Universidad de Guadalajara

CUCSH
Centro Universitario de Ciencias Sociales y Humanidades

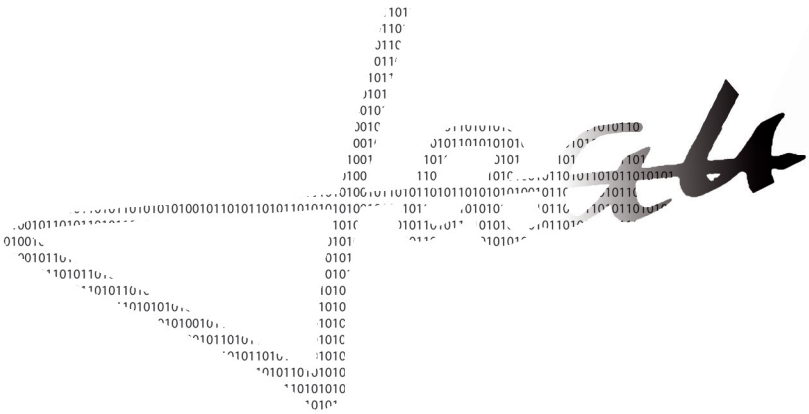
Colección Graduados 2010
Serie Sociales y Humanidades

1

Irma Contreras López

La firma electrónica y la función notarial en Jalisco

Homologación federal y estatal



Este libro se justifica al afirmar que la sociedad en que vivimos es, sin lugar a dudas, sustancialmente diferente a la que se desarrollaba décadas atrás, donde el implacable avance de la tecnología ha modificado la estructura social y ha llegado a diversos ámbitos de la misma: económico, sociocultural, político, científico y –obviamente– también al jurídico; por lo tanto, no podemos oponernos a la realidad que enfrentamos con el uso de tecnologías, tales como, internet, documentos digitales, protocolo electrónico y firma electrónica, los cuales generan nuevas y complejas formas de relación humana, que no siempre pueden pasar inadvertidas por el Derecho. Por ello, esta investigación tiene como principal objetivo reflexionar acerca de los avances científicos-tecnológicos que se conjugan para establecer desafíos en la ciencia del Derecho, pensando principalmente en el Derecho notarial, auxiliado con la firma electrónica y su certificación.

La firma electrónica y la función notarial en Jalisco

Colección Graduados
Serie Sociales y Humanidades

Núm. 1

Irma Contreras López

La firma electrónica y la función notarial en Jalisco

Homologación federal y estatal

Universidad de Guadalajara
2011

D345.733097235
CON

Contreras López, Irma.

La firma electrónica y la función notarial en Jalisco:
Homologación federal y estatal/ Irma Contreras López.

1ª. ed.

Guadalajara, Jal: Universidad de Guadalajara,
Centro Universitario de Ciencias Sociales y Humanidades,
Editorial CUCSH-UDG, 2011

(Colección Graduados)
(Serie Sociales y Humanidades ; 1)

1. Firmas personales.
2. Derecho Notarial – Jalisco.

Universidad de Guadalajara,
Centro Universitario de Ciencias Sociales y Humanidades.

Primera edición, 2011

Centro Universitario
de Ciencias Sociales y Humanidades
Editorial CUCSH-UDG
Guanajuato 1045
Col. La Normal
44260 Guadalajara, Jalisco, México

ISBN Obra completa 978-607-450-377-7
ISBN E-book 978-607-450-378-4

Hecho en México
Made in Mexico

PIFI
PROGRAMA INTEGRAL DE FORTALECIMIENTO INSTITUCIONAL

Esta edición fue financiada con recursos del Programa Integral de Fortalecimiento Institucional (PIFI) 2009 a cargo de la Secretaría de Educación Pública.

Índice

Prólogo

▲

Manuel Bailón Cabrera

La institución notarial, en la trayectoria histórica de la humanidad, ha servido para dar autenticidad y relevancia a los hechos y actos jurídicos que trascienden a la persona y a la sociedad. Notaría es sinónimo de certeza, veracidad y paz social.

El instrumento notarial es digno de fe porque refleja la realidad, y porque fue elaborado por un profesional del Derecho, que en forma independiente del Estado y de las partes interpretó la voluntad y el alcance de las obligaciones.

Todo aquello que preserva la esencia de la función notarial y facilita las labores de los fedatarios es bienvenida a las instituciones notariales; es más, su utilización será factor de la propia evolución y mejoramiento del servicio notarial.

El Colegio de Notarios del Estado de Jalisco impulsó el establecimiento de la maestría en Derecho Notarial y Registral con el reconocimiento, apoyo y directrices de la Universidad de Guadalajara, promoviendo nuevos modelos de investigación, de los cuales tiene además la calificación y el reconocimiento del Consejo Nacional de Ciencia y Tecnología (Conacyt). Por eso, con gran satisfacción escribo este prólogo al trabajo de la ya maestra en Derecho Irma Contreras López.

Esta obra es resultado de una amplia labor de investigación legislativa, documental y bibliográfica que sustenta la dimensión de la importancia y la innovación contractual del derecho informático y del gobierno electrónico.

Recordemos que el pasado 29 de agosto del 2003 se publicaron en el *Diario Oficial de la Federación* las reformas y adiciones de las diversas disposiciones del Código de Comercio en materia de firma electrónica, que comprende de los numerales del 89 al 114, lo que posibilitó que el derecho mercantil mexicano se incorporara a la tendencia universal de la telecontratación con personas ausentes, así como la innovación en los servicios financieros; colateralmente se implementaron de manera electrónica trámites ante la Secretaría de Hacienda y Crédito Público a través del Sistema de Administración Tributaria para la presentación de la Declaración Informativa de Notarios Públicos y demás Fedatarios (DECLARANOT) en lo correspondiente a la Secretaría de Relaciones Exteriores a través del Sistema Integral para

el artículo 27 constitucional (SIPAC), de igual forma en la Secretaría de la Función Pública y en el Registro Único de Personas Acreditadas (RUPA).

Por otro lado, el 23 de agosto de 2006 fue aprobada la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, la cual se publicó el día 14 de septiembre del mismo año y entró en vigor el día 1 de enero de 2007, y su reglamento fue publicado el 28 de noviembre de 2008, los cuales dieron las bases para que la tramitología en materia notarial se pueda dar electrónicamente en el Registro Público de la Propiedad y de Comercio por medio del Sistema Integral Registral de Jalisco a través de los medios electrónicos y en el área de comercio en su referente al Sistema Integral de Gestión Registral (FEDANET), perteneciente a la Secretaría de Economía.

Así, se encuentran en esta plataforma de modernización el Archivo de Instrumentos Públicos, Procuraduría Social, Secretaría de Finanzas, las Oficinas Catastrales y Tesorería Municipales.

Sin dejar de mencionar la importancia de una homologación de lo estatal a lo federal en materia de firmas electrónicas, se tomaría como base el Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal (ITFEA) publicado el día 24 de agosto de 2006 en el *Diario Oficial de la Federación*.

En el trabajo se consignan conceptos de la visión del papel al formato electrónico; el aspecto técnico de la firma electrónica; así como qué existe y qué falta en los dispositivos legales vigentes; la firma electrónica en la práctica; la necesidad de homologación de criterios en su utilización en el ámbito federal, así como el uso de las tecnologías de la información en la actividad notarial, sin restarle importancia al contexto global de la firma como medio de identificación y, finalmente, el problema ante el uso y certificación de la firma electrónica para los usuarios de ésta y la función notarial.

En este orden de ideas, el notario jalisciense está consciente de las aspiraciones de solemnidades contractuales impuestas legalmente a través de la redacción por vía del documento electrónico y firma electrónica.

Finalmente, de manera individual, cada notario debe estar preparado desde el punto de vista técnico para ofrecer los mismos servicios profesionales actuales a través de los medios electrónicos. Es un hecho que nuestra sociedad cada día se encuentra más vinculada a estas tecnologías de la información y demanda actualización de notarios y de su personal.

Introducción

En nuestro tiempo, las nuevas tecnologías de información y comunicación han transformado con su aplicación casi todas las actividades que el ser humano realiza en el umbral de este siglo XXI. En el presente momento histórico son tecnologías e informaciones que circulan en todas las direcciones, están disponibles en cualquier momento y ya no dependen de limitaciones tales como las horas de servicio de oficina pública o de las posibilidades reales de traslación física.

Ello nos lleva a pensar que el Derecho tiene que seguir innovándose para dar soluciones a los esquemas cambiantes y no quedarse con las instituciones obsoletas, dejando en claro que los principios esenciales conservan su valor, puesto que la libertad, la justicia y la solidaridad entre sociedad y gobierno tienen vigencia más que nunca. Visto de esta manera, la ciencia del Derecho, y específicamente la actividad notarial, se insertan paulatinamente en el moderno esquema de sociedad digital, para dar paso a una nueva generación de actividades y procesos sistematizados, cada vez más lejos del papel, considerado como elemento fundamental en la certificación de documentos de orden legal, y que hasta hoy ha sido el sustrato básico del oficio notarial.

La transformación de las relaciones sociales vinculadas al proceso de globalización influye en la celebración de acuerdos de voluntades, y éstos por lo general son originados del tráfico mercantil, para luego extenderse al ámbito del Derecho privado como la fuente primordial de las obligaciones.

Se entiende como *contrato* al instrumento técnico para crear, entre las personas que en él intervienen, relaciones jurídicas y así regular sus múltiples necesidades personales a las que el ordenamiento jurídico reconoce efectos jurídicos (Azar, 2005: 92). Por ello, los avances tecnológicos traen consigo cambios en todos los campos sociales, lo que provoca que las sociedades evolucionen y se produzcan cambios importantes, como generar nuevos ordenamientos o adecuar las leyes existentes a las nuevas necesidades.

La firma digital nace de manera justificable desde el momento en que los contratos, las transacciones económicas, las compras o cualquier acto traslativo

de dominio, entre otras figuras jurídicas de igual importancia, se realizan *online*, es decir, sin la presencia física de las partes; por ello, los mensajes de datos que ostenta una firma electrónica, tienen el mismo efecto que un documento con una firma autógrafa.

Su validez dependerá, entonces, de la fiabilidad de la firma electrónica o, mejor aún, del método en que ésta se generó. Así, el hecho de que una firma sea generada por el usuario a través de medios que mantiene bajo su control (clave privada, contraseña, datos biométricos, tarjeta, chip, etc.), asegurando la imposibilidad de que ocurra una suplantación de personalidad, entonces aplicado al ámbito de Derecho notarial, los actos en los que intervenga el notario de igual forma brindarán la certeza y la seguridad jurídica como los plasmados en papel.

Castells,[1] en su obra *Local y global,* menciona que la tecnología no determina la organización social, sino que es la propia sociedad y el sistema económico vigente los que se encargan de adaptar sus necesidades a los avances tecnológicos que van surgiendo (Castells, 1999).

Bajo esa inercia, en México se ha dado luz verde a diversas legislaciones en el ámbito federal y estatal, a reglamentos orgánicos de dependencias federales, estatales, normas de aplicación y homologación que regulan los aspectos jurídicos y técnicos relativos a la generación, uso y aplicación de la firma electrónica, en donde se le da la misma validez que a la firma manuscrita, además de regular a los prestadores de servicios de certificación digital y firma electrónica.

En Jalisco esa nueva norma se emitió al abrigo del decreto número 21432/LVII/06 por la LVII Legislatura del Congreso del Estado, publicada en el *Periódico Oficial El Estado de Jalisco*, el día 14 de septiembre de 2006, sección II, bajo el nombre de Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, reformando y adicionando artículos en legislaciones del estado de Jalisco.

Así, a más de dos años de su aprobación, los beneficios, lagunas y criterios de aplicación siguen presentes en la función notarial, donde surgen discusiones sobre la certeza y seguridad jurídica al dar forma a la voluntad de las partes, surgiendo entonces una serie de cuestionamientos, como: ¿quién nos garantiza con efectivi-

[1] Sociólogo español nacido en 1942, intelectual moderado e investigador denso. Éste es, sin duda, el intelectual que ha estudiado el impacto "de la sociedad de la información" con mayor extensión, profundidad y perspicacia. Políticamente comprometido (español exiliado en Francia en los 60, fue expulsado de este país durante las revueltas estudiantiles del 68), cercano al socialismo (colaboró activamente en la redacción del Programa 2000 del PSOE y de varios estudios sobre las nuevas tecnologías durante el gobierno socialista). Ha sido profesor de numerosas universidades –París, México, Chile, Madrid y Barcelona– y catedrático de sociología y planificación urbana y regional de la Universidad de California en Berkeley.

dad que los contratantes o las partes sean quienes dicen ser?, ¿cómo saber que la información en su trayecto por internet no ha sido manipulada?, ¿cómo identificamos que un sitio de internet cumple con las características de seguridad para realizar transacciones confiables?

Con el presente trabajo se pretende establecer que la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, a pesar de otorgar bondades y beneficios a la población jalisciense, aún no ha tenido una aplicación real, porque no se tienen los suficientes certificadores registrados ante la Secretaría General de Gobierno, y mucho menos se cuenta con un padrón de registro de usuarios de firmas electrónicas. La problemática real se presenta en la adopción de la firma electrónica por la ciudadanía ya que su uso resulta un privilegio exclusivo de algunos sectores y sólo en materia federal.

Justificación del tema y metodología aplicada

Este libro se justifica al afirmar que la sociedad en que vivimos es, sin lugar a dudas, sustancialmente diferente a la que se desarrollaba décadas atrás, donde el implacable avance de la tecnología ha modificado la estructura social y ha llegado a diversos ámbitos de la misma: económico, sociocultural, político, científico y –obviamente– también al jurídico; por lo tanto, no podemos oponernos a la realidad que enfrentamos con el uso de tecnologías, tales como, internet, documentos digitales, protocolo electrónico y firma electrónica, los cuales generan nuevas y complejas formas de relación humana, que no siempre pueden pasar inadvertidas por el Derecho. Por ello, esta investigación tiene como principal objetivo reflexionar acerca de los avances científicos-tecnológicos que se conjugan para establecer desafíos en la ciencia del Derecho, pensando principalmente en el Derecho notarial, auxiliado con la firma electrónica y su certificación.

Se pretende evidenciar que la vigente Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios no ha tenido una aplicación real, ya que no contamos con suficientes certificadores registrados ante la Secretaría General de Gobierno, ni con un registro de usuarios de firmas electrónicas en el estado, generando que no se aplique de manera efectiva el uso de la firma electrónica en beneficio de la ciudadanía, a pesar de que se cuenta con 309 notarios en el estado, los cuales pudieran actuar como autoridad certificadora, considerados para mí como la figura idónea para dar fe y legalidad a la certificación de firmas electrónicas y documentos en formato digital, por la seguridad y confianza que reviste la figura del notariado para la población en general.

Lo que interesa para este trabajo es analizar el Derecho "que es" y no el Derecho "que debiera ser" (desde el punto de vista positivista), entonces, el Derecho es válido y vigente.

En este contexto, con mi investigación pretendo demostrar que la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios no tiene una aplicación efectiva en el estado.

Esta investigación, en primer término, se forma de la siguiente manera:

Su objeto lo constituye el orden jurídico vigente que no se está aplicando con efectividad.

Su fin es la determinación del contenido normativo del orden jurídico en el contexto de validez.

Su fuente son las normas jurídicas positivas (Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios y otras leyes correlacionadas), la historia de su establecimiento, la interpretación de éstas y su aplicación efectiva.

Con la finalidad de encontrar sustento al realismo jurídico de la práctica social del Derecho como un medio de construcción e ingeniería social, de tal manera que se pueda establecer que un sistema de normas es efectivo en la medida en que éstas son observadas y los destinatarios se sientan vinculados por ellas. Por eso se seguirán tres pasos:

1. *Investigación jurídica descriptiva*. Para dilucidar los principales aspectos históricos, técnicos y jurídicos relacionados con la firma electrónica y el creciente valor que ha adquirido en nuestros días en el mundo de las tecnologías de la información, así como la forma en que tal fenómeno ha repercutido en la sociedad, en el estado y en el ámbito jurídico.

   Se destacan la importancia que la informática jurídica adquiere en dicho escenario y los problemas jurídicos que se han presentado en torno a sus diversos usos e impactos en la adopción de mecanismos que den seguridad en las relaciones y transacciones comerciales, los trámites gubernamentales *on line,* y en general las relaciones entre los usuarios del ciberespacio con el uso de las tecnologías de la información como es en este caso: *la firma electrónica*.

   Todo lo anterior, con el propósito de brindar un panorama general acerca de la importancia de la firma electrónica y su aplicación en la "sociedad digital".
2. *Investigación jurídica exploratoria*. Presentar la necesidad de contar con un estado jurídicamente moderno, acorde al desarrollo de las nuevas tecnologías que permita a la función notarial constituirse como el ente certificador idóneo en el uso de la firma electrónica como un puente efectivo entre el usuario y firma electrónica, actuando como garante de seguridad y confianza para el usuario.
3. *Investigación jurídica comparativa*. Mediante la técnica de Derecho comparado, en sus dos vertientes generadoras:
   a) El Derecho internacional a través del cual proliferan los tratados comerciales multilaterales y regionales.

b) El Derecho local, por ello resulta necesario tratar lo que existe y lo que falta en el Derecho mexicano relacionado con otras legislaciones en el uso y explotación de la firma electrónica.

4. *Investigación jurídica proyectiva*. Una de las características del nuevo milenio es que los asuntos nacionales se vuelven de interés global y que los Estados-nación ven disminuir sus jurisdicciones y sus facultades.
5. *Investigación jurídica analítica*. Estableciendo la problemática a que se puede enfrentar el usuario, la entidad certificadora y todos y cada uno de los actores que intervienen en la implementación de la firma electrónica.

Planteamiento del problema

En un inicio, internet, y en general las grandes redes de comunicación eran usadas tan sólo por la comunidad científica como medio de intercambio de ideas; el sistema era reducido cual pequeña comunidad, no era necesaria una regulación al funcionar prácticamente sin fricciones. No obstante, las autopistas de la información innovaron y se desarrollaron a gran velocidad, y la pequeña comunidad de usuarios se convirtió en una aglomeración de usuarios en la red, ocasionando problemas en su organización, función y en las relaciones entre sus usuarios, transacciones comerciales, envío de información, celebración de convenios diversos. En fin, un sinnúmero de situaciones que suponen un doble cambio para la ciencia jurídica y la informática, ampliando su objeto y extendiéndose a los nuevos medios en todas las dimensiones en que se desenvuelve la vida humana, un nuevo medio que reclama la aplicación de criterios jurídicos.

En este sentido, muchos países han promulgado leyes que buscan resolver dicha problemática. En México, estos ordenamientos aún son incipientes y se encuentran pendientes de una aplicación efectiva, así como de conocer sus alcances.

Un aspecto de gran peso respecto a regular dichos avances tecnológicos, y como consecuencia de las relaciones humanas que se dan en el mundo *on line*, es la firma electrónica, que nace de la necesidad de dar seguridad jurídica e identidad a las partes que celebran actos jurídicos de toda índole en la Red; no obstante, su aplicación aún no ha logrado el empuje que se ha buscado, debido a un desconocimiento en materia de informática casi generalizado, del cual el poder legislativo no está exento. Muchos de nuestros legisladores ni siquiera se explican o conciben términos como internet, telemática, firma electrónica y certificado digital, entre otros, desconocidos para muchos, y más aún su compleja o simple estructura, según el punto de vista.

Sin embargo, el Poder Legislativo no se encuentra solo, pues arrastra también al Poder Judicial y al Ejecutivo en las mismas carencias al no proveerle un marco jurídico que sustente su actuar; lamentablemente, la tipificación de delitos y la regula-

ción de tecnologías de la información, como son los mensajes de datos, las transferencias de información, la celebración de actos traslativos de dominio vía internet, que implican el uso de mecanismos como la firma electrónica o las certificaciones de documentos digitales, se encuentran aún vulneradas por la información contenida en redes públicas o privadas, donde la comprobación de fraudes informáticos o del robo de información, el establecimiento de responsabilidades por errores en la transmisión de datos, así como la seguridad de éstos o la implementación de esquemas probatorios para el caso de futuras controversias, está todavía muy lejos de aplicarse, pero no por eso es carente de viabilidad, y en ese sentido el uso de la firma electrónica aporta grandes avances en la identificación del emisor y receptor, es decir, reconoce a las partes que interactúan en la sociedad de la información dando nombre y apellido a los autores.

Con la aparición de nuevos sistemas de comunicación, la internet se está convirtiendo en un canal de distribución de insumos sumamente atrayente para todo tipo de público, de tal manera que las redes informáticas abiertas son con toda probabilidad el medio clave para la interacción de diversas relaciones que producen numerosas situaciones que pueden llegar a ser violatorias de principios de Derecho como la libertad, justicia, equidad o la igualdad. En este caso se ve la necesidad de aplicar con efectividad y seguridad la firma electrónica –objeto del presente estudio–, y no por ello olvido el resto de situaciones violatorias de Derecho que pueden presentarse dentro de la Red, problemas que existen para el desarrollo de este proceso de integración de diferente orden, y que van desde problemas políticos y económicos hasta problemas técnicos como la incompatibilidad del *hardware* existente, donde algunas dependencias tienen un nivel de equipo de cómputo sumamente innovador mientras que en otras es deplorable; diferencias en el tipo de *software* empleado y la falta de capacitación, o la disparidad en la actuación de las diversas autoridades en el empleo de los programas computacionales; problemas de confidencialidad artificial de la información (falta de ética en el manejo y almacenamiento de ésta); problemas por la armonización de conceptos y definiciones derivadas del alto desconocimiento en la materia como lo vengo señalando; problemas de estandarización de políticas informáticas incompletas o que nunca se han concretizado. Y así podemos enlistar cientos de conflictos técnicos, jurídicos y políticos que hacen que las soluciones se tornen más difíciles, como acertadamente señala Castells, y que ya empieza a verse reflejado en la actualidad nacional e internacional donde se exponen las características de la revolución tecnológica en curso y donde se intenta formalizar las relaciones entre capitalismo, informática y cambio tecnológico.

Por otra parte, las implicaciones tecno-económicas de esta realidad en productividad, competitividad, bienestar de una sociedad "en la era de la información", transferencia de tecnología, gestión del cambio tecnológico y de innovación tecnológica, entre otros, son graves porque, mientras nuestros principales competidores

crean las ventajas competitivas y dinámicas del nuevo siglo, en México el debate "hacia una infraestructura mexicana de información" con miles de trabajos empieza formalmente, lo que nos deja indefensos, es decir, un estado de nulidad de competencia de infraestructura.

Para México, el principal reto no sólo se enfoca a desarrollar la infraestructura física de información (red nacional) sino además los contenidos; y es aquí donde no sólo está el doble reto de, por un lado, estandarizar toda la información de dominio público del gobierno, y además el fomento de los servicios telemáticos, de información privados y la estandarización de mecanismos de seguridad como los certificados digitales, la implementación y homogeneización de la firma electrónica en todos los niveles.

En ese sentido, el problema principal y planteamiento de la hipótesis es que el notario resulta la figura idónea para fungir como certificador**,** de conformidad con la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, y que si no se ha dado la coyuntura es en consecuencia de tres aspectos: primero, el desconocimiento generalizado de la informática, segundo, la falta infraestructura adecuada para la prestación del servicio, y tercero, la falta de interés por parte del Gobierno estatal para impulsar el uso efectivo del ordenamiento legal mediante el registro de autoridades certificadoras, la homologación técnica de la firma electrónica con las normas federales y la difusión de la misma entre la población.

La firma electrónica y sus dimensiones

Antes de aterrizar el tema de la firma electrónica, resulta necesario delimitar su dimensión social, cultural, política y económica.

La firma digital es un instrumento más que permite la adaptación a este nuevo paradigma socio-económico-cultural, que posibilita la expansión del comercio dentro de esta nueva economía digital globalizada, rediseñando las relaciones laborales y la interacción humana en el ámbito administrativo o gubernamental, optimizando la eficiencia a un bajo costo, con intervención y participación de los administrados (ciudadanos). Lo que importa es dotar al sistema de una mayor transparencia y obtener la consecuente reducción del gasto público y restablecer la credibilidad en las instituciones democráticas, algo que debe garantizar todo estado social de Derecho.

Dimensión histórica de la firma electrónica

El término *tecnología*, usado a partir del surgimiento de la Ilustración, con la aparición de las denominadas ciencias positivas, donde su método es al estilo de las ciencias físico-matemáticas, podemos señalar que los ilustrados consideraron a la razón y el procedimiento físico matemático como omnipotentes para resolver los

enigmas del universo y los problemas de la sociedad. Bajo esta perspectiva, se hizo necesario desarrollar métodos que asegurasen conocer la realidad, y es de ahí donde surge la tecnología como herramienta al servicio de las ciencias positivas.

El conocimiento es el fruto de nuestra historia y experiencia anterior; conservar la información que generamos resulta necesario para generaciones futuras, quienes dependen de nosotros para conocer, evaluar y tomar nuevas decisiones. La historia, en cualquier campo de aplicación, actúa como un conjunto de explicaciones, métodos y teorías sobre: ¿cómo?, ¿por qué? y ¿en qué medida? se dan cierto tipo de hechos o tendencias y no se da en otros; se puede tener una perspectiva histórica si contamos con la información necesaria para evaluar.

La firma electrónica y la certificación de documentos digitales permiten conservar, clasificar y almacenar dicha información en espacios menores, permitiendo el acceso del público en general, mediante leyes que se auxilian de dichas tecnologías. Un ejemplo claro en el estado de Jalisco es la Ley de Transparencia e Información Pública, la cual obliga a los entes públicos a conservar y publicar su información en formato digital en los sitios oficiales en la WEB, así como de conservarla por 20 años en sus archivos junto con la información física, aunado a que la información digital requiere de menor espacio físico y permite una conservación infinitamente superior a la física; correlacionadamente es la ley que regula la Administración de Documentos Públicos e Históricos del estado de Jalisco, que ratifica dicha obligación de conservación de archivos públicos por 20 años.

El tratamiento de medios informáticos permite la sustitución del soporte en papel del documento a un nuevo soporte contenido en un medio electrónico, como indica Miguel Ángel Davara Rodríguez, en su manual de Derecho informático (Davara, 2001); el documento puede serlo tanto si se encuentra sobre un papel o sobre cualquier otro soporte apto según su naturaleza, no se debe identificar documento con escritura, en un sentido estricto atendiendo solamente al tradicional sentido realizado por el hombre que en un primer análisis y debido a la costumbre generalizada, lleva al concepto papel.

Así, podemos decir que el documento en soporte electrónico, informático y telemático tiene las mismas características, en principio y en cuanto a su validez jurídica, que cualquier otro de los que tradicionalmente se aceptan en soporte de papel, tal como lo ha declarado el artículo 210-A del *Código Federal de Procedimientos Civiles.*

El documento electrónico o informático se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

Si analizamos la noción tradicional de documento, referida como el instrumento en el que queda plasmado un hecho mediante signos materiales y permanentes del lenguaje, veremos entonces que el documento electrónico cumple con los requisi-

tos del documento en soporte de papel, en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el de los bits) sobre soporte (cinta o disco) destinado a durar en el tiempo.

Dimensión social de la firma electrónica

A pesar de su creciente influencia en la vida cotidiana, la desconfianza en internet como medio para comerciar o realizar trámites administrativos, que exijan acreditar inequívocamente la identidad de una persona, está aún hoy muy extendida.

Los internautas utilizan la red para buscar información o para entretenerse, pero si se trata de dar el número de la tarjeta de crédito o datos de carácter personal, el tema cambia.

La internet es comunicación, pero uno de sus mayores problemas a considerar es la identificación segura y veraz de personas y entidades. La firma electrónica viene para tratar de solucionar estos problemas y dinamizar la administración y el comercio electrónico.

Conseguir una firma electrónica es muy sencillo en otros países, un ejemplo claro es el Gobierno español, quien fue uno de los primeros en toda Europa en regular la firma electrónica a través de un Real Decreto en 1999, medida enmarcada en la apuesta por el desarrollo de la sociedad de la información: no obstante, ello levantó varias críticas tanto por su tramitación, con carácter de urgencia y no mediante una ley debatida en el Parlamento, como por la falta de concreción en los requisitos necesarios para prestar servicios de certificación. Lo que es un hecho es que resultó ser una ley de aplicación y aceptación por la sociedad y un mecanismo eficaz de identificación y seguridad en las relaciones y transacciones en la red de redes "la internet".

México, si bien no ha sido pionero en la implementación de estándares y uso masivo de firma electrónica, sí ha comenzado a dar paso a legislaciones que abren la posibilidad de competir con otras naciones, y más aún, brindan la posibilidad de introducirse a la "sociedad de la información" en el vertiginoso mundo de la Red, para realizar transacciones, convenios, intercambios de información seguros, que les permiten identificarse sin aportar datos personales y sensibles que pongan en riesgo su integridad física y económica.

Dimensión cultural de la firma electrónica

La *cultura* es el conjunto de todas las formas y expresiones de una sociedad determinada, y como tal incluye costumbres, prácticas, códigos, normas y reglas de la manera de ser, vestimenta, religión, rituales, normas de comportamiento y sistemas de creencias.

Desde otro punto de vista se puede decir que la cultura es toda la *información* y habilidades que posee el ser humano. El concepto de cultura es fundamental para las disciplinas que se encargan del estudio de la sociedad, en especial para la antropología y la sociología. La UNESCO en 1982 declaró:

> … la cultura da al hombre la capacidad de reflexionar sobre sí mismo. Es ella la que hace de nosotros seres específicamente humanos, racionales, críticos y éticamente comprometidos. A través de ella discernimos los valores y efectuamos opciones. A través de ella el hombre se expresa, toma conciencia de sí mismo, se reconoce como un proyecto inacabado, pone en cuestión sus propias realizaciones, busca incansablemente nuevas significaciones, y crea obras que lo trascienden.

En ese sentido, la identidad del ser humano resulta ser una característica propia de cada persona que lo identifica de los demás y le permite interactuar con independencia; es decir, que la identidad resulta ser una cualidad del "ser para sí", sólo válido para las personas y consecuentemente de ser *uno mismo* o como parte de un grupo. En ese tenor, la posibilidad de identificarse en un grupo resulta indispensable para un individuo, de tal manera que al interactuar con otras personas en el mundo virtual requiere de una identidad que le brinde seguridad y confianza al momento de identificarse en actos que requieren de mayor solemnidad. Es entonces la firma electrónica un medio que le brinda identidad, en un mundo sin caras ni cuerpos, donde resulta necesario contar con mecanismos que responsabilicen a las personas de su conducta y exteriorización de sus creencias, habilidades e historia del individuo en una imagen consistente de sí mismo, ya que es claro que para alcanzar un buen nivel de autoestima y seguridad se debe antes que nada descubrir la propia identidad.

Un buen ejemplo es la reforma al artículo 16 de la *Constitución* que se publicó el 1 de junio de 2009 en el *Diario Oficial de la Federación*, que incorpora un párrafo segundo y señala:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros.

Es por ello que el objetivo básico de la firma electrónica es aportar al mundo de los documentos electrónicos la misma funcionalidad que aporta la firma manuscrita a un documento impreso, es decir, identificar al autor del mismo y, en el caso de documentos compartidos entre diferentes entidades o personas, fijar el

contenido del documento mediante el cruce de copias firmadas por todas las partes implicadas; que a diferencia de las prácticas que nos son habituales en el mundo físico, como, por ejemplo, concertar una reunión para firmar las copias, la firma electrónica debe además satisfacer la necesidad de firmar un documento por parte de personas que pueden encontrarse a miles de kilómetros y que realizarán la firma sin coincidir en el tiempo.

Cifras de Gartner[2] señalan que para el 2010, el 75% de las organizaciones utilizarán firmas electrónicas, y que para lograrlo, tanto el gobierno como los corporativos, así como los ciudadanos en general, deben sobrepasar la barrera cultural y la desconfianza en el uso de medios electrónicos empujando a la adopción de dicha tecnología.

Dimensión política de la firma electrónica

La administración electrónica es una vía para avanzar hacia el desarrollo del "mejor gobierno" de las administraciones públicas, en donde la tecnología es un medio y no un fin en sí mismo.

El valor de la administración electrónica, por lo tanto, no reside en un mero traslado de los servicios que actualmente presta la administración, sino que debe responder a la optimización y reorganización de los esquemas del servicio público, de tal forma que permitan una mayor eficiencia y eficacia en las relaciones con los ciudadanos y empresas, así como propiciar el cambio cultural que exige la implantación de la sociedad de la información.

La administración electrónica se configura como una nueva forma de "Atención al ciudadano" al que se le facilita una posibilidad más para la realización de gestiones vía internet.

La administración electrónica se define como la utilización de las tecnologías de la información y la comunicación en las administraciones públicas, asociada a cambios en la organización y nuevas aptitudes del personal. El objetivo es mejorar los servicios públicos, reforzar los procesos democráticos y apoyar las políticas públicas; pero para lograrlo es necesario también imprimir ese toque de innovación en el ciudadano para acceder a los servicios públicos en línea, de tal manera que

[2] Gartner, S.A. es un proyecto de investigación de tecnología de la información y de firma consultiva con sede en Stanford, Connecticut; se conocían como el Grupo Gartner hasta 2001. Gartner incluye como clientes algunas empresas grandes y agencias de gobierno así como empresas de tecnología y la comunidad de la inversión como BT, CV, Wall Street Journal, etc.

La empresa consiste en la investigación, programas ejecutivos, consultas y eventos; fue fundada en 1979, tiene 4,000 socios, incluyendo a 1,200 analistas de investigación y consultores en 75 países por todo el mundo.

la firma electrónica permite asegurar la identidad del firmante (del usuario del servicio público o del funcionario público) y la integridad del mensaje (del acto administrativo traducido en una resolución, el cobro de un derecho, o la entrega de información pública, por ejemplo), hecho que tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática, la solicitud o simplemente la identificación.

Otro aspecto importante en la firma electrónica resulta de los avances realizados en la participación efectiva de la ciudadanía por medios electrónicos.

La posibilidad de ejercer el derecho al sufragio –por ejemplo– por medios electrónicos, especialmente por internet, es un tema que se está debatiendo arduamente a nivel mundial y que parece imparable como otras muchas cosas relacionadas con esta materia.

No obstante, conviene recordar desde el principio que cuando hablamos de voto electrónico parece que sólo nos referimos a la capacidad de participar en el estado de derecho en un país democrático, pero contrariamente a eso, existen multitud de ocasiones en las que es necesario ejercer ese derecho a voto, diferente de las elecciones a un país; es el caso, por ejemplo, de las numerosas elecciones empresariales o dentro de cualquier organización.

Además, cada vez que hablamos del entorno electrónico tenemos que distinguir la internet de los demás medios electrónicos, especialmente por la relevancia que tiene dicha red. En concreto, la utilización de la popular red de redes con estos fines podría dar lugar al "voto telemático" como una categoría más específica dentro del voto electrónico.

En la democracia participativa tenemos que garantizar dos cosas: el anonimato y la unicidad del voto (el votante tiene que estar legitimado), donde la firma electrónica pudiera servir únicamente como identificación para legitimar a quien tiene derecho a sufragar, permitiéndole el anonimato al emitir el voto. Ahora bien, en las votaciones de otra índole como, por ejemplo, en las juntas de accionistas debemos tener conocimiento de quién vota, de su capacidad de representación –en su caso– o de la delegación que ostenta.

Dimensión económica de la firma electrónica

Los rápidos avances tecnológicos y la dimensión mundial de internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.

La firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con la utilización de ella. La definición de dichos productos y servicios no debe limitarse a la expedición y gestión de certificados, sino incluir también cualesquiera otros

servicios o productos que utilicen firmas electrónicas o se sirvan de ellas, como los servicios de registro, de estampación de fecha y hora, de guías de usuarios, de cálculo o asesoría relacionados con la firma electrónica.

El mercado interior permite a los proveedores de servicios de certificación llevar a cabo sus actividades transfronterizas para acrecentar su competitividad, y de ese modo ofrecer a los consumidores y a las empresas nuevas posibilidades de intercambiar información y comerciar electrónicamente de forma segura con independencia de las fronteras. Con objeto de estimular la prestación de servicios de certificación en toda la comunidad a través de redes abiertas, los proveedores de servicios de certificación deben tener libertad para prestar sus servicios sin autorización previa. Ésta implica no sólo el permiso que ha de obtener el proveedor de servicios de certificación interesado, en virtud de una decisión de las autoridades nacionales, antes de que se le permita prestar sus servicios de certificación, sino también cualesquiera otras medidas que tengan ese mismo efecto.

Así, la globalización económica de los mercados en sus aspectos productivos, comerciales y financieros atraviesa los estados nacionales.

Capítulo I

Antecedentes de la firma electrónica: del papel al formato electrónico

Las firmas cumplen con la función de "identificación" que determina la personalidad, así como el de avalar derechos y obligaciones convenidas por su autor; sin embargo, este método no es muy fiable puesto que podría ser falsificado, y su autoría debería ser comprobada por un perito. Otro aspecto relacionado a la firma es la "autenticación" que consiste en el proceso por medio del cual se revelan algunos aspectos de la identidad de una persona.

La firma manuscrita

Según el *Diccionario de la Real Academia*: la firma es el nombre y apellido, o título, que una persona escribe de su propia mano en un documento para darle autenticidad o para expresar que aprueba su contenido, con rúbrica o sin ella, al pie de un escrito como señal de autenticidad (Castrillón, 2001).

El vocablo *firma* proviene del latín *firmare,* que significa afirmar y dar fuerza; por otra parte, el vocablo *autógrafa* significa grabar o escribir por sí mismo, y se aplica al escrito de mano de su propio autor en el entendido de que los signos o trazos deben provenir de la mano del autor sin que la impresión se realice por medios mecánicos (VVAA, 2000: 290-293).

En Roma existía la "manufirmatio", que consistía en una ceremonia donde se leía el documento por su autor, o el funcionario, se colocaba el documento desenrollado y extendido sobre la mesa del escribano, y luego de pasar la mano abierta sobre el pergamino en actitud de jurar –pero sin hacerlo– se estampaba el nombre, signo, o una o tres cruces, por el autor o el funcionario en su nombre, haciéndolo seguidamente los testigos. Más que un requisito, la "manufirmatio" era en sí misma parte del espectáculo solemne en que se realizaba el acto (Acosta, 2000: 538).

En la práctica no es más que el conjunto de signos manuscritos por una persona que sabe leer y escribir, con los 0cuales habitualmente caracteriza todos los escritos con los que está de acuerdo o cuyo contenido aprueba (VVAA, 1998: p 1453).

La firma autógrafa además cumple con funciones específicas, como se señalaba anteriormente de medio de "identificación" del documento, así como de "declaración" con la asunción de que el contenido del documento fue hecho por el autor de la firma, siendo el signo principal que representa la voluntad de obligarse; además de poseer un carácter "probatorio", permitiendo identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

En ese mismo sentido, posee además elementos formales y funcionales. Los "elementos formales" destacan como materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo de la misma. La firma es un signo personal que se presenta como un signo distintivo y particular, puesto que debe ser estampada de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

Por su parte, en "elementos funcionales", si tomamos la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función: 1) *Identificadora*. La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado, y 2) *Autentica*, donde el autor del acto expresa su consentimiento haciendo el mensaje.

Algunos autores consideran que la firma como exteriorización de la declaración de voluntad de una persona es imprescindible en los documentos comerciales, no es un mero requisito porque precisa la actuación personal del firmante, una actuación física o corporal del firmante mismo, porque sólo así puede ser instrumento de su declaración de voluntad. En este sentido, no estoy de acuerdo, ya que considero que si la firma es la exteriorización de la declaración de voluntad de una persona, puede hacerse por otro medio, como pudiera ser el electrónico, siempre que la haga el firmante o legalmente se atribuya a él.

La firma electrónica

La firma electrónica tiene poco tiempo de haber surgido, debido al crecimiento de un mundo globalizado, en donde las transacciones y la interacción entre los individuos son impersonales y sin vínculos físicos.

La firma electrónica técnicamente es un conjunto o bloque de caracteres que viaja junto a un documento, fichero o mensaje y que puede acreditar cuál es el autor o emisor del mismo (lo que se denomina autenticación), y que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación (o integridad).

Es aquel conjunto de datos, como códigos o claves criptográficas privadas en forma electrónica, que se asocian inequívocamente a un documento electrónico (contenido en un soporte magnético ya sea en un disquete, algún dispositivo externo o disco duro de una computadora y no de papel) que permite identificar a su autor.

La firma electrónica avanzada permite identificar a la persona que realiza la transacción, puesto que proporciona el servicio de autentificación (verificación de la autoridad del firmante para que esté seguro de que fue él y no otro el autor del documento) y no de repudio (seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones asignadas en él).

Quizás la parte que más interesa a los usuarios es la garantía de detección de cualquier modificación de los datos firmados, proporcionando una integridad total ante alteraciones fortuitas o deliberadas durante la transmisión telemática del documento firmado. El hecho de que la firma sea creada por el usuario mediante medios que mantiene bajo su propio control (clave privada protegida, contraseña, datos biométricos, tarjeta chip, etc.), asegura la imposibilidad de efectuar lo que se conoce como "suplantación de personalidad".

En otras palabras, podríamos definir la firma electrónica avanzada como el conjunto de datos en forma electrónica, que se anexa a otros datos electrónicos o asociados funcionalmente con ellos, considerando en este sentido los datos biométricos utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. La debilidad en cuanto al emisor y al receptor radica en la posible suplantación de la identidad de alguno de ellos por parte de elementos ajenos al sistema.

Según la UNCITRAL, para que una firma electrónica sea considerada como fiable, debe cumplir con lo siguiente:

1. Los datos de creación de la firma, en el contexto en que son utilizados que corresponden exclusivamente al firmante.
2. Los datos de creación de la firma estaban en el momento de la firma bajo el control exclusivo del firmante.
3. Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de realizarla.
4. Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Con lo anterior es factible garantizar:

1. *Autenticación*, para asegurar la identidad de la persona con la que se está comerciando.
2. *Autorización*, para asegurar que esa persona es la indicada para llevar a cabo una operación concreta.
3. *Privacidad*, para garantizar que nadie más va a ver los intercambios de datos que se lleven a cabo.

4. *Integridad*, para asegurar que la transmisión no sea alterada en ruta o en almacenaje.
5. *No repudiación*, para garantizar que quien envía el mensaje no puede negar que lo envió él.

El reto más importante fue equiparar la firma electrónica a la firma autógrafa, dándole los mismos atributos y la misma validez jurídica.

Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica avanzada, que a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.

La firma electrónica entonces será fiable si hay acuerdo entre las partes para su uso (intercambio de claves y contraseñas); ahora bien, por disposición de ley, y salvo prueba en contrario, se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo anterior si:

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.
2. Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante.
3. Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.
4. Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración la misma hecha después del momento de la firma.

De esta manera se pretende que la documentación consignada por medios electrónicos otorgue un grado de seguridad equivalente al del papel, junto con su característica principal de mayor confiabilidad y rapidez, como ocurrió en Estados Unidos, donde fue emitida la primera Ley sobre firmas digitales por el estado de Utah.

Después, la implementación de información electrónica se presentó en otros países.

En nuestro país existen diversos acuerdos que han contribuido a estandarizar y homologar criterios respecto del uso de la firma electrónica. Un ejemplo claro es la aprobación de la Norma Oficial Mexicana PROY-NOM-151-SCFI-2001[1] y 2002 en materia de mensajes de datos.

[1] Proyecto de Norma Oficial Mexicana, Practicas Comerciales-requisitos que deben observarse para la conservación de mensajes de datos, *Diario Oficial de la Federación*, 16/11/2001.

Capítulo II

Aspectos técnicos de la firma electrónica

Previo a aterrizar el tema, resulta necesario delimitar el concepto de firma electrónica, porque es evidente que antes de la gallina surge el huevo,[1] independientemente de que otros puedan pensar lo contrario; parece que la explicación más sencilla suele ser la más acertada;[2] por ello resulta necesario comenzar a delimitar el concepto.

¿Qué es la firma electrónica?

Es un conjunto de datos que se adjuntan a un mensaje electrónico con el objeto de identificar al emisor del mensaje, se puede utilizar un método de encriptación llamado asimétrico o de clave pública. Este método consiste en establecer un par de claves asociadas a un sujeto; una pública, conocida por todos los sujetos intervinientes en el sector, y otra privada, sólo conocida por el sujeto en cuestión.

De esta forma, cuando queramos establecer una comunicación segura con otra parte, basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo.

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un sólo sentido, que aprovechan propiedades particulares como hacerse valer de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil. Por ejemplo, es fácil

---

1 Teoría de la evolución de Darwin, la paradoja del Huevo y la Gallina, no podía resolverse y resulta sorprendente que todavía se crea que no tiene solución.

2 La navaja de Occam (navaja de Ockham o principio de economía o de parsimonia) hace referencia a un tipo de razonamiento basado en una premisa muy simple: *en igualdad de condiciones la solución más sencilla es probablemente la correcta*. El postulado es *entia non sunt multiplicanda praeter necessitatem*, o "no ha de presumirse la existencia de más cosas que las absolutamente necesarias".

multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primos, y conocemos uno de los factores, es fácil computar el segundo.

Ahora bien, existen muchas definiciones de firma electrónica, sin embargo, considero que la más completa es la establecida por la UNCITRAL:

> Por "firma electrónica" se entenderán los datos consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, de forma electrónica que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.[3]

El concepto de firma electrónica aspira a abarcar todos los usos tradicionales de una firma manuscrita con consecuencias jurídicas, siendo la identificación del firmante y la intención de firmar.

El documento electrónico o informático se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones a través de la tecnología. La seguridad en el comercio electrónico es fundamental para su desarrollo.

La tecnología de la firma electrónica está basada en la utilización de medios criptográficos, creados por algoritmos matemáticos de menor a mayor complejidad en relación con los métodos de cifrado más usuales (simétrico o asimétrico) que convierten los datos legibles en ilegibles, haciendo imposible el acceso a terceras personas que desconozcan la clave para descifrarlos (*Revista Política Digital, Innovación gubernamental*, diciembre, 2007 42).

En un flujo de transacciones en donde las partes ya no tienen contacto "físico", surgen las siguientes preguntas: ¿cómo pueden asegurarse de la identidad de aquél con quien están realizando una operación? e, incluso, ¿cómo pueden tener la certeza de que la información intercambiada no ha sido robada, alterada o conocida por personas ajenas?

Según la página web oficial de Microsoft,[4] a diferencia de las prácticas que son habituales en el mundo físico, concertar una reunión para firmar las copias por

---

[3] Artículo 2. Ley Modelo de Firmas Electrónicas promulgada por la Comisión de las Naciones Unidas para el Derecho Mercantil.

[4] http://www.microsoft.com/business/smb/es-es/tecnologia/firma_electronica.mspx

parte de personas que pueden encontrarse a miles de kilómetros y que realizarán la firma sin coincidir en el tiempo, era casi imposible, pero ahora con el uso de la firma electrónica, además satisfacer la necesidad de firmar un documento, se puede realizar casi en tiempo real.

El objetivo básico de la firma electrónica es aportar al mundo de los documentos electrónicos la misma funcionalidad que aporta la firma manuscrita a un documento impreso, identificar al autor del mismo y, en el caso de documentos compartidos entre diferentes entidades o personas, fijar el contenido del documento mediante el cruce de copias firmadas por todas las partes implicadas.

La firma electrónica debe garantizar la identidad del firmante y que el documento no haya sido modificado tras ser firmado.[5]

Para garantizar la identidad del firmante se emplea la tecnología de par de claves vinculada a los datos identificativos del titular del certificado. De este modo, cuando se firma un documento se emplea un número único que sólo pertenece al firmante. El receptor del documento verifica la firma con la parte pública de la clave; de este modo, si el proceso de validación es positivo, debe concluirse que el firmante del documento es el titular del certificado.

La integridad del documento no se refiere al hecho de validar el contenido, sino de garantizar que el documento no ha sido modificado tras su firma. Para garantizarlo no es necesario que un tercero custodie una copia del documento sino que se realiza generando un código único del documento a partir de su estructura interna en el momento de ser firmado. Cualquier alteración del contenido del documento provocará que, al aplicar de nuevo la función de generación de código único, sea imposible reproducir el original; por tanto, quedará rota la integridad del contenido.

Antes, la firma electrónica avanzada demandaba la propiedad de no repudio, que jurídicamente implica que el firmante no pueda negar haber firmado.

Entre otros, los elementos que garantizan el no repudio son:

1. La clave privada vinculada al certificado, y que confiere unicidad a los documentos firmados, sólo que esté en posesión del firmante desde el mismo momento de generar dichas claves y vincularlas a sus datos identificativos. (Datos biométricos, huella dactilar, iris, temperatura, fotografía y algún otro dato característico de la persona en particular.)
2. El certificado y los dispositivos de firma empleados deben basarse en tecnologías y procesos seguros, para evitar el uso o sustracción de la clave por parte de terceros y que se encuentren homologados por la autoridad de certificación emisora del certificado empleado.

[5] Conferencia de la Mtra. Leticia Margarita Domínguez López, expositora por la Universidad de Guadalajara y el Colegio de Notarios de Jalisco.

3. Que el certificado esté activo en el momento de ser empleado. Esto equivale al estado de las tarjetas de crédito, que también pueden ser revocadas por el interesado y caducar con el tiempo.
4. Que los receptores de documentos firmados dispongan de un instrumento de verificación seguro que no permita suplantar identidades del firmante o de la autoridad de certificación que realiza la validación.

Esos conceptos básicos determinan que un sistema de firma electrónica sea empleado con éxito, ya que los aspectos de seguridad se combinan con ventajas ciertas para el usuario y el cuidado de los aspectos funcionales y así evitar costes innecesarios e incidencias.

La aprobación de la Ley de Firma Electrónica en el estado y el establecimiento de un nuevo marco fiscal –para la factura telemática, como ejemplo– han reabierto el debate sobre las ventajas y retos que plantea el uso de documentos electrónicos como soporte definitivo de las relaciones entre empresas, y también entre éstas y los ciudadanos con la administración.

Sobre el papel, las ventajas son evidentes, pero si de algo ha servido la experiencia acumulada hasta la fecha, es para tomar conciencia de que hace falta algo más que una normativa para que el gobierno, organizaciones públicas y privadas, como las notarías, las empresas y los ciudadanos, utilicen la firma electrónica y, por lo tanto, se beneficien al hacerlo.

Los aspectos técnicos de la firma electrónica

Las normas TS 101 733 *y* TS 101 903[6] definen los formatos técnicos de la firma electrónica. La primera se basa en el formato clásico PKCS#7[7] y la segunda en XMLDsig firma XML especificada por el consorcio W3C.[8]

---

[6] La norma TS o el sellado de tiempo (*Timestamping*) es un mecanismo *on line* que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 y está en el registro de estándares de internet. Una autoridad de sellado de tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

[7] En criptografía, PKCS se refiere a un grupo de estándares de criptografía, clave pública concebida y publicada por los laboratorios de RSA en California. A RSA Security se le asignaron los derechos de licenciamiento. El número 7 es usado para firmar y/o cifrar mensajes. También usado para la diseminación de certificados.

[8] El consorcio World Wide Web (W3C) es una empresa internacional donde las organizaciones miembros, con personal a tiempo completo y el público en general,

Bajo estas normas se definen tres modalidades de firma:

1. *Firma básica*. Incluye el resultado de operación de *hash* y clave privada, identificando los algoritmos utilizados y el certificado asociado a la clave privada del firmante.
2. *Firma fechada*. A la firma básica se añade un sello de tiempo calculado a partir del *hash*[9] del documento firmado por una TSA (Time Stamping Authority).
3. *Firma validada o firma completa*. A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP[10] realizada a la autoridad de certificación.
4. La *firma* completa libera al receptor de la firma del problema de ubicar al prestador de servicios de certificación y determinar los procedimientos de validación disponibles.

Cuadro 1
Proceso de la firma electrónica /clave privada

Mensaje proceso de digestión encripción firma mensaje de datos digestión (*hash*) electrónica firmado.

El contenido del mensaje de datos, el conjunto de *bits* que forman el mensaje, en un acuerdo, los participantes negocian el contenido y, una vez aceptado, proceden a firmarlo.

---

trabajan conjuntamente para desarrollar estándares web. La misión del W3C es guiar la web hacia su máximo potencial a través del desarrollo de protocolos y pautas que aseguren el crecimiento futuro de la web.

9 *Hash* se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función *hash* o algoritmo *hash*. Un *hash* es el resultado de dicha función o algoritmo.

10 Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital utilizando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Este protocolo está en el registro de estándares de internet.

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo, haciendo uso de los números primos, puesto que es fácil multiplicar dos números primos juntos para obtener uno compuesto; pero es difícil factorizar uno compuesto en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso.

Cuadro 2
Proceso de la firma electrónica /clave pública

Mensaje firma electrónica desencripción digestión (1) firmado

Mensaje de proceso de digestión (2) datos digestión (*hash*)

Al autentificar una firma electrónica avanzada, es posible identificar si fue aplicada a un mensaje de datos en particular.

Conceptos básicos

Agencia certificadora: entidad responsable de establecer identidades y crear los certificados digitales que forman la asociación entre una identidad y una pareja de claves pública/privada (SAT y agencias prestadoras de servicios de certificación autorizadas por el Banco de México).[11]

Agencia registradora central: entidad responsable de autorizar a las autoridades certificadoras para que presten servicios en su nombre, siendo ésta la que concen-

[11] Servicio de administración tributaria, consultada el día 9 de junio de 2010 a las 12:00 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

tra el directorio de certificados digitales y los movimientos realizados a los mismos (BANXICO).[12]

Agencia registradora: entidad responsable de identificar y registrar en forma inequívoca al solicitante de un certificado fiscal digital. Solicita a la autoridad certificadora la información verificada del solicitante, para emitirle un certificado digital (SAT).[13]

Autoridad certificadora: es la entidad que genera y revoca los certificados para un conjunto de usuarios, y es responsable de su autenticidad (Reyes Krafft, 2004: 192).

Autenticidad: característica intrínseca de la firma electrónica avanzada, en donde el autor del mensaje queda acreditado, puesto que permite verificar la identidad del emisor de un documento.

Biometría: consiste en el estudio de métodos automáticos para el reconocimiento único de humanos, apoyándose en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva del griego, "bios", vida, y "metron", medida.

La biometría en la informática consiste en la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para poder verificar identidades o también identificar individuos.

En las tecnologías de la información, la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento de la persona para poder autentificar.[14]

Cadena original: se entiende como cadena original a la secuencia de datos formada con la información contenida dentro del comprobante fiscal digital, establecida en el rubro C del anexo 20 de la *Resolución miscelánea fiscal*.[15]

Certificado de sello digital: los certificados de sellos digitales son expedidos por el SAT, son para uso específico de comprobantes fiscales digitales. Por medio de ellos, el contribuyente podrá sellar electrónicamente la cadena original de los comprobantes que emita en cada una de sus sucursales; así, se tendrá identificado el origen del comprobante fiscal digital, junto con la unicidad y las demás características que tienen los certificados digitales (integridad, no repudio, autenticidad

[12] Servicio de administración tributaria, consultada el día 9 de junio de 2010 a las 12:10 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

[13] Servicio de administración tributaria, consultada el día 9 de junio de 2010 a las 12:20 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

[14] Unión Europea, consultada el día 7 de junio de 2010, 16:30 horas, http://firma-electronica.eu/7.html.

[15] Servicio de Administración Tributaria, consultada el día 9 de junio de 2010 a las 12:30 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

y confidencialidad). El contribuyente puede optar por pedir un sello digital para cada una de las sucursales, establecimientos o locales, donde emita comprobantes fiscales digitales.[16]

Certificado digital:[17] mecanismo que permite atestiguar la validez de la identidad de un individuo o entidad, contiene el nombre de la persona, su llave pública y está firmado con la llave privada de la autoridad certificadora. Su misión es permitir la comprobación de que la clave pública de un usuario es realmente de él.

Certificado digital: tienen cómo objetivo identificar al dueño de una firma electrónica avanzada. Estos certificados contienen información diversa acerca del firmante, servicios a los que este tiene acceso para utilizar su firma, la fecha de vigencia del certificado, la agencia certificadora que lo emitió, entre otras características.

El artículo 17-G del *Código Fiscal de la Federación* describe a los certificados digitales de la siguiente manera:

Documento electrónico: mensaje de datos u otro registro que asocia una clave pública con la identidad de su propietario, confirmando el vínculo entre éste y los datos de creación de una firma electrónica avanzada o de un sello digital. Además de la clave pública y la identidad de su propietario, un certificado digital contiene los siguientes atributos: (Artículo 17-G del *Código Fiscal de la Federación*) I. La mención de que se expiden como tales. Tratándose de certificados de sellos digitales, se deberán especificar las limitantes para su uso. II. El código de identificación único del certificado. III. La mención de que fue emitido por el SAT y una dirección electrónica. IV. Nombre del titular del certificado y su clave del Registro Federal de Contribuyentes. V. Periodo de vigencia del certificado, especificando el día de inicio de su vigencia y la fecha de su terminación. VI. La mención de la tecnología empleada en la creación de la firma electrónica avanzada contenida en el certificado.

Cuando se trate de certificados emitidos por prestadores de servicios de certificación autorizados por el Banco de México, que amparen datos de creación de firmas electrónicas que se utilicen para los efectos fiscales, dichos certificados deberán reunir los requisitos a que se refieren las fracciones anteriores, con excepción del señalado en la fracción III. En sustitución del requisito contenido en dicha fracción, el certificado deberá contener la identificación del prestador de servicios de certificación y su dirección electrónica, así como los requisitos que para su control establezca el Servicio de Administración Tributaria mediante reglas de carácter general.

Criptografía: ciencia que tiene como objeto mantener en secreto los mensajes, el texto original convertido en códigos.

---

[16] Servicio de Administración Tributaria, consultada el día 9 de junio de 2010 a las 12:40 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

[17] Servicio de Administración Tributaria, consultada el día 9 de junio de 2010 a las 12:50 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

Datos biométricos: son las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, son ejemplos de características físicas (estáticas). Son características dinámicas la firma, el paso y la forma de escribir a máquina. La voz se considera una mezcla de características físicas y de comportamiento, todos los rasgos biométricos comparten aspectos físicos y del comportamiento.[18]

Encriptar: es la acción de codificar información, de tal forma que sólo quien conoce la estructura del código pueda descifrarlo. Para efectos de este proyecto, la información del certificado se codificará de tal manera que sólo las aplicaciones emitidas por el SAT podrán descifrarla.

Factura electrónica: la factura electrónica en México es un tipo de comprobante fiscal digital y se define como un documento digital con validez legal, que utiliza estándares técnicos de seguridad internacionalmente reconocidos, para garantizar la integridad, confidencialidad, autenticidad, unicidad y no repudio del documento.[19]

Firma electrónica o también llamada *firma digital:* son los datos electrónicos consignados a un mensaje de datos que son utilizados para identificar al firmante.

Firma electrónica avanzada: datos electrónicos que permiten la identificación del firmante y que fue generada bajo su exclusivo control utilizando un sistema de cifrado que permita identificar si ha sufrido modificación posterior a su creación.

Firma electrónica avanzada: conjunto de datos asociados a un mensaje, que permiten asegurar la identidad del contribuyente y la integridad (no modificación posterior) del mensaje. Además de contar con un certificado digital expedido por el SAT o por un prestador de servicios de certificación autorizado por Banco de México, esta firma tiene las cualidades de reconocimiento por el marco legal, fiabilidad técnica basada en infraestructura de llave o clave pública, otorgando las garantías de integridad, no repudio, autenticidad y confidencialidad.

Intercambio electrónico de datos: es la transmisión electrónica de información enviada desde una computadora a otra, estructurada conforme a alguna norma técnica acordada para el envío.

IES: la infraestructura extendida de seguridad es un sistema diseñado y administrado por el Banco de México, con el propósito de fortalecer la seguridad de la información que se transmite tanto en los sistemas de pago como entre el sistema financiero mexicano y el instituto central. La IES está basada en el uso de firmas electrónicas mediante la aplicación de algoritmos criptográficos, para garantizar la

[18] Unión Europea, consultada el día 7 de junio de 2010, 16:35 horas, http://firma-electronica.eu/7.html.

[19] Servicio de Administración Tributaria, consultada el día 9 de junio de 2010 a las 13:00 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

confidencialidad e integridad de la información que se transmite y, a su vez, acreditar la identidad del remitente.[20]

Integridad: característica intrínseca de la firma electrónica avanzada, que garantiza que la información contenida en el mensaje quede protegida y no pueda ser manipulada o modificada durante el proceso; es decir, confirma la no alteración de los datos desde su origen.

Infraestructura de clave pública (ICP): también conocida como PKI (Public Key Infrastructure), es un conjunto de protocolos, servicios y estándares, que soportan las aplicaciones basadas en criptografía de clave pública, además de brindar los servicios de creación segura de claves, validaciones de identidades, expedición, renovación y terminación de certificados, validación de certificados, distribución de certificados, generación de firma, establecimiento y administración de relaciones de confianza.

Llave tradicional o simétrica: es aquella en que la llave de encriptación es la misma a la de desencriptación.

Llave pública o asimétrica: es cuando las claves para cifrar y descifrar son distintas y que es imposible calcular una por derivación de la otra.

Mensaje de datos: información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares como son el intercambio electrónico de datos, el correo electrónico, telegrama, telex o telefax. El mensaje de datos no se limita a sólo comunicación sino que pretende abarcar cualquier tipo de información respaldada en un soporte de tipo informático, que no necesariamente esté destinada a ser comunicada, así el concepto de mensaje incluye el de información meramente consignada (Krafft, *op cit:* 164).

Sello digital (trámites electrónicos ante el SAT): cuando los contribuyentes remitan un documento digital a las autoridades fiscales, recibirán el acuse de recibo que contenga el sello digital. El sello digital es el mensaje electrónico que acredita que un documento digital fue recibido por la autoridad correspondiente, y estará sujeto a la misma regulación aplicable al uso de una firma electrónica avanzada. En este caso, el sello digital identificará a la dependencia que recibió el documento y se presumirá, salvo prueba en contrario, que el documento digital fue recibido en la hora y fecha que se consignen en el acuse de recibo mencionado.[21]

---

[20] Banco de México, consultada el día 11 de junio de 2010 a las 13:00 horas, www.banxico.org.mx/tipo/disposiciones/bancos/circ19Bis-2002.html

[21] Servicio de administración tributaria, consultada el día 9 de junio de 2010 a las 13:05 horas, www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html

Autoridades de certificación

Las autoridades de certificación deben prestar servicios más orientados a la realidad de las organizaciones; si desean permanecer en el mercado deberán ofrecer sus certificados en dispositivos económicos que puedan ser empleados en cualquier ordenador sin necesidad de realizar instalaciones y sin renunciar a la máxima seguridad; ello implica, por su puesto, la implementación de infraestructura que no siempre se adquiere de manera sencilla por el alto costo de inversión que ello implica.

Adicionalmente, se deben complementar el proceso de emisión de certificados con servicios de validación en origen para que el receptor de un documento firmado electrónicamente no deba incrementar la complejidad y coste de sus procesos administrativos. En este escenario, la evolución que realizaron los sistemas de tarjetas de crédito, validando las transacciones en origen, resulta suficientemente ejemplarizante.

Una de sus características es que es considerado un ente de confianza para la comunidad, y sus funciones se pueden resumir en:

1. Generación de certificados para garantizar la identidad de los usuarios a través de una firma electrónica.
2. Agendar fechas de expiración de certificados.
3. Revocar certificados.

Entre las que encontramos las siguientes:

1. *Banco de México:* (agencia registradora central) hace uso de la tecnología de firma electrónica con el propósito de aumentar el nivel de confianza en los intercambios de información electrónica entre el sistema financiero mexicano y el instituto central. Dicha tecnología permite comunicarse electrónicamente con las máximas garantías de seguridad, añadiendo a la comunicación los servicios de autenticación, integridad, confidencialidad y no repudio.

   La infraestructura de clave pública (o PKI, por sus siglas en inglés, Public Key Infrastructure) del sistema de pagos mexicano es también denominada "Infraestructura Extendida de Seguridad (IES)". La IES es un sistema diseñado y administrado por el Banco de México. En la tabla de certificados de la IES se muestran los que pertenecen a la agencia raíz, a las agencias certificadoras y registradoras, así como los de las ARA's, junto con el detalle de su número de serie e institución a la que pertenece.[22]

[22] Banco de México, consultada el día 8 de junio de 2010, 17:44 horas, www.banxico.org.mx/sistemas-de-pago/servicios/firma-electronica/firma-electronica.html

2. SAT: es la entidad responsable de establecer identidades y crear los certificados digitales que forman la asociación entre una identidad y una pareja de claves pública/privada (SAT y agencias prestadoras de servicios de certificación autorizadas por el Banco de México).

   Es la entidad responsable de identificar y registrar en forma inequívoca al solicitante de un certificado fiscal digital. Solicita a la autoridad certificadora la información verificada del solicitante, para emitirle un certificado digital (SAT).

   La Administración General de Servicios al Contribuyente es el órgano rector de la Administración Pública Federal en la emisión de políticas en materia de orientación, asistencia y difusión fiscal, y el conducto para la prevención y resolución de problemas del contribuyente, para lo cual emplea a más de 341 personas a nivel central, y 1,290 en el nivel local, estas últimas adscritas a 66 administraciones locales de servicios al contribuyente.[23]
3. *Secretaría de la Función Pública Federal:* con el propósito fundamental de fomentar una creciente interacción a distancia entre el gobierno y la ciudadanía, y reducir costos de cumplimiento de obligaciones y obtención de servicios para los particulares, por lo que se refiere al acreditamiento de la personalidad ante distintas dependencias y organismos descentralizados, con fecha 28 de abril de 2004, el titular del Ejecutivo federal suscribió el decreto por el que se establece el procedimiento y los requisitos para la inscripción en los registros de personas acreditadas operados por las dependencias y organismos descentralizados de la Administración Pública Federal y las bases para la interconexión informática de los mismos, el cual fue publicado en el *Diario Oficial de la Federación* el 4 de mayo del mismo año.[24] Estableciendo los lineamientos para la creación, operación e interconexión informática de los registros de personas acreditadas, por lo que en cumplimiento de dichos preceptos, y a fin de brindar a la ciudadanía y a las propias dependencias y organismos descentralizados el apoyo necesario para facilitar la inscripción en el registro de personas acreditadas correspondiente, así como para la creación, operación e interconexión de los mismos a través del Registro Único de Personas Acreditadas (RUPA).[25]

   El 5 de mayo de 2006 se firmó el convenio de coordinación con la Asociación Nacional de Notarios, para la utilización y expedición de constancias del RUPA.

---

[23] Servicio de Administración Tributaria, consultada el día 9 de junio de 2010, 17.30 horas, http://www.sat.gob.mx/sitio_internet/e_sat/comprobantes_fiscales/15_6542.html

[24] Secretaría de Relaciones Exteriores, consultada el día 10 de junio de 2010, 13:20 horas, http://www.sre.gob.mx/tramites/juridico/decretorupa.htm

[25] Secretaría de Relaciones Exteriores, consultada el día 10 de junio de 2010, 13:00 horas, http://www.sre.gob.mx/tramites/juridico/linrupa.htm

El 16 de agosto de 2006 se firmó el convenio de colaboración con el Colegio Nacional de Correduría Públicas para la utilización y expedición de constancias del RUPA.

4. *Secretaría de Economía:* la Secretaría de Hacienda y Crédito Público y la Secretaría de Economía, como consecuencia del decreto pronunciado por el presidente Felipe Calderón, publicado en marzo de 2008,[26] en el que se otorgan facilidades para la presentación de trámites haciendo uso de los avances tecnológicos, utilizando el RUPA.[27]
5. *Secretaría de Relaciones Exteriores:* maneja el programa SIPAC para realizar trámites vía internet, con la posibilidad abierta para el público en general y para los notarios a través de su firma electrónica.

Principales responsabilidades a considerar: (Reyes Krafft, 2004: 207)

Agencia registradora	Agencia certificadora	Agente certificador
1. Contar con reglas y procedimientos de operación.	1. Reglas y procedimientos sobre prácticas de certificación adoptadas.	1. Identificar a titulares solicitantes con identificación oficial fiable.
2. Mantener registro de certificados digitales.	2. Emitir y en su caso revocar certificados digitales con los requisitos de BANXICO.	2. Obtener declaración con firma autógrafa del titular.
3. Permitir consultas en línea al registro.	3. Proporcionar un certificado digital y los medios para la creación y verificación de la firma electrónica.	3.Conservación de documentación física por 10 años (digitalizada).

[26] Secretaría de Economía, consultada el 9 de junio de 2010, a las 18.00 horas, http://www.economia.gob.mx/swb/work/models/economia/Resource/1010/1/images/decreto.pdf

[27] *Rupa* es el Registro Único de Personas Acreditadas es la interconexión y sistematización informática de los Registros de Personas Acreditadas, es una inscripción que permite a los particulares (personas físicas y morales) la realización de trámites ante dependencias y organismos descentralizados, a través de un número de identificación único basado en el Registro Federal de Contribuyentes. El RUPA se creó a través del decreto presidencial publicado en el 2003.

El RUPA tiene por objetivo integrar la información gubernamental sobre la constitución y funcionamiento de las empresas. Se entrega una sola vez los documentos correspondientes y se recibe un solo número de registro que sirve para distintos trámites en todas las dependencias del Gobierno federal.

4. Difundir disposiciones de BANXICO.	4. Registrar ante la agencia registradora los certificados digitales que emita.	4. Responder por los daños y perjuicios en caso de negligencia en el proceso de identificación del titular.
5. Reportes a BANXICO de actividades.	5. Conservar las solicitudes por 10 años.	5. Contar con respaldo de información y documentación.
6. Responder por negligencia en proceso de registro o revocación.	6. Difundir las disposiciones de BANXICO.	
7. Tener un respaldo electrónico de su base de datos.	7. Reportes a BANXICO de actividades.	
	8. Responder por las negligencias en proceso de emisión o revocación de certificados.	
	9. Informar a titulares de revocación de certificados en su caso.	

Certificado digital

Un certificado digital es un documento mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Si bien existen variados formatos para certificados digitales, los más comunes se rigen por el estándar UIT-T X.509.[28] El certificado contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado, de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

[28] El sistema X.500 nunca se implementó completamente, y el grupo de trabajo de la infraestructura de clave pública (X.509) adaptó el estándar a la estructura más flexible de internet. X.509 incluye también estándares para implementación de listas de certificados en revocación.

1. Nombre, dirección y domicilio del suscriptor.
2. Identificación del suscriptor nombrado en el certificado.
3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
4. La clave pública del usuario.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie del certificado.
7. Fecha de emisión y expiración del certificado.
8. Además de los datos anexos que permiten la plena identificación del firmante.

Factura telemática

La factura telemática es el primer documento mercantil de uso masivo que se beneficiará de la definición de un marco fiscal y legal sobre su desmaterialización. Gracias al reconocimiento de la firma electrónica avanzada como un instrumento capaz de acreditar la identidad del emisor y la integridad, identificado como la no modificación posterior del documento firmado, actualmente es posible emitir y recibir facturas únicamente en soporte electrónico como lo realiza Telmex y Ticketmaster, entre otras.

Durante los últimos meses se ha escrito mucho sobre las ventajas y ahorros de la factura telemática, sin embargo, para que su implantación no sea un generador de costo e incidencias tanto técnicas como administrativas, deben contemplarse diversos factores:

1. Disponibilidad de soluciones que garanticen el ahorro inmediato**.** La premisa básica es el ahorro de costos y el incremento de la eficacia; al emplearse soluciones que garanticen dicho ahorro desde la primera factura emitida o recibida y sin requerir inversiones iniciales. Actualmente existen soluciones que permiten incluso contratar el servicio de emisión con todas las garantías legales y fiscales para emisor y receptor mediante el envío de un mensaje SMS.
2. Uso de soluciones integradas en las aplicaciones de gestión**.** El usuario final, y teniendo en cuenta la proporción de organismos tanto públicos como privados de nuestro país, debe encontrar las soluciones integradas en su aplicación de gestión, contemplando así un modelo que integre los aspectos fiscales, funcionales y tecnológicos.
3. Uso de estándares internacionales**.** Para que la factura telemática aporte ventajas tanto en origen como en destino, resulta imprescindible que el documento con los datos de la factura se base en estándares internacionales; de este modo, el sistema de gestión del receptor podrá automatizar el proceso de introducción

de los datos en su sistema de información y beneficiarse de la recepción de facturas en formato electrónico más allá del ahorro en el almacenamiento.

4. Uso de modelos de firma intervenida**.** El uso de la factura como un documento justificativo de deducción fiscal recae en el receptor de la misma; por lo tanto, éstos se inclinarán por soluciones que permitan la emisión de factura previa comprobación del estado del certificado, y de este modo se garantiza la validez de la firma electrónica vinculada al documento.
5. Modelos asimétricos emisor-receptor. El nuevo marco fiscal (establecido por el propio SAT) establecido para la factura telemática, permite que el receptor del documento pueda beneficiarse de las ventajas que aporta sin necesidad de realizar ninguna inversión.
6. Recursos de formación y difusión positiva. Resulta obvio que todas las partes implicadas, autoridades de certificación, empresas titulares de aplicaciones de gestión, perfiles profesionales responsables de asesorar fiscalmente, debiendo potencializar el desarrollo y difusión de recursos informativos y formativos.

Otro aspecto importante a considerar en el tema de las facturas telemáticas, y dentro de la legislación mexicana, resulta con la aprobación e inclusión en el artículo 31 del *Código Fiscal de la Federación* durante las reformas efectuadas en el año 2000, cuya finalidad se encaminaba a que el contribuyente pudiera efectuar declaraciones anuales en el año 2001 mediante medios electrónicos (vía internet).

La internet es una de las consecuencias de la revolución informática que hoy en día nos propone un amplio y novedoso escenario para todas las áreas de nuestra vida, entre ellas las relaciones comerciales entre proveedores y consumidores. La preocupación se centra entonces en definir las reglas adecuadas para este nuevo comercio a fin de ofrecer seguridad y certidumbre jurídica a los actores.

Estas relaciones son plasmadas a través del contrato. "El contrato como negocio jurídico que no es más que un acuerdo de voluntades, o confluencia de voluntades que produce efectos jurídicos, se crean, se extinguen o se transmiten derechos y obligaciones". En el contrato, la reunión de la información con la voluntad, nos lleva a un acto creador, los contratantes generan en el mundo del Derecho algo que afecta su esfera personal patrimonial y de obligaciones.

El documento ha sido la institución jurídica por excelencia creada para recibir aprobaciones o solemnidades, actos jurídicos y dejar constancia de esos efectos, ya que ahí queda constancia de lo que las partes decidieron en un momento, así como los efectos jurídicos que ese contrato produce (Meján, 2006: 85).

La voluntad de las partes siempre ha sido la creadora de las figuras jurídicas; las consecuencias dependerán del contrato específico que se esté celebrando. La mencionada voluntad de las partes es plasmada al momento que llegan a estampar su firma en el contrato como signo de aceptación. En tal contexto, hablemos de dos

grupos: la firma autógrafa conocida como firma personal y la firma no autógrafa, que sería toda aquella realizada por cualquier otro medio que no sea la inscripción manual de los rasgos que identifican a una persona. En esta categoría podríamos incluir la firma digital, electrónica y cualquier otra que se pueda realizar por medios técnicos o de cualquier otra especie.

Capítulo III

La firma electrónica: qué existe y qué falta en los dispositivos legales vigentes

No existe ley en el mundo que regule este uso y distribución global de la información. Las modificaciones legales que se proponen en los diversos estados son sólo de jurisdicción local, y seguramente estos problemas se irán resolviendo conforme la situación se vaya desarrollando, sobre todo cuando el uso de internet sea mayor y la problemática se torne urgente de resolver mediante el uso del derecho internacional privado y público. De alguna manera, en la actualidad el uso del internet y de las diversas tecnologías de la información en México es incipiente en algunos sectores marginados, porque hay poca gente que cuenta con los medios económicos para acceder a éstos, lo que no significa que la situación no se haya agravado significativamente; sin embargo, las encuestas respecto a su uso y accesibilidad se encuentran en ascenso.

Pero lo importante es preguntar: ¿podemos controlar jurídicamente estas tecnologías? Esta pregunta puede sonar a ciencia ficción o tener un sesgo de utopía, pero el Derecho debe y puede cambiar a favor de los avances de la humanidad y correr tras ellos tratando de ponerse a tono con los tiempos.

Este capítulo tiene como finalidad establecer la existencia e importancia de las diversas legislaciones extranjeras, nacionales y estatales, que aunque en su momento proveyeron a la comunidad de protección jurídica en una realidad fáctica, hoy muchas de ellas ya son obsoletas e inaplicables, y además sus inconsistencias, redundancias y lagunas normativas provocan impunidad y no pueden por analogía aplicarse a situaciones virtuales que plantea el uso de las tecnologías de la información.

Regulación de la firma electrónica en algunos países

Alemania. El 13 de junio de 1997 fue promulgada la Ley sobre Firmas Digitales y el 7 de junio del mismo año fue publicado su reglamento: Law Governing Frarnework Conditions for Electronic Signatures and Amending Other Regulations (publicado el 16 de mayo del 2001, en el periódico *Official Journal* núm. 22.

Argentina. El 17 de marzo de 1997, el subcomité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la resolución 45/97 –firma digital en la Administración Pública– y el 14 de diciembre del año 2001 aprueba la Ley de Rama Digital para la República Argentina 25/506.

Bélgica. La Ley "Loi fixant certaines regles relatives au cadre juridiqe pour les signatures électroniques et les services de certification" de firma electrónica y servicios de certificación el día 29 de septiembre del 2001.

Unión Europea. Directiva 1999/93/CE del Parlamento Europeo y del Consejo del 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica. Decisión de la Comisión del 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la directiva 1999/93/CE del Parlamento europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica (2000/709/CE).

Canadá. "British Columbia Bill" en el año 2001 se emite "The Electronic Transactions Act."

Colombia. Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación.

Chile. Ley sobre documentos electrónicos, firma electrónica y servicios de certificación en el 2002.

Dinamarca. El 31 de mayo del 2000 se regula sobre firma electrónica y requerimientos para autoridades certificadoras.

España. Real Decreto Ley 14/1999 sobre Firmas Electrónicas. Septiembre de 1999, Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos Orden de 21 de febrero de 2000, por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. Ley de Servicios de la Sociedad de Información. El Proyecto de Ley de Firma Electrónica, de 20 de junio de 2001 ha introducido diversas modificaciones respecto del vigente Real Decreto, ley 14/1999 de firma electrónica. Tras su ratificación por el Congreso de los Diputados, se acordó someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. Entre los puntos más importantes que considera están: promoción de autorregulación de la industria, concepto de firma electrónica reconocida, *time stamping*, declaración de prácticas de certificación, documento nacional de identidad electrónico y, el más debatido, certificados para personas morales, un caso distinto a la firma electrónica de los representantes de las personas morales, pues se persigue dar firma a las empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados. Hasta la aprobación de la Ley 59/2003 de Firma Electrónica el día 19 de diciembre de 2003.

Francia. Mediante el decreto 2001-272 del 30 de marzo del año 2001 por aplicación del artículo 1316-4 del *Código Civil* con relación a la firma electrónica, mediante la ley 2000-230 del 13 de marzo del 2000 se da una importante adaptación de la firma electrónica como auxiliar en el uso de las tecnologías de la información.

Irlanda. Se regula sobre comercio electrónico durante el año 2000.

Italia. El 15 de marzo de 1997 fue publicado el "Reglamento sobre: acto, documento y contrato en forma electrónica", aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999 las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la Ley sobre Firma Electrónica.

Japón. El 1 de abril del año 2001 se aprueba la Ley sobre Firma Electrónica y Servicios de Certificación.

Luxemburgo. Se reglamenta sobre firma electrónica y pagos electrónicos, así como la creación de un comité de determinación, el 1 de junio del año 2001.

Panamá. El 3 de agosto del 2001 se aprueba la Ley 43 de Comercio Electrónico.

Portugal. El decreto de Ley 290-D/99 relativo a firma electrónica.

Reino Unido. Se regula sobre comunicaciones electrónicas en el año 2000.

Suecia. Se regula sobre firma electrónica en el año 2000.

Uso de la firma electrónica en México y su regulación

El 29 de mayo del año 2000 se publicó en el *Diario Oficial de la Federación* el decreto por el que se reforman y adicionan diversas disposiciones del *Código Civil para el Distrito Federal en materia común y para todo México en materia federal* (ahora *Código Civil Federal*), del *Código Federal de Procedimientos Civiles*, del *Código de Comercio* y de la *Ley Federal de Protección al Consumidor*.

La legislación existente hasta esa fecha, requería para la validez del acto o contrato de la forma escrita y la firma autógrafa para vincular a las partes en forma obligatoria.

Las reformas y adiciones al *Código Civil Federal* se centraron en el reconocimiento a la celebración de actos jurídicos a través de medios electrónicos, ópticos o de cualquier otra tecnología, añadiéndose los "medios tecnológicos" como medio idóneo para expresar el consentimiento. Es importante resaltar que se estableció una equivalencia funcional entre el consentimiento expresado por medios tecnológicos y la firma autógrafa, "siempre que la información generada o comunicada en forma íntegra a través de dichos medios será atribuible a las personas obligadas y accesible para su ulterior consulta".

Se reconoció en el *Código Federal de Procedimientos Civiles*, como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador: la fiabilidad del método para generar, comunicar, recibir o archivar la información

(que pueda conservarse sin cambio), su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas. Asimismo, y para que la información generada, comunicada, recibida o archivada por medios electrónicos se considere como original (para su conservación o presentación), deberá acreditarse que dicha información se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

En el *Código de Comercio* se definió el concepto "mensaje de datos" como la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

Respecto de la obligación a los comerciantes de conservar por un plazo mínimo de 10 años los originales de su contabilidad, así como aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones[1] fiscales, civiles y mercantiles –en los estados financieros–; en el caso de mensajes de datos se requerirá que el contenido de la información se haya mantenido íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, y sea accesible para su ulterior consulta. La Secretaría de Economía se obligará a emitir una Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

Se estableció una presunción en materia mercantil, salvo pacto en contrario, de que el mensaje proviene del emisor (atribución a la persona obligada) si ha sido enviado:

1) Usando medios de identificación tales como claves o contraseñas de él (*para lo que se requerirá de un previo acuerdo entre las partes*).
2) Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

En materia mercantil, al igual que en la civil, cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.

---

[1] El primer párrafo del artículo 49 del *Código de Comercio* se refiere a que: Los Comerciantes están obligados por un plazo mínimo de diez años a conservar los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Lo anterior parece redundante, toda vez que el *Código Civil Federal* define al Contrato como el convenio que produce o transfiere obligaciones o derechos.

Y se reconoce como prueba a los mensajes de datos; para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

Se reformó la Ley Federal de Protección al Consumidor para reconocer la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones (confidencialidad, certeza, seguridad en la información proporcionada al consumidor, etc.), previendo sanciones administrativas para el caso de que los proveedores no cumplan con dichas disposiciones (Reyes Krafft, 2004: 2).

De lo anterior, resulta necesario hacer las siguientes consideraciones:

Para que un mensaje de datos en el que se consignen contratos pueda considerarse legalmente válido, es necesario asegurar que reúna las siguientes características, aplicando:

1. Integridad, entendida en dos vertientes; la primera, respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla, y la segunda, como la forma de garantizar que la información en él contenida no fue alterada.

Al respecto, la Secretaría de Economía elaboró una Norma Oficial Mexicana que establece los requisitos que deben observarse para la conservación de mensajes de datos con fundamento en lo dispuesto por el artículo 49, segundo párrafo del Código de Comercio. El martes 19 de marzo del 2002 se firmó el texto final de la NOM, el cual fue publicado el DOF el día 4 de junio del 2002, para su entrada en vigor se requiere de existencia de infraestructura y publicación de aviso en el *Diario Oficial de la Federación*.

2. Atribución, considerada como la forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad libre de vicios. Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es más que una "firma electrónica", la cual puede ser de dos tipos:

Simple: definida como 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 (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes).

Avanzada: que podemos conceptuar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula, sin duda, al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste, entendida como

proceso electrónico que permite al receptor de un mensaje de datos únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

Para esto, se hizo necesaria la legislación federal relativa a la firma electrónica "avanzada" donde se regule la actividad de los prestadores de servicios de admisibilidad y forma de presentar como prueba en juicio a los mensajes de datos en una NOM para tales efectos, procurando preservar la independencia tecnológica.

3. Accesibilidad, se refiere a que el contenido de un mensaje de datos en el que se consignen contratos pueda estar disponible al usuario (emisor, receptor, juez, auditor, autoridades, etc.) para ulterior consulta siempre y cuando reúna las características antes anotadas. Para ello, será necesario establecer, en la legislación federal, que al efecto deberá emitirse, la forma de presentar a los usuarios estos mensajes de datos, la cual podría hacerse previa certificación de atribución e integridad por parte del prestador de servicios de certificación.

Es importante recalcar que el medio físico a través del cual el contenido de un mensaje de datos se pone a disposición del usuario, puede ser diferente de aquél en que se creó, ya que se debe garantizar la integridad del mensaje de datos y no así del medio físico que lo contiene. Esto es, que el mensaje puede estar contenido en el disco duro de una computadora y ponerse a disposición del usuario en un disquete; el copiarse a ese medio físico distinto del que fue creado, no lo hace de ninguna manera perder integridad.

El objeto del presente trabajo consiste en ofrecer una breve exposición que sirva de marco conceptual al decreto de reformas al *Código de Comercio* en materia de firma electrónica, que el pasado 26 de noviembre del 2002 fue aprobado en la Cámara de Diputados por 422 votos a favor y 1 abstención, el cual en proceso legislativo fue aprobado por el Senado de la República el 8 de abril del 2003, por unanimidad (85 votos a favor) y será vigente 90 días después de su publicación en el *Diario Oficial de la Federación* (29 de agosto de 2003). El mismo adopta básicamente la ley modelo sobre firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) e introduce en la legislación mexicana el concepto de firma electrónica fiable o avanzada y complementa la parte relativa a "mensaje de datos", detallando conceptos como: intermediario, acuse de recibo, copia y error, entre otros.

Establece el uso voluntario y la posibilidad de convenir cualquier método de firma que determinen las partes, obviamente bajo la responsabilidad de uso del firmante. Incorpora la figura del "prestador de servicios de certificación", a quien como tercero confiable estará investido de la facultad de validar, por su probidad y su tecnología (no fe pública), el proceso de emisión, identificación y atribución de firmas electrónicas. Pueden ser:

1. Notarios o corredores públicos.
2. Empresas privadas.
3. Instituciones públicas.

Reconoce como Autoridad Registradora Central a la Secretaría de Economía (además del Banco de México y la Secretaría de la Función Pública) y no descuida el reconocimiento y validez de los certificados extranjeros.

Con fecha 24 de agosto de 2006, se emite el acuerdo interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, por la Secretaría de Economía, de la Función Pública, y el Servicio de Administración Tributaria, con apego a lo dispuesto por los artículos 17, 31 fracción XXV, 34 fracciones I y XIV y 37 fracciones VI y XXVI de la Ley Orgánica de la Administración Pública Federal; 1, 2, 7 fracción XVIII y 14 fracciones I y VIII de la Ley del Servicio de Administración Tributaria; tercero transitorio del decreto por el que se reforman, adicionan y derogan diversas disposiciones contenidas en la Ley del Servicio de Administración Tributaria, publicado en el *Diario Oficial de la Federación* el 12 de junio de 2003; 5 del Reglamento Interior de la Secretaría de Economía; 6 fracción I del Reglamento Interior de la Secretaría de la Función Pública y 3 fracciones VIII, XV y XX del Reglamento Interior del Servicio de Administración Tributaria.

Se consideraron básicamente, en los términos del *Código de Comercio*, de la Ley Federal de Procedimiento Administrativo y del *Código Fiscal de la Federación*, la Secretaría de Economía, la Secretaría de la Función Pública y el Servicio de Administración Tributaria, respectivamente, la posibilidad de homologar criterios diversos sobre el uso de la firma electrónica, los mensajes de datos, las entidades certificadoras, entre otros aspectos.

Esta situación y la falta de criterios y mecanismos tecnológicos para su mutuo reconocimiento habían implicado que los usuarios de certificados digitales del Gobierno federal no puedan utilizar éstos, sólo en las dependencias donde fueron emitidos para realizar diferentes trámites y servicios electrónicos, ya que el 9 de diciembre de 2005 se publicó en el *Diario Oficial de la Federación* el acuerdo por el cual se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, a fin de promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones entre las dependencias y entidades de la Administración Pública Federal, por medio de la Subcomisión de Firma Electrónica Avanzada integrada por los representantes designados por los titulares de las Secretarías de Economía, de la Función Pública y del Servicio de Administración Tributaria, con el objetivo de coordinar las acciones necesarias para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal; se buscó la manera cumplir con los propósitos

principales de la referida Subcomisión y evitar la duplicidad o multiplicidad de certificados digitales de firma electrónica avanzada asociados a una misma persona y el de establecer el reconocimiento de los mismos por las autoridades o agencias certificadoras de las dependencias, entidades, prestadores de servicios de certificación y los artículos vigésimo cuarto, fracción v y cuarto transitorio del citado acuerdo por el que se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, previendo la emisión de los lineamientos sobre las políticas, procedimientos y estándares técnicos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, por parte de los titulares de las Secretarías de Economía, de la Función Pública y del Servicio de Administración Tributaria.

A pesar de las reformas que reconocen la validez jurídica de la firma electrónica, las empresas y los organismos públicos y privados de nuestro país requieren de la motivación para la práctica de nuevas tecnologías en su "portafolio" de estrategias de negocio.

En cuanto a los estados de México que cuentan con legislación al respecto de la firma electrónica, es de mencionar a los siguientes:

Baja California: "Ley de Firma Electrónica para el estado de Baja California," publicada el día 6 de noviembre de 2009 y que entró en vigor a partir del día siguiente de su publicación.

Chiapas: "Normatividad en materia de firma electrónica de la Administración Pública Estatal", publicada en septiembre de 2006, y el 21 de octubre de 2009 publicaron en el periódico oficial de su estado la Ley de Firma Electrónica Avanzada del estado de Chiapas, misma que entró en vigor a partir del día siguiente al de su publicación.

Guerrero: "Ley que regula el Uso de la Firma Electrónica Certificada del estado de Guerrero," publicada el día 30 de diciembre de 2008 y que entró en vigor seis meses después de su publicación.

Guanajuato: "Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el estado de Guanajuato y sus Municipios", publicada en el periódico oficial el día 9 de julio de 2004, entrando en vigor a partir del día 1 de noviembre de 2004.

Hidalgo: "Ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el estado de Hidalgo", publicada en el periódico oficial el día 10 de marzo de 2008 y que entró en vigor al día siguiente al de su publicación.

Jalisco: Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, publicada el 14 de septiembre de 2006 y que entró en vigor el 1 de enero de 2007.

Sonora: **"**Ley sobre el Uso de Firma Electrónica Avanzada para el estado de Sonora", publicada en el mes de julio del año 2006 y que entró en vigor seis meses después a su publicación.

Yucatán: "Ley sobre el Uso de Medios Electrónicos y Firma Electrónica del estado de Yucatán", publicada en el *Diario Oficial* el día 13 de abril de 2009 y que entró en vigor 180 días posteriores a su publicación.

Puebla: estudian la iniciativa de Ley de Firma Electrónica Certificada para el estado de Puebla, presentada ante el congreso el 1 de junio de 2010.

Uso de la firma electrónica en Jalisco

En el estado de Jalisco, de los dispositivos legales respecto a la firma electrónica y la función notarial, son a considerar los siguientes:

La Ley del Notariado para el estado de Jalisco, aprobada el 12 de septiembre de 2006, en la que se incorporó un capítulo dedicado al protocolo electrónico y que se encuentra vigente desde el día 26 de octubre de 2006.

El otro caso a comentar es la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, la cual entró en vigor a partir del día 1 de enero del 2007 y su reglamento respectivo.

En Jalisco, esa nueva norma se publica al abrigo del decreto número 21432/LVII/06 derivado de la aprobación de la iniciativa de ley presentada por el diputado Mario Alberto Salazar Madera en la LVII Legislatura del Congreso del Estado y bajo dictamen de la "Comisión de Puntos Constitucionales, Estudios Legislativos y Reglamentos", aprobándose finalmente el 23 de agosto de 2006, publicada en el *Periódico Oficial del estado de Jalisco*, el día 14 de septiembre de 2006, sección II, entrando en vigor el 1 de enero de 2007, expidiéndose bajo el nombre de "Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios," reformando y adicionando diversos artículos del *Código Civil*, Ley del Registro Público de la Propiedad, Ley del Notariado, Ley del Gobierno y la Administración Pública Municipal, Ley Orgánica del Poder Ejecutivo, Ley Orgánica del Poder Legislativo, Ley Orgánica del Poder Judicial y *Código de Procedimientos Civiles*, todos ellos del estado de Jalisco, y en cuya exposición de motivos planteada por el diputado Mario Salazar se manifestó que la intención principal era, entre otras:

> … crear un marco jurídico confiable que permita fomentar, promover y difundir el uso de medios electrónicos, como instrumento para optimizar los servicios técnicos y administrativos que brindan los organismos públicos y privados…

Que continuando en el cuerpo de la misma iniciativa comenta:

> El motivo de la presente iniciativa, que Jalisco cuente con la Ley de Firma Electrónica Certificada del estado de Jalisco y sus Municipios, que tiene como objeto central regular la eficacia jurídica de la firma electrónica certificada, la prestación

de servicios de certificación así como de simplificar, facilitar y agilizar los actos o negocios jurídicos, comunicaciones y procedimientos administrativos entre los sujetos obligados del sector público, los particulares y las relaciones que mantengan éstos entre sí.

Sin embargo, hasta el 19 de noviembre de 2008, mediante acuerdo[2] del gobernador Emilio González Márquez, se emite el Reglamento de la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, mismo que entró en vigor el día 28 de noviembre del año 2008, con la finalidad de que se regularan aspectos operativos de la ley sustantiva en la materia, ya que la ley señalaba que para efectos de creación y validez de la firma electrónica certificada existirán prestadores de servicios de certificación debidamente acreditados por la Secretaría General de Gobierno, quienes serán los facultados para expedir los certificados electrónicos que avalen el uso de la firma electrónica certificada.

De tal manera que mediante dicho acuerdo se creó por el Gobierno de Jalisco la Dirección de Firma Electrónica, a través de la cual se certificarán las rúbricas digitales en la entidad. El nuevo sistema permitiría reducción de costos, agilidad en el envío de información y mayor eficiencia en el quehacer gubernamental, para que dichos prestadores de servicios de certificación pudieran ser autorizados por la Secretaría General de Gobierno, debiendo cumplir con una serie de requisitos generales plasmados en la ley.

En virtud de lo anterior, resulta necesario establecer de manera detallada todos y cada uno de los elementos humanos, materiales, económicos y tecnológicos que debe tener el solicitante de la autorización como prestador de servicios de certificación y determinar los estándares internacionales con los que debe cumplir, de tal forma que se garantizará la seguridad y confiabilidad de los certificados expedidos, así como la confidencialidad de los datos proporcionados por los particulares al solicitar la expedición de un certificado electrónico.

El 28 de noviembre del 2008, el titular de Estudios Legislativos y Acuerdos Gubernamentales de la Secretaría General de Gobierno del estado de Jalisco, Francisco Castillo, declara a Notimex que el sistema de firma electrónica se instauraría en la entidad para plasmar la voluntad de los usuarios y darles seguridad jurídica, que junto con el director de Firma Electrónica, Isaac Manuel Luna Romo, y el sub-

[2] Dirección General de Estudios Legislativos y Acuerdos Gubernamentales: Acuerdo DIGELAG/ACU-087/2008, emitido con fundamento en los artículos 36, 46 y 50 fracciones VIII y XXV de la Constitución Política; 1, 2, 3, 5, 6, 19 fracción II, 21, 22 fracciones I y XXIV y 30 de la Ley Orgánica del Poder Ejecutivo; así como las disposiciones de la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus municipios.

secretario de Asuntos Jurídicos, Martín García Topete, se inauguraron las oficinas ubicadas en el Palacio de Gobierno donde se certificarán las rúbricas digitales.

A su vez, Luna Romo comentó que la firma electrónica es como utilizar una pluma convencional, pero con la certeza de que la persona que usa ese mecanismo sabe realmente lo que firma y el Gobierno del estado verifica que la firma contenga las medidas de certificación.

Destacó que con la implementación en Jalisco de la firma electrónica incrementaría la eficiencia en el quehacer gubernamental, particularmente reduciendo costos y agilizando el envío de información con una firma válida. Manifestó que el gobierno del estado de Jalisco, a través de la Dirección de Firmas Electrónicas, verificará que las personas que la emitan cumplan con todos los registros de seguridad para que las firmas digitales sean confiables. Hasta aquí la versión oficial expuesta por el Gobierno del Estado.

Pero a la fecha de su entrevista no se contaba con prestadores de servicios de certificación, por lo que la Dirección de Firma Electrónica se ha limitado a orientar algunos interesados como son los Ayuntamientos de Zapopan, Guadalajara, Tlaquepaque, Tonalá y a centros universitarios como la Universidad de Guadalajara, la UNIVA, la Universidad Panamericana y la Universidad Autónoma de Guadalajara, así como al Colegio de Notarios del Estado de Jalisco. A todos los ha orientado en aspectos técnicos, materiales, económicos y de recursos humanos necesarios para la prestación del servicio.

En ese sentido, la propuesta e intención del Gobierno estatal expuesta en el II punto de la exposición de motivos del acuerdo de creación del Reglamento de la Ley de la materia –firma electrónica–, el cual textualmente refiere que la generación de condiciones que permitan y garanticen incorporar, desarrollar y potenciar nuevas tecnologías en los diferentes contextos de la actividad humana. Para ello, resulta trascendental la participación de las entidades e instituciones de la administración pública y del sector privado mediante la creación de un marco jurídico confiable que permita fomentar, promover y difundir el uso de medios electrónicos, como instrumento para optimizar los servicios técnicos, financieros y administrativos.

El uso de la firma electrónica certificada se ha constituido en muchos países como una herramienta indispensable en el desarrollo de las actividades de la administración pública y de los particulares, por lo que mediante decreto No. 21432 publicado en el periódico oficial "El Estado de Jalisco" el 14 de septiembre de 2006 se expidió la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, misma que entró en vigor el 1 de enero de 2007. Dicha ley tiene por objeto regular la firma electrónica certificada y la prestación de servicios de certificación para simplificar, facilitar y agilizar los actos y negocios jurídicos, comunicaciones y procedimientos administrativos, entre las dependencias, entidades y organismos que conforman el sector público, los particulares y las relaciones que

mantengan éstos entre sí; pero aún constituye una de tantas buenas intenciones de nuestra legislación y de la propia Administración Pública que, al igual que otras tantas políticas públicas, aún debe mucho a la sociedad jalisciense, en espera de su verdadera aplicación e implementación no sólo entre particulares, sino también en la facilitación y agilidad en la prestación de servicios públicos.

Resulta oportuno señalar el contenido de la información emitida por la Secretaría de Planeación del Estado de Jalisco, relativa a la implementación de la Regulación de la Firma Electrónica en el Estado, el cual señala:

> Desde el año 2007, el Congreso del Estado emitió la ley que decreta la instrumentación de la firma electrónica certificada para el estado de Jalisco. Con el ánimo de dar un debido cumplimiento de la ley, durante este año 2008, se destinaron cerca de tres millones de pesos para la puesta en marcha de la autoridad certificadora que regulará en el estado, la utilización de la Firma Electrónica. Así pues, una vez que durante este 2008 se han sentado las bases para su funcionamiento, es necesario e indispensable que durante 2009 se refuercen los insumos tecnológicos que actualmente se tienen para la autoridad certificadora, de manera que podamos ampliar su capacidad de servicio y garantizar aún más la seguridad necesaria, de manera que se cumpla cabalmente con los lineamiento que señala la autoridad certificadora federal ITFEA.

El mismo documento señala que el programa deriva del fortalecimiento institucional para la calidad de los sistemas de gestión pública, cuyo objetivo es la consolidación de la infraestructura necesaria para dar cumplimiento a los procesos de certificación de los actos jurídicos a través de la firma electrónica; no obstante, se señala en el porcentaje de avance un factor de 0.0%, con fecha de inicio del 1 de enero del año 2009, para su implementación y fijando como meta el 31 de diciembre del mismo año para su consolidación, por conducto de la Dirección de Firma Electrónica de la Secretaría General de Gobierno con un presupuesto anual estatal asignado de $5,540,240.00, y un presupuesto anual estatal ejercido de $454,560.69. Paradójicamente, dicho programa señala en su proyección de la consolidación de la firma electrónica en el estado, que para el mes de abril –fecha de expedición– se llevará un porcentaje de aplicación del 54%, es decir, más de la mitad del avance, no obstante la propia Dirección encargada de sentar las bases e implantarlas, reconoce que aún no se cuentan con certificadores al 2 de marzo del año 2009 y, por ende, no se tiene la posibilidad de acceder a los servicios previstos por la propia ley a beneficio de la ciudadanía, ya que, como señala dicha Dirección, no está facultado el propio gobierno del estado para "otorgar firmas electrónicas", sólo reconocer prestadores de certificación.

Según los indicadores de avances que emite la Secretaría de Planeación del Gobierno del Estado de Jalisco, respecto de la regulación de la prestación de servicios

de certificación de firma electrónica en el estado, a través de la certificación que debe otorgarse a la entidad que solicite convertirse en prestador de dichos servicios, iniciado en el mes de enero de 2010 hasta diciembre del mismo año, se cuenta con un presupuesto anual asignado de 2'188,340.00 pesos, del cual han ejercido la cantidad de 699,610.47 pesos; mencionando que cuentan con avance del 50% de las metas anuales, considerando que toman como meta anual la cantidad de 0 y han autorizado como prestador de servicios de certificación sólo a una entidad, y en lo que respecta a la asesoría señalan a diez dependencias públicas y organismos públicos o privados.[3]

[3] Secretaría de Planeación del Estado de Jalisco, http://seplan.app.jalisco.gob.mx/table/reporte/ficha_proyecto.html, información actualizada el día 29 de mayo de 2010.

Capítulo IV

La firma electrónica en la práctica: la necesidad de homologación de criterios en su utilización (ITFEA)

El 9 de diciembre de 2005 se publicó en el *Diario Oficial de la Federación* el acuerdo por el cual se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, la cual se encargaría de promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones, entre las dependencias y entidades de la Administración Pública Federal.

El acuerdo creaba con carácter permanente la Subcomisión de Firma Electrónica Avanzada, integrada por los representantes designados por los titulares de las Secretarías de Economía, de la Función Pública y del Servicio de Administración Tributaria, con el objetivo de coordinar las acciones necesarias para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal.

Dentro de los propósitos principales de la Subcomisión se encontraba el de evitar la duplicidad o multiplicidad de certificados digitales de firma electrónica avanzada asociados a una misma persona y el de establecer el reconocimiento de los mismos por las autoridades o agencias certificadoras de las dependencias, entidades, prestadores de servicios de certificación, de tal manera que en cumplimiento de los artículos 24 fracción V, y cuarto transitorio del citado acuerdo, la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico emite los lineamientos sobre las políticas, procedimientos y estándares técnicos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, por parte de los titulares de las Secretarías de Economía, de la Función Pública y del Servicio de Administración Tributaria.

Acuerdo interinstitucional

El 19 de abril del año 2006 se aprobó el acuerdo interinstitucional en el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, mismo que fue publicado

en el *Diario Oficial de la Federación* el día 24 de agosto del mismo año de su aprobación.[1] La Secretaría de Hacienda y Crédito Público, por conducto del Servicio de Administración Tributaria, la Secretaría de Economía y la Secretaría de la Función Pública, contaban con diferentes instrumentos normativos que regulan la operación de la firma electrónica avanzada en cada uno de sus ámbitos de competencia, esto ocasionaba que los ciudadanos usuarios de los servicios del Gobierno federal tuvieran que obtener múltiples certificados de firma electrónica avanzada, por eso se creo la Subcomisión para la homologación de la operación de la firma electrónica avanzada en todas las dependencias y entidades de la Administración Pública Federal, mediante dicho acuerdo,[2] cuyo propósito principal es evitar la duplicidad o multiplicidad de certificados digitales de firma electrónica asociados a una misma persona y establecer el reconocimiento de los mismos que hayan sido emitidos por cada una de las dependencias y entidades.

Con el fin de buscar la estandarización de los procedimientos y tecnologías para la emisión de certificados digitales que permitan la interoperabilidad entre las autoridades certificadoras de la Administración Pública Federal, se emitieron diversos lineamientos sujetos a las limitaciones previstas en las leyes, convenios y acuerdos vigentes de la materia, y en caso de existir incompatibilidades esta subcomisión se abocaría a elaborar y promover las iniciativas de reformas legales y reglamentarias procedentes; ello, considerando que términos del *Código de Comercio*, de la Ley Federal de Procedimiento Administrativo y del *Código Fiscal de la Federación*, la Secretaría de Economía, la Secretaría de la Función Pública y el Servicio de Administración Tributaria, respectivamente, cuentan con las atribuciones para emitir certificados de firma electrónica avanzada y ya que la falta de criterios y mecanismos tecnológicos para su mutuo reconocimiento había implicado que los usuarios de certificados digitales del Gobierno federal no puedan utilizar éstos más que en las dependencias donde fueron emitidos para realizar diferentes trámites y servicios electrónicos. El acuerdo cumpliría con las necesidades para la solución de los problemas.

---

1 http://www.politicadigital.com.mx/pics/pages/marcolegal_base/Acuerdo-firma-240806.pdf

2 Con las facultades previstas por los artículos 17, 31 fracción XXV, 34 fracciones I y XIV y 37 fracciones VI y XXVI de la Ley Orgánica de la Administración Pública Federal; 1, 2, 7 fracción XVIII y 14 fracciones I y VIII de la Ley del Servicio de Administración Tributaria; tercero transitorio del decreto por el que se reforman, adicionan y derogan diversas disposiciones contenidas en la Ley del Servicio de Administración Tributaria, publicado en el *Diario Oficial de la Federación* el 12 de junio de 2003; 5 del Reglamento Interior de la Secretaría de Economía; 6 fracción I del Reglamento Interior de la Secretaría de la Función Pública y 3 fracciones VIII, XV y XX del Reglamento Interior del Servicio de Administración Tributaria.

El acuerdo se encuentra dividido en nueve capítulos que establecen los criterios y lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, los cuales se encuentran divididos de la siguiente manera:

El capítulo I contiene las disposiciones generales, en el que básicamente conceptualiza el objeto del acuerdo interinstitucional, siendo éste el de establecer los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, que deberán observar y promover la Secretaría de Economía, la Secretaría de la Función Pública y el Servicio de Administración Tributaria para el reconocimiento de certificados digitales de firma electrónica avanzada de personas físicas. Para llevar a cabo el reconocimiento de certificados digitales, los integrantes de la Subcomisión implementarán una infraestructura tecnológica de firma electrónica avanzada que operará conforme a los medios y mecanismos de comunicación (F1) que se encuentran en la dirección electrónica http://www.cidge.gob.mx.[3]

En segundo término, conceptualiza tecnicismos tales como: las AC (las dependencias, entidades, organizaciones, instituciones y proveedores de servicios de certificación que cuentan con la infraestructura tecnológica para la emisión y registro de certificados digitales de firma electrónica avanzada), los certificados digitales**,** las claves privadas, la clave pública**,** las dependencias (que integran la Administración Pública Federal centralizada en términos de los artículos 1 y 2 de la Ley Orgánica de la Administración Pública Federal, incluyendo en su caso a sus órganos administrativos desconcentrados) las entidades (Los OPD'S, las empresas de participación estatal mayoritaria y los fideicomisos públicos que tengan el carácter de entidad paraestatal, a que se refieren los artículos 1, 3, 45, 46 y 47 de la Ley Orgánica de la Administración Pública Federal); la FEA, ahora FIEL (Firma Electrónica Avanzada) ITFEA (infraestructura tecnológica que permite la interoperabilidad y el reconocimiento de certificados digitales de firma electrónica avanzada entre las autoridades o agencias certificadoras que la integran), mensaje de datos**,** las organizaciones e instituciones**,** los PSC (Prestador de Servicios de Certificación) los RCD (Registro de Certificados Digitales), requerimientos de certificación**,** a las Secretarías (SAT, SE, SFP)**,** a la propia Subcomisión y al titular de un certificado digital.

El capítulo II contiene las funciones de la Subcomisión en el ámbito de la ITFEA, cuyas actividades principalmente se encuentran encaminadas a coordinar con la Secretaría de Gobernación, por medio de la Dirección General del Registro Nacional de Población e Identificación Personal (RENAPO), los mecanismos de registro e identificación de las personas, así como los procedimientos de certificación electrónica

[3] Pagina web oficial de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, consultada por última ocasión el día 29 de mayo de 2010.

de identidad; a emitir el dictamen de acreditación para la integración de una AC a la ITFEA, y en su caso, para la revocación o suspensión; publicar la acreditación, revocación y/o suspensión de una AC en el *Diario Oficial de la Federación*, así como difundir y promover información de interés para los titulares de los certificados digitales de FIEL; mantener la actualización permanente de los presentes lineamientos; supervisar y revisar periódicamente la operación e infraestructura tecnológica de las AC que integran la ITFEA de acuerdo a los presentes lineamientos; emitir las recomendaciones de carácter técnico y operativo para el mejor funcionamiento de las AC; establecer procedimientos y mecanismos comunes dentro de la ITFEA; promover la celebración de acuerdos de colaboración; difundir el ámbito de aplicación de los certificados digitales emitidos por las AC integrantes de la ITFEA. Para efectos de las fracciones L, LL, LLL, VI Y VII de este lineamiento, la SE será la encargada de realizar las actividades a que se refieren dichas fracciones con respecto de los PSC acreditados por ella.

El resto de los apartados se encuentran divididos en el capítulo III: Reconocimiento de certificados digitales de firma electrónica avanzada de la ITFEA; capítulo IV: Integración a la ITFEA (que van desde la elaborarán la solicitud correspondiente, de acuerdo al formato de solicitud de integración a la ITFEA, la revisión documental de la infraestructura tecnológica, el formato de revisión documental de la infraestructura tecnológica y de la operación de la infraestructura tecnológica y el dictamen); capítulo V: Solicitud de un certificado digital de firma electrónica avanzada; capítulo VI: Revocación de un certificado digital de firma electrónica avanzada; capítulo VII: Estructura del certificado digital; capítulo VIII: Obligaciones de una AC; capítulo IX: Uso de los certificados digitales de FEA, más cuatro transitorios y tres anexos que contienen: anexo I: Solicitud de certificado digital de firma electrónica avanzada; anexo II: Comprobante de emisión de certificado digital de firma electrónica avanzada y anexo III: Comprobante de revocación de certificado digital de firma electrónica avanzada.

Criterios para seleccionar una autoridad de certificación según Microsoft México

Existe una amplia polémica respecto de los criterios más importantes que debe cumplir una autoridad de certificación para proporcionar todos los servicios a ella vinculados, incluida la firma electrónica necesaria para la emisión de facturas telemáticas o documentos sustitutivos en formato electrónico. La revista[4] *Windows TI,* en su publicación 135 del año 2008, señala criterios básicos con que deben contar las

[4] http://www.windowstimag.com/N%C3%BAmerosanteriores/N%C3%BAmero124Octubre2007/FirmaAutoridadesdecertificaci%C3%B3nelectr%C3%B3nica/tabid/295/Default.aspx

entidades certificadoras, para cubrir las necesidades de calidad y seguridad para los usuarios, entre los que destacaban:

a) Reconocimientos oficiales

Un requisito indispensable es que el certificado seleccionado sea reconocido en términos de la legislación aplicable, en este caso por la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios.

Existen otras legislaciones aplicables, que serán tratadas a detenimiento en lo sucesivo, un ejemplo claro en su uso en efectos fiscales, donde existe el reconocimiento de la autoridad tributaria, sería como en el caso de las facturas telemáticas, las cuales pueden ser un elemento necesario en litigios, reclamaciones o incluso en procesos internos de auditoría.

En ese mismo sentido, resulta importante citar la regla general 2.22.1 de la resolución miscelánea fiscal para el 2005, en la cual el procedimiento para la obtención del certificado de la firma electrónica avanzada, desde la cinta hasta la obtención del programa que genera las llaves pública y privada, llamado solicitud de certificado digital (SOLCEDI) sin que en la legislación fiscal se hayan establecido los lineamientos al Ejecutivo para la emisión de esta regla general, puesto que el artículo 17-D, quinto párrafo, del Código Fiscal de la Federación, sólo señaló que: "Los datos de creación de firmas electrónicas avanzadas podrán ser tramitados por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios de certificación autorizado por el Banco de México", hecho que causó conflicto para muchos contribuyentes, originando que se establecieran criterios encaminados a considerar que la autoridad fiscal se excedía y violaba las garantías consagradas en los artículos 72, inciso F y 89, fracción I de la Constitución Federal, ya que se establecía que la obtención del certificado digital se haría mediante el *software* denominado SOLCEDI, cuando el legislador en la ley no autorizó el uso de ningún *software*, ni dejó a elección de la autoridad optar o no por ello, considerándose que la regla general 2.22.3 de la propia resolución miscelánea establecía más requisitos de los que el legislador señalaba para la obtención de los certificados digitales en la propia ley, tales como la obligación de que el certificado deberá contener los datos del emisor, su número de serie y el periodo de validez del certificado.

b) Sistemas de almacenamiento y custodia de certificados

Otro elemento a valorar es el dispositivo de almacenamiento del certificado (fichero, tarjeta chip o USB flash securizado). Del cual cabe hacer las siguientes consideraciones:

I. *Fichero* (certificado formato PKCS12). Es la fórmula más económica, pero presenta el problema de que resulta extremadamente sencillo realizar copias y que

permite generar firmas incluso cuando el certificado ha sido revocado o caducado. En un escenario de deslealtad interna, la empresa titular del certificado no podría evitar que el certificado se siguiese empleando, trasladando una inseguridad al receptor de los documentos.

II. *Tarjeta SmartCard* (certificado en formato PKCS15). Resulta mucho más seguro que el anterior. Como elementos a tener en consideración, debe contemplarse la necesidad de mantener un dispositivo dedicado de conexión con el ordenador y la necesidad de introducir el PIN para cada documento que se desea firmar en la mayoría de las configuraciones de este dispositivo. En un escenario de factura telemática, en el que se desea firmar múltiples documentos, este proceso no es asumible por el usuario.

III. *USB Flash securizado* (certificado PKCS15 en dispositivo). Esta solución ha sido diseñada específicamente para las necesidades de uso que se plantean en las empresas. Firma desde diferentes ordenadores sin necesidad de instalar controladores del dispositivo ni programas en el ordenador, soporte económico disponible en cualquier tienda; tecnología de notariado electrónico incorporada en el propio dispositivo y accesible desde aplicaciones de terceros para procesos de firma y autenticación.

c) Dispositivos de firma homologados por la autoridad de certificación (ejemplo: acuerdo ITFEA)

A efecto de garantía fiscal y jurídica debe verificarse que la autoridad de certificación reconoce u homologa dicho dispositivo. Esto es así ya que de lo contrario la AC podría inhibirse frente a un proceso de impugnación de la firma o en caso de incidencia.

Existen entidades de certificación digital para personas y empresas, entre otras.

d) Soluciones de alto rendimiento homologadas por la AC

En el caso de que la empresa requiera firmar un número elevado de documentos, en un corto espacio de tiempo, resulta recomendable emplear soluciones de alto rendimiento.

e) Disponibilidad y coste de los servicios de verificación

Aspecto fundamental dado que, si el cliente receptor del documento debe asumir costes por el hecho de verificar las facturas o realizar procesos administrativos, no aceptará la recepción por este medio.

f) Servicios de verificación para firmas de larga duración

La verificación debe ser realizada en cualquier momento durante la vigencia del documento. En el caso de la factura, un mínimo de cuatro años, que puede ser muy

superior si se realizan amortizaciones del bien adquirido cuya compra se justifica con las facturas recibidas del proveedor.

g) Capacidad de integración con entornos y soluciones informáticas

Resulta fundamental que los dispositivos de firma y verificación hayan sido diseñados para permitir la máxima integración con las aplicaciones de gestión y ERP empleadas por las empresas. La necesidad de realizar procesos independientes, o el adoptar modelos de firma que presuponen la necesidad de realizar tareas mediante dedicación manual, pueden eliminar el coste operativo que aporta la factura telemática.[5]

h) Uso de estándares de formato

El formato que será más ampliamente adoptado por las soluciones de gestión es el ebXML-UBL,[6] debido a su flexibilidad intersectorial y proyección internacional, con el valor añadido de ser compatible con la especificación EDIFACT, aunque, en este caso, existen especificaciones particulares para algunos receptores.

I) Responsabilidades asumidas con emisor y receptor

Antes de seleccionar un certificado, emisor y receptor deberán consultar la Declaración de Prácticas de Certificación de la AC,[7] para obtener información precisa sobre las responsabilidades que asumen emisor y receptor y la cobertura que aporta a ambos la propia autoridad de certificación.

---

[5] Desde el pasado 31 de marzo del 2004, se realizó la legislación para la integración de los comprobantes fiscales digitales y que abarca los mensajes de factura, notas de crédito, cargo, recibos de honorarios. En la actualidad, en México existen algunos sectores que están integrando a una comunidad interesante de proveedores para la emisión de facturas electrónicas; los sectores que están impulsando más activamente la integración de los comprobantes fiscales digitales son el del Retail, aseguradores, automotriz en donde la parte del Gobierno mexicano también está impulsando su uso mediante la incorporación de PEMEX al proceso de la emisión y recepción. http://www.facturasat.com/

[6] Es una especificación técnica para la integración a las nuevas transacciones electrónicas que están definidas en dos secciones: 1) librería de datos, por ejemplo, dirección, productos, pagos, etc., y 2) schemas que define los documentos y tipos de datos en las etiquetas; la definición del UBL es compatible con la norma ISO 15000 y están definidos en las transacciones electrónicas que se encuentran liberadas.

[7] Este documento describe la Declaración de Prácticas de Certificación para Autoridades Certificadoras que son parte de la infraestructura de clave pública de la Secretaría de Economía, así como de aplicar las políticas de lineamientos del acuerdo en cita al inicio del presente capítulo.

Norma Oficial Mexicana NOM-151-SCFI-2002

La NOM-151-SCFI-2002 es aplicada por la Dirección General de Normatividad Mercantil. Es una unidad administrativa de la Secretaría de Economía que cuenta con los recursos técnicos e infraestructura necesarios para llevar a cabo las tareas de vigilancia e inspección, así como la evaluación de la conformidad de la Norma Oficial Mexicana NOM-151-SCFI-2002 y de otros servicios de firma electrónica.

El 20 de marzo de 2002, el Comité Consultivo Nacional de Normalización de Seguridad al Usuario, Información Comercial y Prácticas de Comercio (Diario Oficial de la Federación, 2005: 47) aprobó por unanimidad la publicación de la Norma Oficial Mexicana NOM-151-SCFI-2002 en el *Diario Oficial de la Federación*, relativa a las "Prácticas comerciales-requisitos que deben observarse para la conservación de mensajes de datos, lo cual se realizó el 4 de junio de 2002". En el único transitorio de la citada NOM, para llevar a cabo la evaluación de la conformidad de la misma se cuenta con la infraestructura necesaria para regular los requisitos que deben observarse para la conservación de mensajes de datos; que las tecnologías, *software* y lenguajes a que hace referencia el inciso 5.3 y el apéndice normativo de la mencionada Norma Oficial Mexicana NOM-151-SCFI-2002, constituyen meros ejemplos de aquellos que deben utilizar los comerciantes para garantizar la conservación de los mensajes de datos; los lineamientos generales del gobierno procuran minimizar los impactos adversos que puedan derivarse del cumplimiento de las regulaciones que la sociedad requiere.

La NOM, en su primera fase, sólo considera la conservación de los documentos que se generan, dejando para una segunda fase la conservación de los documentos generados con anterioridad a esta fecha; desde el punto de vista jurídico, la aplicación de la NOM 151 a los documentos electrónicos debe considerarse de total beneficio ya que, de decidir no utilizarla, la empresa estaría en estado de indefensión ante un conflicto. Además, permite complementar los procesos de las empresas al cumplir con los elementos de validez fiscal y con las obligaciones mercantiles.

En el caso de que una empresa decida utilizar los documentos sin que tengan carácter probatorio, no está prevista sanción alguna de acuerdo a lo comentado por las autoridades. Sin embargo, es importante resaltar el valor que tiene la conservación de documentos como elementos probatorios en caso de controversia.

Por otro lado, aunque la constancia debe ser expedida por un prestador de servicios de certificación, existe la posibilidad de que la misma empresa pueda ser certificada por la Secretaría de Economía para la conservación de sus propios documentos, precisando que los requisitos de infraestructura, personal y procedimientos para constituirse en PSC son estrictos. En términos económicos, sólo convendría a una empresa cuyo volumen de documentos fuera muy grande o que tuviera la intención de concurrir al mercado; de cualquier manera, la recomendación de las

autoridades[8] es que las empresas se vayan preparando para adoptar la NOM 151, ya que ésta traerá ventajas en los procesos mercantiles.

Acuerdos diversos sobre criterios de uso de firma electrónica

Acuerdo por el que se delegan facultades a la Dirección General de Normatividad Mercantil en materia de evaluación de la conformidad de la Norma Oficial Mexicana NOM-151-SCFI-2002, "prácticas comerciales-requisitos que deben observarse para la conservación de mensajes de datos" y otros servicios de firma electrónica, competencia de la Secretaría de Economía.

Contiene un artículo único, mediante el cual se delegan en la Dirección General de Normatividad Mercantil de la Secretaría de Economía, ciertas facultades de evaluación de la conformidad a la NOM-151-SCFI-2002, "Prácticas comerciales-requisitos, que deben observarse para la conservación de mensajes de datos", incluida la de los programas informáticos para la prestación de los servicios regulados por la misma, así como realizar inspecciones, visitas, requerir información y, en general, todo lo necesario para vigilar e inspeccionar el cumplimiento de la NOM-151-SCFI-2002, además de establecer criterios y procedimientos mediante la emisión de lineamientos para la migración de información, así como emitir los criterios interpretativos o lineamientos para la aplicación de la NOM-151-SCFI-2002.[9]

Acuerdo general 21/2007 del pleno del Consejo de la Judicatura Federal, que establece la Firma Electrónica para el Seguimiento de Expedientes (FESE). Este acuerdo fue publicado en el *Diario Oficial de la Federación* el 7 de junio de 2007, en el que se establece ante los órganos jurisdiccionales la utilización por las partes o personas autorizadas, la Firma Electrónica para el Seguimiento de Expedientes (FESE) para todos aquellos trámites señalados en el acuerdo 21/2007 del Pleno del Consejo de la Judicatura Federal.[10]

Acuerdo de la Comisión de Administración del Consejo de la Judicatura Federal 14/X/08 No. 10, 1ª sección, página 110. El cual modifica el segundo párrafo del punto tercero; segundo párrafo del punto cuarto; primer párrafo del punto quinto; el punto sexto, el tercer párrafo del punto octavo; punto décimo y se elimina el segundo párrafo del punto quinto del acuerdo de la Comisión de Administración del

---

8 http://www.amece.org.mx/amece/NOM151_Factura_Electronica.php.

9 Publicación en la página web oficial de la Secretaría de Economía http://www.economia.gob.mx /pics/p/p437/A361.pdf

10 http://www.scjn.gob.mx/NR/rdonlyres/556FDA90-BE12-40D7-B697-48B32BE2F799/0/N070607.PDF

Consejo de la Judicatura Federal, que establece el procedimiento de asignación, certificación y uso de la firma electrónica para el seguimiento de expedientes (FESE).

Acuerdo que modifica las reglas generales a que deben sujetarse los prestadores de servicios de certificación. Este acuerdo fue publicado en el *Diario Oficial de la Federación* el 27 de marzo de 2007, en el cual se establecen criterios a que se deben de apegar los PSC, relacionados básicamente al análisis de evaluación de riesgos en la prestación del servicio.[11]

[11] http://www.amece.org.mx/amece/Documentos/procesos/factura/ACUERDO.pdf

Capítulo V

Uso de la firma electrónica y de las tecnologías de la información en la función notarial

El uso de las nuevas tecnologías de información y comunicación han transformado con su aplicación casi todas las actividades del ser humano, hecho del que no se escapa el Derecho y específicamente la actividad notarial, la cual se ha tenido que adaptar paulatinamente en el moderno esquema de sociedad digital para dar paso a una nueva generación de actividades y procesos sistematizados, cada vez más lejos del papel, elemento fundamental en la certificación de documentos de orden legal y básico del oficio notarial.

El notario público como garante en la certificación digital

El notario es un profesionista en Derecho que desempeña una función pública investido por el Estado para dotar de fe pública y hacer constar hechos, actos y negocios jurídicos a los que se quiera o deba dar autenticidad y seguridad jurídica, y que además tiene a su cargo asesorar personalmente e ilustrar con imparcialidad a quienes soliciten sus servicios, por lo que debe recibir, interpretar y dar forma a su voluntad, proponiendo los medios legales adecuados para el logro de los fines lícitos que se proponen alcanzar y advertirles de las consecuencias legales de su voluntad.

El notario cumple una de las más importantes finalidades del Derecho, que es brindar seguridad jurídica a través del ejercicio de varias funciones, entre las que destacan:

I. *Asesorar:* ofrece su consejo jurídico a cualquier persona, institución o empresa que lo requiera, dentro de un marco legal de servicio obligatorio institucional a los ciudadanos.
II. *Interpreta la voluntad:* recibe e interpreta la voluntad de las personas que acuden ante él para la obtención de un servicio notarial concreto.
III. *Da forma, legaliza y legitima:* cumple con la formalidad exigida por la legislación vigente para ciertos actos jurídicos, es decir, dota de plena validez jurí-

dica a ciertos actos jurídicos que deben otorgarse de manera obligatoria ante su fe, como la compraventa de inmuebles, el condominio, el testamento, entre otros, y confiere además al documento público que produce la garantía de legalidad absoluta.

IV. *Tiene el poder de la fe pública:* confiere autenticidad y certeza jurídica a ciertos hechos y actos jurídicos mediante la consignación de ellos en el protocolo, dotándolos así de valor de prueba plena ante las autoridades y la sociedad.

V. *Crea documentos auténticos:* es autor responsable de los instrumentos públicos notariales que circulan con valor de prueba plena ante la comunidad nacional e internacional. Además, conserva los instrumentos originales otorgados y autorizados en el protocolo y expide un primer testimonio auténtico con fuerza ejecutiva a solicitud de los interesados y reproduce ilimitadamente nuevas copias auténticas.

VI. *Auxilia a la Administración Pública y al Poder Judicial:* actúa como auxiliar de la administración pública local y federal, dando informes y avisos y actúa como un eficiente recaudador de impuestos federales y locales. Además, desempeña la función de auxiliar en la administración de justicia en colaboración del Poder Judicial.

VII. *Tiene el novedoso papel de asesor internacional:* le permite emitir dictámenes jurídicos y opinar como jurista nacional en el comercio internacional.

VIII. *Puede actuar como mediador, conciliador y árbitro:* en la prevención y solución extrajudicial de controversias, desahogando así la enorme carga pública de atender la demanda de justicia y paz en la sociedad.

En todo este desarrollo tecnológico y la aparición de un nuevo tipo de instrumento público, como lo es el instrumento y/o documento electrónico, la función del notario se hace imprescindible para darle fe a los mismos, por eso la importancia de su estudio dentro de la investigación.

Estos nuevos instrumentos notariales deben pasar por la intervención de un funcionario público que le de pleno valor jurídico, protegiendo los actos y los documentos en los que participe.

El documento notarial debe de estar firmado como anteriormente aclarábamos por el autor del mismo, firma que el caso de los electrónicos debe ser digital para que tengan plena seguridad en el acontecer del Derecho actual en su relación con la informática.

En todo caso, podemos afirmar que la función notarial no es ni será obsoleta, sólo tendrá que adecuarse a la manera de prestar el servicio notarial, con base en el tradicional documento que era basado únicamente en soporte papel. Lo que el notario requiere es adaptarse a las exigencias y transformaciones del mundo actual

e incorporar en su quehacer herramientas como la informática, la criptografía[1] y la telemática, con el uso de la firma electrónica, el certificado digital, e incluso la propia factura electrónica.

Esta problemática es la que ha traído consigo el inconveniente de la inseguridad de este tipo de operaciones tan vistas en el mundo desarrollado y necesitadas en el resto de los países.

Desde este ángulo se encuentran la confidencialidad y la autenticidad como unas de las propiedades más importantes de los documentos electrónicos; refiriéndose la primera a la posibilidad de mantener un documento electrónico inaccesible a todos excepto a una lista de individuos autorizados. La autenticidad, por su parte, es la capacidad de determinar si uno o varios individuos han reconocido como suyo y se han comprometido con el contenido del documento electrónico. El problema de la autenticidad en un documento tradicional se soluciona mediante la firma autógrafa. Mediante su firma autógrafa, un individuo o varios de ellos manifiestan su voluntad de reconocer el contenido de un documento y, en su caso, a cumplir con los compromisos que el documento establezca para con él o los individuos.

Los problemas relacionados con la confidencialidad, integridad y autenticidad en un documento electrónico se resuelven mediante la tecnología llamada *criptografía*.

---

[1] En la criptografía, según refiere la maestra Leticia Margarita Domínguez, en sus conferencias respecto del tema que se pueden distinguir dos tipos: la criptografía simétrica es el método criptográfico que usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma; y la criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública*, y se puede entregar a cualquier persona; la otra es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo *n* pares de claves por cada *n* personas que deseen comunicarse entre sí.

Se ha visto la importancia de la firma digital en los documentos electrónicos, y cómo, mediante este sistema de clave pública o criptografía cerrada, pueden garantizarse de forma segura, efectiva y pormenorizada los documentos. El procedimiento de firma de un documento digital, por ejemplo, implica que mediante un programa de cómputo un sujeto prepare un documento a firmar y su llave privada (que sólo él conoce). El programa produce como resultado un mensaje digital denominado firma digital; juntos, el documento y la firma, constituyen el documento firmado.

Sólo prueba la firma electrónica que se utilizó la llave privada del sujeto y no necesariamente el acto personal de firma; por lo tanto, no es posible establecer con total seguridad que el individuo firmó un documento, sino que sólo es posible demostrar que es el individuo el responsable de que el documento se firmara con su llave privada. En otras palabras, si un documento firmado corresponde con la llave pública de un sujeto, entonces éste debe de reconocer el documento como auténtico.

En todo este proceso, la figura del notario en nuestra legislación estatal cumple una función social relevante por demás, puesto que funge como asesor y consejero, previendo en los actos que la capacidad legal de las partes, sus facultades, propiedades, gravámenes de las mismas, entre otras cosas, se vean siempre ajustadas a derecho; es decir, que él mismo constituye la figura de un perito y fedatario en los actos jurídicos para su perfeccionamiento, buscando, ante todo, el reducir al mínimo los problemas jurídicos y sociales que se generan con la celebración de actos jurídicos que requieren solemnidad y de su fe pública.

La relevancia que adquiere la "fe pública"; según Enrique Giménez-Amau, (Giménez, 1976: 15) en su libro de *Derecho notarial* al señalar que: "El que tiene fe, tiene una creencia, una convicción, una persuasión, una certeza, una seguridad o una confianza en algo", algo que pudo o no haber percibido por medio de sus sentidos, pero que con independencia de ello lo acepta como verdadero, sin emitir una duda. Existen diversos tipos de fe pública, entre ellas destacan fe pública notarial, fe pública judicial, fe pública registral y fe pública administrativa, ello se colige de que la "fe pública" (Ríos, 2000: 141) es sólo una y es poder y facultad de los Estados, quien puede ejercerla por sí mismo o delegarla como a un particular como es el caso del notario público, quién a lo largo del tiempo ha gozado de un reconocimiento público derivado de la solemnidad de sus actos y de su facultad de ostentar la fe pública.

En ese sentido, resulta oportuno afirmar que es el notario público,[2] y es un delegado del estado con función fedante, el cual tiene la encomienda por un acto de autoridad (FIAT) sin considerarse parte del aparato burocrático, la tarea de ser vigilante y garante de los actos de los que da testimonio.

La Ley del Notariado del Estado de Jalisco, en su artículo 3 define al notario público como: "el profesional del Derecho que desempeña una función pública,

[2] Idem.

investido por delegación del Estado a través del titular del Poder Ejecutivo, de la capacidad de formalizar y dar fe para hacer constar hechos, actos y negocios jurídicos a los que se quiera o deba dar autenticidad y seguridad jurídica".

Es así que con la evolución de la tecnología han aparecido nuevas figuras como la del "cibernotario" o "cibernotary", que son aquellas personas "competentes para proveer servicios de seguridad jurídica en actos traslativos de dominio vía internet, el uso de firmas electrónicas y certificados digitales, entre otros.

Ya se ha establecido que la función notarial clásica tenía determinados principios generales, los cuales pueden ser plasmados también cuando usamos las nuevas tecnologías; entre ellos, tenemos el principio de integridad, confidencialidad, autenticidad, legalidad, registro y conservación.

En ese sentido, el notario público puede darle al documento un valor agregado además del que le dio la seguridad informática con los logaritmos de cifrado y confidencialidad, ya que el notario puede ser el depositario de las conocidas claves o llaves públicas y privadas que utilicen las personas al hacer sus negocios. Muchas veces podemos pensar que las nuevas tecnologías ponen en peligro el principio de autenticidad; pero no es así, ya que en soporte papel también existe ese peligro de que el documento pueda ser adulterado o falsificado. Pero aquí lo que se requiere para esta nueva forma de contratar es que exista una persona imparcial, que a su vez sea un experto en Derecho y que asegure quién es realmente el emisor y que identifique a esa persona adecuadamente, y quién mejor que el notario público, que ha tenido desde los comienzos de su existencia la facultad de certificación de la identidad de las personas**.**

En cuanto la legalidad de los hechos del notario público, ejerce una función de control con respecto a los actos que se realizan a través de la red de redes, más conocida por internet, participando en negociaciones que se van a realizar a distancia, debiendo éste aumentar sus conocimientos de Derecho comparado, ya que muchas veces su colega o la otra parte puede estar en un país al otro lado del mundo; por ejemplo, teniendo que controlar no sólo la ley y la jurisdicción aplicables, sino también cómo proteger al individuo que busca de sus servicios, de los abusos de que pudiera ser objeto.

Actualmente, los registros y actuaciones notariales se conservan en papel, en archivos, con las nuevas tecnologías vemos que esos soportes pueden cambiar de papel a disquetes, CDs, discos duros, entre otros, pero tomando como siempre las precauciones del caso, para que estos permanezcan en buen estado de conservación y que con el correr del tiempo podamos leer esos archivos, a pesar del avance de las nuevas tecnologías.

Es así que se debe prever que los documentos conserven su identidad, permanencia e inalterabilidad y tener presente que las reproducciones tienen el mismo valor que los originales y se nos dificulta saber cuál es el original y cuál es la copia.

El surgimiento de las nuevas tecnologías no significa que el ejercicio de la profesión se vea amenazado, sino que, por el contrario, la buena implementación de los medios informáticos y tecnológicos va a lograr que la actividad notarial, cumpliendo con su función notarial, sea más rápida y eficaz. Y que las nuevas tecnologías se implementen, mediante capacitación y el trabajo disciplinario necesario, y que el notario público esté en facultad de brindar la seguridad jurídica necesaria en la actualización informática de la oficina notarial mediante el vínculo con otros organismos que se encuentran relacionados con la función notarial.

El documento electrónico y el instrumento público

Es evidente que la formulación de un sistema normativo integral relativo al instrumento público notarial electrónico debe tener en consideración diversas técnicas que resultan imprescindibles en su construcción, tales como la informática jurídica destinada a poner al servicio del Derecho, los medios propios de procesar información, incluidas las bases de datos correspondientes y el Derecho informático.

Lo anterior con la finalidad es resolver normativamente los problemas planteados por la técnica informática y así incluirá aspectos como la protección del *software*, legislación sobre contratación informática, normas sobre Derechos de autor y otros.

Dentro de la informática jurídica, es preciso incluir a la informática jurídica documental, técnica aplicada destinada a poner al servicio del Derecho al documento electrónico, el cual, una vez regulado jurídicamente, se transforma en un instrumento útil para el mundo jurídico. En este sentido, se debe considerar las múltiples variables que a la informática jurídica documental importa. En relación con los aspectos normativos que afectarán al instrumento, son de dos tipos:

I. El uso de un soporte diferente al papel, sistemas de cifrado electrónico destinados a otorgar seguridad jurídica, aspectos probatorios, efectos que produce el instrumento electrónico, responsabilidades que genera, aspectos de Derecho internacional privado y de derechos autorales documentales.
II. Aquellas relativas a las formalidades a cumplir y a la manera de poner en práctica las diferentes solemnidades a que estén sujetos los diversos actos y contratos, tales como: las de fe de conocimiento, la unidad de acto, la conservación documental, la dación de copias y, en general, todas aquellas propias de la observancia de las formas a que quedan sujetos los actos otorgados por notario público.

Es necesario tener presente que la formulación de un sistema normativo relativo al instrumento electrónico, si bien debe comprender las variables enunciadas, debe tener un valor intrínseco que se le da por la eficacia de que lo dotará el Derecho; en

cuanto a seguridad y garantía que aporte por la intervención del notario público lo dotará de fe pública y autenticidad.

Es en este sentido que adoptó la intervención del notario en el instrumento público electrónico, al igual que con el instrumento público actual, su existencia e intervención se justificará desde un doble punto de vista: a) desde el Derecho, el notario lo dotará de la fe pública necesaria para la tranquilidad de las relaciones jurídicas contractuales y b) desde la informática, contribuirá con su presencia y en calidad de autoridad certificadora a permitir que técnicamente tenga lugar ante él la fase asimétrica de cifrado y desciframiento, así como la aposición de la firma digital, fases de las cuales deberá dar fe.

Conceptualmente, el documento es analizado desde una óptica estructural y funcional.

Es, por lo dicho, que se acostumbra distinguir entre documento e instrumento; en cuanto el primero, no necesariamente deberá pertenecer a la esfera del Derecho, en tanto que el segundo sí es plenamente jurídico, ya que posee eficacia. De este último, agreguemos finalmente que, además de eficacia, es inviolable no sujeto a dudas en relación con su contenido.

El protocolo electrónico

El protocolo es el conjunto de folios ordenados numérica y cronológicamente, en los que el notario, al observar los requisitos establecidos en la ley, (Ley del Notariado del Estado de Jalisco) asienta las escrituras y actas que se otorguen ante su fe. También forman parte del protocolo los libros de documentos, los índices, las actas de apertura y cierre de cada tomo, así como sus soportes informáticos.

El protocolo electrónico es un registro similar al del papel, en donde el sistema electrónico generaría automáticamente el número del documento, fecha y hora cierta, autenticando las calidades del notario para su ejercicio.

La aplicación informática correspondiente tendría todos los servicios que ellos y el Estado realizan con el protocolo, pudiendo hacerse desde cualquier parte del país o en el exterior, incluso en movimiento por cualquier dispositivo que permita autenticar al notario por medio de una firma electrónica y el certificado digital que la ampare.[3] El Estado tendría acceso en tiempo real a todos los negocios jurídicos notariales, pudiendo ejercer de mejor manera el presupuesto en control y supervisión.

La Ley del Notariado del estado de Jalisco vigente, en su sección segunda, regula el uso del protocolo electrónico. El artículo 76 de dicho ordenamiento define a esta figura como "el conjunto de documentos, implementos y archivos electrónicos en que

[3] Derivado de los lineamientos publicados en los "Medios y mecanismos" aprobados por la Comisión de Firma Electrónica, en cumplimiento con la ITFEA.

constan los hechos y actos autorizados por el notario por ese medio, los libros que se formen con la impresión de ellos, sus índices y actas de apertura y cierre".

Resulta evidente que el notario público debe estar preparado técnicamente para ofrecer los mismos servicios profesionales actuales, a través de los medios electrónicos, pues aunque hagan muchas o pocas escrituras, nada cambiará el hecho de que cada día más la gente vinculada a los negocios utiliza los modernos medios de comunicación. Esto supone también un trabajo de actualización tecnológica por parte del profesional y de su personal.

En el estado de Jalisco, los instrumentos públicos redactados o impresos en soporte electrónico conservan ese carácter, siempre que contengan la firma electrónica certificada necesariamente integrada con impresión digital del notario y, en su caso, de los otorgantes, obtenidas éstas de conformidad con la normatividad aplicable al uso de firma electrónica. La Secretaría General de Gobierno, la dependencia competente, a través de la cual se dispondrá la impresión de un registro simplificado de instrumentos públicos asentados en soporte electrónico en el que los notarios públicos deberán hacer constar los actos que autorizan en orden progresivo, de conformidad con su numeración, que contienen además el día y hora de la autorización del acto, nombre de las personas cuyas firmas electrónicas se contienen en el documento e impresión del documento electrónico que servirá para formar el ejemplar que debe ser conservado por la autoridad competente antes mencionada. Además, se implementa el libro general de documentos, que deberá ser rubricado, firmado y sellado por el notario público.

Cada tomo del protocolo informático contendrá 800 registros, los notarios forman el libro general de documentos conforme a las mismas reglas del correspondiente al protocolo. Para la entrega del registro simplificado del protocolo electrónico, se observarán las formalidades que para los tomos de protocolo instaura la Ley del Notariado, así como en su reglamento, donde se establecen los requisitos indispensables para la autorización y conservación del instrumento público electrónico.

La intervención del notario en el documento público autorizado en soporte electrónico está sujeta a los requisitos de todo documento público notarial autorizado en el protocolo, y goza de fe pública cuando se haya realizado; en el caso de que las copias sean trasladadas a papel por notario deberá adherir en cada hoja un holograma.

Ahora bien, hablando del consentimiento de las partes para la celebración de actos jurídicos mediante instrumentos públicos, podrá otorgarse a través de medios electrónicos, ópticos o de cualquier otra tecnología siempre y cuando se observen las disposiciones de la Ley de Firma Electrónica Certificada del estado de Jalisco y sus Municipios.

Un punto importante en este tema, y que resulta idóneo señalar a manera de comparativa en su posible aplicación en el Estado, resultan los "Mecanismos y me-

dios de comunicación" aprobados por la Comisión de Firma Electrónica sobre procedimientos y requisitos que deben de cumplir las entidades certificadoras**.**

Las autoridades certificadoras deben de contar con infraestructura propia para emitir certificados digitales. Sin embargo, se requiere de medios y mecanismos de comunicación que permitan consultar el estado que guardan dichos certificados a efecto de lograr su reconocimiento.

La consulta del estado del certificado digital se llevará a cabo directamente en el RCD de cada autoridad certificadora a través de un servicio para verificar el estado de un certificado digital en línea, basado en el protocolo de comunicación "Online Certificate Status Protocol" (OCSP), el cual permitirá a los usuarios consultar el estado que guarda un certificado digital vía internet emitido por una autoridad certificadora que forma parte de la ITFEA.[4]

La importancia del notario en la función notarial

El notario constituye un protector y garante de la seguridad jurídica, cumple un rol estratégico en la sociedad, dotando de certeza las relaciones entre los particulares al brindarles asesoría técnico-legal y ajustar su voluntad a lo establecido en las leyes, bajo la investidura estatal de la fe pública.[5]

Esta función medular de la actividad notarial, ante el auge del comercio electrónico, ha de replantearse muchos de los principios e instituciones que le rigen para seguir siendo útil, tributando como herramienta eficaz en el complejo engranaje que implica la contratación electrónica y la utilización de documentos electrónicos en aras de garantizar la confidencialidad de las comunicaciones, la identidad y capacidad de las partes contratantes, la integridad y autenticidad de los mensajes en todo el proceso de intercambio electrónico de información en actos y negocios jurídicos de naturaleza civil o mercantil.

A partir del decreto del 29 de mayo del 2000, se dieron reformas en materia de Comercio Electrónico al *Código Civil Federal*, al *Código Federal de Procedimientos Civiles*, al *Código de Comercio* y a la Ley Federal de Protección al Consumidor (Leal, 2001), no sólo se discute doctrinalmente el papel del fedatario público en los actos y negocios jurídicos por medios electrónicos, sino que ya se están instrumentando jurídicamente disposiciones que atañen a instituciones tan importantes como el Protocolo Notarial.

---

[4] Esta posibilidad de consulta se puede equiparar al Registro Publico de la Propiedad y Comercio, donde se pueden consultar los antecedentes de las escrituras publicas de inmuebles, testimonios de actos testamentarios y de constituciones de asociaciones y sociedades.

[5] www.ciberhabitad.gob.mx/gobierno/textos/texto_notaria.htm, La TIC en el quehacer notarial, Ciber Hábitad Ciudad de la Informática, febrero 2003.

Otro ejemplo al respecto, y que atañe igualmente a los instrumentos públicos, lo constituye la Ley Modelo sobre Garantías Mobiliarias adoptada en el mes de febrero del 2002, en el marco de la Sexta Conferencia Especializada Interamericana sobre Derecho Internacional Privado, celebrada en Washington bajo los auspicios de la Organización de Estados Americanos. Dicha normativa de suma importancia para la actividad notarial en su artículo 7 enumera los requisitos mínimos que deberá tener la escritura pública de constitución de la garantía mobiliaria y, a tal efecto dispone: (Di Martino, 2002).

> La escritura podrá hacerse a través de cualquier medio fehaciente que deje constancia del consentimiento de las partes en la constitución de la garantía, incluyendo el télex, telefax, intercambio electrónico de datos, correo electrónico y medios ópticos o similares, de conformidad con las normas aplicables en esta materia.

El cibernotario, cuyo rol será combinar experiencia legal y técnica en una sola especialización, constituye una figura que promete dar respuesta a los retos que la tecnología, como medio de exteriorización de la voluntad en las relaciones interpersonales, impone al Derecho y que supone la celebración de contratos entre ausentes perfeccionados por medio de un sistema telemático.

En tal sentido, constituyen funciones del notario electrónico desde el punto de vista jurídico y técnico; un alto grado de especialización en seguridad dentro de las tecnologías de la información como la legalización electrónica de firmas digitales, autenticaciones o verificaciones acerca de los términos y ejecución del documento, como depositario de los actos jurídicos en formato electrónico, entre otras.

Cumplirá de esta manera con todos aquellos requisitos que, como autoridad certificadora, le es exigible desde el punto de vista de las diferentes legislaciones estatales, encontrándonos ante la presencia de una nueva institución, la fe pública informática (Ochoa), cuyo depositario cumple el rol de tercero certificador neutral, como dador de una nueva clase de fe pública, que a diferencia de la fe pública tradicional no se otorga sobre la base de la autentificación de la capacidad de personas, del cumplimiento de formalidades en los instrumentos notariales o a los certificados de hechos, sino que se aplica a la certificación de procesos tecnológicos de resultados digitales, códigos y signaturas electrónicas.

Sucede que el notario público cuando certifica procesos tecnológicos, resultados digitales, códigos y signaturas electrónicas, está autenticando, confiriendo veracidad y certeza a hechos, circunstancias o actos que tienen trascendencia jurídica; es evidente que las mayores inquietudes giran en torno, no a la naturaleza de la fe pública, sino más bien a los principios que fundamentan el Derecho notarial como la inmediatez, permanencia, matricida o protocolo, representación instrumental, o

el de unidad del acto, por citar algunos que de cierta forma se ven amenazados por el ejercicio de una práctica notarial electrónica, con su consecuente repercusión en la legislación sustantiva.

Se impone reflexionar sobre estas ideas que prometen amplio debate y discusión como única vía para la adopción de soluciones técnico-jurídicas adecuadas a los imperativos propios de las nuevas relaciones que surgen en el campo de la Informática y el Derecho.

Sistema de Información para la Gestión Registral (SIGER)

El objetivo del Sistema de Información para la Gestión Registral (SIGER) es automatizar el proceso registral en las oficinas del Registro Público de la Propiedad y de Comercio.

El SIGER debe controlar y dar seguimiento a las actividades y funciones relacionadas con la gestión registral, que se desarrollan dentro del Registro Público de la Propiedad, asistiendo el flujo de trabajo de principio a fin en forma rápida y confiable, logrando así concluir rápida y satisfactoriamente el trámite solicitado.

Los principales beneficios del SIGER están enfocados a la mejora en tiempos de respuesta de las solicitudes de trámite hechas por los contribuyentes en las oficinas del Registro Público de la Propiedad y de Comercio.

El SIGER contempla un sistema de folio electrónico y una asignación objetiva de solicitudes a celdas de trabajo multihabilidades, con la finalidad de evitar rezago de inscripciones y optimizar el desempeño del personal. El sistema de archivo se basará en un número de folio electrónico que actúa como índice: esto permite contar con un riguroso control del archivo para asegurar su organización en todo momento.

El SIGER comprende las funciones de control, administración y seguimiento de los trámites de los actos jurídicos que son llevados a cabo en el Registro Público. Tiene la capacidad de llevar un registro de todos y cada uno de los movimientos que se realizan durante el proceso registral, desde la fase de recepción de documentos hasta la entrega del documento que avala la terminación del trámite.

El proceso inicia cuando el usuario solicita un trámite al Registro Público de la Propiedad y de Comercio y efectúa el pago de Derechos correspondiente. Es en este momento cuando el sistema le asigna un número de prelación para darle seguimiento.

El flujo de trabajo inicia en recepción de documentos donde se recibe la documentación del trámite, se capturan los datos y se informa al solicitante el monto de los derechos que el sistema calculó como importe de acuerdo a su solicitud. Una vez pagados los derechos, el subsistema de Registro manda el trámite al módulo de análisis, donde se ingresa la información dentro de la forma precodificada existente en el sistema, la cual corresponde al trámite que se está realizando. Posteriormente,

el sistema manda el trámite al módulo de calificación, en donde el registrador firma el trámite electrónicamente, con lo cual queda registrado y tiene validez jurídica. Al firmarse la precodificada, por un lado se imprime una copia de ella y, por el otro, el sistema la manda electrónicamente al módulo de archivo, en donde la persona encargada rectificará que el trámite esté firmado, conservará la copia impresa de la forma precodificada para guardarla en el archivo y mandará el trámite al módulo de entrega –último paso del proceso–, donde la persona que solicitó el trámite recogerá sus documentos y el sistema registrará el trámite como terminado.

De acuerdo a este flujo de trabajo, y a las distintas funciones contempladas dentro del sistema, los componentes del SIGER son:

- *Subsistema de registro:* abarca desde el momento en que el usuario solicita al registro un trámite hasta la fase de análisis, calificación, archivo y entrega de documentos.
- *Subsistema de certificaciones:* es similar al subsistema de Registro. La diferencia estriba en que el producto no es un cambio en la situación jurídica de una entidad sino la emisión de un documento que indique dicha situación.
- *Subsistema de consultas:* se divide en dos partes: consultas locales por usuarios y personal del registro, y consultas remotas por otras personas o instituciones. Las consultas externas son similares a las internas, con la diferencia que en aquéllas los usuarios acceden al acervo del registro a través de internet, habiendo pagado primero sus derechos correspondientes y habiendo recibido una clave de usuario válida en el sistema.
- *Subsistema de control de gestión:* es el encargado de administrar adecuadamente la operación del sistema. Este subsistema genera estadísticas de volumen de operación, de desempeño de celdas y del comportamiento de movimientos.
- *Subsistema de seguridad:* este subsistema se vale de dígitos verificadores que tienen la función de una firma electrónica, la cual evita que usuarios no autorizados entren al sistema y modifiquen directamente la base de datos. En resumen, este subsistema es el responsable de asegurar la integridad del sistema.

La "Autoridad de certificación notarial" en España

La Agencia Notarial de Certificación (ANCERT) es una entidad constituida por el Consejo General del Notariado (CGN) de España, inicialmente como INTI (Instituto Notarial de Tecnologías de Información), dedicada a la provisión de servicios a los más de tres mil notarios españoles y a la prestación de servicios de certificación necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en las relaciones que se produzcan entre personas físicas y jurídicas.

La primera institución especializada en certificación y firma electrónica en la que participaron los notarios y corredores de comercio (fedatarios públicos cuya profesión se integró en la de los notarios, en España, en el año 2000) fue la Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE).

La Agencia Notarial de Certificación (ANCERT), antes el Instituto Notarial para las Tecnologías de la Información (INTI), fue constituida en España en julio de 2002 por el Consejo General del Notariado (CGN) de España con el objetivo de poner en práctica el ambicioso plan de modernización tecnológica del notariado español. Es titularidad al cien por ciento del Consejo General del Notariado.

Desde el día 20 de marzo de 2004, ANCERT emite certificados electrónicos reconocidos ante notario a personas físicas, personas jurídicas, corporaciones privadas y corporaciones de Derecho público y cumple con todos los requisitos impuestos por la Ley 59/2003 de 19 de diciembre de firma electrónica.

Las actividades de ANCERT se integran en la estrategia del Consejo General del Notariado y se orientan a la creación de nuevos servicios, la gestión de la plataforma PKI (Infraestructura de Clave Pública) para la firma electrónica reconocida notarial y a la innovación tecnológica de carácter estratégico o inexistente en el mercado. Sus resultados se dirigen a proporcionar un mejor servicio a las notarías y, por extensión, a la sociedad en su conjunto.

Esta propuesta está basada en la Ley 59/2003 de Firma Electrónica: en el régimen de los Prestadores de Servicios de Certificación. Y la eficacia jurídica de la Firma Electrónica; y la Ley 24/2001 de Medidas Fiscales, Administrativas y del Orden Social, y se encuentra encaminada principalmente a:

En relación a los prestadores de servicio:

I. Utilizar sistemas fiables de firma y demostrar que son fiables (PIN de acceso y PUK de desbloqueo).
II. Conservar la documentación durante 15 años.
III. Constitución de una garantía de 3,000 000.
IV. Disponer de una declaración de prácticas de certificación.
V. Mantener un directorio de certificados emitidos y revocados.
VI. Respetar las normas de protección de datos.
VII. Informar al firmante de sus obligaciones.
VIII. Comprobar la identidad del firmante.

En relación a los certificados reconocidos:

I. Código identificador único del certificado.
II. Código identificador del prestador.
III. Datos de identificación del firmante.

IV. Comienzo y fin del periodo de validez.
V. Límites de uso, o de las cuantías.
VI. Si contienen representación, datos de los que derive.

Estas políticas de implementación han permitido, en España, a 3 mil notarios el manejo de hasta tres certificados simultáneamente, imposibilidad de exportación de certificados, proceso de firma dentro de la tarjeta (tarjeta electrónica que se asigna al notario), no caducidad de la tarjeta, PIN (personalizable) y clave de desbloqueo. Así como del registro de mas de 500 mil firmas electrónicas en un mes.

Por los que ve a los Servicios corporativos:

I. Remisión de índices únicos informatizados.
II. Inscripción telemática de documentos en registros mercantiles y de la propiedad.
III. Gestión expedientes para órgano centralizado de prevención del blanqueo de capitales (OCP).
IV. Base de datos jurídica.
V. Archivo de poderes revocados.
VI. Bases de concurso (ABACO).
VII. Partes testamentarios y actas de declaración de herederos previos, entre otros.

Como agencia dedicada a la emisión de certificados, ANCERT ofrece diversos productos y servicios relacionados con PKI (Infraestructura de clave pública) y la firma electrónica reconocida:

- Emisión de certificados notariales: se emiten conforme a los requerimientos de la Ley 59/2003 del 19 de diciembre de firma electrónica. Se trata de certificados electrónicos reconocidos emitidos ante notario, tanto a personas físicas como jurídicas, en nombre propio o representación.
- Servicio de sellado de tiempo: el sellado de tiempo proporciona a una empresa los mecanismos necesarios para garantizar la existencia de cualquier archivo electrónico, transacción o comunicación antes de una fecha, y garantiza la integridad de los datos a partir de ese instante.
- Servicio de Hosting: permite a cualquier empresa privada, pública, o colegio profesional crear su propia autoridad de certificación o disponer de una autoridad de registro para la gestión de sus certificados electrónicos.

Capítulo VI

Contexto global: La firma electrónica en el contexto internacional y como medio de identificación electrónica global

Durante la última década hemos vivido un intenso y creciente proceso de modernización en la vida social general, y en particular como especial expresión en los que se refiere a los medios de comunicación. La llegada de la televisión por cable y su creciente masificación, la digitalización de las líneas telefónicas, la difusión de la telefonía celular, el uso del correo electrónico en las empresas, escuelas, hogares y oficinas de gobierno, la proliferación de computadoras personales, el uso del fax, la instalación de una gran red de banda ancha (ATM), que conecta a universidades e instituciones para la transferencia masiva de información. Sin embargo, de todas ellas, el uso de internet es, sin duda, abrumador.

Todos estos avances nos dejan a la vanguardia en el área de las telecomunicaciones, tanto en el ámbito nacional y continental como global; no obstante, a pesar de que estas herramientas han demostrado sus capacidades, no son usadas por toda la población. Estas tecnologías de la comunicación han comenzado a formar parte de nuestra vida diaria y han modificado nuestras actividades, rutinas y la manera de ver al mundo que nos rodea. La velocidad de comunicación afecta nuestros sentidos del tiempo y el espacio, y hacen parecer que formamos parte de todo, sin fronteras ni limitaciones.

La fuerza de los hechos demuestra que la globalización de la economía digital tendrá una incidencia fundamental en la economía de los países. De hecho, hoy prevalece el uso de internet en la transmisión de información entre empresas y organismos gubernamentales, entre esos usos destaca el correo electrónico, que ha probado ser un excelente mecanismo de comunicación intra, inter y extra empresa. A fin de garantizar que la transmisión de correo electrónico se realice de una forma segura, se puede hacer uso de la firma electrónica, pues permite comprobar la procedencia de los mensajes intercambiados y su integridad, así como evitar el repudio de dicha comunicación por el remitente.

Gracias a la firma electrónica, los ciudadanos pueden realizar transacciones de comercio electrónico seguras y trámites con la Administración Pública con el

mayor respaldo legal. Para un adecuado uso de la firma electrónica, los usuarios deben ser informados en cuanto a las políticas de seguridad para firmar y cifrar un correo electrónico. Ese efecto de acortar distancias y desdibujar fronteras gracias al internet, donde las relaciones, transacciones e intercambios de información se dan en tiempo real al margen de las distancias, son parte indudable del fenómeno mundial de la globalización.

Para teorizar el concepto de globalización, debemos comprender el concepto de acción social, también llamada comunitaria (Pizzolo, 2002: 29). Max Weber dice: "Por acción debe entenderse una conducta humana (consista en hacer externo o interno, omitir o permitir) siempre que el sujeto de la acción enlace a ella un sentido subjetivo. La acción social, por tanto, es una acción donde el sentido mentado por su sujeto está referido a la conducta de otros orientándose por ésta su desarrollo" (2005: 5). Entonces, la acción social es la conducta humana orientada por las acciones de otros sujetos, la globalización es un hecho social que surge de una acción que hemos creado, que ha proporcionado una serie de ventajas, así como desventajas a la comunidad en general. En ese sentido, la internet constituye una convergencia entre sociedad y comercio.

Un factor determinante de una cultura globalizada son los avances tecnológicos que cada día inciden más en el campo del Derecho, de tal manera que nos enfrentamos a nuevos retos donde se tienen que cambiar los conceptos tradicionales y adecuar el desarrollo tecnológico a las necesidades jurídicas de la sociedad.

En el Plan Nacional de Desarrollo 2001-2006 y actualmente el 2006-2012**,** así como en la Agenda de Buen Gobierno, se consideró la necesidad de incorporar de manera competitiva a nuestro país en la economía digital, para lo cual se encargó a la Secretaría de la Función Pública la responsabilidad de promover las estrategias y acciones que permitieran transformar la gestión pública al hacer llegar los beneficios de las nuevas tecnologías a toda la ciudadanía, con el objetivo de mejorar el acceso y la calidad de los servicios públicos.

En esos términos, el artículo 28, fracción V, de la Ley Orgánica de la Administración Pública Federal y 34 fracción IV del Reglamento interior de la Secretaría de Relaciones Exteriores en vigor, corresponde a esta dependencia, a través de la Dirección General de Asuntos Jurídicos, otorgar los permisos para la constitución de sociedades mexicanas civiles o mercantiles, y para el cambio de denominación o razón social, así como recibir y registrar los avisos a que se refiere el Reglamento de la Ley de Inversión Extranjera y del Registro Nacional de Inversiones Extranjeras.

Por su parte, el artículo 35, fracción II de la Ley Federal de Procedimiento Administrativo, prevé la posibilidad de que las resoluciones administrativas definitivas puedan realizarse a través de medios de comunicación electrónica o cualquier otro medio, cuando así lo haya solicitado por escrito el interesado. En ese mismo

contexto, con fecha 9 de diciembre de 2005, se publicó en el *Diario Oficial de la Federación* el "acuerdo por el que se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico", con el objeto de promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones entre las dependencias y entidades de la Administración Pública Federal; dicho acuerdo estableció la creación de la Subcomisión de Firma Electrónica Avanzada, con carácter permanente, integrada por los representantes de las Secretarías de Economía, de la Función Pública y del Servicio de Administración Tributaria. El propósito es homologar los procedimientos y la tecnología de la firma electrónica avanzada, y establecer las condiciones técnicas que permitan el reconocimiento de certificados digitales correspondientes.

La publicación en el *Diario Oficial de la Federación* del acuerdo interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal ha contribuido en gran medida, no obstante que su aplicación es de índole federal únicamente. Realmente resulta interesante plantearse la posibilidad de que su aplicación se extendiera a todas las entidades federativas. Otro punto importante es la figura del cibernotario, cuyo reto real en el Derecho notarial sería más que propia la utilización y adaptación a las nuevas tecnologías, el constituir a una figura como es el notario público en una persona con fe pública para en un ámbito internacional de competencia.

Las modificaciones hechas en las reglas 2.25 y 2.26 de la Resolución Mis-celánea Fiscal de 2004 publicada en el Diario Oficial de la Federación el 19 de noviembre del mismo año, prevén el pago de Derechos, productos y aprovechamientos (DPA'S) correspondientes a los servicios que presta la Secretaría de Relaciones Exteriores, vía Internet y por ventanilla bancaria, así como del recibo bancario del pago de DPA'S, mediante transferencia electrónica de fondos vía Internet con el sello digital de las instituciones de crédito autorizadas por el Servicio de Administración Tributaria.

La Administración General de Asistencia al Contribuyente del Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito público, mediante oficio 339-SAT-124 de fecha 9 de noviembre de 2006, manifestó que no encuentra inconveniente en que la Secretaría de Relaciones Exteriores establezca los procedimientos internos necesarios para la recepción de los comprobantes de pago que los fedatarios públicos realicen a través de las Instituciones de crédito autorizadas, para el pago de derechos vía Internet y aunado a ello para el permiso de constitución de sociedades o para la modificación de una denominación o razón social, consistente en una reso-lución que recae a una solicitud, con el propósito de permitir que los fedata-rios públicos que cuenten con un certificado de firma electrónica avanzada emitido por el Servicio de Administración Tributaria, puedan utilizarlo en los trámites que realizan ante la Dirección de Permisos, artículo

27 constitucional de la Dirección General de Asuntos Jurídicos de la Secretaría de Relaciones Exteriores.

Se emitió también un acuerdo por medio del cual se establece el me-canismo bajo el cual los fedatarios públicos que cuenten con un Certificado Digital de Firma Electrónica Avanzada emitido por el Servicio de Administra-ción Tributaria (SAT) puedan utilizarlo para realizar los trámites SRE-02-001 "Permiso para la constitución de sociedades", SRE-02-002-A "Modificación de estatutos" y SRE-02-008-A "Aviso del uso de los permisos para la consti-tución de sociedades o cambio de denominación o razón social y de la liqui-dación, fusión o escisión de sociedades. Modalidad: A-Aviso de Uso de Permiso para Constituir Sociedades", ante la Dirección de Permisos Artículo 27 Constitucional de la Dirección General de Asuntos Jurídicos de la Secre-taría de Relaciones Exteriores, pudiéndose llevar a cabo únicamente por conducto de los Fedatarios públicos, que serían los Notarios públicos y Co-rredores públicos de la República mexicana.

Pese a las acciones del Gobierno Federal en materia de política tecnológica e informática, se han orientado básicamente a impulsar la difusión y aplicación de las innovaciones tecnológicas y a alentar y facilitar la capacidad de aprendizaje de las empresas y de las organizaciones, contribuyendo a superar las deficiencias que impiden el flujo adecuado de los conocimientos, información y recursos en los mercados del saber tecnológico y apoyar los proyectos innovadores que aumenten la competitividad de la economía. Sin embargo, no se han logrado los avances que han pretendido muchos de nuestros municipios, y aunque los resultados pueden ilustrar condiciones particulares en cuanto a los fenómenos de gestión en nuestro país, no se puede generalizar.

Beneficios del uso e implementación de la firma electrónica a escala nacional como Mundial. Sin duda, son múltiples los beneficios que se generan con la implementación de la firma electrónica, no sólo para la población en general sino incluso en su implementación en el sector público, ya que el uso de los documentos digitales y la firma electrónica implica un ahorro considerable en el uso de papelería y del gasto que implican los traslados traducidos en distancia y tiempo, que se transforma en gasto de recursos públicos, aunado al beneficio ecológico que implica. Entre estos beneficios, destacan:

1. Elaborar declaraciones de impuestos por medios electrónicos de una forma más sencilla y segura.
2. Los documentos firmados electrónicamente tendrán las mismas funcionalidades y garantías de un documento físico.
3. Reducir el uso de papel en los sectores público y privado.
4. Servirá para expedir facturas electrónicas.

5. Gracias a sus características de no repudio y de autenticidad, se brindará mayor certeza jurídica a los contribuyentes en sus transacciones.
6. Mayor seguridad en las transacciones de comercio electrónico (*e-Commerce*).
7. La firma electrónica avanzada, gracias a sus características intrínsecas de integridad, confidencialidad, autenticidad y no repudio, agregará un valor legal importante a muchos servicios.
8. Incremento en productividad.
9. Reducción de tiempos en procesos administrativos.
10. Rapidez y seguridad en el intercambio de información.
11. Agilidad en la recepción de mercancía.
12. Mejor servicio al cliente.
13. Ahorro en costos administrativos y de oficina.
14. Reducción en volumen de papeleo, correo, fax y otros gastos fijos.
15. Mejor utilización de espacios físicos.
16. Evita captura reiterativa de la información.
17. Reducción de tiempos de edición y remisión.
18. Menor cantidad de disputas por facturación.
19. Reducción en tiempos operativos.
20. Ciclo de resurtido y facturación.
21. Generación de facturas.
22. Hacer más eficiente la operación y el gasto de las dependencias y entidades federales.
23. Profesionalizar el servicio público para mejorar el rendimiento de las estructuras orgánicas de la Administración Pública Federal.
24. Adoptar un modelo de diseño del presupuesto basado en resultados que facilite la rendición de cuentas y genere los incentivos para que la Administración Pública Federal cumpla las metas planteadas.
25. Evaluar el desempeño de los programas de gobierno y su impacto en la población y su amplia difusión en la red.

El gobierno electrónico ha sido fundamental en la construcción de un gobierno competitivo y eficiente, pero sobre todo capaz de generar a costos cada vez menores una respuesta satisfactoria a las expectativas y demandas de la ciudadanía.

En lo que va de esta administración, los logros y avances de las dependencias y entidades de la APF en materia de tecnología de información y comunicaciones han situado al gobierno digital de México en una mejor posición en el contexto internacional.

Capítulo VII

Problemas ante el uso y certificación de la firma electrónica para los usuarios de ésta y la función notarial

Existen diversos problemas que, aun con acuerdos de colaboración entre dependencias o incluso naciones, no han logrado resolverse y que ponen al descubierto la verdadera dificultad en la adopción efectiva de la firma electrónica. A continuación, una breve reseña de los principales obstáculos.

La falta de mecanismos de fomento al desarrollo y uso de la informática

Los más recientes desarrollos en la tecnología que afectan a la comunidad internacional de los negocios, ha provocado un creciente interés de parte de los administradores, públicos y privados, del valor de las computadoras y de los sistemas de información.

Para seguir siendo competitivos en el mundo actual de los negocios y de las actividades productivas, los administradores deben contar con estos nuevos elementos de manejo de información como parte integral de sus operaciones y estrategias. Sin embargo, la política informática en nuestro país no siempre le da la importancia que merece, el fomentar la intervención de todos los organismos y empresas competentes diseñada con una amplia participación de la comunidad informática nacional a través de cuerpos colegiados formalmente establecidos y representativos de la comunidad; que tengan continuidad, ajustándose y corrigiéndose periódicamente, en la búsqueda del aprovechamiento de las tecnologías de la información como una herramienta básica para producir mejores niveles de bienestar de la población y aumentar la competitividad del país.

Es en este entorno de alta dependencia en personas, equipos, programas, medios, instalaciones, estándares y procedimientos que la relación con proveedores de bienes y servicios toma un papel crítico en la marcha y continuidad de las organizaciones.

Acceso a bases de datos

Toda red bien diseñada lleva consigo una categorización de la información, una definición de usuarios y una asignación de permisos de acceso. Se deben definir las categorías de la red y dentro de la misma establecer quién puede qué.

En una red existe una pirámide en cuya cumbre se halla el administrador del sistema, quien a su vez establece los grupos de usuarios y permisos concedidos a cada uno de ellos. La entrada ilegal consiste en violar los permisos de acceso, utilizando permisos que no le han sido adjudicados a una persona. Sin embargo, cuando hablamos de un ordenador conectado a una red, nos hallamos con un problema, definir qué es dentro y qué es fuera de un ordenador; nos encontramos con dos escenarios, uno en el que se nos solicita contraseña para obtener un servicio y otro en el que no se nos solicita la misma. Con respecto a la primera, los límites entre dentro y fuera del ordenador están claros. No corresponden a un espacio físico sino a un uso indebido de las claves. Previamente a la emisión de una clave de entrada, se definen, por parte de los responsables del servidor, los servicios que dicha clave permite obtener. Nos remitimos a nuestro ejemplo con respecto al correo electrónico, donde se accede a los mensajes asociados a esa clave y usuario, o en transacciones mercantiles y bancarias.

La intimidad en la transferencia electrónica de datos

La intimidad es un derecho constitucional del individuo, que con los medios de comunicación tradicionales, como el correo postal, correo certificado, los apartados de correo, están más que garantizados. En cambio, con el uso generalizado de los sistemas de comunicación electrónicos, la intimidad y el anonimato de las personas resultan crecientemente amenazados, de hecho no se ha garantizado la seguridad en algunos casos para preservar esta intimidad de agentes externos. Cada vez que alguien utiliza el correo electrónico, navega por la web, o ingresa a redes internas en las organizaciones, interviene en foros de conversación, participa en los grupos de noticias, o hace uso de un servidor de FTP, realiza compraventas o accede a servicios públicos, lo que revelan son datos sensibles acerca de su personalidad, economía, gustos, hábitos sociales, residencia, que pueden ser maliciosamente recolectados y utilizados por terceros, en perjuicio del usuario inocente.

La mayoría de los usuarios no es consciente de la cantidad de información privada que, de forma inadvertida e involuntaria, está revelando a terceros al hacer uso de internet. Quizás lo que los usuarios toman más en cuenta son los ataques a la confidencialidad, autenticidad e integridad del correo electrónico. Hoy resulta sencillo enfrentar estos ataques mediante los protocolos de comunicaciones basados en procedimientos criptográficos, como los que dan su base y confianza a la firma electrónica.

El delito electrónico o informático en la legislación nacional vigente

En torno a los delitos en internet, se ha dicho y escrito una cantidad impresionante de versiones e historias; en la legislación mexicana empiezan a tipificarse los delitos electrónicos, pero el problema real va más allá y descansa en la nula aplicación de justicia y la impunidad existente.

La posibilidad del delito electrónico en un país sin reglamentación específica, y que puede viajar de una jurisdicción y pasa por ellas con distinto carácter, es la misma razón por la que deberán clasificarse estas diferencias para reclamar obligaciones y responsabilidades. Cada una de estas jurisdicciones fijará distinto grado de responsabilidad legal como la emisión, tránsito, recepción y el almacenamiento de datos.

Cuando no existen estructuras jurídicas para fijar las responsabilidades legales, se provocan conflictos de leyes entre países y además se hace muy difícil una serie de encuadres comerciales en los que todos los países participantes se vean beneficiados por igual, ya que el desequilibrio lo propicia la mayor o menor información, provocando prácticas monopólicas perjudiciales e ilícitas.

Desconocimiento informático por parte de autoridades y notarios

Es precisamente este problema el que se planteaba inicialmente al señalar que las autoridades y los notarios públicos, en su generalidad, no se encuentran preparados tecnológicamente hablando –ni en conocimiento ni en infraestructura– para fungir como certificadores, y es entonces una consecuencia de la falta de los elementos técnicos necesarios para su óptimo desempeño. Es justo comprender que la Secretaría General de Gobierno se limitará a asesorar en la forma y requisitos para obtener el reconocimiento como prestadores del servicio de certificación, aunado al desinterés por cumplir con los requisitos.

Confidencialidad y seguridad notarial

El notario público, como protector y garante de la seguridad jurídica, cumple un rol estratégico en la sociedad, dotando de certeza las relaciones entre los particulares al brindarles asesoría técnico-legal y ajustar su voluntad a lo establecido en las leyes bajo la investidura estatal de la fe pública.

El punto de discusión resulta, en este caso, cuando se cuestiona si el problema será más que contar con los procedimientos técnicos y la creación de infraestructuras que garanticen la seguridad de la información almacenada en las bases de datos que de los protocolos notariales electrónicos. Esto ayudará a que se cree un código de ética efectivo entre los miembros del notariado y su personal, de tal manera que se conserve la integridad, autenticidad y confidencialidad inherente

a los documentos públicos para su permanencia y resguardo a través del tiempo. Esto aunado a que aún existen reservas para quienes tienen en cuenta las desventajas del sistema que puede inhibirse o colapsar con la consecuente pérdida de los datos contenidos, o el hecho de que la tecnología está condenada a rebasarse a sí misma, y con ello a tener vulnerabilidades que luego habrán de ser sobrepasadas de igual forma.

Ahora bien, la unidad del acto es otro de los principios notariales que, junto al de inmediatez, permanencia, matricidad o protocolo, por citar algunos, ha de tenerse en cuenta cuando de actividad notarial electrónica se trate, y es que la unidad del acto supone audiencia notarial plena dada por la presencia en el mismo espacio y tiempo de los sujetos del instrumento notarial en el acto de otorgamiento y autorización del documento público.

Para Alberto Gaete (Gaete, 2001), la contratación electrónica resulta estructuralmente diferente a la clásica. El contrato electrónico al decir del notario chileno, produce importantes cambios debido a la realidad virtual en que se desarrolla, bien sea en torno a las formas documentales como en cuanto a su contenido mismo, y en relación con sus elementos esenciales, naturales o accidentales. Específicamente, en materia de principios notariales, el autor considera que desaparece la unidad del acto entendida como unidad temporal y espacial propia de la expresión del consentimiento contractual, tanto material –que implica simultaneidad en la exteriorización de las voluntades– como formal, o simultaneidad entre las voluntades de las partes y aquella del oficial público o funcionario autorizante, y que es de un doble carácter. En cuanto al acto, debe ser ininterrumpida, y en su dimensión papel, debe estar contenida en un solo instrumento. Esta última, según el autor, constituye verdaderamente unidad de texto y es la que permanece en el documento electrónico.

Comprobación de la hipótesis

Hasta aquí se ha tratado de plantear un panorama más o menos amplio que permita tener una perspectiva más amplia de lo que es la firma electrónica (su funcionamiento, impacto legislativo, su adopción por la sociedad y sobre todo sus implicaciones en el mundo notarial); es decir, se ha partido del conocimiento general como parte del proceso deductivo (Método deductivo), que implica partir del conocimiento general para arribar a uno particular, ello mediante la observación, la investigación bibliográfica y documental, la experimentación y la recolección de datos, que permitan comprobar si la suposición inicial era la correcta.

Para ello, lo primero es recordar la hipótesis planteada inicialmente:

Es el notario la figura idónea para fungir como certificador de conformidad con la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios.

El axioma[1] señalado en la hipótesis permite establecer la primera afirmación:

I. Es el notario público una figura aceptada públicamente por dar seguridad, confianza y garantía a la celebración de los actos jurídicos en México.

El primer ejemplo resulta de lo manifestado por la Presidencia de la República el 31 de julio del 2001:

> Como fedatarios públicos, ustedes le dan transparencia a una gran cantidad de actos legales, en los cuales las personas desean expresar su voluntad de manera inequívoca. Y por ello, ustedes tienen una gran responsabilidad en sus manos. Del absoluto apego a la legalidad y de su vocación de servir lealmente a la sociedad, depende la certidumbre en los tratos y acuerdos y, con ello, la seguridad jurídica de que los documentos pasados por la fe notarial no sólo son auténticos, sino también dignos de absoluta confianza para todos los mexicanos y para quienes en el extranjero necesitan de cualquier documentación.
>
> Qué bueno que contemos con esta noble y prestigiada institución, y más en estos momentos de globalización cuando la velocidad y la integración oportuna de trámites son una condición básica para participar de sus beneficios. Su tarea no sólo es autenticar documentos, ustedes le prestan un apoyo directo a la sociedad y al Estado. Por una parte, ayudan a quienes necesitan de consejo para terminar y tramitar una escritura, un poder, una sucesión, una herencia; pero también por su basta experiencia ayudan de manera muy importante a las pequeñas, medianas y grandes empresas a determinar las mejores condiciones de operación legal.

El segundo ejemplo es cuando el gobernador Ney González, del estado de Nayarit, el 26 de junio del año 2009, manifiesta la importancia que ha tenido la intervención del notariado para la democracia mexicana:

> … por otro lado, el notariado mexicano y el Colegio de Notarios de Nayarit fortalecen las finanzas públicas; además de credibilidad, además de confianza, el

[1] Un axioma, en epistemología, es una "verdad evidente" que no requiere demostración, pues se justifica a sí misma, y sobre la cual se construye el resto de conocimientos por medio de la deducción; aunque no todos los epistemólogos están de acuerdo con esta definición "clásica". El axioma gira siempre sobre sí mismo, mientras los postulados y conclusiones posteriores se deducen de éste. En matemática, un axioma no es necesariamente una verdad evidente, sino una expresión lógica utilizada en una deducción para llegar a una conclusión.

notario, la oficina del notario público le aporta otras fortalezas a los gobiernos; creo que los poderes legislativos local y federal, deben tener esto muy en cuenta cuando en sus debates parlamentarios, cuando en sus conclusiones convertidas en leyes, tejen en torno a la actividad notarial; no basta con que haya, para generalizar, un fedatario público en una de las cámaras para que eso haga expertos a todos, ni siquiera los integrantes de las comisiones en las que participa, pueden aportar muchos elementos, sin duda, pero no necesariamente el interés de uno puede ser el interés de todos.

El tercer ejemplo lo encontramos con la celebración del pasado 28 de abril de 2009 de un Convenio de Colaboración y Apoyo a nivel nacional con el Instituto Federal Electoral (IFE), que firmaron por parte del IFE Leonardo Valdés, el consejero presidente y Edmundo Jacobo Molina, secretario ejecutivo; y por parte del gremio notarial, Heriberto Castillo Villanueva y José Ignacio Sentíes Laborde, presidente de la Asociación Nacional del Notariado Mexicano y presidente del Colegio de Notarios del Distrito Federal, respectivamente, entre otros. Leonardo Valdés, consejero presidente del IFE, señaló:

El 5 de julio podrán ser llamados, por ejemplo, para dar fe de casillas que por alguna razón no se instalen en tiempo y forma por aquellas en las que se detecten procedimientos prohibidos como hacer propaganda el día de la elección, acarreo de votantes, entrega de dinero o regalos a los votantes, etc. También pueden ser requeridos previamente por los partidos, sus candidatos y representantes en los casos en que puedan presentarse violaciones a las leyes electorales, y que se relacionen con fijación o retiro de propaganda, bloqueo o destrucción de la misma, difusión de cierto tipo de mensajes por medios de comunicación masiva, etc.

En ese sentido, el Colegio de Notarios recuerda que los notarios son únicamente testigos calificados que reciben declaraciones o presencian hechos de los cuales dejan constancia en los protocolos, pero no son fiscalizadores del cumplimiento de promesas ni interventores o sancionadores de actos delictivos durante la jornada.

Las denuncias ante notario son gratuitas para funcionarios de casilla y ciudadanos en general (no así para los partidos políticos) y pueden hacerse acudiendo a cualquier notaría con su credencial de elector. No se atenderán llamadas anónimas denunciando irregularidades.

Segunda afirmación:

II. El notario público está plenamente reconocido con anterioridad a la aprobación de la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Muni-

cipios como certificador de documentos digitales, como es el caso del protocolo electrónico, siendo éste la base de su actuar como la persona más idónea en el estado de Jalisco como autoridad certificadora.

En ese sentido, se puede señalar, para obtener dicha comprobación, que mediante dos dispositivos legales estatales se ha dado un giro importante al tema de la firma electrónica y su relación con la función notarial como ya se ha explicado en capítulos anteriores.

Primer caso, la Ley del Notariado para el estado de Jalisco que fue aprobada el 12 de septiembre de 2006, la cual incorporó un capítulo dedicado al protocolo electrónico.

Segundo caso, la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios, aprobada por decreto número 21432/LVII/06, misma que entró en vigor a partir del día 1 de enero del 2007 y su reglamento respectivo, la cual manifiesta en su artículo 21 fracción I (artículo 2 fracción XIV y artículo 7 de su reglamento) que el notario público puede fungir como autoridad certificadora.

Por otra parte, se encuentra el "Convenio de colaboración y coordinación para la realización de los trabajos de modernización del Registro Público de la Propiedad y de Comercio del estado de Jalisco", celebrado desde el año 1998, estando como gobernador Alberto Cárdenas Jiménez. El convenio surge del Plan Nacional de Desarrollo 1995-2000, el cual establecía entre sus objetivos una reforma integral del gobierno federal y de los estados que integran la Federación, entre éstos, Jalisco; y la modernización de la administración pública (Punto 3.9 del Plan Nacional de Desarrollo 1995-2000), y la consolidación de un régimen de seguridad jurídica sobre la propiedad y posesión de los bienes y las transacciones de los particulares (Punto 2.2 del Plan Nacional de Desarrollo 1995-2000), que permitiera contar con una administración pública accesible, eficiente y al servicio de la población, coadyuvando a la seguridad de las relaciones jurídicas entre particulares.

Así como el Programa de Comercio Interior, Abasto y Protección al Consumidor 1995-2000, en concordancia con el Plan Nacional de Desarrollo, prevé que el fortalecimiento de la seguridad jurídica requiere de una modernización integral de los servicios registrales de comercio y de la propiedad, para lo cual se debería de promover, en coordinación con los gobiernos estatales, la modernización de los registros públicos de las entidades federativas, así como diseñar y coordinar acciones de automatización de dichos registros.

Y para septiembre del 2000, el presidente Ernesto Zedillo Ponce de León reafirma dichas políticas lanzando el "Programa para la modernización de los registros públicos de la propiedad de los estados", con la finalidad de realizar las adecuaciones jurídicas y desarrollar la plataforma tecnológica que permitiera transitar a

un registro público de la propiedad estandarizado y homologado a nivel nacional, con el propósito de avanzar hacia una mejor regulación; y estableciendo objetivos básicos de homogenización para todos los registros en el país.

Al impulsar el protocolo electrónico mediante un sistema que generaría automáticamente el número del documento, fecha y hora cierta, autenticando las calidades del notario para su ejercicio, la aplicación informática correspondiente tendría todos los servicios que ellos y el Estado realizan con el protocolo, pudiendo hacerse desde cualquier parte del país o en el exterior, incluso en movimiento por cualquier dispositivo que permita autenticar al notario por medio de una firma electrónica y el certificado digital que la ampare.[2]

El Sistema de Información para la Gestión Registral (SIGER), surgió con el objetivo de automatizar el proceso registral en las oficinas del Registro público de la Propiedad y de Comercio, así como para controlar y dar se-guimiento a las actividades y funciones relacionadas con la gestión registral, los principales beneficios del Sistema de Información para la Gestión Regis-tral (SIGER) estaban enfocados a la mejora en tiempos de respuesta de las solicitudes de trámite hechas por los contribuyentes en las oficinas del Re-gistro público de la Propiedad y de Comercio, donde, obviamente, el notario juega un papel preponderante.

Ahora bien, dando forma al silogismo hipotético que nos ocupa, el cual puede tener términos válidos o no, resulta necesario establecer el siguiente silogismo categórico, para la conclusión y comprobación de la hipótesis en su aspecto positivo:

P → Q.
Q → R.
Entonces (*ergo*), P → R.

P: si el notario público goza de aceptación y credibilidad pública por la sociedad en general, incluidas nuestras autoridades (los tres poderes gubernamentales), por considerar que su actuar brinda seguridad, confianza y legalidad → y Q: si con anterioridad ya se le ha reconocido como una autoridad certificadora en el proceso de la certificación de los protocolos electrónicos, que no dejan de ser certificados digitales → y R: si la propia Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios otorga al notario la posibilidad de actuar como autoridad certificadora.

Entonces: P: el notario público por su fe pública → R: resulta ser la persona idónea para actuar como autoridad certificadora conforme a la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios.

[2] Derivado de los lineamientos publicados en los "Medios y mecanismos" aprobados por la Comisión de Firma Electrónica, en cumplimiento con la ITFEA.

Ahora se procederá a comprobar el aspecto negativo de la hipótesis planteada respecto de las tres causas por las cuales no se le ha dado una aplicación efectiva a la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios:

Primero, el desconocimiento generalizado de la informática:

México ganó seis posiciones en el *ranking* del índice de disponibilidad de la Red del Foro Económico Mundial, al pasar del lugar 55, en 2005, a la posición 49 en un total de 122, en el 2008. De esta manera, pasa a formar parte de los cuatro países latinoamericanos que se encuentran dentro de los 50 primeros del Informe global sobre tecnología de la información 2006-2007.[3] No obstante, más del 60% de las personas usa las tecnologías de la información en foros de chat, para bajar música, imágenes, y archivos no educativos, que los que realmente las explotan al máximo, y sólo 1 de cada 100 ha efectuado alguna transacción comercial en la red.

Segundo, la falta infraestructura adecuada para la prestación del servicio:

El documento denominado "Regulación de firma electrónica certificada" relativo al programa "Fortalecimiento institucional", publicado en la página web[4] oficial de la Secretaría de Planeación del estado de Jalisco, la cual señala que el programa deriva del fortalecimiento institucional, para la calidad de los sistemas de gestión pública, cuyo objetivo es la consolidación de la infraestructura necesaria para dar cumplimiento a los procesos de certificación de los actos jurídicos a través de la firma electrónica; no obstante, se señala en el porcentaje de avance un factor de 0.0, con fecha de inicio del 01 de enero del año 2009 para su implementación, y fijando como meta el 31 de diciembre del mismo año para su consolidación, por conducto de la Dirección de Firma Electrónica de la Secretaría General de Gobierno con un presupuesto anual estatal de $5,540,240.00 y un presupuesto anual estatal ejercido de $454,560.69. Paradójicamente, dicho programa señala en su proyección de la consolidación de la firma electrónica en el estado que para el mes de abril –fecha de expedición– se llevará un porcentaje de aplicación del 54%, es decir, más de la mitad del avance, cuando lo único que se tiene es una ley, un reglamento, una Dirección de Firma Electrónica, y ninguna autoridad certificada para expedir certificaciones de firmas electrónicas; aunado a que la propia Dirección encargada de sentar las bases e implantarlas, reconoce que aún no se cuentan con certificadores al 2 de marzo del año 2009, y por ende, no se tiene la posibilidad de acceder a los servicios previstos por la propia ley a beneficio de la ciudadanía, ya que, como señala dicha Dirección, no está facultado el propio gobierno del estado para "otorgar firmas electrónicas", sólo reconocer prestadores de certificación. En ese tenor, los ciudadanos jaliscienses se encuentran con nula

[3] http://ciberhabitat.com.mx/noticias/marzo07.htm

[4] *seplan.jalisco.gob.mx/table/reporte/ficha_proyecto/14;jsessionid...*

posibilidad de obtener una firma electrónica de conformidad con lo dispuesto por la multicitada ley.

Tercero, la falta de interés por parte del Gobierno estatal de impulsar el uso efectivo del ordenamiento legal mediante el registro de autoridades certificadoras, la homologación técnica de la firma electrónica con las normas federales y la difusión de la misma entre la población.

A la fecha aún no se cuenta en el estado de Jalisco con prestadores de servicios de certificación, y la Dirección de Firma Electrónica se ha limitado a orientar algunos interesados como son los Ayuntamientos de Zapopan, Guadalajara, Tlaquepaque y Tonalá, y a centros universitarios como la Universidad de Guadalajara, la UNIVA, la Universidad Panamericana y la Universidad Autónoma de Guadalajara, así como al Colegio de Notarios, para la obtención de dicho reconocimiento, así como de darles a conocer aspectos técnicos , materiales, económicos y de recursos humanos necesarios para la prestación del servicio. Tal y como consta en el oficio numero DFE/032/2009, emitido por la propia Dirección de Firma Electrónica, en respuesta a la solicitud de acceso a información pública, remitida a esta postulante por la Unidad de Transparencia de la Secretaría General de Gobierno.

Comprobación de la hipótesis en su aspecto negativo:

P → Q.
Q → R.
Entonces (*ergo*), P → R.

P: si existe un alto índice de desconocimiento informático sumado a sí el interés parte de las autoridades por resulta nulo ante la implementación y cumplimiento efectivo de la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios → y Q: si la Secretaría General de Gobierno del estado de Jalisco no cuenta aún con autoridades certificadoras conforme a la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios → y R: si la población del Estado no ha logrado a la fecha contar con una firma electrónica.

Entonces → P: La falta de implantación de la Ley y el interés parte de las autoridades → R: La Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios resulta ser estéril.

Conclusión de la comprobación

Es el notario la figura idónea en el estado para la prestación del servicio de certificador de conformidad con la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios.

Y a la fecha la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios no ha tenido una aplicación real, como consecuencia del desconocimiento generalizado de la informática, la falta de infraestructura adecuada para la prestación del servicio y la falta de interés por parte del Gobierno estatal de impulsar el uso efectivo del ordenamiento legal mediante el registro de autoridades certificadoras, la homologación técnica de la firma electrónica con las normas federales y la difusión de la misma entre la población.

Conclusiones

Conclusiones generales

1. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el manejo adecuado de las tecnologías para aprovechar mejor sus ventajas.
2. El auge de la interconexión entre redes abre nuevos horizontes para la navegación por internet, y con ello surgen nuevas amenazas para los sistemas computarizados, como son la pérdida de confidencialidad y autenticidad de los documentos electrónicos, pero también abre posibilidades para la celebración de transacciones comerciales mediante una identificación con el uso de la firma electrónica sin necesidad de tener que aportar datos personales sensibles.
3. La criptografía es una disciplina/tecnología orientada a la solución de los problemas relacionados con la autenticidad y la confidencialidad que provee las herramientas idóneas para la sustentabilidad de la firma electrónica.
4. Los usuarios son quienes deben elegir la conveniencia de una u otra herramienta para la protección de sus documentos electrónicos.
5. La creación de los fedatarios públicos electrónicos nos llevará a tener mayor seguridad en la autenticación de los documentos que circulen a través de las líneas de comunicación.
6. Una única entidad de certificación de ámbito internacional es inviable, por tanto, deberán existir una o varias redes de autoridades, por ejemplo, nacionales o estatales, pero con la celebración de convenios federales y tratados internacionales.

Conclusiones y propuestas medulares

Primera. El Derecho tiene que seguir innovándose para dar soluciones a los nuevos esquemas cambiantes y no quedarse con las instituciones obsoletas y específicamente la función notarial, la cual se encuentra innovando paulatinamente en el

esquema de sociedad digital para dar paso a una nueva generación de actividades y procesos sistematizados trascendiendo del papel al documento digital.

Propuesta. En ese sentido se debe de instituir al notario público como autoridad certificadora de manera automática, dando un tiempo prorrogable para cumplir con los requisitos de ley y contar con los medios tecnológicos idóneos; lo anterior en virtud de la investidura que éste ostenta como fedatario público de origen.

Que sea creado un Consejo Estatal de Firma Electrónica y Certificación Notarial Electrónica, conformado por un integrante de la Secretaría General de Gobierno, un integrante del Colegio de Notarios, un integrante de la Cámara de Comercio de Guadalajara, un integrante del Congreso del Estado y uno de la Comisión Nacional de Firma Electrónica, quienes puedan certificar a la autoridades, auditarlas y establecer criterios apoyándose en el ITFEA.

Segunda. La firma electrónica nace de manera justificable desde el momento en que los contratos, las transacciones económicas, las compras o en los actos traslativos de dominio, entre otras figuras jurídicas que se realizan *online*, es decir, vía internet, requieren de la manifestación de la voluntad que se ostenta con una firma electrónica en sustitución de la autógrafa, debiendo ambas tener el mismo efecto. Su validez dependerá de la fiabilidad de la firma electrónica o, mejor aún, del método en que ésta se generó, y asegura la imposibilidad de que ocurra una suplantación de personalidad. Entonces, si lo aplicamos al ámbito del Derecho notarial, los actos donde intervenga el notario, de igual forma brindarán la certeza y la seguridad jurídica como si fuera plasmado en papel.

Propuesta. Se modifiquen las leyes aplicables a efecto de que se le reconozca el mismo valor de la firma electrónica o digital, como al de la firma autógrafa, y se establezca además por la ley estatal una *firma electrónica única* para transacciones comerciales en el estado, trámites ante autoridades administrativas y judiciales.

Si bien es cierto que el acuerdo interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal y la aprobación de la Norma Oficial Mexicana NOM-151-SCFI-2002 "Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos", han establecido criterios de homologación y estandarización, sólo tienen aplicación a la Administración Pública Federal, la sugerencia sería entonces que su aplicación sea adoptada por todos los estados que conforman la Federación.

Se sugiere que se modifiquen la legislación vigente en el estado con la finalidad de que se otorgue validez a la firma electrónica en actos de notificación judicial, administrativa y comercial en el estado.

Tercera. Lamentablemente, la *Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios* ha resultado hasta el momento una ley estéril, a pesar de que

constituye un gran avance en la legislación estatal. Sin embargo, no se aplica y aun no se ven materializados sus beneficios ya que la intención del Gobierno estatal inicialmente era la generación de condiciones que permitan y garanticen incorporar, desarrollar y potenciar nuevas tecnologías mediante la creación de un marco jurídico confiable, que permitiera fomentar, promover y difundir el uso de medios electrónicos, como instrumento para optimizar los servicios técnicos, financieros y administrativos en el uso de la firma electrónica certificada y su aplicación en la prestación de servicios de certificación para simplificar, facilitar y agilizar los actos y negocios jurídicos, comunicaciones y procedimientos administrativos, entre las dependencias, entidades y organismos que conforman el sector público, los particulares y las relaciones que mantengan entre sí; constituye una de tantas buenas intenciones de legislación que nos rige y de la propia administración pública, que como tantas políticas públicas se quedan sólo como proyectos sexenales.

Se reanalicen las políticas implementadas para la ejecución de la novísima Ley de Firma Electrónica y el presupuesto público que la respalda. No obstante, a la fecha aún no se tienen suficientes certificadoras reconocidas por la Secretaría General de Gobierno del Estado y, por ende, limitan a los particulares a la obtención de una firma electrónica.

Cuarta. El desconocimiento informático y la falta de infraestructura constituyen el más grande problema para las autoridades y los notarios públicos en su generalidad, ya que no se encuentran preparados tecnológicamente hablando para fungir como certificadores, y es entonces una consecuencia de la falta de los elementos técnicos necesarios para su óptimo desempeño. Es justo comprender que la Secretaría General de Gobierno se limitará a asesorar en la forma y requisitos para obtener el reconocimiento como prestadores del servicio de certificación por el desinterés de cumplir con los requisitos. Por otra parte, las implicaciones tecno-económicas son graves para las organizaciones públicas y privadas que pretenden fungir como certificadoras de conformidad con la *Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios,* porque mientras nuestros principales competidores crean las ventajas competitivas y dinámicas con tecnologías del nuevo siglo, en México el debate "Hacia una infraestructura mexicana de información" con miles de trabajos empieza formalmente, lo que nos deja indefensos y podríamos considerarlo como nulidad de competencia informática y tecnológica.

Quinta. Que como parte de las políticas públicas planteadas en el Plan Nacional de Desarrollo 2006-2012, así como en la Agenda de Buen Gobierno, de incorporar –como meta– de manera competitiva a nuestro país en la economía digital, para lo cual se encargó a la Secretaría de la Función Pública la responsabilidad de promover las estrategias y acciones que permitieran transformar la gestión pública al hacer llegar los beneficios de las nuevas tecnologías a toda la ciudadanía, con el objetivo de mejorar el acceso y la calidad de los servicios públicos.

Propuesta. Se incluya en la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios y su reglamento el equiparar la firma electrónica de conformidad con el "Acuerdo interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal", y se destinen presupuestos especiales a efecto de que las entidades públicas establezcan mecanismos idóneos para el uso e implementación de la firma electrónica por parte de los servidores públicos, y que las certificaciones de los documentos digitales sea una opción viable con la finalidad de eliminar la doble pérdida que implica la reproducción de información publica en papel –físico– y su almacenamiento en cumplimiento con lo dispuesto por la Ley de Transparencia e Información Pública.

GLOSARIO

Alfanumérico: Conjunto de letras, números y otros símbolos, como signos de puntuación o símbolos matemáticos. Hace referencia a los caracteres del teclado y al conjunto de caracteres disponibles para las diferentes operaciones de transferencia de datos del ordenador.

Almacenamiento en disco: Grabación de datos en un disco magnético. Los datos se organizan en pistas concéntricas similares a las de un disco fonográfico.

APANET (Advanced Research Projects Agency Network / Red de la Agencia de Proyectos de Investigación Avanzada): Una de las primeras redes de computadoras interconectadas a través de líneas telefónicas. Este proyecto fue financiado por DARPA y, sin duda, constituye uno de los proyectos piloto que sirvió de base para el desarrollo de internet.

APD (Data Protection Agency / Agencia de Protección de Datos): Fue en 1993 cuando en España se crea con el fin de proteger la intimidad de los usuarios de internet del ataque a su intimidad a través de medios informáticos.

Bit (*bit*, bitio): Se trata de la unidad mínima de información que se maneja en una computadora. Se deriva de la contracción de la expresión *binary digit* (dígito binario).

Browser (navegador, visor, visualizador): La manera como viajamos a través de internet es por medio de un navegador. Se componen de aplicaciones de hipertexto que facilitan la comunicación con los diversos servidores en internet, los más populares son internet Explorer de Microsoft y Netscape de Netscape Communications. Nos permiten el acceso a servidores WWW, FTP, etc.

Byte (*byte*, octeto): Dentro de las unidades de medición de memoria en las computadoras un byte representa la suma de ocho bits los cuales forman un carácter (que puede ser una letra, un número, un signo o un espacio en el texto).

Chat (conversación, *charla,* chateo, platicar): Los tan populares chats en internet representan la comunicación entre dos o más usuarios. Existen diversos programas para el uso del chat que permiten mandar imágenes, transferencia de

audio y video en tiempo real. La adicción a estos sitios implica grandes problemas porque puede convertirse en un vicio, y pueden surgir amenazas a la intimidad, la vida y la seguridad de las personas.

Cipherpunk (*descifrador de claves,* resuelve cifras): Es por lo general un especialista informático de alta capacidad cuya función primordial es romper las claves criptográficas y superar los sistemas de seguridad por sofisticados que sean. Persona especializada en romper claves criptográficas y superar sistemas de seguridad. No debe confundirse con *cyberpunk*.

Click (clic, cliqueó/cliquear, *hacer click*): Sin duda una de las acciones que más realizamos cuando trabajamos en una computadora es el hacer clics con el mouse sobre la pantalla. Lo anterior puede traducirse como el colocar el puntero del mouse sobre un área en específico para realizar determinada tarea en nuestra computadora.

Computer (computadora, máquina, ordenador): Poderosa herramienta de trabajo electrónico capaz de procesar información para cumplir determinada tarea. Anteriormente fueron mecánicas, para posteriormente evolucionar al medio electromecánico.

Cookie (*cuqui,* espía, delator, *fisgón,* galletita, pastelito): Se trata de un conjunto de programas, en ocasiones encriptados en el mismo navegador, que se almacenan en el disco duro de la computadora del usuario cuando éste entra a determinadas páginas en internet. Numerosas protestas se han originado respecto al tema, ya que en muchas ocasiones las compañías utilizan esto para conocer las preferencias de los usuarios, y de esta manera enfilar una campaña publicitaria. Para muchos, el uso de las cookies se considera como la violación a la intimidad de las personas y de las organizaciones.

Copyright (derecho de copia): Los derechos que tiene un autor ya sea de un sistema, programa, *hardware*, etc., sobre todas y cada una de las obras que cree, así mismo establece las condiciones y el uso que se hará con respecto a la utilización y comercialización de las mismas. Este derecho es irrenunciable y las restricciones acerca de su uso quedan estrictamente bajo las condiciones que el autor decida. Para mostrar de manera este derecho se utiliza el símbolo ©.

Cracker (*intruso,* saboteador): Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad, y muchas veces cifran o descifran información para que pueda o no ser vista por otros. Son personas muy capaces que cuentan con una serie de herramientas para lograr su cometido.

Cryptography (Criptografía): Este término se forma del vocablo griego *kruptos*, "oculto", que en otras palabras se traduce como: "Arte de escribir de manera peculiar o de modo esotérico." En computación se refiere a los mensajes que son enviados por un emisor que oculta el contenido del mensaje a manera de

que sólo ciertas personas previamente seleccionadas tendrán acceso a la información por medio de una clave después de haberla descifrado.

Cryptology (Criptología): Rama de la criptografía cuyo objetivo es descifrar los criptogramas cuando no se tiene conocimiento de la clave.

Cyber-(ciber): Se ha popularizado el uso de este término dentro de la cultura de internet para definir conceptos relacionados con la misma, como son: cibernauta, ciberespacio, etc. Su origen viene del vocablo griego "cibernao", que significa "pilotear una nave".

Cybercoffee (cibercafé): Negocio que tiene como principal característica la explotación de la señal de internet, la cual proporcionan al público a un costo por hora utilizada. El primero de estos negocios se remonta a California, Estados Unidos, en 1994, en la actualidad se encuentran en gran auge en México, los cuales no han sido regulados en ningún sentido por la legislación mexicana.

Cyberética: Se define como el conjunto de normas de conducta que generan los usuarios que navegan en la red.

Cybermarketing (Cibemercadotecnia, *Cibermarketing*): Dentro de la comercialización de espacios a través de internet se considera como una campaña de promoción acerca de productos o servicios.

Cybernaut (cibernauta): Usuario que navega por la red.

Cyberspace (Ciberespacio): Se utilizó por vez primera en la novela *Neuromancer* de William Gibson, en donde se aplicaba para describir un universo de computadoras y una civilización creada en torno a estas máquinas.

Cybertrash (ciberbasura): Lamentablemente, no podía faltar en internet la gente que se dedique a subir información peligrosa o no benéfica, no aporta nada y sí llegan a ser peligrosos virus o páginas de pésimos contenidos que pueden poner en peligro la salud mental de los usuarios de la red y la seguridad informática de la red.

Data (datos): Plural de la palabra latina *datum* (dato). Puede caerse en el error al emplearse en inglés y pensar que se refiere a un solo dato.

De-encryption (*descifrado,* desencriptación): Es el proceso mediante el cual se recupera el contenido real de una información cifrada previamente.

Digerati (entendidos): Dentro de la cultura de internet se entiende como aquellas personas que se especializan en temas de la denominada sociedad de la información. Su raíz proviene del término latino *ligerati* (letrados).

Digital signature (firma electrónica o digital): Se trata de un protocolo en internet a través del cual se verifica la autentificación de un usuario y nos confirma que es quien dice ser.

EDI (Intercambio Electrónico de Datos / Electronic Data Interchange): Popular sistema de transferencia de datos a través de la red que se emplea la mayor parte en empresas.

Electronic mail (*correo electrónico*): Sin duda, una de las más populares aplicaciones de internet que ha cambiado la forma de comunicación de miles de personas en todas partes del mundo, de esta manera un usuario puede intercambiar información con otros desde puntos remotos. Se le llama así también a los mensajes que se manda a través de este medio.

Electronic mail address (dirección de correo electrónico): Es el conjunto de letras, números y signos que juntos dan por resultado al dirección de correo electrónico de un usuario. Técnicamente, se compone de tres partes: el nombre del usuario, la arroba y el nombre del servidor, por ejemplo: heidi@podernet.com.mx.

Encryption (*cifrado,* encriptación): Se trata de un mecanismo de seguridad en internet cuya principal función es hacer llegar la información a un determinado usuario sin que nadie más acceda a ella. Existen diversos tipos de cifrados que en cierta manera son la base de la seguridad de la red.

File (archivo, *fichero*): Es la base de la estructura de organización de la información en una computadora, de esta manera se puede manipular por el sistema operativo de la misma. Un archivo se compone de tres partes fundamentales: el nombre del archivo, el punto (.) y la extensión, de esta manera tenemos "ejemplo. html" (en este caso se trata de un archivo HTML cuyo nombre es ejemplo).

File transfer (transferencia de archivos): Es la acción que consiste en sacar una copia de un archivo de una computadora a otra a través de una red.

File Transfer Protocol-FTP (Protocolo de Transferencia de Archivos): Uno de los protocolos más utilizados en internet lo es, sin duda, el FTP, el cual nos permite bajar información de los servidores que se encuentran en internet, para lo cual debemos de teclear un nombre de usuario y una contraseña.

Global Information Infrastructure (GII) (Infraestructura Global de Información): Es un ambicioso proyecto a futuro, en donde se denomina así a la gran autopista de información que cubrirá por completo el planeta.

Globalization (*globalización,* mundialización): Se trata de un fenómeno que ha cobrado mucha fuerza a últimos días, fomentado ampliamente por el efecto internet, en donde se traspasan fronteras y las distancias se acortan entre un país y otro en segundos, se da en todos los ámbitos, tanto social, cultural y económico.

Hacker (pirata): Persona de elevados conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer; este término no debe de llevarse al extremo de alguien malo con fines de destruir sistemas, esto encaja mejor en la definición de *cracker*.

Hardware (fierros, *hardware,* maquinaria): Se trata de todos los componentes físicos de una computadora, entre los cuales se pueden mencionar el disco duro, procesador y monitor que, en conjunto con el *software* (programas), hacen que funcione nuestra máquina.

Hash: Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, resumir o identificar un dato a través de la probabilidad, utilizando una función *hash* o algoritmo *hash*. Un *hash* es el resultado de dicha función o algoritmo.

Host (*sistema anfitrión*, sistema principal / albergar, *hospedar*): Esto es un servidor o computadora muy potente que, por medio de protocolos TCP/IP, permite a los usuarios la comunicación con otros servidores en internet. Los usuarios pueden para ello hacer uso de infinidad de aplicaciones como el correo electrónico, telnet, FTP, etc. La acepción verbal (*to host*) indica el hecho de almacenar cierto tipo de información en un servidor no propio.

http: Ver "HyperText Transmission Protocol".

Informática Se trata de la técnica de procesado automático de datos codificándolo en ordenadores por medio del sistema binario.

Information (información): Se trata de la suma de varios datos que tiene un significado completamente distinto al de cada uno de ellos visto de manera individual. Por ejemplo, j, o, s, u y e son datos, Josué es una información. Es un recurso invaluable dentro del desarrollo y expansión de las tecnologías.

TIC (Tecnologías de la Información y de las Comunicaciones / Information and Communication Technologies): Se refiere al conjunto de herramientas tecnológicas que poseemos para la manipulación de la información en general.

Information Society (Sociedad de la Información): Se denomina así a la sociedad en que el poder de las computadoras y la tecnología en general repercute de manera directa en la mente, sentimientos y sueños del hombre.

Internaut (internauta): Se trata de un usuario que navega por la súper carretera de la información.

Internet: Se denomina así al conjunto de redes interconectadas entre sí que forma la llamada súper carretera de la información.

Internet (*internet*, la Red): Se denomina así a la red de telecomunicaciones que surgió en Estados Unidos en 1969, y que en sus orígenes era de carácter meramente militar, para el día de hoy convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en aspectos sociales, culturales y económicos. Se puede clasificar en tres niveles: el primero lo conforman las redes troncales, el segundo las redes de nivel intermedio y el tercero lo constituyen las redes aisladas. El internet es además una red multiprotocolo capaz de soportar cualquier tecnología.

Proveedor de Servicios internet (Internet Service Provider o ISP): Es una asociación con fines de lucro que, aparte de dar diversos servicios de internet como el acceso, proporciona el hospedaje de páginas, diseño, consultoría, redes e intranets.

Internet Protocol (Protocolo internet): Se trata de una serie de normas que regulan la transferencia de paquetes de información a través de internet.

Intranet (*intranet,* intrarred): Hace referencia a una red propia que ha sido creada para satisfacer las necesidades específicas de una compañía u organización, la cual sigue debidamente los protocolos ya establecidos de internet, muy en específico el TCP/IP. Puede darse el caso de que sea una red aislada, o sea, que no se encuentre en internet.

Key (clave): Se trata de una serie de signos previamente convenidos que sirven como clave o fórmula para transmitir mensaje secretos o privados.

LAN (Red de Área Local / Local Área Network): Con una velocidad aproximada de 100 Mbps (100 megabits por segundo), esta red de datos presta el servicio en un área limitada a pocos kilómetros cuadrados, lo cual implica una optimización en los protocolos de señal de la red.

Mail (correo): Ver: e-mail.

Mouse (mouse, *ratón*): El multiconocido *mouse* o ratón es el dispositivo electrónico que nos permite dar instrucciones a nuestra computadora a través de un cursor que aparece en la pantalla, y haciendo clic para que se lleve a cabo una acción determinada.

On line (en línea, *conectado, on line*): Es el estado en que nuestra computadora se encuentra en línea, o sea, conectada a internet.

Password (*contraseña,* palabra de paso): Conjunto de números, letras y caracteres especiales que dan acceso a un usuario a un determinado recurso del sistema o de internet.

PC (computador personal, computadora personal, *ordenador personal,* Personal Computer): Se trata del avance tecnológico que en los últimos años cambió al mundo. Cada día se revoluciona la tecnología haciéndolas más poderosas y capaces de realizar múltiples tareas.

Privacy (*intimidad,* privacidad): Se refiere al derecho que todo usuario tiene de individualidad.

Secure Electronic Transaction SET (Transacción Electrónica Segura): Es un protocolo de seguridad desarrollado por las empresas MasterCard y Visa, con la finalidad de permitir las transacciones electrónicas a través de internet.

Secure server (servidor seguro): Es un servidor al que, además de los sistemas de seguridad comunes, se le han implementado otros que lo refuerzan contra los ataques en internet. Sobretodo se emplean para las transacciones de comercio electrónico.

Server (servidor): Se le llama así a todo aquel servidor que se encuentra en línea y que proporciona información a los usuarios.

Site (lugar, *sitio*): Se puede expresar como un punto en internet con una dirección única a la cual acceden los usuarios para obtener información.

Software (componentes lógicos, programas, *software*): Se llama así a todos los programas o elementos lógicos que hacen que una computadora funcione, poniéndose en interacción con los componentes físicos de la computadora.

Technologitis (tecnologitis): Es una ideología que actualmente ha tomado fuerza entre la sociedad y se basa en la creencia de que todos los problemas pueden resolverse a través de los avances tecnológicos.

Virtual (virtual): Es lo que no existe o no es real aparentemente.

Virtual Private Network (Red Privada Virtual): Es una red que funciona de manera privada y en donde, cuando menos alguno de sus componentes, está conectado a internet; se utilizan tecnologías de cifrado.

Virus (virus): Se le llama así a todo programa computacional que se duplica a sí mismo dentro de un sistema y que se añade a otros programas que se utilizan ocasionando fallas. En la actualidad son la principal preocupación de los usuarios que navegan en internet, en donde, por cierto, tienen su mayor campo de acción.

Visit (visita): Se le llama así a la trayectoria o camino que un usuario hace por una página de internet; este tipo de datos es muy importante en lo que respecta a la publicidad en internet, para comprobar qué tan efectivo es nuestro sitio.

WWW (World Wide Web, W3, Telaraña Mundial, Red Mundial, WWW): Sistema global de la información basado en la tecnología del hipertexto, que se crea en los noventa por Tim Berners Lee, investigador en el CERN, Suiza. Este sistema soporta todo tipo de información (audio, video, imagen, texto) y se accede muy fácil a través de los navegadores.

Web server (servidor web): Es el servidor que se conecta directamente a internet y en la que físicamente se encuentran guardadas todas las páginas que componen nuestro sitio de internet.

Bibliografía

Acosta Romero, Miguel: *Nuevo derecho mercantil,* Porrúa, México, 2000.

Andrés Cámpoli, Gabriel: *La firma electrónica en el régimen comercial mexicano*, Porrúa, México, 2007.

Arce Gargollo, Javier: *Contratos mercantiles atípicos*, Porrúa, México, 2008.

Azar, Édgar Elías: *La contratación por medios electrónicos*, Porrúa, México, 2005.

Bernal Torres, César Augusto: *Metodología de la investigación*, Pearson Educación, México, 2006.

Bueno Castellanos, Carmen: *Globalización una cuestión antropológica*, Ciesas, México, 2000.

Castrillón y Luna, Víctor Manuel: *Diccionario jurídico de la UNAM*, Oxford, 2001.

Davara Rodríguez, M.A.: *Manual de Derecho Informático*. Chile: Aranzadi, 2001, pp. 465.

Di Martino, Rosa Elena: *El notariado de tipo latino en la contratación electrónica*, Madrid, 2002.

Díaz, González Luis Raúl: *Los medios electrónicos en el derecho mexicano,* Gasca, México, 2006.

García Canclini, Néstor: *La globalización imaginada,* Paidós, Barcelona, 1999.

Giménez Amau, Enrique: *Derecho notarial,* Ediciones Universidad de Navarra, Pamplona, 1976.

Leal, Hugo: *El protocolo del cibernotario,* Aguascalientes, 2001.

Mantilla Molina, Roberto L: *Derecho mercantil*, Porrúa. México, 1998.

Meján Carrer, Luis Manuel C.: *Contratación por medios electrónicos*, Podium Notarial número 33, editado por el Colegio de Notarios del Estado de Jalisco, junio 2006, p. 85.

Pizzolo, Calogero: *Globalización e integración. Ensayo de una teoría general*, Argentina. Ediar, 2002.

Reyes Krafft, Alfredo: *La firma electrónica y las entidades de certificación*, Porrúa, México, 2004.

— *La firma electrónica y las entidades de certificación,* Porrúa, México, 2008.
Ríos Helling, Jorge: *La práctica del derecho notarial,* Mc Graw Hill, México, 2000.
Solís García, José Julio*: Factura y firma electrónica avanzada*, Editorial Gasca, México, 2005.
Vargas García, Salomón: *Algunos comentarios sobre el comercio electrónico y la correduría pública en México*, Porrúa, México, 2004.
VVAA: *Diccionario jurídico mexicano*, Instituto de Investigaciones Jurídicas. México: Porrúa, 1998, p. 1453.
Weber Max: *Economía y sociedad*, México: Fondo de Cultura Económica, 2005.
Weber Max: *Teorías sociales del derecho*, 1864-1920.

Publicaciones

Plan Nacional de Desarrollo 2007-2013.
Podium Notarial, Revista del Colegio de Notarios del Estado de Jalisco, Número 33, C. Meján, Luis Manuel: Contratación por medios electrónicos, junio 2006.
Política digital, innovación gubernamental, diciembre 2007.
Acuerdo DIGELAG/ACU-087/2008 Dirección General de Estudios Legislativos y Acuerdos Gubernamentales, emitido con fundamento en los artículos 36, 46 y 50 fracciones VIII y XXV de la Constitución Política; 1, 2, 3, 5, 6, 19 fracción II, 21, 22 fracciones I y XXIV y 30 de la Ley Orgánica del Poder Ejecutivo; así como las disposiciones de la Ley de Firma Electrónica Certificada para el estado de Jalisco y sus Municipios.
Revista Política Digital, Innovación gubernamental, "Firma electrónica en México, su problemática jurídica", p. 42, diciembre 2007.
Proyecto de Norma Oficial Mexicana. PROY-NOM-151-SCFI-2001. Prácticas comerciales-requisitos que deben observarse para la conservación de mensajes de datos. *Diario Oficial de La Federación*, 16/11/2001.
Instituto de Investigaciones Jurídicas. Diccionario jurídico mexicano. p.1453, Porrúa.

Páginas Web consultadas

SAT:
http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_1472.html
http://www.sat.gob.mx/sitio_internet/e-sat/comprobantes_fiscales/15_6542.html
http://www.facturasat.com/

México legal:
http://www.mexicolegal.com.mx/consultas/r3035.htm

http://www.mexicofiscal.com.mx/novedades/dec290803.htm

Secretaría de Economía

http://www.economia.gob.mx/pics/p/p437/A361.pdf

Suprema Corte de Justicia de la Nación

http://www.scjn.gob.mx/NR/rdonlyres/556FDA90-BE12-40D7-B697-48B32BE2F799/0/N070607.PDF

Diario Oficial:

Diario Oficial de la Federación publicación lunes 19 de diciembre del año 2005, p. 47, Primera Sección: http://www.profeco.gob.mx/juridico/normas/resol_nom151scfi2002.pdf

Banco de México

Banco de México, www.banxico.org.mx/sistemas-de-pago/servicios/firma-electronica/firma-electronica.html

Páginas gubernamentales

http://ciberhabitat.gob.mx/comercio/firma/index.html
http://www.gobiernoelectronico.org/node/3939
www.ciberhabitad.gob.mx/gobierno/textos/texto_notaria.htm
http://www.politicadigital.com.mx/pics/pages/marcolegal_base/Acuerdo-firma-240806.pdf

Otras

http://www.alambre.info/2004/01/12/la-firma-electronica-en-la-ley-mexicana/
http://www.alfa-redi.org/rdi-articulo.shtml?x=1521
http://catarina.udlap.mx/u_dl_a/tales/documentos/laex/de_i_m/capitulo_2.html
http://www.utem.cl/cyt/Derecho/firma.html
http://www.alambre.info/2003/11/24/firma-electronica-en-mexico/
http://www.windowstimag.com/N%C3%BAmerosanteriores/N%C3%BAmero124Octubre2007/FirmaAutoridadesdecertificaci%C3%B3nelectr%C3%B3nica/tabid/295/Default.aspx
Ochoa, José: "Respuesta de derecho positivo peruano al reto de la fe pública en materia informática". VII Congreso Iberoamericano de Derecho e Informática.

La firma electrónica y la función notarial en Jalisco:
homologación federal y estatal
Núm. 1

Se terminó de editar en abril de 2011
en el despacho de Verónica Segovia González
Marsella Sur 510, interior M, Colonia Americana
Guadalajara, Jalisco, México
La edición consta de 1 ejemplar

Epígrafe. Diseño editorial: VSG / *Diagramación:* Juan Francisco Bojórquez
Corrección de textos: Jorge Orendáin