha sido denominado *infraestructura de clave pública o infraestructura de firma electrónica,* que es el verdadero soporte para que la firma electrónica pueda ser utilizada en las relaciones jurídicas.

En líneas generales, esta infraestructura tiene como objetivo brindar la mayor seguridad posible y generar la consecuente confiabilidad para los usuarios. Ello se logra por medio del diseño, generación e implementación de un sistema con suficientes controles como para garantizar la reducción del riesgo hasta niveles muy bajos, con el aseguramiento de las siguientes condiciones:

a) Que la clave pública del emisor no haya sido cambiada y que efectivamente se corresponda con su clave privada.
b) Que las técnicas de encriptación utilizadas sean confiables.
c) Que las diferentes tecnologías de encriptación utilizadas para generar las claves sean interoperables.
d) Que los directorios de claves sean actualizados rápidamente, incorporando las bajas de aquellas que hubieren sido comprometidas.
e) Que haya sido probada fehacientemente la identidad de los usuarios (titulares de las claves).

5.7. Arquitectura del Sistema.

Por lo general, los esquemas de la infraestructura de clave pública están basados en una relación jerárquica de entidades y se prevén certificaciones cruzadas. Estas son aquellas en las que hay emisión recíproca de certificados entre participantes y pueden darse en cualquier

nivel de la estructura jerárquica de los integrantes del sistema. Convencionalmente, la arquitectura de un sistema como el mencionado está diseñada de la manera que se explica a continuación:

1) Autoridad de aprobación de políticas. Es la autoridad que establece las políticas que regirán todo el sistema. Sus funciones son:
    a) Establecer los estándares a los que deberá de ajustarse la autoridad de políticas de certificación en el establecimiento de su política;
    b) Aprobar las políticas emitidas por dicha autoridad; y,
    c) Emitir los certificados para la autoridad de políticas de certificación.

2) Autoridad de políticas de certificación. Es la autoridad que determina las tecnologías a utilizar y las prácticas de seguridad de todos los integrantes del sistema. Sus funciones son
    a) Establecer las políticas para el funcionamiento de las autoridades de certificación.
    b) Emitir los certificados para las autoridades certificadoras.

3) Autoridades de certificación. Son las instituciones que tienen a su cargo la emisión de certificados y la confección y mantenimiento de los directorios de claves públicas. Su actividad está normada por las políticas establecidas por la autoridad de políticas de certificación. Sus funciones son:

a) Emitir certificados para otras autoridades de certificación;
b) Emitir certificados paras las autoridades registrantes;
c) Emitir certificados para los usuarios finales; y,
d) Mantener actualizados los directorios de claves públicas vigentes y revocadas.

4) Autoridades registrantes. Son instituciones de inferior rango que las autoridades de certificación, encargadas de facilitar las pruebas de identificación y de comprobar la identidad de los potenciales usuarios. Sus funciones son:
   a) Realizar los procedimientos de registro para las autoridades de certificación, y
   b) Controlar la identidad del usuario cuando se lleva a cabo el registro.
   c) No esta dentro de sus funciones emitir certificados.

5) Usuarios. Son las personas físicas o jurídicas que utilizan las claves.

CONCLUSIÓN

Sin duda, la incorporación de las nuevas tecnologías de la información hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades.

El avance de su implantación en todas nuestras actividades ha provocado cambios de tal magnitud que podemos afirmar que la sociedad actual está inmersa en la era de la revolución informática.

Este avance no es sólo cualitativo, sino de algo más importante, que podemos acceder a todo tipo de información y obtener con ello el beneficio correspondiente.

La información ha sido calificada como un auténtico poder de las sociedades avanzadas, ya tenía su importancia en la antigüedad, pero con el desarrollo de la informática, su valor ha crecido de forma tal que se dirige a un futuro prometedor para unos e incierto para otros.

Las viejas instituciones jurídicas que, a través de los siglos han ido incorporando nuevas realidades sociales, cuando tienen que hacerlo

respecto a estas nuevas tecnologías, en cierto modo ofrecen cierta reticencia y las admiten con reservas.

Hemos comprendido que la informática es un instrumento al servicio del derecho. Contribuye a acelerar y hacer más eficiente algunas labores tradicionales del jurista. Pero es más que un instrumento en la medida que ofrece resultados que no serían posibles de otro modo.

Así ocurre cuando tratamos de adaptar el concepto de firma, tal como antiguamente se concebía, al nuevo campo de las transferencias electrónicas. El objetivo que se pretende con el trabajo que acabamos de exponer es introducirnos dentro del tema del documento informático, haciendo un breve repaso de su aceptación internacional e internacional.

La firma es definida en la doctrina como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto.

La Real Academia de la Lengua, la define como "nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice".

La firma electrónica supone una serie de características añadidas al final de un documento. Es elaborada según procedimientos criptográficos y lleva un resumen codificado del mensaje, y de la identidad del emisor y receptor.

Una firma electrónica es simplemente cualquier método símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Las firmas electrónicas consisten básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la confidencialidad.

La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no violación del secreto.

Los criptosistemas de clave pública, son los más idóneos como firma electrónica, están basados en el uso de un par de claves asociadas: una clave privada, que se mantiene en secreto y una clave pública, libremente accesible por cualquier persona. Este par de claves están matemáticamente

relacionado de tal forma que sólo con la clave pública correspondiente a la clave privada utilizada para firmar puede verificarse el mensaje firmado; además técnicamente son muy resistentes, se calcula en miles de siglos la duración media que tardaría el ordenador más potente para poder romper la clave. Su mecanismo de guardarse y en la certificación de la clave pública por la autoridad certificadora.

Entre los objetivos de la firma electrónica está el conseguir una universalización de un estándar de firma electrónica.

De las anteriores definiciones y exposición realizada podemos inferir las siguientes características:

a) Debe permitir la identificación del signatario.
b) No puede ser generada más que por el emisor del documento, infalsificable e inimitable.
c) Las informaciones que se generen a partir de la signatura electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.
d) La aposición de una signatura debe ser significativa y va unida indisociablemente al documento a que se refiere.
e) No debe existir dilación de tiempo ni de lugar entre aceptación por el signatario y la aposición de la signatura.

En el desarrollo de este tema hemos tratado de dar una idea de los cambios tan importantes que ha experimentado la firma desde sus orígenes hasta nuestros días y como debemos tratar de adaptar estos cambios a la realidad social y dejar la puerta abierta a futuros cambios y otras nuevas tecnologías que sin duda vendrán.

Las nuevas tecnologías de la información y las comunicaciones, unidas a otras técnicas dan fiabilidad al documento electrónico y tratan de lograr una mayor seguridad mediante el desarrollo y extensión de remedios técnicos y procedimientos de control basados en la criptografía.

Esta mayor seguridad que se pretende con una adecuación normativa nos conducirán hacia la autenticación electrónica.

El miedo que existe hacia estas nuevas tecnologías de la información no está en la electrónica, ni en las comunicaciones sino a su mala utilización debido a la no formación y adecuación de las personas y medios a la realidad social.

La firma electrónica con las garantías exigidas por una cada vez más necesaria seguridad jurídica, puede abrir un prometedor camino que deje en entredicho la eficacia real de la fe pública tradicional.

PROYECTO DE LEY DE FIRMA ELECTRÓNICA
EXPOSICIÓN DE MOTIVOS

La comunicación entre los seres humanos, particularmente las comunicaciones a distancia se han facilitado conforme avanza la tecnología. El telégrafo, el teléfono, la radio, la televisión, el fax, cada uno a su tiempo, han representado importantes pasos en materia de comunicación humana, y han conformado una base tecnológica de mucha capacidad, la cual ha iniciado una verdadera revolución en las comunicaciones y el desarrollo de las sociedades contemporáneas. Por su misma naturaleza, requiere cada vez más de mecanismos ágiles y eficientes pero también seguros de comunicación.

Esta cadena de logros tecnológicos en materia de comunicación ha alcanzado un punto muy alto con la extensión de la red internacional o Internet (red de redes), la cual ha ampliado exponencialmente las posibilidades y facilidades de comunicación entre los seres humanos. Es, definitivamente, un medio que no puede ser ignorado por ninguna persona, mucho menos por el sector comercial alrededor de todo el orbe. Y en efecto, no lo ha sido. Los expertos coinciden en afirmar que la Sociedad de la Información ha encontrado en Internet el canal de flujo ideal, por sus preciados atributos: rápido, barato, y cada vez más extendido y eficiente. Cada vez más empresas deciden incursionar en el mercado virtual, y asan

sus comunicaciones externas en ella; igualmente, con más pausa y mesura pero con la misma decisión, los operadores financieros comienzan a utilizar el nuevo medio. Y no podría ser de otra forma ya que en el mercado virtual adquieren ventajas comparativas que sencillamente no existen en el mundo físico, siendo la reducción de costos uno de sus principales beneficios. Es notable que este tipo de instrumento accesible actualmente a una parte de la población, era accesible hasta hace pocos años, únicamente a las corporaciones más poderosas del planeta. La pequeña y mediana empresa ven en efecto en la Internet la posibilidad de un acceso sin precedentes a la información y los mercados mundiales a un costo reducido, y con tendencia a bajar, no a subir, a medida que la red de redes se extiende en todo el orbe. Estamos presenciando una verdadera revolución en el acceso al conocimiento, a la información y la comunicación con consecuencias apenas imaginables para el futuro de la humanidad.

Para las economías en desarrollo como la nuestra, el maximizar los beneficios que ofrece el comercio electrónico es un imperativo; pero también es lograr una posición de vanguardia en la transferencia de tecnología e información, con base al potencial que tiene nuestro país en cuanto a recursos humanos calificados en el área informática, tecnológica y profesional, en general.

Desde el punto de vista jurídico esta revolución tecnológica e nformática ha significado un reto complejo y desafiante: dotar de seguridad jurídica el tráfico, tanto de información como de bienes y servicios. La contratación electrónica debe ser objeto de regulación, en forma muy cuidadosa, para que las nuevas tecnologías de la información no se vuelvan inoperantes. Uno de los temas esenciales a tratar, si no el más importante, es el del reconocimiento legal de la Firma Electrónica. No es posible concebir un creciente desarrollo del ámbito electrónico, y la incursión de otro tipo de transacciones jurídicas en la red, si no se provee de la adecuada seguridad para el normal desempeño de estas actividades. La Firma Electrónica es un mecanismo concebido en función de esta meta prevaleciente, y es objetivo del presente proyecto regular la de forma tal, que existan los elementos jurídicos fundamentales para su desarrollo en un contexto razonable.

Este proyecto de ley es coherente con el derecho internacional en tema de ámbito electrónico, con el propósito de obtener la adecuada seguridad y certidumbre en las transacciones electrónicas basadas en la red de redes. La importancia que reviste la uniformidad respecto al tratamiento de los aspectos más importantes sobre comercio electrónico, es insoslayable. La regulación propuesta pretende mantener la armonía con los elementos principales de la regulación internacional sobre el tema, brindando el marco jurídico adecuado y viable para la contratación electrónica, y en general, las relaciones jurídicas basadas en la comunicación mediante medios

informáticos o telemáticos, sean o no de índole comercial. Esto se haría entonces, esencialmente, a través del reconocimiento de eficacia, desde el punto de vista probatorio, de la Firma Electrónica vinculada a un proveedor de servicios de certificación.

Debe despejarse cualquier duda respecto de la validez jurídica como prueba del documento electrónico, el cual, de conformidad con nuestra legislación procesal civil, es admisible como prueba en sede jurisdiccional.

En concreto, para lograr los objetivos supracitados es preciso: regular el reconocimiento legal expreso de la Firma Electrónica; determinar los efectos de la misma; el reconocimiento del principio de equivalencia funcional por medio del cual se confiere al documento electrónicamente firmado los mismos efectos que se le imputan al documento escrito; acoger el "principio de neutralidad tecnológica", de forma tal que la normativa no limite el mecanismo de Firma Electrónica a una sola tecnología; establecer reglas mínimas en materia de conservación, envío y recepción de mensajes de datos para aquellos casos en que las partes no hayan estipulado reglas especiales.

LEY DE FIRMA ELECTRONICA

TÍTULO I

PRINCIPIOS Y NORMAS GENERALES

CAPÍTULO PRIMERO

DISPOSICIONES GENERALES

ARTÍCULO 1.- La presente Ley tiene por objetivo regular el uso y el reconocimiento jurídico de la Firma Electrónica, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como el autor izar al Estado para su utilización.

ARTÍCULO 2.- Para los propósitos de la presente Ley se establecen las siguientes definiciones:

1.- Acreditación: La acreditación es el procedimiento mediante el cual un organismo autorizado reconoce formalmente que una entidad o empresa es competente para realizar tareas específicas.

2.- Acreditación voluntaria del prestador de servicios de certificación: Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se emite, a petición del interesado, por el Órgano Rector y la Autoridad Competente de acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa intencional aplicable.

3.- Certificado Digital: Es la certificación digital que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

4.- Certificado Digital Reconocido: Es el certificado que cumple con los requisitos establecidos en la presente Ley y su reglamento, y que vincula un documento digital con determinada persona como su signatario, mediante un proceso seguro de certificación y es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la autoridad competente de acreditación.

5.- Datos de creación de firma: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la Firma Digital.

6.- Datos de verificación de firma: Son los datos como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma Digital.

7.- Dispositivo de creación de firma: Es un mecanismo que sirve para aplicar los datos de creación de firma.

8.- Dispositivo de verificación de firma: Es un mecanismo que sirve para aplicar los datos de verificación de firma.

9.- Dispositivo seguro de creación de firma: Es el mecanismo de creación de firma que cumple adicionalmente con los requisitos establecidos en la presente Ley y su reglamento.

10.- Documento: Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra naturaleza, y que se puede recuperar o reproducir en una forma perceptible e inteligible.

11.- Firma Electrónica: Es el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

12.- Firma Electrónica Avanzada: Es la Firma Electrónica Certificada por un prestador de servicios de certificación debidamente acreditado ante la autoridad competente de acreditación.

13.- Información: Es aquel mensaje comunicado mediante datos, textos, imágenes, sonidos, códigos, programas, información almacenada en bases de datos, aplicaciones, o similares.

14.- Iniciador: Es quien envía un mensaje de datos, esté o no suscrito digitalmente.

15.- Información Íntegra: Se entenderá por integra aquella información que haya permanecido completa e inalterada, sin menoscabo de cualquier adición o cambio, inherente al proceso de comunicación, almacenamiento, archivo o presentación. El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

16.- Intermediario: Es aquella persona, física o jurídica, que actuando por cuenta de otra, envíe, reciba, almacene dicho mensaje o preste algún otro servicio con respecto a él.

17.- Mensaje de datos: Es la información generada, enviada, recibida, almacenada, o comunicada por medios digitales, electrónicos, ópticos o similares.

18.- Prestador de servicios de certificación o entidad certificadora: Es la persona física o jurídica que expide certificados.

19.- Procedimiento seguro: Es el procedimiento empleado con el propósito de verificar que una Firma electrónica es atribuible a determinada persona como su signatario, o para detectar cambios y errores en un documento digital, incluyendo cualquier proceso que implique el uso de algoritmos matemáticos,

códigos, sistemas de encriptamiento, y cualquier otro medio o tecnología de identificación o reconocimiento.

20.- Producto de Firma Electrónica: Es el instrumento y sus componentes específicos, destinados a la prestación de servicios de Firma Electrónica por el prestador de servicios de certificación o para la creación o verificación de Firma Electrónica.

21.- Receptor: Es la persona a quien el signatario dirige el mensaje o documento electrónico.

22.- Signatario: Es la persona física o jurídica que cuenta con un mecanismo de creación de firma, que actúa en nombre propio o con poderes de representación de otra persona física o jurídica.

23.- Sistema: Es el conjunto de elementos independientes pero interrelacionados entre sí para conseguir un propósito común.

24.- Sistema de información: Es un conjunto de elementos ordenado utilizado para generar, enviar, recibir, almacenar o procesar de alguna forma mensajes de datos.

ARTÍCULO 3.- En la presente Ley se utilizará el término electrónico entendido como cualquier información codificada en dígitos.

CAPÍTULO II
RECONOCIMIENTO JURÍDICO DE LA FIRMA ELECTRÓNICA

ARTÍCULO 4.- La Firma Electrónica Avanzada, deberá crearse mediante un dispositivo seguro de creación de firma.

ARTÍCULO 5.- La Firma Electrónica Avanzada, siempre que esté basada en un certificado electrónico reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel. Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento electrónico, si el mismo ha sido firmado mediante una Firma Electrónica Avanzada, creada por un dispositivo seguro de creación de firma. Se presumirá que la Firma Electrónica Avanzada y el medio de creación de firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en este apartado cuando el certificado reconocido es emitido por un prestador de servicios de certificación acreditado.

ARTÍCULO 6.- Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado, o de cualquier otra forma reconocido, verificado o certificado, tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma electrónica o Firma Electrónica avanzada.

CAPÍTULO III
USO DE LA FIRMA ELECTRÓNICA Y LOS DOCUMENTOS ELECTRÓNICOS POR EL ESTADO

ARTÍCULO 7.- Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, , así como a los organismos públicos descentralizados para la utilización de la Firma Electrónica avanzada y los documentos electrónicos firmados electrónicamente en sus relaciones internas, entre ellos y con los particulares, de conformidad con las previsiones de esta Ley y su reglamento.

TÍTULO II
DE LOS SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA
CAPÍTULO I
DEL ÓRGANO RECTOR

ARTÍCULO 8.- Para la debida vigilancia y aplicación de la presente Ley; se creara un organismo público descentralizado denominado Centro Estatal de Ciencia y Tecnología.

ARTÍCULO 9.- El Poder Ejecutivo, a través del Centro Estatal de Ciencia y Tecnología, utilizará un sistema de acreditación voluntario, en el ámbito de los prestadores de servicios de certificación de Firma Electrónica Avanzada, coordinando para ello con la Autoridad de Acreditación, la cual será un ente con participación activa y equilibrada de los sectores involucrados. La autoridad de acreditación mediante la función de acreditación, reconoce formalmente que una organización es competente para llevar a cabo tareas específicas de acuerdo a los requisitos de normas nacionales e internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente, los derechos de los usuarios, para lo cual deberá llevar a cabo el proceso de evaluación correspondiente, un registro de las entidades acreditadas y velar por que se cumplan los requisitos establecidos por esta Ley y su reglamento.

CAPÍTULO II

CERTIFICADOS DIGITALES

ARTÍCULO 10.- Los certificados digitales se vinculan con una persona confirmando su identidad, los cuales deberán contener al menos:

1.- Los datos que identifiquen individualmente al firmante.

2.- Los datos que identifiquen a la entidad de certificación.

3.- Número de serie del certificado.

4.- Fecha de emisión y plazo de vigencia.

5.- Los demás que el reglamento establezca.

ARTÍCULO 11.- Los certificados digitales se podrán cancelar y revocar en los siguientes casos:

1.- A solicitud del titular de la firma.

2.- Por expiración del plazo.

3.- Por cese de operaciones de la entidad de certificación.

4.- Por muerte del titular de la Firma Digital.

5.- Por incumplimiento contractual con la entidad de certificación.

6.- Las demás que el reglamento establezca.

TÍTULO III

LOS DISPOSITIVOS DE FIRMA ELECTRONICA AVANZADA Y LA EVALUACIÓN DE SU CONFORMIDAD CON LA NORMATIVA APLICABLE

CAPÍTULO ÚNICO

ARTÍCULO 12.- Los dispositivos seguros de creación de Firma Electrónica para considerarse como tales deberán cumplir con:

1.- Garantizar que los datos utilizados para la generación de firma puedan producirse sólo una vez y asegurar, razonablemente, su secreto, dentro de las posibilidades o limitaciones tecnológicas.

2.- Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado.

3.- Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros.

4.- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

ARTÍCULO 13.- Los dispositivos de verificación de Firma Electrónica Avanzada deben garantizar al menos lo siguiente:

1.- Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.

2.- Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.

3.- Que aparezca correctamente la identidad d el signatario.

4.- Que se verifique de forma fiable el certificado.

5.- Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.

ARTÍCULO 14.- Las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Electrónica basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte.

ARTÍCULOS TRANSITORIOS

ARTÍCULO PRIMERO. La presente Ley entrará en vigor al día siguiente de su publicación el Periódico Oficial del Estado.

ARTÍCULO SEGUNDO. El reglamento de la Presente Ley deberá expedirse en un plazo no mayor a sesenta días naturales, contados a partir del siguiente de su entrada en vigor.

ARTÍCULO TERCERO. El Centro Estatal de Ciencia y Tecnología deberá de comenzar sus funciones a los tres días de haber sido publicada la presente Ley en el Periódico Oficial del Estado y su reglamento interior deberá de ser aprobado y publicado en el mismo instrumento de comunicación gubernamental siete días después de haber iniciado sus operaciones.

BIBLIOGRAFÍA

1. Aldrich, Douglas. Dominio del Mercado Digital. Ed. Oxford. México, 2000.

2. Alvarez Cienfuegos Suárez, José María. Documento Electrónico, Norma Legal y Deontológico de la Informática. Ed. McGraw-Hill. México, 1995.

3. Arellano García, Carlos. Métodos y Técnicas de la Investigación Jurídica. Ed. Porrúa. México, 1999.

4. Asís Roig, Agustin. Documento Electrónico en la Administración Pública. Cuadernos de Derecho Judicial, Escuela Judicial y Consejo General del Poder Judicial. Madrid, 1996.

5. Barriuso Ruiz, Carlos. Interacción del derecho y la informática. Ed. Dykinson. Madrid, 1996.

6. Davara Rodríguez, Miguel Angel. Manual de Derecho Informático. Ed. Aranzandi. Pamplona, 1997.

7. Davara Rodríguez, Miguel Angel. La sociedad de la información y el tratamiento de datos de carcater personal. Facultad de Derecho e Instituto

de Informática Jurídica de la Universidad Pontificia de Comillas. Ed. Aranzandi. Madrid, 1998.

8. Diccionario de Ciencias Jurídicas, Políticas, Sociales y de Economía. Ed. Universidad. México, 2000.

9. Diccionario Jurídico Espasa. Ed. Espasa. Madrid, 1999.

10. Gallardo Ortiz, Miguel Angel. Criptología; seguridad informática y derecho. Leyes del Ciberespacio. Centro Regional de Extremadura. Ed. Aranzandi. Madrid, 1994.

11. Gallardo Ortiz, Miguel Angel. Firmas electrónicas mediante cripotología asimétrica. Revista de Informática y Derecho. Centro Regional de Extremadura, 1995.

12. Julia Barcelo, Rosa. Firma digital y Trusted Third Parties: Iniciativas reguladores a nivel internacional. Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas. Madrid, 1998.

13. Kegley, Charles W. Y Wittkopff, Eugene. The Global Agenda. Issues and Perspectives. Ed. McGraw-Hill. Estados Unidos de Norteamérica, 1992.

14. Larrieu, J. Les nouveaux moyens de preuve: pour ou contre l'identification des documents informatiques à des escrits sous seig privé. Cahiers Lamy du Droit de l'informatique. Ed. Pantin. Francia, 1988.

15. Maqueo, Ana María- Redacción. Ed. Limusa. México, 1985.

16. *Pardini, Aníbal a. Derecho de internet. Ediciones* La Rocca. Buenos Aires, 2002.

17. Revista Jurídica de la Universidad Autónoma de Madrid.

18. Rodríguez Campos, Ismael. Técnicas de la Investigación Documental. Lazcano Garza, Editores. México, 1997.

19. Sarra, Andrea. Convenio Electrónico y Derecho. Ed. Astrea. Buenos Aires, 2001.

20. Tellez Valdés, Julio. Derecho Informático. Ed. McGraw-Hill. México, 1999.

21. Universidad Nacional Autónoma de México. Diálogo sobre la informática jurídica. Instituto de Investigaciones Jurídicas, 1989.

22. Wittker, Jorge y Larios, Rogelio. Metodología Jurídica. Ed. McGraw-Hill. México, 1997.

www.legatek.com

www.kriptopolis.com. Criptografía y seguridad en internet.

www.map.es. Comité Técnico del Consejo Superior de Informática.

www.ilpf.org. Digital Signature Legislation.

www.alltheweb.com

www.google.com

www.worldbank.org

www.jurídicas.com

www.diccionarios.com