UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE DERECHO
Y CIENCIAS SOCIALES

DIVISIÓN DE ESTUDIOS DE POSGRADO

FIRMA ELECTRÓNICA AVANZADA PARA EL ÁMBITO FEDERAL MERCANTIL, ADMINISTRATIVO Y FISCAL, MEDIANTE ESTÁNDARES "SHA" Y "RSA"

TESIS

QUE PARA LA OBTENCIÓN DEL GRADO DE
MAESTRO EN DERECHO

SUSTENTA
LIC. JAVIER MARTÍN ESCAMILLA BÁEZ

DIRECTORES DE TESIS
DR. EDUARDO ALEJANDRO LÓPEZ SÁNCHEZ
DR. FRANCISCO RAMOS QUIROZ

MORELIA, MICHOACÁN OCTUBRE DE 2019

CONTENIDO

Página

RESUMEN 6

INTRODUCCIÓN 7

CAPÍTULO PRIMERO EL MARCO JURÍDICO FEDERAL DE LA FIRMA ELECTRÓNICA EN MÉXICO 10

I.- Ámbito administrativo federal 10

1.- *Antecedentes* 10

2.- *La Ley de Firma Electrónica Avanzada* 12

3.- *Reglamento de la Ley de Firma Electrónica Avanzada* 19

II.- Ámbito fiscal federal 19

1.- El Código Fiscal de la Federación 20

2.- *La Resolución Miscelánea Fiscal* 23

III.- Ámbito mercantil 26

1.- *Antecedentes* 26

2.- *El Código de Comercio* 30

3.- *El Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación* 37

4.- *Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación* 38

5.- *Norma Oficial Mexicana relativa a los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos* 41

IV. Disposiciones comunes a los ámbitos administrativo, fiscal y mercantil 44

V. Comentarios finales de este capítulo 46

CAPÍTULO SEGUNDO NOCIONES DE SEGURIDAD INFORMÁTICA Y FIRMA ELECTRÓNICA 51

I.- Antecedente: la seguridad jurídica por medios autógrafos.....51

1.- *Fundamento jurídico*.....51

2.- *Ventajas y desventajas* 53

II.- Mecanismos de seguridad informática 54

1.- *Plástico y firma* 54

2.- *Plástico y contraseña* 57

3.- *Nombre de usuario y contraseña* 58

4.- *Posesión y uso de dispositivo electrónico*.....60

5.- *Identificación a través de datos biométricos* 61

III. Mecanismos criptográficos de seguridad jurídica 63

1.- *Nota histórica sobre la criptografía* 64

2.- *Criptografía e informática* 66

3.-*Ventajas y desventajas* 70

CAPÍTULO TERCERO EL RESUMEN DIGITAL CON ALGORITMO *HASH* SEGURO (SHA) 73

I.- Generalidades de los procesos de resumen digital.....73

1.- *Algoritmos abiertos al público* 73

2.- *Procesos irreversibles* 74

II.- El proceso de resumen digital mediante algoritmo *hash* seguro (SHA) 76

1.- *Los antecedentes: algoritmos MD* 76

2.- *El proceso de resumen digital mediante algoritmos hash seguros (SHA)* 78

III.- Ejemplo de un documento jurídico resumido digitalmente mediante algoritmo hash seguro (sha) 81

CAPÍTULO CUARTO EL MÉTODO DE ENCRIPTACIÓN “RSA” 86

I.- Los métodos criptográficos de clave pública 86

1.- *Criptografía asimétrica* 87

2.- *Proceso reversible* 87

3.- *Estándar público* 88

II.- La firma electrónica avanzada basada en métodos criptográficos de clave pública 88

1.- *Correspondencia exclusiva de los datos de creación* 89

2.- Control exclusivo de los datos de creación 90

3.- *Garantía de integridad del mensaje y la firma* 91

III.- El método de encriptación “RSA” 91

1.- *Nota histórica* 91

2.- *Descripción del estándar RSA* 92

CAPÍTULO QUINTO EL FUNCIONAMIENTO CONJUNTO DEL RESUMEN DIGITAL CON ALGORITMO HASH SEGURO (SHA) Y EL MÉTODO DE ENCRIPTACIÓN “RSA” 95

I.- Funcionamiento conjunto de los estándares SHA y RSA 95

II.- Ejemplos de documentos jurídicos firmados electrónicamente con los estándares “SHA-256” y “RSA” 96
CAPÍTULO SEXTO CONCLUSIONES 102
I.- La superioridad teórica de la firma electrónica 102
II.- La solidez técnica y jurídica de los estándares SHA y RSA 103
III.- Las dificultades prácticas de la firma electrónica 104
IV.- Las oportunidades de uso de la firma electrónica y otras tecnologías en el campo jurídico 107
ANEXO I 110
FUENTES DE INFORMACIÓN 151
Fuentes bibliográficas 151
Fuentes hemerográficas 152
Fuentes electrónicas 153
Normatividad 158
Jurisprudencia 159
Otras fuentes 160
Software utilizado 162

RESUMEN

La firma electrónica es una alternativa moderna para verificar la autoría y la integridad de cualquier documento jurídico. Por ello, nuestro orden jurídico federal ha establecido una detallada regulación en la materia, especialmente en las áreas administrativa, fiscal y mercantil. En esta tesis se analiza, desde un enfoque jurídico y técnico, el método de firma electrónica más reconocido por la normatividad mexicana, basado en los estándares informáticos “SHA” y “RSA”, para entender su funcionamiento, sus grados de eficiencia y eficacia y, muy especialmente, la seguridad jurídica que proporciona a los usuarios, a la luz de las exigencias de nuestra normatividad vigente.

ABSTRACT

The electronic signature is a modern alternative to verify the authorship and integrity of any legal document. Therefore, our federal legal order has established a detailed regulation on the matter, especially in the administrative, fiscal and commercial areas. This thesis analyzes, from a legal and technical approach, the method of electronic signature most recognized by Mexican regulations, based on the computer standards "SHA" and "RSA", to understand its operation, its degrees of efficiency and effectiveness and , especially, the legal security it provides to users, considering the requirements of our current regulations.

Palabras clave: Jurídico, normas, seguridad, digital, criptografía.

INTRODUCCIÓN

En años recientes, las tecnologías informáticas empiezan a tener cada vez mayor uso en los actos jurídicos emitidos por las autoridades administrativas. En estas nuevas tecnologías se ha encontrado una oportunidad para las autoridades de acelerar sus diversos procedimientos administrativos, automatizándolos en gran medida.

Es por ello que en el ámbito administrativo y, de manera especial, en la materia fiscal se han implementado diversas adecuaciones legislativas y reglamentarias tendientes a regular el uso de los medios electrónicos y la firma electrónica en los procedimientos del Poder Ejecutivo Federal. Se ha iniciado de esta manera con diversos proyectos encaminados a construir un llamado “gobierno electrónico”.

En este mismo contexto, vivimos en una época en que las relaciones comerciales en todo el mundo se han intensificado de una forma sin precedentes. El número y la magnitud de las transacciones mercantiles ha aumentado explosivamente debido, en gran medida, al uso de la tecnología moderna utilizada de diversas maneras.

Aunque la tecnología ha sido utilizada en el comercio habitualmente para la generación y transformación de productos o la prestación de servicios, en años recientes se ha aprovechado también para una faceta trascendental y delicada de las operaciones mercantiles: la contratación entre los comerciantes. Así, la típica contratación mercantil que se efectuaba en forma escrita -con papel y tinta-, se empieza a sustituir, cada vez con más frecuencia, por una moderna contratación realizada por medios electrónicos.

También ante esta nueva realidad, desde hace varios años el legislador mexicano se ha visto en la necesidad de reformar y adicionar las leyes mercantiles, a fin de adoptar y regular formalmente en México el llamado “comercio electrónico”, que es el conjunto de actos jurídicos mercantiles, en cuya formalización o ejecución se utilizan medios ópticos, electrónicos o de cualquier otra tecnología. Por ello es que a partir de 1996 hemos visto diversas modificaciones legislativas a las leyes

mercantiles, principalmente al Código de Comercio, con las que se ha modernizado el derecho mercantil mexicano para regular el uso de las nuevas tecnologías en los tratos de comerciantes. Cabe decir que estas mejoras legislativas se han hecho, en términos generales, de conformidad a los estándares internacionales en materia de comercio electrónico.

Así que no es de extrañar que desde la expedición de todas estas modificaciones legislativas y reglamentarias se han publicado diversos estudios jurídicos que han analizado con profundidad las nuevas disposiciones en materia de comercio electrónico y de digitalización gubernamental, haciendo énfasis en su modernidad y sus múltiples ventajas frente a las formas tradicionales de contratación mercantil y de emisión de actos administrativos.

Sin embargo, no debe limitarse el análisis jurídico al campo abstracto, sino que éste debe también debe enriquecerse mediante un análisis en sentido inductivo, que parta desde el estudio particular de cada una de las tecnologías de firma electrónica para contrastarlas con la legislación administrativa, fiscal y mercantil, verificando si se ajustan a ella o no, si dan seguridad jurídica a los comerciantes o no.[1]

Con toda seguridad, este tipo de estudios abonarían en mayor entendimiento del fenómeno del comercio electrónico y en una mayor confianza en él.

Por ello, en esta investigación se inicia con esa tarea, analizando uno de los procesos de firma electrónica más utilizado en la actualidad, para conocer sus características técnicas particulares, verificar si cumple con las exigencias de fiabilidad de la legislación administrativa fiscal y mercantil, e identificar su uso práctico. Se trata del proceso de firma electrónica mediante el uso de resumen digital con algoritmo seguro *hash* (SHA) y encriptado con método RSA.

Cabe hacer énfasis en que esta obra está principalmente dirigida a los juristas o a las personas que –sin la necesidad de tener muchos conocimientos matemáticos

[1] Algunas de las obras que, por excepción, han entrado al estudio de específico de tecnologías informáticas específicas y su aplicación práctica dentro del derecho mexicano son Téllez Valdés, Julio, *Derecho informático*, 4ª edición, México, McGraw Hill, 2009; Téllez Valdés, Julio, Lex cloud computing*. Estudio jurídico del cómputo en la nube en México*, México, Instituto de Investigaciones Jurídicas-UNAM, 2013; y León Tovar, Soyla H. *et al.*, *La firma electrónica avanzada. Estudio teórico práctico y técnico*, México, Oxford, 2006.

e informáticos– desean conocer las implicaciones jurídicas y la validez del uso de este proceso de firma electrónica. Por lo tanto, aunque nos adentraremos a los detalles técnicos de este proceso de firma electrónica, el análisis de esta tecnología de la información se hará con un lenguaje sencillo, con la finalidad de hacerlo más accesible a los juristas ya todas las personas interesadas.

Así las cosas, en el capítulo 1 se aborda brevemente el marco jurídico vigente en México en materia de firma electrónica administrativa, fiscal y mercantil. Se busca que este análisis legal sólo sea una parte menor del trabajo, pues, como se ha dicho, ya hay abundante bibliografía al respecto.

En el capítulo 2 se da una breve introducción al tema de la seguridad informática y la firma electrónica, para conocer sus conceptos básicos y su utilidad e importancia prácticas.

En el capítulo 3 y 4 se abordan individualmente los dos estándares utilizados en el método de firma electrónica que aquí se analiza. En cada caso se hace un repaso técnico del estándar, una confrontación con las exigencias de las leyes mexicanas y una revisión de sus aplicaciones prácticas.

En el capítulo 5 se aborda la manera en la que se complementan ambos estándares.

En el último capítulo se plasman las conclusiones de este trabajo, respondiendo a la interrogante de si el método de firma electrónica aquí analizado cumple con las exigencias de la legislación mexicana en materia de firma electrónica y si resulta práctico y seguro su uso, además de exponer los principales retos y oportunidades encontrados en el ámbito de la firma electrónica en México.

Esperamos que este trabajo resulte interesante para quienes buscan conocer la realidad práctica del comercio electrónico y que sirva para fomentar el uso de la firma electrónica en las transacciones comerciales en México y la confianza en la misma.

CAPÍTULO PRIMERO
EL MARCO JURÍDICO FEDERAL DE LA FIRMA ELECTRÓNICA EN MÉXICO

I.- Ámbito administrativo federal

1.- *Antecedentes*

La parte inicial del primer párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece textualmente que **"**Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento".

Esta porción constitucional, que se ha mantenido intacta desde la promulgación de la Carta Magna de 1917, establece los requisitos básicos que deben regir a todo acto de autoridad, incluyendo, por supuesto, a los de índole administrativa.

De especial interés para nuestro trabajo es la exigencia constitucional de que los actos administrativos consten siempre por escrito.

La forma escrita de los actos administrativos se relacionó siempre con las diversas técnicas de impresión disponibles en cada época, como la simple combinación de la tinta y el papel, la imprenta, la máquina de escribir, hasta las modernas impresoras personales de nuestros tiempos. Pero, en todo caso, de manera generalizada se ha entendido que el artículo 16, primer párrafo, de la constitución contenía la exigencia implícita de que todos esos actos administrativos escritos se acompañaran de la firma autógrafa del respectivo funcionario que la emite.

Muestra de ello tenemos la jurisprudencia P./J. 125/2004 emitida por el Pleno de la Suprema Corte de Justicia de la Nación, que se encuentra bajo el rubro "FIRMA AUTÓGRAFA. TRATÁNDOSE DE ACTOS O RESOLUCIONES ADMINISTRATIVAS LA ANULACIÓN POR CARECER DE AQUÉLLA PUEDE SER CON O SIN DETERMINACIÓN DE EFECTOS", en la que se estableció lo siguiente:

> Para que un acto o resolución administrativa cumpla con las exigencias establecidas en el artículo 16 constitucional debe contener firma autógrafa del funcionario emisor, por ser este signo gráfico el que otorga certeza y eficacia a los actos de autoridad ya que constituye la única forma en que puede asegurarse al particular que la autoridad emisora acepta su contenido.[2]

En este mismo sentido se ha pronunciado la Segunda Sala de la Suprema Corte de Justicia de la Nación, en su tesis de jurisprudencia 2a./J. 2/92, que se encuentra bajo el rubro "FIRMA FACSIMILAR. DOCUMENTOS PARA LA NOTIFICACION DE CREDITOS FISCALES" y que enseguida se transcribe:

> Esta Segunda Sala de la Suprema Corte de Justicia de la Nación ha establecido reiteradamente el criterio de que de conformidad con lo dispuesto por los artículos 14 y 16 de la Constitución General de la República, para que un mandamiento de autoridad esté fundado y motivado, debe constar en el documento la firma autógrafa del servidor público que lo expida y no un facsímil, por consiguiente, tratándose de un cobro fiscal, el documento que se entregue al causante para efectos de notificación debe contener la firma autógrafa, ya que ésta es un signo gráfico que da validez a los actos de autoridad, razón por la cual debe estimarse que no es válida la firma facsimilar que ostente el referido mandamiento de autoridad.[3]

Al respecto, conviene señalar que también la legislación secundaria federal establece como regla general que los actos administrativos se emitan en forma escrita y con la firma autógrafa de la autoridad. Esto se constata con la lectura del artículo 3º, fracción IV, de la Ley Federal de Procedimiento Administrativo, que textualmente dice:

> "**Artículo 3.-** Son elementos y requisitos del acto administrativo:
>
> (…)
>
> **IV.** Hacer constar por escrito y con la firma autógrafa de la autoridad que lo expida, salvo en aquellos casos en que la ley autorice otra forma de expedición;
>
> (…)";

---

[2] Pleno de la Suprema Corte de Justicia de la Nación, "Tesis de jurisprudencia P./J. 125/2004", *Semanario Judicial de la Federación y su Gaceta*, Novena Época, Tomo XXI, enero de 2005, Materia(s): Administrativa, p. 5. Registro: 179578.

[3] Segunda Sala de la Suprema Corte de Justicia de La Nación, "Tesis de jurisprudencia 2a./J. 2/92", *Gaceta del Semanario Judicial de la Federación*, Octava Época, núm. 56, agosto de 1992, Materia(s): Administrativa, p. 15, Registro: 206419.

Incluso el artículo 6, primer párrafo, de la ley comentada establece la nulidad para cualquier acto administrativo que incumpla con el requisito de ser expedido en forma escrita y con firma autógrafa de la autoridad.

Sobre este particular, Sánchez Gómez explica que la forma escrita es uno de los requisitos de formalidad del acto jurídico, que a su vez es uno de "los elementos del acto administrativo [que] nos permiten conocer su conformación jurídica, técnico-práctico".[4]

En suma, vemos que la constitución, la legislación, la jurisprudencia y la doctrina, tradicionalmente han sido coincidentes al considerar la forma escrita y con firma autógrafa del funcionario como uno de los elementos *sine qua non* de los actos administrativos federales.

Este paradigma jurídico se rompió hasta la expedición de la Ley de Firma Electrónica Avanzada, como lo veremos enseguida.

2.- *La Ley de Firma Electrónica Avanzada*

La Ley de Firma Electrónica Avanzada se publicó en el Diario Oficial de la Federación el 11 de enero de 2012, entrando vigor al día siguiente.

En la exposición de motivos de la iniciativa de esta ley, presentada en el Senado por el Poder Ejecutivo,[5] se indicó que la necesidad de transitar hacia un "Gobierno Electrónico" provenía de recomendaciones hechas en el seno de diversos organismos o foros económicos internaciones en los que México había participado, como la Comisión Económica para América Latina y el Caribe de las

[4] Sánchez Gómez, Narciso, *Primer curso de derecho administrativo*, 7ª ed., México, Porrúa, 2015, p. 349. *Cfr.* Serra Rojas, Andrés, *Derecho administrativo*, *Primer curso*, 29ª ed, México, Porrúa, 2016, pp. 265 a 267.
[5] Poder Ejecutivo de los Estados Unidos Mexicanos, *Iniciativa de decreto por el que se expide la Ley de Firma Electrónica Avanzada*, presentada ante el Senado de la República en sesión de fecha 9 de diciembre de 2010, p. 1.

Naciones Unidas y el Plan de Acción de Ginebra sobre la Cumbre Mundial de la Sociedad de la Información de 2003. Asimismo, se expuso lo siguiente:

> al considerar la tendencia creciente en el ámbito mundial hacia el uso de medios de comunicación electrónica en la prestación de todo tipo de trámites y servicios, así como la experiencia positiva obtenida en los últimos años en nuestro país en esta materia, se refuerza la convicción del Ejecutivo Federal… de que el uso de las tecnologías de la información y comunicaciones en la gestión pública es una opción que debe impulsarse para generar condiciones que permitan hacer más efectiva la provisión de trámites, servicios y procedimientos públicos.[6]

Por otra parte, en su iniciativa, el Presidente de la República explicó que la transición hacia trámites gubernamentales electrónicos sería de mucha ayuda en todas las acciones oficiales para la conservación y mejora de nuestro sistema ecológico.[7]

Concluyendo sustancialmente su exposición de motivos el Poder Ejecutivo de la siguiente manera:

> En tal sentido, además de los beneficios jurídicos, ecológicos y económicos actuales que representa la utilización de la firma electrónica, su regulación a través de una Ley en la materia, permitirá que dichos beneficios se incrementen, generando la posibilidad de trámites más ágiles y transparentes, que permitan su inicio y desarrollo a través de plataformas informáticas que garanticen certidumbre jurídica.[8]

Es de notarse que la exposición de motivos de la ley en comento es muy escueta en explicar el funcionamiento y en justificar la seguridad técnica de la firma electrónica propuesta.

En el dictamen de las comisiones unidas de gobernación y de estudios legislativos con opinión de la comisión de ciencia y tecnología, todas ellas del

---

[6] *Ibidem*, p. 2.
[7] *Ibidem*, p. 6.
[8] *Idem*.

Senado de la República, con respecto a la referida iniciativa de la Ley de Firma Electrónica Avanzada, se compartieron en general los motivos expuestos por el Poder Ejecutivo.[9]

Es de destacarse que las comisiones dictaminadoras del Senado detectaron un tema de gran relevancia, como son algunos inconvenientes prácticos del uso de medios electrónicos para la celebración actos jurídicos. No obstante, en el dictamen comentado se expresa que tales inconvenientes se controlan con el uso de firmas electrónicas avanzadas y certificados. Enseguida me permito transcribir la parte conducente del dictamen:

> Esta nueva modalidad de contrato [realizado a través de medios electrónicos] plantea problemas como la ausencia del soporte físico (un contrato escrito en papel), la dificultad de tener medios probatorios del contrato, la posible alteración o destrucción del mismo y la problemática que trae consigo acreditar la autenticidad de una firma autógrafa (como manifestación clara e indubitable de la voluntad) que le otorgue existencia y validez al documento.
>
> Al respecto debe sostenerse que la firma electrónica avanzada y los certificados digitales son herramientas que permiten celebrar actos jurídicos y que evitan, en gran medida, los problemas que trae consigo cambiar las formas tradicionales de manifestar la voluntad.[10]

En cuanto al dictamen de las comisiones unidas de la función pública, y de economía de la Cámara de Diputados, relativa al proyecto de decreto que expide la Ley de Firma Electrónica Avanzada, debemos de decir que expresa la coincidencia con el Poder Ejecutivo y la Cámara de Senadores sobre la importancia de implementar el uso de la firma electrónica avanzada en materia administrativa, haciendo énfasis en que se trataba de un asunto “inaplazable”.[11]

Finalmente se aprobó la Ley de Firma Electrónica que conocemos, publicándose en el Diario Oficial de la federación el día 11 de enero de 2012.

---

[9] Senado de la República, “Dictamen de las comisiones unidas de gobernación y de estudios legislativos con opinión de la comisión de ciencia y tecnología, todas ellas del Senado de la República, con respecto a iniciativa presentada por el Poder Ejecutivo de decreto que expide la Ley de Firma Electrónica Avanzada”, *Gaceta del Senado*, 22 de marzo de 2011, Consideración Primera.
[10] *Ibidem*, Consideración Segunda.
[11] Cámara de Diputados, “Dictamen de las comisiones unidas de la función pública, y de economía de la Cámara de Diputados, relativa al proyecto de decreto que expide la Ley de Firma Electrónica Avanzada”, *Gaceta Parlamentaria de la Cámara de Diputados*, 24 de noviembre de 2011, Consideraciones Quinta y Sexta.

La Ley de Firma Electrónica Avanzada se divide en cuatro títulos, que enseguida revisaremos de manera breve.

El primer título trata de los aspectos generales de la ley, tales como el ámbito de aplicación de dicha norma y la terminología que utiliza.

Así pues, la Ley de Firma Electrónica Avanzada inicia estableciendo que su finalidad es regular el uso de la firma electrónica avanzada y los servicios relacionados con la misma, en todos los ámbitos de la administración pública federal. Cabe señalar que la ley comentada no es aplicable a las materias fiscal y aduanera a nivel federal, ya que en el Código Fiscal de la Federación se regula el uso de la firma electrónica avanzada. Asimismo, la Ley de Firma Electrónica Avanzada no es aplicable en materia mercantil, pues el comercio electrónico está normado por el Código de Comercio. [12] Por ello es dable resumir que la referida ley permite el uso de la firma electrónica avanzada en todos los trámites oficiales que sean competencia de la administración pública federal.

Al revisar las definiciones d ellos términos usados en la Ley de Firma Electrónica Avanzada salta a la vista que el artículo 2º, fracción XIII, de la Ley de Firma Electrónica Avanzada define a la firma electrónica avanzada como “el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa”. Asimismo, se utilizan los conceptos de “certificado digital”, “clave pública”, “clave privada”, que denotan la exigencia de que se utilicen estándares de infraestructura de clave pública para la firma electrónica avanzada en el ámbito administrativo federal.[13]

La ley comentada[14] prevé la posibilidad de que se genere un certificado todos los servidores públicos federales adscritos a:

[12] Véanse artículos 1º, 2º, fracción IV, y 4º de la Ley de Firma Electrónica Avanzada.
[13] Véase artículo 2º, fracciones V, VI y VII, de la Ley de Firma Electrónica Avanzada.
[14] Véanse los artículos 2º, fracciones IX, XII, XXIII, y 3º, fracciones I y II, de la Ley de Firma Electrónica Avanzada.

a) Las secretarías de Estado

b) Los órganos administrativos desconcentrados de las Secretarías de Estado.

c) La Consejería Jurídica del Ejecutivo Federal.

d) Las unidades administrativas de la Presidencia de la República.

e) La Procuraduría General de la República.

f) Los organismos públicos descentralizados.

g) Las empresas de participación estatal mayoritaria.

h) Los fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal.

Ahora bien, todos estos funcionarios públicos están facultados para utilizar sus firmas electrónicas en los siguientes actos de autoridad:

a) Comunicaciones. [15]

b) Trámites.[16]

c) Servicios.[17]

d) Actos jurídicos y administrativos.[18]

e) Procedimientos administrativos.[19]

f) Notificaciones.[20]

g) Citatorios. [21]

h) Emplazamientos. [22]

i) Requerimientos. [23]

---

[15] Artículos 1º, fracción I, 2º, fracción I, y 9º de la Ley de Firma Electrónica Avanzada.
[16] *Idem*.
[17] *Idem.*
[18] *Idem.*
[19] *Idem.*
[20] Artículos 2º, fracción II, 11, fracción II, de la Ley de Firma Electrónica Avanzada.
[21] *Idem*.
[22] *Idem*.
[23] *Idem*.

j) Solicitud de informes o documentos. [24]

k) Las resoluciones administrativas definitivas que, en su caso, se emitan en los procedimientos administrativos. [25]

La ley en la materia también prevé la posibilidad de que los particulares obtengan sus certificados digitales para poder realizar en forma electrónica todo tipo de trámites oficiales ante los servidores públicos federales antes mencionados.[26] Por lo tanto, cualquier promoción que efectúen los particulares a dichas autoridades, en ejercicio de su derecho de petición reconocido en el artículo octavo de la Constitución Política de los Estados Unidos Mexicanos, se podrían emitir en forma electrónica.

Del título segundo de la ley que analizamos hay que destacar que el artículo 7º otorga pleno valor jurídico y probatorio a los documentos administrativos que se generen con firma electrónica avanzada y que cumplan con los principios enunciados en el artículo 8º, a saber:

> **I.** Equivalencia Funcional: Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos;
> **II.** Autenticidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;
> **III.** Integridad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;
> **IV.** Neutralidad Tecnológica: Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma

[24] *Idem*.
[25] *Idem*.
[26] Véanse los artículos 1, fracción I, 3, fracción III, de la Ley de Firma Electrónica Avanzada.

electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;

V. No Repudio: Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y

VI. Confidencialidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

Como se verá más adelante, se trata de requisitos técnicos muy homogéneos con los previstos en las legislaciones fiscal y mercantil.

Ahora bien, de la lectura del artículo 9º de la Ley de Firma Electrónica Avanzada se entiende que en la materia administrativa federal sólo serán admisibles firmas electrónicas generadas y validadas mediante claves privadas y certificados digitales (claves públicas), lo que necesariamente implica el uso de algún método criptográfico de infraestructuras de clave pública.[27]

El título tercero de la ley comentada prevé de manera detallada el contenido mínimo de los certificados digitales que se utilizarán para firmar electrónicamente documentos de índole administrativa y describe de manera general los procesos que se deben realizar para la emisión de dichos certificados, los derechos y obligaciones de sus titulares y las autoridades facultadas para emitirlos.

Los artículos 28 y 29 de la Ley de Firma Electrónica Avanzada contemplan la posibilidad de que se dicten medidas oficiales de homologación de los diversos tipos de certificados digitales emitidos por las distintas autoridades certificadoras del Poder Ejecutivo Federal, como lo son el servicio de Administración Tributaria, la Secretaría de Economía y la Secretaría de la Función Pública, e incluso por autoridades certificadoras de los otros dos poderes federales, órganos constitucionales autónomos, gobiernos de las entidades federativas, los municipios y los órganos político-administrativos del Distrito Federal. Con ello, se abrió la posibilidad de utilizar de manera generalizada determinado tipo de certificados

[27] Sobre los métodos criptográficos de clave pública, véase el capítulo cuarto, apartado I, de esta obra.

digitales, para todo tipo de acto administrativo federal, tal como sucedió con la expedición de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada, de las que hablaremos más adelante.[28]

Por otra parte, resulta interesante que esta legislación también permite la digitalización de documentos, entendiéndose como la migración de documentos impresos a una forma digital, siempre y cuando "haya sido realizada o supervisada por un servidor público que cuente con facultades de certificación de documentos en términos de las disposiciones aplicables o, en su caso, por el particular interesado, quien deberá manifestar, bajo protesta de decir verdad, que el documento electrónico es copia íntegra e inalterada del documento impreso".[29]

3.- *Reglamento de la Ley de Firma Electrónica Avanzada*

El Reglamento de la Ley de Firma Electrónica Avanzada aporta poco a la regulación hecha por la ley principal, sobre todo en el aspecto técnico del funcionamiento la firma electrónica. Para efectos del presente trabajo, de este reglamento únicamente podemos destacar que reitera la adopción de una infraestructura de clave pública para implementar la firma electrónica en materia administrativa federal. Esto lo podemos ver cuando se utilizan en este reglamento términos como "clave privada", y "certificado digital", que son propios de una infraestructura de clave pública.

II.- Ámbito fiscal federal

El 5 de enero de 2004 se publicó en el Diario Oficial de la Federación el decreto mediante el cual, entre otras cosas, se adicionó al Código Fiscal de la Federación un Capítulo Segundo del Título I, que se denominó "De los Medios Electrónicos". De esta manera se dio inicio con un proceso de digitalización de los procedimientos fiscales que, después de más de quince años, ha puesto a México a la vanguardia en materia de uso de medios informáticos para la emisión de comprobantes fiscales.

[28] Sobre estas disposiciones, véase apartado D de este capítulo.
[29] Artículo 16, fracción I, de la Ley de Firma Electrónica Avanzada.

En la actualidad, nuestro país es modelo para todo el mundo en materia de facturas electrónicas.

Sin embargo, poco se comenta con respecto a la digitalización generalizada de todos los procedimientos que se tramitan ante la autoridad fiscal, y que también representan el caso de mayor vanguardia en el país.

En este apartado analizaremos todos estos usos de la firma electrónica avanzada en el ámbito fiscal federal, siguiendo la ruta de sus diversas normas jurídicas, desde lo general hasta lo particular.

1.- El Código Fiscal de la Federación

El capítulo adicionado al Código Fiscal de la Federación en la reforma fiscal de 5 de enero de 2004, que se denomina “De los Medios Electrónicos” contiene una normatividad general acerca de la implementación de los medios electrónicos en la emisión de todos los documentos electrónicos emitidos por los contribuyentes y por las autoridades fiscales.

En este contexto, el artículo 17-D, primer párrafo, del código fiscal federal establece la regla general consistente en que todos los documentos que se deban emitir conforme a la normatividad fiscal deberán constar en formato digital y contar con firma electrónica avanzada. Esta tajante obligación de digitalización fiscal fue vista con escepticismo en un inicio, en cuanto a las posibilidades reales de su implementación. Sin embargo, con el paso de los años se ha logrado una observancia generalizada de esta regla, que se ha traducido en una mayor eficacia recaudatoria.

El segundo párrafo de la misma disposición detalla que la firma electrónica avanzada de los documentos electrónicos se realizará por medio de certificado público emitido por el Servicio de Administración Tributaria o por un prestador de

servicios de certificación autorizado por el Banco de México que “confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada”. Cabe destacar que el artículo 17-G, fracción VII establece que el certificado de firma electrónica para materia fiscal contendrá, entre otras cosas, la clave pública que se utiliza para la creación de la firma electrónica. De esto se desprende que el legislador pensó en una infraestructura de clave pública para lograr la digitalización de los documentos fiscales.

El principio de equivalencia funcional entre firma autógrafa y firma electrónica lo encontramos en el tercer párrafo del artículo 17-D del código comentado, donde se estipula lo siguiente:

> En los documentos digitales, una firma electrónica avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.

Como vemos, el mismo precepto citado indica que la firma electrónica avanzada, creada generada conforme al método previsto por la normatividad fiscal, garantiza la integridad del mensaje de datos firmado electrónicamente.

A diferencia de los ordenamientos generales de otras materias, el Código Fiscal de la federación, en su artículo 17-E, prevé de manera específica el método para certificar el intercambio de los documentos digitales entre la parte emisora y la parte destinaria, es decir entre el contribuyente y la autoridad fiscal. Al respecto, se establece que la autoridad fiscal receptora generará un “sello digital”, que es una especie de acuse de recibido electrónico que la autoridad receptora firma electrónicamente con un método idéntico al utilizado por el contribuyente. En contrapartida, el artículo 17-K de la codificación fiscal prevé el mecanismo de comunicación de las autoridades fiscales hacia los contribuyentes, a través de un

buzón tributario, dejando a la reglamentación administrativa la descripción de su funcionamiento.

Este ordenamiento fiscal también describe de manera más concreta el método de verificación de la integridad y la autoría de los documentos y los sellos digitales, que es mediante la "remisión al documento original con la clave pública del autor". Con ello, nuevamente se hace referencia a la infraestructura de clave pública y a su método típico de verificación, que es la desencriptación del mensaje a través de la clave pública, para llegar al mensaje original o a su resumen digital, como se explica en el capítulo cuarto, apartado III, de este trabajo.

Es de destacarse que el último párrafo del artículo 17-D del Código Fiscal de la Federación establece la posibilidad de aceptar para efectos fiscales certificados de firma electrónica avanzados emitidos por la Secretaría de la Función Pública o por prestadores de servicios de certificación autorizados por alguna dependencia federal competente, como podría ser la Secretaría de Economía.

En este mismo sentido de homogenización de los certificados de firmas electrónicas federales, el último párrafo del artículo 17-E de dicho ordenamiento permite a los particulares utilizar los certificados de firma electrónica emitidos en el ámbito fiscal para la firma y autenticación de todo tipo de documentos privados. En tal caso, dice este precepto, los particulares podrán solicitar al Servicio de Administración Tributaria que les proporcione el correspondiente servicio de verificación y autenticación de los certificados.

Asimismo, el artículo 17-L del Código Fiscal de la Federación abre la puerta para que el buzón tributario sea utilizado como medio de comunicación de otras autoridades hacia los particulares, cuando estos últimos otorguen su consentimiento expreso.

2.- *La Resolución Miscelánea Fiscal*

Como es natural, la descripción técnica y detallada del funcionamiento de la firma electrónica fiscal se reservó a la correspondiente reglamentación administrativa a cargo del Servicio de Administración Tributaria. En la materia fiscal, la facultad reglamentaria fiscal es ejercida a través de resoluciones misceláneas fiscales que se emiten anualmente, en las cuales precisamente se detalla el funcionamiento de la firma electrónica fiscal. Se trata de la reglamentación más amplia, detallada y precisa que existe en México sobre un mecanismo de firma electrónica avanzada. Enseguida revisaremos sus aspectos más relevantes.

La Resolución Miscelánea Fiscal para 2019 le otorga una denominación especifica al certificado que se utiliza para la creación de la firma electrónica avanzada a la que se refiere el Código Fiscal de la Federación. A dicho certificado se le denomina “e.firma”, según la definición 27 del glosario de la resolución miscelánea.

El capítulo 2.2. de la Resolución Miscelánea Fiscal contiene las reglas relativas a los medios electrónicos previstos en el Código Fiscal de la Federación.

La regla 2.2.3 de la resolución bajo análisis remite al rubro III.A del anexo 20 de la misma para conocer todos los detalles técnicos de los estándares informáticos de los algoritmos para la creación de la e.firma, la clave privada y la clave pública, mismos que revisaremos enseguida.

Cabe señalar que en el artículo transitorio tercero de la Resolución Miscelánea Fiscal para 2019, se prevé que “se prorrogan los anexos 2, 4, 5, 6, 8, 10, 12, 13, 17, 18, 19, 20, 21, 22, 26, 26-Bis, 27, 28 y 29 de la Resolución Miscelánea Fiscal vigente hasta antes de la entrada en vigor de la presente Resolución, hasta en tanto no sean publicados los correspondientes a esta Resolución”.

Es por ello que el anexo 20 al que se refiere la resolución miscelánea fiscal de este año es precisamente el mismo que se utiliza desde el 19 de julio de 2017,[30] pues en el año 2018 tampoco se expidió dicho anexo 20, sino que se prorrogó la vigencia del anterior.

El rubro III.A del anexo 20 lleva el título de "Estándares y especificaciones técnicas que deben cumplir las aplicaciones informáticas. para la generación de claves de criptografía asimétrica a utilizar para Firma Electrónica Avanzada".

En síntesis, establece que los datos de creación de la firma electrónica avanzada en materia fiscal serán una clave privada, una clave pública y un certificado digital, mismo que a su vez contiene la clave pública informáticamente vinculados a los datos de su titular. Asimismo, se establece que estos elementos de generarán con los estándares RSA de 2048 bits y SHA-2 256, que son precisamente los que se estudian en esta obra.[31] En específico, se prevé que la clave pública se generará conforme al estándar PKCS10 mientas que la clave pública se generará conforme al estándar PKCS8.[32]

Ahora bien, la resolución miscelánea fiscal que analizamos no hace una mención específica de la manera de utilizar las claves para firmar electrónicamente los

---

[30] El anexo 20 vigente se expidió mediante la Segunda Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2017 y sus anexos 1, 1-A, 3, 7, 9, 11, 14, 15, 16, 18, 20, 23, 25 y 25-Bis, publicada en el Diario Oficial de la Federación del 18 de julio de 2017, con entrada en vigor al día siguiente de su publicación oficial.

[31] Sobre este punto, el rubro III.A del anexo 20 de la Resolución Miscelánea Fiscal vigente, en su inciso 1, establece textualmente que "Las claves a generar deben ser de tipo RSA de 2048 bits con SHA-2 256".

[32] Sobre este punto, el rubro III.A del anexo 20 de la Resolución Miscelánea Fiscal, en su inciso 2, establece textualmente que "Los requerimientos digitales contienen la clave pública y se rigen por el estándar PKCS10 en formato DER. Mientras que la clave privada se almacena en un archivo configurado de acuerdo con el estándar PKCS8 en formato DER". Los estándares PKCS8 y PKCS10 son estándares de criptografía en clave pública creados por RSA Laboratories, publicados en Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés), *memorando RFC 2314 (actualizado en los memorandos RFC 2986 y RFC 5967)*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc2314/ e IETF, *memorando RFC 5208 (actualizado en el memorando RFC 5958)*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc5208/.

documentos digitales. Únicamente podemos ver que en la regla 1.9 se consigna una lista de anexos, que forman parte de la propia resolución miscelánea fiscal, entre los cuales tenemos al anexo 21, que se refiere al "marco general de los documentos digitales y el mecanismo de comunicación entre los proveedores de certificación de recepción de documentos digitales y los contribuyentes".[33]

En este contexto, el anexo 21 que se encuentra vigente es el que se publicó en el Diario Oficial de la Federación desde el 10 de marzo de 2015.

En el rubro I.A, en esencia, se establece la obligatoriedad de que los documentos digitales en materia fiscal se redacten en formato XML (siglas en inglés del *extensible marckup language*, o lenguaje de marcas extensible). Cada mensaje debe generarse conforme a una plantilla XSD que define la manera en la que se debe redactar cada tipo de documento, con elementos, tipos de datos, orden, etc. predefinidos. El estándar XML es muy utilizado en la actualidad para permitir el análisis informático de los mensajes de datos.[34] La adopción de este estándar obligatorio es lo que ha permitido a las autoridades fiscales una mayor agilidad en el análisis para efectos recaudatorios de los comprobantes fiscales digitales.

En el rubro I.B se trata el tema de la "generación de la firma y sello para documentos digitales". Aquí se reitera que la generación de la firma electrónica por parte de los emisores y de los sellos por parte de los receptores se debe hacer mediante los mismos estándares.

El primero de estos estándares informáticos es la función de "digestión" o resumen digital SHA-256, que "produce una salida compleja de 256 bits de salida, 128 para seguridad del mensaje y 128 para la identificación del mensaje (32 bytes)". Mediante este estándar se resume digitalmente el mensaje original, para obtener siempre un resultado de 256 bits (128 bytes)

[33] Regla 1.9, fracción XXIII, de la Resolución Miscelánea Fiscal para 2009.
[34] Véase Téllez Valdés, Julio, *Derecho informático*, *cit.*, pp. 61 a 65.

El segundo estándar que se menciona es el RSA que se utiliza para encriptar, por medio de la clave privada, el resumen digital obtenido con el estándar SHA-256.

III.- Ámbito mercantil

1.- *Antecedentes*

Sabemos que el derecho mercantil surgió siglos pasados en el viejo continente, principalmente por la necesidad de brindar un marco jurídico eficaz y flexible a los comerciantes que intensificaron y agilizaron el intercambio de mercancías a lo largo de Europa.[35] Con el tiempo, el derecho mercantil europeo se expandió a muchos otros lugares del mundo, principalmente los pertenecientes al sistema romano-canónico-germánico, incluyendo a México.[36]

Este derecho mercantil adoptó con mucha fuerza los mecanismos de contratación a distancia, consistentes en cartas de oferta, contraoferta y aceptación de condiciones, que permitían a los comerciantes radicados en lugares distantes entre sí negociar y pactar los contratos mercantiles que regirían sus negocios.

En esa misma dirección, el derecho mercantil fue adquiriendo durante su evolución el uso de otros mecanismos de contratación aún más simples y estandarizados, a saber: la letra de cambio y otros títulos de crédito.[37]

Todas estas formas de contratación, en términos generales, solucionaron durante mucho tiempo las necesidades jurídicas de los comerciantes de México y muchos otros lugares del mundo.

Sin embargo, con el paso del tiempo, aumentó la actividad mercantil a nivel mundial, impulsada por los nuevos medios de transporte y de intercambio de

---

[35] Véase Tena, Felipe J., *Derecho mercantil mexicano,* 22ª edición, México, Porrúa, 2010, pp. 25 a 31.
[36] Véase Instituto de Investigaciones Jurídicas de la UNAM, *Diccionario Jurídico Mexicano*, edición histórica, México, Porrúa, 2011, voz: DERECHO MERCANTIL, tomo II, p. 1199.
[37] *Ibidem*, voz: TÍTULOS VALOR, tomo 4, p. 3685.

información, trayendo como resultado una considerable intensificación de productos y servicios a lo largo y ancho de todo el mundo. Esta circunstancia ha exigido en forma crecientemente una nueva revolución en los mecanismos de contratación mercantil, para lograr efectuarla en tiempos ínfimos y en forma completamente remota y con absoluta seguridad jurídica.

Ante dicha exigencia, las legislaciones internacionales y nacionales han recurrido a los medios electrónicos de contratación.

El primer esfuerzo importante de regulación del llamado "comercio electrónico", lo encontramos en la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI).[38]

Dicha ley modelo se emitió debido a que se observó que "un número creciente de transacciones comerciales internacionales se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, habitualmente conocidos como "comercio electrónico", en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel".[39]

Con base en ello, la Asamblea General de las Naciones Unidas, consideró que esa ley modelo lograría "contribuir de manera significativa al establecimiento de relaciones económicas internacionales armoniosas" y "[ayudar] de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación en los casos en que carezcan de ella". [40]

La Ley Modelo sobre Comercio Electrónico se encuentra dividida en dos partes, una relativa al comercio electrónico en general y otra al comercio electrónico en materias específicas.

---

[38] Organización de las Naciones Unidas, *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su Incorporación al Derecho Interno*, recomendada por resolución de la Asamblea General aprobada en la 85ª sesión plenaria el 16 de diciembre de 1996.
[39] *Ibidem*, p. 1.
[40] *Ibidem*, p. 2.

La parte correspondiente al comercio electrónico en general, se encuentra dividida a su vez en tres capítulos: uno relativo a las disposiciones generales, otro relativo a la aplicación de los requisitos legales a los mensajes de datos y otro relativo a la comunicación de mensajes de datos.

Mientras que la parte que trata del comercio electrónico en materias específicas cuenta solo con un capítulo relativo al transporte de mercancías.

Posteriormente, en el año 2001, se emitió la Ley Modelo de Firmas Electrónicas, en la que se desarrollaron los aspectos básicos que sobre firma electrónica se trataron inicialmente en la Ley Modelo sobre Comercio Electrónico.[41]

Mientras que la ley modelo en materia de comercio electrónico se concentra en regular los aspectos de validez y funcionamiento general de los mensajes de datos –es decir, la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares– la ley modelo en materia de firmas electrónicas describe con mayor detalle técnico el funcionamiento de las firmas electrónicas –que son métodos para asegurar la integridad y la autoría de los mensajes de datos– puntualizando los requerimientos técnicos que deben observarse para considerar como fiable o avanzado un determinado método de firma electrónica.

Asimismo, en la Ley Modelo sobre Firmas Electrónicas se propone una regulación detallada de los efectos jurídicos generados por el uso de las firmas electrónicas y de las obligaciones para los firmantes y las partes que confían en los documentos firmados electrónicamente.

Es destacable que en esta ley modelo surge la propuesta de regular a los prestadores de servicios de certificaciones, o sea aquellas personas o entidades autorizadas para expedir certificados y prestar otros servicios relacionados con las firmas electrónicas.

Estas leyes modelos son precisamente el antecedente más importante para la legislación en materia de comercio electrónico para nuestro país, pues lo cierto es que las diversas adiciones y modificaciones que se han hecho al Código de

---

[41] Organización de las Naciones Unidas, *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su Incorporación al Derecho Interno*, recomendada por resolución de la Asamblea General aprobada en la 85ª sesión plenaria el 12 de diciembre de 2001.

Comercio en materia de comercio electrónico se basan precisamente en las propuestas de la CNUDMI.

En efecto, la reforma del 29 de mayo del año 2000, donde se incorporaron al Código de Comercio las disposiciones básicas del comercio electrónico, se basó principalmente en la Ley Modelo sobre Comercio Electrónico la CNUDMI. Así lo confirma precisamente el dictamen de las Comisiones Unidas de Justicia y de Comercio, con proyecto de decreto por el que se dictaminan diversas reformas y adiciones al Código Civil Federal, al Código de Comercio y a la Ley Federal de Protección al Consumidor en materia de comercio electrónico.[42]

Es importante detectar esta raíz inmediata, pues nos permite saber que la legislación mexicana en materia de comercio electrónico se enmarca en un estándar mundial que predomina en la mayor parte de los países del mundo y que se utiliza tanto para transacciones locales como para internacionales.

La modificación legislativa del 29 de mayo de 2000, basada en la Ley Modelo sobre Comercio Electrónico de la CNUDMI, adicionó un Título Segundo al Libro Segundo del Código de Comercio, dedicado exclusivamente al comercio electrónico. Sin embargo, esta regulación fue muy escueta, por lo que no abordó todos los tópicos contemplados por la ley modelo de la CNUDMI.

Posteriormente, el 29 de agosto de 2003 que se publicó en el Diario Oficial de la Federación un nuevo decreto que adicionó y reformó varios artículos del Código de Comercio en materia de comercio electrónico. Esta nueva adecuación legislativa se basó en la Ley Modelo sobre Firmas Electrónicas de la CNUDMI y dio al capítulo de comercio electrónico una fisionomía mucho más completa, regulando más detalladamente lo concerniente a las firmas electrónicas, las firmas electrónicas avanzadas y los prestadores de servicios de certificación.

Le regulación actual en materia de comercio electrónico se configuró el 7 de abril de 2016 con algunas adecuaciones mínimas al Código de Comercio, relativas a la digitalización de los documentos mercantiles.

---

[42] Cámara de Diputados, *Gaceta Parlamentaria de la Cámara de Diputados*, año III, número 500, miércoles 26 de abril de 2000.

A las diversas modificaciones legislativas del Código de Comercio ha seguido la emisión de las correspondientes disposiciones reglamentarias que complementan la legislación mexicana en materia de comercio electrónico.

2.- *El Código de Comercio*

En nuestro país hay abundante doctrina que analiza con detalle cada uno de los artículos del Código de Comercio y demás disposiciones reglamentarias en materia del comercio electrónico, por lo que no es el objetivo de este trabajo hacer un análisis semejante. En un sentido diverso, este trabajo tiene como finalidad analizar si la firma electrónica realizada conforme a los ampliamente utilizados estándares xml, sha y rsa, cumple con las exigencias de la legislación mexicana. Por tanto, la revisión al Código de Comercio y a las normas reglamentarias que se hace en este apartado y los siguientes tendrá un carácter muy general, con la única finalidad de describir someramente el marco normativo en vigor.

El Código de Comercio establece la regulación básica del comercio electrónico en México. Esta regulación se concentra en el Título Segundo del Libro Segundo del código mercantil, el cual se denomina “del comercio electrónico”. Sin embargo, en otras partes del Código de Comercio podemos encontrar algunos artículos aislados que también tratan este tema.

El título del comercio electrónico se divide en cinco capítulos: el primero relativo a los mensajes de datos, el capítulo I bis a la digitalización de documentos mercantiles, el segundo a las firmas, el tercero a los prestadores de servicios de certificación, y el cuarto al reconocimiento de certificados y firmas electrónicas extranjeros.

En el capítulo de los mensajes de datos encontramos prácticamente todo el contenido de la ley modelo de la CNUDMI. Del mismo, básicamente podemos destacar los siguientes tópicos:

1) En el artículo 89 se consigna un glosario muy preciso de los conceptos técnicos básicos que se utilizan en todo el título.

2) De manera muy relevante, en el artículo 89, en lo relativo a la firma electrónica, así como los artículos 89 bis, 93 y 93 bis, se decreta la plena validez jurídica de los actos jurídicos celebrados mediante mensajes de datos firmados electrónicamente, lo cual constituye el principio de equivalencia funcional con los documentos firmados autógrafamente en forma impresa.

3) En el artículo 89, segundo párrafo, se establece el principio de neutralidad tecnológica que implica la aceptación jurídica de cualquier tecnología que pueda cumplir con las disposiciones en la materia para celebrar actos de comercio en forma electrónica.

4) En la misma disposición se prevé el principio de autonomía de la voluntad, mismo que reitera el contenido del artículo 78 del Código de Comercio en el sentido de que "en las convenciones mercantiles cada uno se obliga en la manera y términos que aparezca que quiso obligarse, sin que la validez del acto comercial dependa de la observancia de formalidades o requisitos determinados".[43]

5) Ahí mismo se prevé el principio de compatibilidad internacional, lo cual quiere decir que estas reglas en materia de comercio electrónico responden a un estándar internacional, por lo cual es posible admitir en México la validez de diversos métodos de firma electrónica usados a nivel mundial.

6) En los artículos 90 a 92 bis se consignan las reglas generales sobre el envío y la recepción de los mensajes de datos.

El capítulo I bis, referente a la digitalización de documentos mercantiles, fue adicionado en la última reforma de fecha 7 de abril de 2016 en el que se establece la posibilidad de que los comerciantes digitalicen sus archivos físicos, conservando su plena validez, siempre y cuando se respeten los lineamientos planteados en dicho capítulo y en las disposiciones reglamentarias que se emitan con posterioridad.

[43] Esta interpretación del principio de autonomía de la voluntad también la comparte Reyes Krafft, Alfredo Alejandro, en *La firma electrónica y las entidades de certificación*, 2ª edición, México, Porrúa, 2008, p. 224.

En el segundo capítulo, relativo a las firmas electrónicas posee un contenido normativo valioso. En el artículo 96 se reitera el principio de neutralidad tecnológica en materia de métodos de firma electrónica. En el artículo 97 se regulan de manera general las características técnicas que deben llenar las firmas electrónicas para que sean jurídicamente fiables. Adicionalmente, en el artículo 99 se consignan las obligaciones de los firmantes, mientras que en el artículo 98 se prevé la obligación de los prestadores de servicios de certificación de confirmar a sus clientes si las firmas electrónicas que ofrecen son realmente fiables.

En el siguiente capítulo volveremos a analizar con más detalle el tema de las firmas electrónicas avanzadas.

En el tercer capítulo se regula de manera detallada la participación de los prestadores de servicios de certificación, personas físicas o morales que auxilian a los comerciantes brindándoles los siguientes servicios, conforme al artículo 100:

1) Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica.
2) Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación.
3) Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las Firmas Electrónicas Avanzadas y emitir el Certificado.
4) Expedir sellos digitales de tiempo para asuntos del orden comercial.
5) Emitir constancias de conservación de mensajes de datos.
6) Prestar servicios de digitalización de documentos.
7) Cualquier otra actividad no incompatible con las anteriores.

Conforme a este capítulo, los prestadores de servicios de certificación requieren de la previa acreditación de la Secretaría de Economía, entidad que se encargará de su permanente supervisión.

De manera aislada al resto de las disposiciones en materia de comercio electrónico, encontramos también el artículo 49 del Código de Comercio establece

que la correspondencia de los comerciantes también se integra con los mensajes de datos que se hayan intercambiado y que los mismos se deberán conservar por 10 años de manera “íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta”, ello de conformidad con los requerimientos de la respectiva Norma Oficial Mexicana que emita la Secretaría de Economía. En el apartado d de este capítulo se revisa dicha norma oficial.

Para efectos de este trabajo, de todas estas disposiciones del Código de Comercio, enseguida apuntaremos los aspectos de mayor utilidad para determinar los rasgos principales que caracterizan a una firma electrónica avanzada.

El artículo 89 del Código de Comercio establece las siguientes definiciones jurídicas que nos permiten entender la figura de la firma electrónica mercantil:

> **Datos de Creación de Firma Electrónica:** Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
>
> **Firma Electrónica:** Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
>
> **Mensaje de Datos:** La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Vemos pues que la firma electrónica mercantil es en esencia un mensaje de datos al que se le han adjuntado o lógicamente asociado por cualquier tecnología

otros datos (los datos de creación) que permiten identificar al firmante y verificar su conformidad con el contenido del mensaje.

Notamos también que los datos de creación de la firma electrónica son códigos o claves criptográficas privadas, que el firmante genera de manera secreta –con lo que se presume su exclusivo uso y responsabilidad sobre los mismos–.

No obstante, las definiciones anteriores dejan la duda sobre cuáles son esos métodos tecnológicos de los que habla el Código de Comercio, mediante los cuales se pueden asociar los datos de creación de la firma electrónica al mensaje de datos firmado.

Sin duda alguna, todos los métodos básicos de seguridad informática que analizamos en este capítulo pueden catalogarse como firma electrónica en términos del artículo 89 del Código de Comercio, al fungir como ese vínculo entre los datos de generación y el mensaje de datos; es decir los mecanismos de plástico y firma, de plástico y contraseña, de nombre de usuario y contraseña y de posesión y uso de dispositivo electrónico.

Pero especialmente los métodos criptográficos modernos de seguridad informática de los que hemos hablado en párrafos anteriores se pueden utilizar como firma electrónica mercantil avanzada, brindando una mayor seguridad a los comerciantes.

Para explicar esto, debemos recordar que el artículo 97, segundo párrafo, del Código de Comercio establece las características que debe reunir un método de firma electrónica para ser considerado avanzado o fiable:

> **Artículo 97.-** (…)
>
> La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:
>
> **I.** Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
>
> **II.** Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
>
> **III.** Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

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

(…)

Pero los métodos criptográficos modernos de seguridad informática cumplen con todos los citados requisitos mencionado en las fracciones III y IV del citado artículo 97, como enseguida se detallará.

En primer lugar, los métodos criptográficos de seguridad informática se inician con la generación de contraseñas, códigos, claves o llaves únicas e irrepetibles (datos de creación de la firma) por quienes participarán en la relación mercantil electrónica. Los protocolos modernos de seguridad informática permiten que estos datos de creación se generen en forma secreta por cada uno de los participantes. Las partes no intercambian sus datos de creación, sólo acuerdan el protocolo que utilizarán para cifrar y descifrar los mensajes.

Por lo tanto, podemos decir que con estos métodos se cumple con la fracción I del artículo 97 del Código de Comercio, pues en su contexto cada una de las partes genera de manera secreta y exclusiva sus datos de creación y se puede hacer absolutamente responsable de los mismos durante toda la relación electrónica mercantil.

Ahora bien, en los métodos modernos de seguridad informática las partes no requieren revelar los datos de creación en ningún momento, ni siquiera para validar el documento firmado, ni para el funcionamiento automático del programa informático correspondiente, por lo que no se guarda un registro de los mismos.

En efecto, en los métodos modernos de seguridad informática no sólo se encripta el mensaje de datos, sino que también se encriptan los datos de creación, con lo que se asegura que sólo el titular conozca sus propias contraseñas, códigos, claves o llaves.[44]

Esta peculiaridad permite que la criptografía moderna cumpla con la exigencia de la fracción II del artículo 97 del Código de Comercio, pues se garantiza

[44] Como un ejemplo de esto, en los capítulos cuarto y quinto de esta obra analizaremos los métodos de criptografía con llave pública.

que cada vez que las partes firman, transmiten o validan un mensaje de datos, los datos de creación permanecen en secreto para el uso exclusivo de sus titulares.

Nos obstante lo anterior, como lo indica la fracción II del artículo 99 del Código de Comercio, cada una de las partes está obligada a actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de sus datos de creación. Por ello, en estos métodos criptográficos se suelen contemplar mecanismos para revocar los datos de ceración y comunicarlos a las demás partes en los casos en que se haya perdido el control sobre los mismos.

Finalmente, podemos decir que la seguridad informática basada en criptografía moderna cumple con los requisitos previstos en las fracciones III y IV del artículo 97 del Código de Comercio en tanto que permiten la detección de cualquier alteración al mensaje de datos firmado.

Cabe apuntarse que, aunque pareciera que se trata de dos requisitos diversos por estar contemplados en dos fracciones distintas del artículo 97 del Código de Comercio, en realidad se trata del mismo requisito, pues hay que recordar que la firma electrónica contempla tanto al mensaje de datos como al conjunto de datos adjuntos o lógicamente asociados al mismo que permiten identificar al firmante y su aceptación con el mensaje de datos.

Por lo tanto, si el mensaje de datos y la firma electrónica son elementos inseparables, es obvio que la alteración de uno o la otra se pueden detectar mediante un único proceso. De ahí que sea dable decir que el Código de Comercio no exige sendos procesos para detectar alteraciones en el mensaje de datos y en la firma electrónica sino uno sólo que pueda detectar conjuntamente ambos tipos de alteraciones.

¿Pero, cómo es posible detectar alteraciones en el mensaje de datos y en la firma electrónica después de la firma? Con el uso de protocolos basados en fórmulas matemáticas altamente complejas que garantizan teóricamente un único resultado criptográfico para cada mensaje de datos firmado posible. En estas condiciones, con la reversión o la repetición del proceso criptográfico es posible verificar si el mensaje firmado electrónicamente (es decir el mensaje encriptado) corresponde al mensaje original. De ser así, se estaría constatando la integridad del

mensaje. En caso contrario se estaría detectando que el mensaje encriptado es apócrifo.

Cabe señalar que estos métodos de verificación de la integridad del mensaje son tan altamente efectivos que bastaría cualquier alteración al mensaje de datos –incluso de una sola de sus letras– para que se genere un resultado encriptado diverso y se descubra el engaño.

Nuevamente: todas estas exigencias del artículo 97 del Código de Comercio se cumplen de manera automática y prácticamente instantánea con los programas informáticos modernos. Aunque parecieran muy complejos, se realizan de manera imperceptible y en fracciones de segundos.

3.- *El Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación*

El 19 de julio de 2004, después de la reforma de 2003 del Código de Comercio, se publicó este reglamento en el que el Poder Ejecutivo de la Federación desarrolló de una manera más detallada la regulación de los prestadores de servicios de certificación.

Debe destacarse que este reglamento mantuvo respeto por los principios de neutralidad tecnológica y compatibilidad internacional, al establecer en su artículo 2º lo siguiente:

> La Secretaría aceptará cualquier método o sistema para crear una Firma Electrónica, Firma Electrónica Avanzada o Certificado, y promoverá que éstos puedan concurrir o funcionar con diferentes equipos y programas de cómputo, de conformidad con los principios de neutralidad tecnológica y compatibilidad internacional, en términos del Código de Comercio, este Reglamento y las Reglas Generales que expida la Secretaría.

En términos generales, podemos decir que este reglamento contiene normas principalmente de carácter administrativo sobre la manera en la que la Secretaría de Economía realiza su función de acreditar y supervisar a los prestadores de servicios de certificación, aunque también contiene algunas normas técnicas sobre firmas electrónicas y expedición de certificados para actos de comercio.

4.- *Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación*

El artículo 5º, fracción III, del Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, preveía que la Secretaría de Economía determinaría a detalle los elementos humanos, materiales, económicos y tecnológicos con los que deberían contar los prestadores de servicios de certificación.

Estas reglas de carácter general se publicaron originalmente el 10 de agosto de 2004,[45] sufriendo una reforma en fecha 5 de marzo de 2007.

Se trataba de una serie de disposiciones que detallaban de una manera muy exhaustiva cada uno de los requisitos que deben cumplir las personas que deseen recibir la acreditación por parte de la Secretaría de Economía como prestadores de servicios de certificación. Gran parte de estas reglas ya están redactadas en un nivel técnico muy elevado en materia de seguridad informática

De estas reglas podemos destacar que contemplaban la implementación de los siguientes estándares informáticos utilizados a nivel mundial:

1) Estándar ISO 17799.[46]
2) Estándar ETSI TS 102 042.[47]
3) Estándar ISO/IEC 17799.[48]
4) Estándar FIPS-140 nivel 3.[49]
5) Estándar Procesos descritos en NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems; NIST Special Publication 800-34,

[45] Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación, publicadas en Diario Oficial de la Federación el 10 de agosto de 2014.
[46] *Ibidem*, reglas 2.1.4., 2.4.4.3, 2.4.5.3, 2.4.6.1.1 y 2.4.6.2.2.
[47] *Ibidem*, reglas 2.1.4, 2.2.15, 2.4.5.3, 2.4.11.1.6, 2.4.12.1.10 y 2.4.15.5.
[48] *Ibidem*, regla 2.2.15.
[49] *Ibidem*, reglas 2.4.3.5, 2.4.15.4,

Contingency Planning Guide for Information Systems, June 2002; y NIST Special Publication 800-30 Risk Management Guide.[50]

6) Estándar ISO/IEC 9594-8.[51]

7) Estándares de la industria "RFC 3280. Internet X509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo, April 2002".[52]

8) Estándares de la industria sobre funciones *hash*, actuales y que provean el adecuado nivel de seguridad para este tipo de firmas tanto del Prestador de Servicios de Certificación como del usuario.[53]

9) Estándar RFC 3647.[54]

10) Estándar Internet X.509 "Public Key Infraestructure Time Stamp".[55]

11) Estándares RFC 3161 y 3628.[56]

Sin embargo, estas reglas fueron sustituidas íntegramente por unas nuevas que se publicaron el 14 de mayo de 2018 en el Diario Oficial de la Federación, entrando en vigor al día siguiente.[57]

Las nuevas reglas, exigen a los prestadores de servicios de certificación la utilización de los siguientes estándares informáticos:

1) NIST Special Publication 800-144[58]

2) ETSI TS 102 042[59]

3) RFC 3161 Internet X.509[60]

---

[50] *Ibidem*, regla 2.4.5.3.
[51] *Ibidem*, reglas 2.4.7.1, 2.4.8.1, 2.4.9.
[52] *Ibidem*, regla 2.4.7.2
[53] *Ibidem*, regla 2.4.7.3.
[54] *Ibidem*, regla 2.4.12.1.10.
[55] *Ibidem*, regla 7.2.
[56] *Ibidem*, regla 7.2.
[57] Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación, publicadas en Diario Oficial de la Federación el 14 de mayo de 2018.
[58] *Ibidem,* regla 8.
[59] *Ibidem,* reglas 36, 55, 65, 67.XIII, 110, 120.VIII, 137, 156, 165.VIII, 207 y 214.VII.
[60] *Ibidem,* regla 39.III

4) RFC 3628 "Policy Requirements for Time-Stamping Authorities (TSAs)" [61]

5) FIPS 140-2 nivel 3[62]

6) NIST Guide to Security for Full Virtualization Security, Special Publication 800-125, 2011.[63]

7) NIST Special Publication 800-30 Revisión 1.[64]

8) ISO/IEC de la serie 27000.[65]

9) Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST).[66]

10) NIST Special Publication 800-18 Revisión 1, Guide for Developing Security Plans for Federal Information Systems.[67]

11) NIST Special Publication 800-34, Contingency Planning Guide for Information Systems.[68]

12) NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems.[69]

13) RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.[70]

14) ISO/IEC 9594-8.[71]

15) RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.[72]

16) FIPS PUB 186-4. Digital Signature Standard (DSS).[73]

17) Función hash 256.[74]

---

[61] *Ibidem,* reglas 39.III, 116 y 118.VI.
[62] *Ibidem,* reglas 39.IV, 69.VII, 69.IX, 94.II, 120.VII, 140.II, 165.VII y 193.III.
[63] *Ibidem,* reglas 41, 95, 141 y 193.XIV.
[64] *Ibidem,* reglas 43.VIII, 55, 98.VII, 110, 144.VII, 156, 195.VIII y 207.
[65] *Ibidem,* reglas 45.III, 49, 55, 100.III, 110, 146.III, 150, 156, 197.III y 207.
[66] *Ibidem,* reglas 45.VIII, 146.VIII y 197.VIII.
[67] *Ibidem,* reglas 52, 107, 153 y 204.
[68] *Ibidem,* reglas 55, 110, 156 y 207.
[69] *Ibidem,* reglas 55, 110, 156 y 207.
[70] *Ibidem,* reglas 65 y 67.XIII.
[71] *Ibidem,* reglas 71, 74 y 75.
[72] *Ibidem,* reglas 74 y 75.
[73] *Ibidem,* regla 74.I.
[74] *Ibidem,* regla 74.II.

18) Estándar ISO/IEC 11179 Metadata Registry (MDR)[75]

19) Estándar XML Extensible Marckup Language.[76]

La mayoría de estos estándares hacen referencia a *hardware* específico, elementos materiales y políticas de seguridad que los prestadores de servicios de certificación requieren tener y seguir para el desarrollo de sus procesos.

Para efectos de este trabajo, es necesario destacar los estándares ETSI TS 102 042,[77] y RFC 3647,[78] pues se trata de los ejes centrales para la emisión de certificados de firma electrónica por parte de los prestadores de servicios, mismos que contemplan el uso de una infraestructura de clave pública.

Adicionalmente, estas reglas hacen una remisión a la norma oficial mexicana NOM-151-SCFI-2016 que revisaremos en el siguiente apartado, reiterando su aplicación obligatoria para los prestadores de servicios de certificación en materia de conservación de mensajes de datos y digitalización de documentos en soporte físico.[79]

5.- *Norma Oficial Mexicana relativa a los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos*

[75] *Ibidem,* regla 230.
[76] *Ibidem,* regla 230.
[77] Instituto Europeo de Estándares de Telecomunicaciones (ETSI, por sus siglas en inglés), *Estándar ETSI TS 102 042*, consultable en el sitio de internet de dicho organismo en la dirección https://www.etsi.org/.
[78] IETF, *Memorando RFC 3647 Infraestructura de clave pública de Internet X.509 Política de certificados y marco de prácticas de certificación*, consultable en el sitio de internet de dicho organismo en la dirección https://datatracker.ietf.org/doc/rfc*3647*/.
[79] Véase títulos séptimo y octavo de las reglas Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación publicadas el 14 de mayo de 2018 en el Diario Oficial de la Federación.

Como se mencionó en el apartado b de este capítulo, el artículo 49 del Código de Comercio prevé la emisión de una Norma Oficial Mexicana por parte de la Secretaría de Economía relativa a los requisitos que deben observarse para la conservación de los mensajes de datos que integren la correspondencia de los comerciantes.

El 4 de junio de 2002 por primera vez se publicó dicha norma en el Diario Oficial de la Federación, entrando en vigor hasta el 17 de febrero de 2006.[80] Esta norma se identificó como "Norma Oficial Mexicana NOM-151-SCFI-2002 relativa a las prácticas comerciales-requisitos que deben observarse para la conservación de mensajes de datos".

Esta norma de carácter muy técnico en materia de seguridad informática establecía los diversos estándares que debían observarse en materia de conservación de mensajes de datos intercambiados entre comerciantes, a saber:

1) El estándar ASN.1 (versión 1 de *Abstract Sintax Notation*).
2) El algoritmo MD5.
3) Las reglas de codificación básicas (BER, por sus siglas en inglés).
4) El método de encriptación "RSA".
5) El juego de caracteres ISO 8859-1.

Aunque de la lectura de la resolución publicada el 4 de junio de 2002 en el Diario Oficial de la Federación, en la que se emite la norma oficial comentada, se entiende que tales estándares resultan obligatorios, lo cierto es que la resolución publicada el 19 de diciembre de 2005 en el Diario Oficial de la Federación determinó que dichos estándares "constituyen meros ejemplos de aquellos que deben utilizar los comerciantes para garantizar la conservación de los mensajes de datos". De

[80] Dicha norma entró en vigor en forma posterior a su emisión debido a que su único artículo transitorio establecía que entraría en vigor "una vez que la Secretaría de Economía por conducto de la Dirección General de Normas, publique en el Diario Oficial de la Federación el aviso mediante el cual dé a conocer la existencia de infraestructura para llevar a cabo la evaluación de la conformidad en los términos de la Ley Federal sobre Metrología y Normalización y su Reglamento", lo cual aconteció el día 19 de diciembre de 2005, cuando se publicó una resolución en la que se determinó que la Norma Oficial Mexicana NOM-151-SCFI-2002 entraría en vigor 60 días naturales después de la publicación de esta última resolución, es decir el 17 de febrero de 2006.

esta manera *sui generis* se termina respetando el principio de neutralidad tecnológica que rige en materia de comercio electrónico.

El día 30 de marzo de 2017 en el Diario Oficial de la Federación se publicó la nueva norma NOM-151-SCFI-2016, relativa a los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos. Con esta nueva norma se sustituyó la previa NOM-151-SCFI-2002.[81] Entró en vigor 180 días naturales después de su publicación oficial.

A diferencia de la anterior, esta nueva norma oficial mexicana es muy escueta al establecer estándares criptográficos para la conservación de mensajes de datos, pues se limitó a referir, en el inciso A.1.2. del apéndice A, que "la Secretaría [de Economía] mantendrá a disposición del público en general, en su portal en internet, un listado de algoritmos criptográficos a utilizar".

Sobre este punto, por medio de una solicitud de acceso a la información pública, preguntamos la Secretaría de Economía sobre los estándares a los que se refiere el inciso A.1.2. del apéndice A de la norma oficial mexicana en análisis, a lo que se dio la siguiente respuesta:

> "I. En relación a lo dispuesto en el numeral A.I.2 del Apéndice (Normativo) de la Norma Oficial Mexicana NOM-751-SCFI-2075, "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-757-SCFI-2002)", el listado de los algoritmos criptográficos permitidos en relación a dicha norma y sus fechas de uso, se encuentran disponibles para su consulta a través de la siguiente liga de acceso público: http://www.firmadigital.gob.mx/directorio.html; en cuyo sitio de internet podrá visualizar en la parte superior derecha la opción "Marco Jurídico", y al acceder a ella se desplegará una pantalla con el Marco Jurídico Aplicable al Prestador de Servicios de Certificación y la información solicitada consistente en lo siguiente: "El algoritmo que deben utilizar los Prestadores de Servicios de Certificación, para la generación de las Constancias de Conservación de Mensajes de Datos NOM-757, será

[81] La principal razón de la emisión de la nueva norma oficial mexicana fue en mandato del artículo 34 del Código de Comercio, en el sentido de que la Secretaría de Economía debería de expedir una norma oficial mexicana que, además de versar sobre la conservación de datos, trataría también del tema de digitalización de documentos.

SHA256, mismo que deberá ser usados en tanto avance tecnológico requiera su ajuste; situación que será comunicada por parte de la Secretaría".[82]

Por otro lado, en el inciso A.2.1 del apéndice A de la norma en comento, se menciona específicamente el estándar “RFC 3161” para efectos de la formación de la constancia de conservación de mensaje de datos.[83]

Sin embargo, resulta muy criticable que la norma oficial mexicana haya dejado al arbitrio momentáneo de la Secretaría de Economía el establecimiento de los estándares criptográficos para la conservación de mensajes de datos, sin preverse ni siquiera lineamientos mínimos para orientar a dicha dependencia y a los comerciantes en general.

Por lo que ve al apéndice B de la norma oficial en comento, este contiene los detalles técnicos que se deben respetar al momento de

IV. Disposiciones comunes a los ámbitos administrativo, fiscal y mercantil

Como hemos mencionado en párrafos anteriores, al analizar las normativas que regulan el uso de la firma electrónica en las materias administrativa, fiscal y mercantil, encontramos diversas disposiciones que abren la puerta a que los certificados de firma electrónica avanzada emitidos por autoridades certificadores o prestadores de servicios de certificación acreditados en cada uno de estos campos, puedan ser utilizados y aceptados de manera general en el resto de los campos.

Esta posibilidad se empezó a materializar el 21 de octubre de 2016, cuando se publicó en el Diario Oficial de la Federación las llamadas “Disposiciones Generales de la Ley de Firma Electrónica Avanzada”, emitidas por la Secretaría de

[82] Dirección General de Normas de la Secretaría de Economía, *Respuesta a solicitudes de información con folios 0001000189019, 0001000189119 y 0001000189219*, Oficio No. DGN.312.01.2019.3365 despachado el 13 de septiembre de 2019.
[83] IETF, *Memorando RFC 3161 protocolo de internet X.509 de sellado de tiempo de infraestructura de clave pública*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc3161/. Dicho documento ha sido actualizado por IETF, *memorando RFC 5816*, ambos consultables en el sitio de internet de dicho organismo en la dirección https://datatracker.ietf.org/doc/rfc5816/.

Economía, la Secretaría de la Función Pública y el Servicio de Administración Tributaria.

La principal finalidad de estas disposiciones es la creación de un marco técnico común para el uso de certificados de firmas electrónicas, con validez jurídica reconocida en cualquier ámbito del derecho público y privado. Para ello, básicamente se reitera la aplicabilidad de los estándares informáticos ya previstos en las normatividades particulares de los ámbitos administrativo, fiscal y mercantil, a saber:

a) Algoritmo de resumen digital SHA256.[84]

b) Método de encriptación RSA con longitud de 1024, 2048 bits o superior.[85]

c) Estándar RFC 6960.[86]

d) Estándar RFC 5652.[87]

e) Estándar RFC 5958.[88]

f) Estándar RFC 2986.[89]

g) Estándar RFC 5280.[90]

---

[84] Disposición quinta, inciso 2 de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada.

[85] *Idem*.

[86] Disposiciones quinta, inciso 5, y décima primera de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada. Se refiere al estándar contenido en IETF, *memorando RFC 6960 protocolo X.509 de estado de certificado en línea de infraestructura de clave pública de Internet*, consultable en el sitio de internet de dicho organismo en la dirección https://datatracker.ietf.org/doc/rfc6960/.

[87] Disposición décima, párrafo segundo, inciso c, de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada. Se refiere al estándar contenido en IETF, *memorando RFC 5652 sintaxis de mensaje criptográfico*, consultable en el sitio de internet de dicho organismo en la dirección https://datatracker.ietf.org/doc/rfc5652/.

[88] Disposición décima, párrafo segundo, inciso a, de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada. Se refiere al estándar contenido en IETF, *memorando RFC 5958 paquete de llaves asimétricas (estándar antes conocido como PKCS#8)*, consultable en el sitio de internet de dicho organismo en la dirección https://datatracker.ietf.org/doc/rfc5958/.

[89] Disposición décima, párrafo segundo, inciso b, de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada. Se refiere al estándar contenido en el IETF, *memorando RFC 2986 estándar PKCS #10 sobre especificación de sintaxis de solicitud de certificación*, actualizado mediante IETF, *memorando RFC 5967 tipo de medio para aplicación PKCS #10*, consultables en el sitio de internet de dicho organismo en las direcciones https://datatracker.ietf.org/doc/rfc2986/ y https://datatracker.ietf.org/doc/rfc5967/ , respectivamente.

[90] Disposición décima segunda, fracción I, de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada. Se refiere al estándar contenido en IETF, *memorando RFC 5280 estándar de internet X.509 sobre certificado de infraestructura de clave pública y perfil de lista de revocación de*

Todos estos estándares nuevamente relacionados con mecanismos de infraestructura de clave pública para firma electrónica.

Cabe también señalar que en la disposición tercera de estas disposiciones generales se hace referencia a la norma oficial mexicana que establezca la Secretaría de Economía para la conservación de mensajes de datos, que actualmente se identifica como NOM-151-SCFI-2016 y que hemos analizado en un apartado anterior.

V. Comentarios finales de este capítulo

Después de analizar específicamente las normas jurídicas que regulan el uso de la firma electrónica en el ámbito federal administrativo, fiscal y mercantil, encontramos varios aspectos que vale la pena destacar.

Inicialmente, queda clara la apertura para el uso de la firma electrónica en todas las materias analizadas, confiriéndole un reconocimiento jurídico total, pues se reconocen sus amplias ventajas frente a los procedimientos basados en papel y firma autógrafa. Esto se desprende con claridad de la lectura de las leyes secundarias. Aunque debe reconocerse que, por su naturaleza, estas leyes solo delinean los elementos básicos del tema, sin entrar a detalles técnicos.

En las normas reglamentarias se percibe un mayor trabajo de las autoridades administrativas al trata de apuntar minuciosamente las formas en las que se pueden utilizar los medios electrónicos para expresar la voluntad de llevar a cabo actos jurídicos.

En el caso de las normas fiscales hay una precisión muy notoria en el establecimiento de estándares informáticos, dejándose clara su obligatoriedad. Ello explica el éxito alcanzado en el uso de firma electrónica para la emisión de

---

certificados, actualizado mediante los IETF, *memorando RFC 6818*, IETF, *memorando RFC 8398* e IETF, *memorando RFC 8399*, todos consultables en el sitio de internet de dicho organismo en las direcciones https://datatracker.ietf.org/doc/rfc5280/, https://datatracker.ietf.org/doc/rfc6818/, https://datatracker.ietf.org/doc/rfc8398/ y https://datatracker.ietf.org/doc/rfc8399/.

documentos fiscales, especialmente los comprobantes fiscales y los escritos de las autoridades fiscales.

Con relación a las normas administrativas y mercantiles, se ha optado por hacer referencia vaga a algunos estándares internacionales, para dejarlos como muestra de los mecanismos informáticos que se pueden utilizar para firmar electrónicamente los mensajes de datos. Esa imprecisión deja la duda sobre la obligatoriedad de esos estándares y la posibilidad de utilizar otros estándares similares o superiores. Pero tomando en cuenta el principio de neutralidad tecnológica que impera en ambas materias,[91] podemos considerar que los estándares mencionados en las normas reglamentarias son únicamente de carácter ejemplificativo, pudiéndose utilizar otros estándares con igual o superior nivel de seguridad informática.

Sin embargo, la técnica reglamentaria utilizada en las tres materias es muy cuestionable por otras razones. Se realiza con base en una compleja e intrincada enumeración de títulos de estándares informáticos, sin especificar quiénes son los autores de estos o las fuentes oficiales en las que pueden ser encontrados. Esto genera incertidumbre para los gobernados acerca del contenido real y la validez de los estándares informáticos referidos, máxime que su contenido se encuentra generalmente en inglés. Al respecto, hay que recordar que la Segunda Sala de la Suprema Corte de Justicia de la Nación ya se pronunció en alguna ocasión sobre la inconstitucionalidad de esta técnica reglamentaria, en la tesis de jurisprudencia 2a./J. 148/2016 (10a.), que se encuentra bajo el rubro “CONTABILIDAD ELECTRÓNICA. EL ANEXO 24 DE LA RESOLUCIÓN MISCELÁNEA FISCAL PARA 2015, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 5 DE ENERO DE 2015, VIOLA LOS DERECHOS A LA LEGALIDAD Y A LA SEGURIDAD JURÍDICA”, y que es del tenor literal siguiente:

> Al establecer las reglas de estructura planteadas dentro del estándar de los formatos respectivos para cumplir con la obligación de llevar la contabilidad en medios electrónicos, la autoridad administrativa dispuso que el contribuyente que utilice dicho estándar deberá sujetarse tanto a las disposiciones fiscales vigentes, como a los lineamientos técnicos de

[91] Sobre este principio, véanse el artículo 96 del Código de Comercio y el artículo 8º, fracción IV, de la Ley federal de Firma Electrónica Avanzada.

> forma y sintaxis para la generación de archivos XML especificados por el consorcio w3. Lo que significa que con dicha remisión la autoridad excedió los límites de la habilitación legal que le fue conferida a través del artículo 28 del Código Fiscal de la Federación, al encomendar al consorcio referido la labor de desarrollar las disposiciones correspondientes para hacer operativo el sistema; lo que además de la insubordinación jerárquica que esa actuación provoca, ocasiona inseguridad jurídica al gobernado, al obligarlo a cumplir con ciertos lineamientos emitidos "por una comunidad internacional" y no por una autoridad competente, bajo algún procedimiento de creación normativa o bajo determinadas exigencias mínimas de fundamentación y motivación. Máxime que, al establecer los lineamientos y formatos respectivos para cumplir con la obligación de llevar la contabilidad en medios electrónicos, tenía la obligación de hacerlo en idioma castellano o español, a fin de brindar seguridad jurídica a los contribuyentes al permitirles conocer plenamente la forma de operar los formatos establecidos al efecto, lo cual no se hizo, ya que al ingresar a la página de internet http://www.w3.org., se advierte que su contenido está en el idioma inglés; de ahí que el Anexo 24 de la Resolución Miscelánea Fiscal para 2015, viola los derechos a la legalidad y a la seguridad jurídica.[92]

Sobre ese mismo tema, la propia Segunda Sala de la Suprema Corte de Justicia de la Nación delineó una manera válida en la que se puede reglamentar el uso de un estándar informático obligatorio, precisamente al aprobar una resolución miscelánea fiscal con la que el Servicio de Administración Tributaria subsanó los vicios de inconstitucionalidad declarados en la tesis jurisprudencia arriba citada. En el nuevo criterio judicial, identificado con el número 2a. XXIV/2018 (10a.), bajo el rubro “CONTABILIDAD ELECTRÓNICA. EL ANEXO 24 DE LA RESOLUCIÓN MISCELÁNEA FISCAL PARA 2017, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 6 DE ENERO DE 2017, ACTUALIZA LOS SUPUESTOS A LOS QUE ESTABA SUJETA LA CONCESIÓN DEL AMPARO CONTRA DICHO ANEXO PARA 2015”, se estableció lo siguiente:

> En las jurisprudencias 2a./J. 148/2016 (10a.) y 2a./J. 160/2016 (10a.), la Segunda Sala de la Suprema Corte de Justicia de la Nación sostuvo que el Anexo 24 de la Resolución Miscelánea Fiscal para 2015 violaba los derechos a la legalidad y a la seguridad jurídica, por lo que debía desincorporarse de la esfera jurídica del quejoso la obligación de atender los lineamientos técnicos para la generación de archivos XML especificados por el consorcio w3 en la página de Internet http://www.w3.org., hasta que el Servicio de Administración Tributaria formulara y publicara en alguno de los medios a su alcance los lineamientos a seguir para la generación de archivos XML en idioma español. Por su parte, con el Anexo 24 de la Resolución Miscelánea Fiscal para 2017 y su documento técnico, el Jefe del Servicio de Administración Tributaria (SAT) no sólo actualizó la condición a la que estaban supeditados los efectos de la concesión del amparo, sino que además proporcionó los medios necesarios para cumplir la obligación de ingresar mensualmente la información

[92] Segunda Sala de la Suprema Corte de Justicia de la Nación, “Tesis de jurisprudencia: 2a./J. 148/2016 (10a.)”, *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 35, octubre de 2016, Tomo I, p. 699, Materia(s): Constitucional, Registro digital: 2012921.

> contable a través de la página de internet del SAT, en la medida en que: i) estableció la descripción de la información que deben contener los archivos de contabilidad electrónica; ii) proporcionó una guía básica de carácter opcional de las características, para la generación de archivos XML, sin la remisión a lineamientos fijados por una comunidad internacional (consorcio W3); iii) redactó los documentos en idioma español; y iv) en el documento técnico se dieron a conocer los lineamientos técnicos de forma y sintaxis necesarios para la construcción de archivos XML y la explicación del porqué se hace referencia a ciertos aspectos relacionados con un lenguaje de programación. En consecuencia, el contribuyente está en condiciones de cumplir la obligación formal contenida en el artículo 28, fracción IV, del Código Fiscal de la Federación respecto de aquel ejercicio en el que estaba imposibilitado para hacerlo.[93]

Además, pudimos observar que existe una gran dificultad en la tarea de actualizar las normas reglamentarias en las que se optó por establecer una lista larga de estándares informáticos, pues las mismas se suelen mantener intocadas por muchos años, a pesar del surgimiento de nuevos estándares en la materia.

Determinar cuál es forma adecuada en la que se pueden adoptar estándares informáticos internacionales en los ordenamientos locales requiere de un análisis que va más allá del objeto de este trabajo. Pero, al menos *a priori*, parece que la corte tiene razón al requerir que se utilice una más clara y segura técnica legislativa y reglamentaria.

También es claro que las normas revisadas carecen de protocolos sobre la exhibición y valoración de los mensajes firmados electrónicamente, por parte de las autoridades competentes, en especial de las judiciales. Esta carencia normativa es uno de los principales motivos de la falta de uso de los medios electrónicos entre particulares, pues genera desconfianza acerca de su fuerza probatoria.

De cualquier forma, en las tres materias analizadas es notoria la preferencia por el uso de ciertos estándares informáticos que se aprecia en las normas reglamentarias. En concreto nos referidos al algoritmo *hash* seguro (SHA, por sus siglas en inglés) y al método de encriptación RSA. Estos estándares son mencionados constantemente en todas las normas reglamentarias analizadas. Por supuesto, que esto es un buen indicio sobre la confiabilidad de estos estándares informáticos para generar firmas electrónicas. Pero, para efectos de nuestro trabajo,

[93] Segunda Sala de la Suprema Corte de Justicia de la Nación, “Tesis aislada 2a. XXIV/2018 (10a.)”, *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 53, Abril de 2018, Tomo I, p. 853, Materia(s): Administrativa, Común, Registro digital: 2016592.

sigue siendo necesario la revisión de los aspectos técnicos de dichos estándares y su análisis a la luz de las exigencias generales planteadas en las leyes principales de cada una de las materias.

CAPÍTULO SEGUNDO
NOCIONES DE SEGURIDAD INFORMÁTICA Y FIRMA ELECTRÓNICA

I.- Antecedente: la seguridad jurídica por medios autógrafos

Cuando la humanidad empezó a plasmar por escrito sus ideas, obtuvo también un importantísimo medio para dejar constancias de todo tipo de normas y acuerdos jurídicos, con una certeza y seguridad que nunca antes había existido.

Las normas jurídicas de los gobernantes ya constarían plasmadas en objetos de larga durabilidad y accesibles a cualquier consulta necesaria. Sin duda alguna, esto resolvió los principales problemas de las normas jurídicas transmitidas en forma oral: la facilidad de su distorsión, la dificultad para conocer a su autor y la dificultad para verificar el contenido de la norma original.

Pero también el uso de la escritura fue permeando entre los particulares que celebraban todo tipo de pactos. Y así los contratos entre personas se empezaron a plasmar con tinta en el papel, un método de seguridad jurídica que lleva muchos siglos en uso.

Con este tipo de contratos, las partes obtienen un documento en el que pueden consultar la literalidad de sus acuerdos por muchas décadas y tener una constancia muy fiable de que fue su voluntad pactar precisamente lo ahí plasmado.

Se trata de un medio altamente seguro, pues de lo contrario no llevaría tantos años en uso. Pero no es un método infalible ni es el más ágil en la actualidad.

En los siguientes apartados, analizaremos brevemente su funcionamiento jurídico, sus ventajas y sus desventajas.

1.- *Fundamento jurídico*

Los medios autógrafos de contratación son todos aquellos objetos en los que se plasma o graba físicamente y en forma escrita la manifestación de la voluntad de una persona o un grupo de personas para crear, transferir, modificar o extinguir derechos y obligaciones.

El Código Civil Federal que en su artículo 1834, primer párrafo, les denomina "documentos". Sin embargo, no debemos entender por tales simplemente a los escritos plasmados con tinta en papel, pues –según la Real Academia Española– la palabra documento tiene incluso el siguiente significado: "Cosa que sirve para testimoniar un hecho o informar de él, especialmente del pasado. Un resto de vasija puede ser un documento arqueológico".[94]

Por lo tanto, se puede plasmar o grabar un contrato en cualquier objeto, incluso una piedra o un trozo de madera. Pero obviamente lo más práctico y común es plasmar un contrato en papel.

La legislación civil federal no exige tampoco ningún material ni medio específico para plasmar la información escrita en el documento. Entonces es tan válido el uso de tinta plasmada en forma manual o mecánica como cualquier otra técnica de escritura. Por supuesto, siempre resultarán más prácticas las técnicas de escritura que mejor impidan la alteración o degradación de la información escrita.

Ahora bien, el propio artículo 1834 añade un requisito *sine qua non* a los contratos celebrados en forma de documentos: la firma.[95]

Al respecto, podemos decir que la Real Academia Española define la firma como "Nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido".[96]

Puesto que la ley no exige que las partes del contrato lo elaboren por sí mismos, resulta entonces válido que el documento sea redactado por cualquiera de sus autores o incluso por una tercera persona, bastando que las partes lo firmen en señal de aprobación.

---

[94] Real Academia Española, *Diccionario de la Lengua Española*, 23ª edición, Madrid, Espasa, 2014, VOZ: documento, acepción 3.

[95] El segundo párrafo de dicho numeral permite que una segunda persona firme a ruego del interesado, quien de cualquier forma deberá plasmar imprimir su huella digital. Pero este es un caso excepcional.

[96] Real Academia Española, *op. cit.*, VOZ: firma, acepción 1.

El contrato plasmado en documento firmado es la prueba más típica del consentimiento expreso para, 1803, fracción I, para crear, transferir, modificar o extinguir obligaciones.

2.- *Ventajas y desventajas*

Como mencionábamos en párrafos anteriores, los medios autógrafos de contratación son un medio muy seguro y que ha sido utilizado en forma generalizada desde hace mucho tiempo. Sin embargo, no se trata de un método infalible ni del más seguro. Expliquémoslo.

Los medios autógrafos de contratación, tienen al menos tres ventajas sobre otros medios de contratación:

1) Son medios muy accesibles. Cualquier persona puede hacerse de una pluma y papel para redactar y firmar un contrato. Incluso, el acceso a máquinas de escribir, computadoras e impresoras personales es cada vez más generalizado en la actualidad.
2) Son medios fácilmente consultables. Si se quiere saber lo que se pactó, basta tomar el documento correspondiente y leerlo por cuenta propia, sin necesidad de ningún artefacto.
3) Son medios a los que está habituada la generalidad de personas. Casi cualquier persona entiende su funcionamiento y lo admite con facilidad.

Sin embargo, estos medios también tienen algunas deficiencias –principalmente de seguridad– pocas veces tomadas en cuenta, que los ponen en desventaja frente a los medios electrónicos de contratación:

1) Son vulnerables a alteraciones en su contenido. Resulta relativamente fácil añadir o quitar contenido a un documento ya firmado, quizá escribiendo algo en espacios en blanco o borrando algún texto con químicos especiales.

2) Son muy frágiles, por lo que su pérdida o mutilación son peligros que siempre se deben tomar en cuenta.
3) Son fácilmente falsificables. Es relativamente fácil imitar la firma de cualquier persona. En la actualidad hay incluso máquinas que pueden reproducir de manera exacta cualquier firma. Además, para comprobar si un documento jurídico ha sido realmente firmado por alguien se requieren peritajes complicados y altamente subjetivos.
4) Su transporte –sobre todo a largas distancias– es complicado, costoso y riesgoso.

II.- Mecanismos de seguridad informática

Con la llegada de la computadora, el uso de la informática ha penetrado en diversos campos de la vida humana moderna, facilitando, agilizando y haciendo más fáciles diversos procesos.

Uno de los campos que se han visto beneficiados con el uso de la informática es el de las transacciones comerciales, que han encontrado métodos cada vez más seguros de dejar constancia de un acuerdo comercial y de la voluntad de las partes con el uso de las computadoras.

En este apartado haremos un breve recorrido por diversos métodos básicos de seguridad informática que se han utilizado de manera generalizada en la época moderna para celebrar contratos mercantiles. En cada caso mencionaremos la forma en la que dichos métodos brindan seguridad jurídica a las partes, así como sus fortalezas y debilidades en general.

1.- *Plástico y firma*

Se trata de uno de los primeros y más populares métodos informáticos utilizados para dejar constancia de transacciones mercantiles –especialmente las transacciones bancarias–.

Este método consiste en la autenticación de las partes celebrantes del contrato y la manifestación de su voluntad mediante el uso de su firma aunado a un elemento adicional: una tarjeta de plástico a la que se incorpora información grabada tanto físicamente como en un medio magnético o electrónico, la cual es teóricamente irrepetible y que se constituye en un mecanismo de identificación del titular.

Estas tarjetas de plástico se suelen regir, entre otros, por los siguientes estándares internacionales:

1) Estándar ISO/IEC 7810:2003 relativo a las caracterísiticas físicas de las tarjetas de identificación.[97]

2) Estándar ISO/IEC 7811-1:2014 relativo los métodos de grabado de las tarjetas de identificación.[98]

3) Estándar ISO/IEC 10373:2006 relativo a los métodos de verificación de las tarjetas de identificación.[99]

4) Estándar ISO/IEC 7816-1:2011 relativo a las tarjetas de identificación con circuitos integrados.[100]

Frecuentemente se utiliza este método en el medio bancario, donde el banco otorga a su cliente un plástico con información irrepetible como medio de identificación para futuras transacciones con el banco. El cliente acepta que usará en forma exclusiva dicho medio de identificación y se responsabiliza de cualquier operación que se autorice con el uso del mismo. Así el cliente utiliza dicho plástico para autorizar sus operaciones bancarias, mismas que el banco acepta de buena fe.

---

[97] Organización Internacional para Estandarización (ISO, por sus siglas en inglés) y Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés), *estándar ISO/IEC 7810:2003*, consultable en la página de internet http://www.iso.org.

[98] ISO e IEC, *estándar ISO/IEC 7811-1:2014*, consultable en la página de internet http://www.iso.org.

[99] ISO e IEC, *estándar ISO/IEC 10373:2006*, consultable en la página de internet http://www.iso.org.

[100] ISO e IEC, *estándar ISO/IEC 7816-1:2011*, consultable en la página de internet http://www.iso.org.

Por supuesto que el grabado y la lectura de la información contenida en el medio magnético o electrónico de la tarjeta no se puede hacer de forma simple, sino que se requieren dispositivos electrónicos especializados para tal fin. Por tal razón, este es uno de los primeros métodos que califican como firma electrónica en términos del artículo 89 del Código de Comercio. Sin embargo, este método no colma por sí solo los requisitos del artículo 97 del Código de Comercio para ser considerado como firma electrónica avanzada.

Típicamente este método se reforzaba mediante el uso simultáneo de la firma autógrafa del cliente en el comprobante impreso de la operación, al cual se le suele denominar "*váucher*".

Este método otorgó mucha mayor agilidad a las transacciones bancarias, sobre todo a las disposiciones de crédito realizadas a través de compras con terceros, pues hasta la fecha otorga una confianza muy alta al banco y a terceras personas sobre la identidad y la voluntad del cliente del banco. Esto debido a la razonable confianza que otorgan las tarjetas de plástico,[101] las cuales suelen ser difíciles de falsificar y al cuidado que generalmente tienen los titulares para evitar usos nos autorizados.[102]

Sin embargo, el uso de la tarjeta de plástico por sí misma no permite documentar los detalles de la operación celebrada,[103] por lo que se ha requerido además de la firma autógrafa del titular en el comprobante impreso de la operación. Esto resta agilidad y seguridad al método, pues se sigue cayendo en los inconvenientes de la contratación por medios autógrafos que se han mencionado en el apartado A de este capítulo.

---

[101] Las tarjetas de plástico usualmente han utilizado medios de almacenamiento de información de difícil falsificación. Inicialmente se utilizó una banda magnética, que en su tiempo fue muy segura. Actualmente –ante el avance de la tecnología que ha permitido falsificar bandas magnéticas– se utilizan medios me almacenamiento más modernos y seguros, como los microchips.

[102] Por lo general, los titulares tienen la opción de reportar robos o extravíos de sus tarjetas, para que estas sean canceladas y se evite su uso no autorizado.

[103] Esta es precisamente la razón por la que este método no cumple con los requisitos previstos en las fracciones II y IV del segundo párrafo del artículo 97 del Código de Comercio y no puede ser considerada como firma electrónica avanzada.

2.- *Plástico y contraseña*

Otra variante del método anterior es la que utiliza una contraseña como medio de identificación personal aunado a la tarjeta de plástico, en lugar de la firma autógrafa.

La contraseña es una combinación secreta de caracteres que debe ser presentada por el titular junto con la tarjeta de plástico como medio de identificación y de conformidad con la operación mercantil que se llevará a cabo. Por lo general, se trata de una serie de cuatro caracteres numéricos, conocidos como número de identificación personal (por sus siglas, NIP), aunque es teóricamente es posible la utilización de contraseñas alfanuméricas de cualquier extensión.

Dicha contraseña debe ser conocida sólo por el titular de la tarjeta de plástico para asegurar su carácter secreto y su uso exclusivo.

Al igual que ocurre con la información secreta que se graba en la tarjeta de plástico, la contraseña debe generarse y validarse por medios electrónicos.

Nuevamente este método se utiliza principalmente en el medio bancario. Inicialmente se usó para que los clientes del banco pudieran acceder a cajeros automáticos en los que podían consultar saldos y disponer de efectivo, entre otras operaciones. Pero en la actualidad algunas instituciones bancarias también utilizan este método para autorizar compras que sus clientes hacen con terceros mediante terminales remotas a través de las que se valida la tarjeta de plástico y la contraseña, sin requerir ya el estampado de la firma autógrafa en el *váucher*.

Debe reconocerse que este método ha demostrado una mayor agilidad y practicidad que su predecesor antes analizado, pues evita todos los inconvenientes del uso de la tinta y el papel –principalmente su transporte y resguardo. Y también debe reconocerse que se trata de un método más seguro que el previamente analizado, pues materialmente resulta más fácil imitar o inventar una firma autógrafa, altamente difícil de verificar por un comerciante común, que descubrir una contraseña guardada en secreto por el titular de la tarjeta.

Así, al ser un método que se ejecuta totalmente por medios electrónicos califica como firma electrónica, según el artículo 89 del Código de Comercio. Pero este método no colma por sí solo los requisitos del artículo 97, segundo párrafo,

fracciones III y IV, del Código de Comercio para ser considerado como firma electrónica avanzada, porque sólo sirve para validar la identidad de las partes del contrato mercantil. Sin embargo, el carácter 100% electrónico de este método ya le permite combinarse con técnicas de encriptación que sí generarían certidumbre sobre la integridad del contrato.

3.- *Nombre de usuario y contraseña*

Al expandirse el uso del internet a nivel global, se generó un aumento exponencial en las transacciones comerciales efectuadas remotamente a través de esa red mundial.

Para ese fin se requería el uso de métodos fáciles y ágiles de autenticación de personas. En algunos casos se optó por el uso de tarjetas bancarias, de las que el titular proporcionaba únicamente los datos impresos como prueba de su titularidad.[104]

Sin embargo, las transacciones por internet han requerido nuevos métodos de autenticación de las partes, incluso sin la participación de los bancos como intermediarios.

En este contexto, se ha generado un gran auge en el uso de un método que se vale combinadamente de dos datos generados por la parte interesada en la transacción: un nombre de usuario y una contraseña.

El nombre de usuario es un conjunto de caracteres formado libremente por el usuario, aunque a veces debe tomar la forma de una dirección de correo electrónico o cumplir con cierta forma requerida. Este nombre de usuario es un dato que se puede comunicar libremente, sobre todo para ser usado como medio de contacto.

Por su parte, la contraseña es un conjunto de caracteres generado en forma secreta por el mismo usuario. Esta contraseña sí debe permanecer en secreto permanentemente para garantizar la seguridad del método al usuario.

---

[104] Este método puede considerarse como una variable del método de tarjeta de plástico y contraseña, donde la contraseña suele ser una clave numérica impresa en forma discreta en cierto lugar de la tarjeta o alguna información personal del titular, proporcionada previamente al banco.

El método funciona de la siguiente manera:

1) El usuario proporciona a la otra parte su nombre de usuario y su contraseña secreta.
2) La otra parte verifica remotamente que ambos datos sean los correspondientes y, en tal caso, tendrá por válida la petición hecha por el usuario.

Existe una variante de este método en la que una tercera persona funge como intermediaria de las partes, prestando el servicio de verificación de los nombres de usuario y contraseña –sin revelar estas– para tengan seguridad de efectuar el trato.[105]

Por supuesto que se requiere el uso de dispositivos electrónicos con capacidad de conectarse a internet para generar y validar los nombres de usuario y contraseña. Por ello, en este caso también estamos en presencia de una firma electrónica artículo 89 del Código de Comercio.

Pero, como en el caso anterior, este método por sí solo no cumple con los requisitos previstos en el artículo 97, segundo párrafo, fracciones III y IV, del Código de Comercio, pues sólo sirve para verificar la identidad de las partes. Pero si se llega a utilizar en combinación con técnicas de encriptado puede conformar un verdadero método de firma electrónica avanzada que deje constancia también de la integridad del pacto.

Es fácil inferir que la popularidad de este método de firma electrónica –sin duda alguna el más usado en la actualidad– se debe a su simplicidad pero también a su amplia seguridad, misma que se ve robustecida cuando la contraseña es más compleja y cuando es cuidadosamente guardada por el usuario y la parte que la almacena electrónicamente para su posterior verificación. Sin embargo, no es el mejor método, pues todos conocemos casos en los que terceras personas han

[105] Un par de ejemplos muy conocidos de estos servicios de intermediación son el conocido como “Mercado Libre” ®, que se presta a través de la página de internet http://www.mercadolibre.com.mx/ y el de “Pay Pal” ®, que se proporciona en la página de internet https://www.paypal.com/mx/home , entre otros.

logrado revelar las contraseñas de usuarios con el uso de la tecnología para romper las medidas de seguridad del propio usuario o de quien las almacena.

4.- *Posesión y uso de dispositivo electrónico*

Este método consiste en identificar a la parte de un acto jurídico demostrando que tiene bajo su dominio un dispositivo electrónico propio y de características irrepetibles, previamente reconocido por todas las partes como elemento de identificación.

El método funciona de la siguiente manera: En primer término, las partes manifiestan que son los únicos propietarios y poseedores del dispositivo electrónico. Posteriormente utilizan dicho dispositivo electrónico como método de identificación, generalmente de manera remota y mediante programas de cómputo que identifican algunas características individuales del dispositivo. Así, cada una de las partes se hace responsable del uso del dispositivo electrónico como medio de identificación al momento de efectuar operaciones mercantiles.

Actualmente este método se utiliza mucho por medio de teléfonos celulares, los cuales cuentan con números individuales e irrepetibles de identificación que les asignan las compañías fabricantes o las que proporcionan el servicio telefónico. Con el uso de estos celulares, los usuarios pueden identificarse remotamente con otras personas para autorizar todo tipo de operaciones mercantiles.

Sin embargo, también se puede llevar a cabo este método mediante el uso de dispositivos diseñados especialmente para brindar la función de autenticación. Por ejemplo, en el ámbito bancario se suelen utilizar dispositivos conocidos como *tokens* de seguridad, los cuales tienen la única función de emitir contraseñas individualizadas y dinámicas –las cuales varían en función de los dígitos ingresados por el usuario. La contraseña respectiva es enviada por el usuario al banco, quien la valida remotamente y, en su caso, tiene por autorizada la operación solicitada.

Por supuesto, es habitual que las partes acuerden un mecanismo para darse aviso de la pérdida del dispositivo, en cuyo caso se le deja de aceptar como medio de identificación.

En cualquier caso, la seguridad de este método depende de que las partes previamente reconozcan en forma inequívoca el dispositivo que se utilizará, así como su particular funcionamiento, y lo acepten como un medio de identificación del que se responsabilizará absolutamente su tenedor.

Este método empieza a popularizarse de manera considerable, sobre todo mediante el uso de teléfonos celulares como medio de identificación. Es un método que brinda una notable y evolutiva seguridad por encima de los antes tratados, especialmente si se combina con el uso de alguna contraseña. El uso de dispositivos electrónicos hace calificar a este método como firma electrónica, de acuerdo al artículo 89 del Código de Comercio, pero no califica *per se* como firma electrónica avanzada, pues adolece de las características previstas en las fracciones III y IV del segundo párrafo del artículo 97 del propio Código de Comercio.

5.- *Identificación a través de datos biométricos*

Otro método utilizado para identificar una persona que participa en la emisión de un acto jurídico, es constatando uno o varios de sus datos biométricos, que son todas aquellas características biológicas singulares, medibles y, consecuentemente, registrables y verificables de la persona.[106]

Entre los datos biométricos humanos que la ciencia ha logrado identificar y medir se encuentran las huellas dactilares, la fisonomía del iris de los ojos, la fisonomía del rostro, la voz, los genes e incluso la impedancia de los dedos.[107] Partiendo de esto, se han desarrollado diversos dispositivos electrónicos capaces de identificar estos datos biométricos y registrarlos, vinculándolos a las personas a las que pertenecen, para contrastarlos con futuros usuarios que pretendan identificarse para cualquier fin.

---

[106] Véase Real Academia Española, *Diccionario de la lengua española*, 23ª edición, México, Espasa, 2014, voz: biometría.

[107] Véase, Hyung Wook Noh *et al*, "Ratiometric impedance sensing of fingers for robust identity authentication", *Scientific reports. Nature Research*, 19 de septiembre de 2019, consultable en https://www.nature.com/articles/s41598-019-49792-9.pdf.

Los métodos de identificación basados en datos biométricos humanos son de altísima exactitud, al ser datos totalmente únicos e irrepetibles.

Además, estos mecanismos de identificación son sumamente prácticos, pues los usuarios no requieren de objetos o contraseñas fabricados y ajenos a su persona para identificarse, por lo que no existe riesgo de extravío u olvido.

En la actualidad, se ha detonado el diseño, fabricación y la implementación de dispositivos de identificación a través de datos biométricos, por lo que los usuarios pueden acceder a ellos fácilmente, incluso a través de teléfonos celulares. Sin embargo, la identificación mediante biometría generalmente se usa solo con fines personales, para desbloquear dispositivos electrónicos o acceder a cuentas electrónicas, y apenas empieza a utilizarse en algunos actos jurídicos bilaterales de cuantías económicas moderadas.

La principal desventaja de estos métodos de identificación es la falta de estándares y protocolos informáticos de reconocimiento y difusión generalizada, que permitan a las personas utilizarlas con mayor confianza y conocimiento sobre su funcionamiento. A diferencia de métodos criptográficos de infraestructura de clave pública, que funcionan con base a estándares altamente documentados y difundidos,[108] la identificación por biométricos apenas se encuentra en desarrollo por parte de actores tecnológicos aislados que mantienen en secreto sus protocolos.

Un problema actual de esta tecnología es la inseguridad de las bases donde se almacenan los datos biométricos, pues, al no haber protocolos ni estándares claros, no existe certeza sobre la manera en la que los protegerán o la posibilidad de que sean usados para suplantar identidades.[109]

---

[108] Véase capítulo cuarto, apartado III, inciso 2, de este trabajo.
[109] Véase Editores de *Scientific American*, “Biometric Security Poses Huge Privacy Risks”, *Scientific American*, enero 1 de 2014, consultable en https://www.scientificamerican.com/article/biometric-

De cualquier manera, en la actualidad se utiliza la identificación por biométricos como auxiliar de los métodos de firma electrónica basados en infraestructura de clave pública. Por ejemplo, el estándar RFC 3647 contempla la posibilidad de que los certificados de firma electrónica incluyan datos biométricos del titular "como son huella digital del dedo pulgar, huella digital de los diez dedos, y reconocimiento facial, de la palma de la mano o de la retina".[110]

Sin duda alguna, se trata de una tecnología con gran potencial, que se avizora como la principal forma de identificación de personas en un futuro cercano, pero por ahora resta el desarrollo de protocolos informáticos y jurídicos sólidos, que permitan su uso de una forma más segura.

III. Mecanismos criptográficos de seguridad jurídica

Hasta esta parte hemos analizado diversos métodos de firma electrónica de nivel básico. Como hemos indicado, se trata de métodos que, por sí mismos, sólo generan la posibilidad de dejar constancia de la identidad de las partes firmantes.

Sin embargo, la informática actual permite la existencia de otros métodos avanzados de firma electrónica que además de autenticar la autoría de los contratos mercantiles permiten también conservarlos íntegros para futuras consultas y detectar cualquier alteración que se pretendiera hacer a los mismos. Estos métodos se basan en criptografía moderna efectuada a través de sistemas de informática.

En este apartado haremos un breve recorrido en la historia de la criptografía. Luego daremos una descripción técnica general del funcionamiento de la criptografía moderna. Enseguida veremos como la legislación mercantil actual reconoce la validez jurídica de estos mecanismos cuando se utilizan para la realización de firmas electrónicas. Finalmente hablaremos de sus ventajas y

security-poses-huge-privacy-risks/ y Catanzaro, Michel *et al*, "Voice Analysis Should Be Used with Caution in Court", *Scientific American*, 25 de enero de 2017, consultable en https://www.scientificamerican.com/article/voice-analysis-should-be-used-with-caution-in-court/ .

[110] IETF, *Memorando RFC 3647… cit.,* inciso 4.3.2, y nota 5.

desventajas frente a la firma autógrafa y a los mecanismos básicos de seguridad informática antes revisados. Después de esto, estaremos en condiciones de iniciar con el estudio del método de firma electrónica avanzada objeto de este trabajo.

1.- *Nota histórica sobre la criptografía*

Desde antiguas épocas se han ideado diversas técnicas para ocultar el contenido de ciertos mensajes escritos confidenciales. Este conjunto de técnicas es lo que se conoce como criptografía. Ciertos autores comentan al respecto que "básicamente, el objeto de la Criptografía es permitir la transmisión de información privada por un canal inseguro, de forma que cualquier intruso que intercepte la comunicación no entienda su significado".[111]

Se piensa que la criptografía se ha utilizado desde la propia introducción de la escritura en la historia de la humanidad, pero su uso regular comienza con los árabes en la Edad Media.[112]

El primer método de criptografía consistía en la simple sustitución de los signos o letras comunes de un idioma por otros signos o letras diversos o incluso por cifras, conforme a un patrón previamente conocido por el emisor y el destinatario del mensaje. A dicho patrón se le denomina "clave". El resultado de dicha sustitución era un mensaje ininteligible –al menos *a priori*– para cualquier interceptor, quien requeriría de la clave para poder entender la manera en que se efectuó la sustitución y, por lo tanto, el mensaje. Este método, se conoce como métodos criptográficos de sustitución.[113]

---

[111] Ortega Triguero, Jesús J. y otros, *Introducción a la criptografía. Historia y actualidad*, Cuenca, Universidad de Castilla-La Mancha, 2006, p. 9.
[112] *Ibidem*, p. 19.
[113] Véase Fúster Sabater, Amparo y otros, *Criptografía, protección de datos y aplicaciones*. *Guía para estudiantes y profesionales*, México, Alfaomega, 2015, p. 33; Maiorano, Ariel, *Criptografía. Técnicas de desarrollo para profesionales*, Buenos Aires, Alfaomega, 2009, p. 6; y Ortega Triguero, Jesús J. y otros, *op. cit.* pp. 19 a 24.

Una clave muy simple podía ser relativamente fácil de inferir por un descifrador.[114] Por lo que fue necesario ir generando claves cada vez más impredecibles y complejas para evitar que los mensajes fueran develados.

Otro método criptográfico del que podemos hablar es el de trasposición, que consistía en cambiar el orden de las letras o signos gráficos de un texto a fin de evitar su comprensión. El emisor y el destinatario del mensaje pactaban previamente la forma de desordenar y reordenar el mensaje y para ello se podían valer incluso de utensilios o aparatos diseñados para tal fin.[115]

Con la llegada del telégrafo nació una nueva época para la criptografía, en donde surgieron métodos con los que los mensajes secretos se podían transmitir en forma de señales eléctricas. Para tal efecto, se asignaba a cada letra o a cada palabra una correlativa combinación de señales eléctricas –que incluía señales de electricidad de diversas duraciones. Al catálogo de letras o palabras con su correlativa expresión en forma de señales eléctricas se denomina “código”.

El Código Morse fue el primero en utilizarse en forma masiva por medio del telégrafo. Desarrollado por Samuel Morse, era un código abierto, por lo que estaba disposición de cualquier persona u organización interesada en utilizar la telegrafía y, por lo tanto, no era muy adecuado para el uso criptográfico.

Sin embargo, la poca difusión del Código Morse entre la población en general y el difícil acceso a su medio de comunicación –el cableado eléctrico y el espectro electromagnético– permitieron su uso en la criptografía, aunque sea simple y limitado.

De cualquier manera, al poco tiempo se empezaron a elaborar códigos secretos que permitieron ocultar con mucho éxito el significado de mensajes enviados por vía telegráfica. Así el uso del telégrafo para fines criptográficos se dio en el ámbito comercial, gubernamental y militar.[116]

---

[114] Véase Ortega Triguero, Jesús J. y otros, *op. cit.*, p. 26.
[115] Véase Fúster Sabater, Amparo y otros, *op. cit.*, p. 34; Maiorano, Ariel, *op. cit.*, p. 7; y Ortega Triguero, Jesús J. y otros, *op. cit.*, p. 93.
[116] Véase Ortega Triguero, Jesús J. y otros, *op. cit.*, pp. 71 y 72.

Ahora bien, en 1929 Lester S. Hill propuso el primer sistema criptográfico que –en lugar de una clave o un código– utilizaba ecuaciones algebraicas. Esta propuesta fue el inicio de una revolución en el campo de la criptografía a partir de la cual se desarrollaron muchos sistemas criptográficos basados en el álgebra que superaron en seguridad a los antes mencionados.[117] Otro importante personaje de la criptografía matemática fue Claude Shannon, quien escribió abundantes artículos y libros sobre el tema alrededor del año 1950.[118]

Cabe señalar que para facilitar la aplicación todos los métodos criptográficos anteriormente revisados, desde finales del siglo XIX se inventaron diversos aparatos mecánicos capaces de realizar automáticamente el cifrado y descifrado de textos a partir de claves o ecuaciones algebraicas. Los más destacados de estos artefactos fueron los llamados "rotores", que tuvieron un gran uso comercial y militar a lo largo del siglo XX. Estos aparatos ayudaron a hacer criptografía de una forma más compleja y precisa.[119]

Sin embargo, fue la llegada de la computadora a mediados del siglo XX la que preparó el terreno de la criptografía moderna efectuada a partir de sistemas de informática.

2.- *Criptografía e informática*

Sin lugar a duda, la criptografía tuvo una revolución sin precedentes con la llegada de las computadoras. Por medio de éstas es posible ejecutar en forma inmediata y con absoluta precisión todos los métodos de encriptación antes comentados, desde la sustitución hasta la criptografía matemática, tanto para ocultar como para revelar mensajes. Por ello es que todos los métodos de encriptación desarrollados previamente quedaron obsoletos con la llegada de la computadora, porque simplemente dejaron de ser seguros.

No obstante lo anterior, debe mencionarse que las computadoras también permitieron el desarrollo de nuevos y extremadamente complejos métodos de

[117] Véase Ortega Triguero, Jesús J. y otros, *op. cit.*, p. 133.
[118] Maiorano, Ariel, *op. cit.*, p. 9.
[119] Véase *ibidem*, pp. 147 y 152.

encriptación basados en las matemáticas. La capacidad de cálculo de las computadoras permite desarrollar y ejecutar programas de encriptación basados en fórmulas matemáticas extremadamente complejas.[120]

Este tipo de métodos funciona de la siguiente manera: En primer lugar, se diseña una fórmula matemática extremadamente compleja, la cual no puede ser utilizada en forma manual por ninguna persona, sino que siempre se requerirá de alguna computadora para poder hacer operaciones con ella. Esta fórmula sólo debe ser poseída por el emisor y el receptor de los mensajes secretos. Así, con la ayuda de una computadora, el emisor cifra el mensaje con la fórmula matemática y oculta de esa manera su verdadero contenido. El mensaje puede ser enviado por cualquier medio electrónico, comúnmente por internet. Una vez que el receptor obtiene el mensaje cifrado procede a revelarlo con la ayuda de una computadora revirtiendo la operación matemática.

En teoría, y dadas ciertas circunstancias, con la ayuda de una computadora es posible descubrir la fórmula mediante la cual se cifra y descifra el mensaje. Pero cuando la fórmula utilizada es altamente compleja, tomaría incluso siglos descubrirla aún con la ayuda de las más avanzadas computadoras de la época. Esto es lo que hace extremadamente seguros los métodos modernos de criptografía efectuados con la ayuda de dispositivos electrónicos.

Aunque pareciera que estos métodos son muy difíciles de utilizar, lo cierto es que se llevan a cabo de manera automática mediante programas informáticos en los que viene cargada la correspondiente fórmula matemática de encriptación y desencriptación.

Ahora bien, no sólo la criptografía se ha beneficiado de los avances de la informática, sino que también la informática se ha valido de la criptografía para hacer sus sistemas más seguros.

En efecto, actualmente a la criptografía se le ha dado un uso adicional al de el ocultamiento de mensajes entre personas: la verificación de la autoría del mensaje y la verificación de su integridad. Al respecto, Fúster Sabater indica que

---

[120] Véase Fúster Sabater, Amparo y otros, *op. cit.,* p. 36; y Ortega Triguero, Jesús J. y otros, *op. cit.*, pp. 209 y 210.

una de las finalidades de la criptografía es “garantizar la autenticidad tanto del criptograma, llamada *integridad*, como del par remitente/destinatario. Si la autenticidad se refiere solo al remitente y al destinatario como individuos, se suele hablar de *identificación*”.[121]

Estas dos funcionalidades de la criptografía son absolutamente indispensables para la seguridad informática moderna, pues un número incalculable de operaciones informáticas de toda índole que se llevan a cada minuto –sobre todo por internet– requiere de una autenticación fiable de los participantes y de la integridad de los mensajes intercambiados.

Para ilustrar el uso de la criptografía con fines de seguridad informática veamos tres ejemplos.

En primer lugar, tomemos como ejemplo los teléfonos celulares, *tablets*, o computadoras personales modernas. Todos estos dispositivos cuentan con sistemas operativos que encriptan de una manera única la información en ellos contenida para hacerla inaccesible a todas las personas, excepto a su propietario y a las personas por él autorizadas. Para ello, el sistema operativo cifra toda la información del dispositivo (archivos, carpetas, etcétera) y sólo permite su descifrado mediante el ingreso de alguna contraseña generada por el propietario o algún medio de identificación biométrico. En caso de que no se proporcione la contraseña, cualquier intruso sólo podrá extraer del dispositivo información ininteligible e imposible de procesar. Estos métodos de protección de la información funcionan de manera prácticamente imperceptible para la mayoría de los usuarios de estos dispositivos, quienes únicamente solemos “iniciar las sesiones” en los mismos sin percatarnos de estas avanzadas medidas de seguridad.

Por supuesto que estos métodos de protección de la información se utilizan con un mayor grado de sofisticación para proteger bases de datos de alta trascendencia, como las de índole gubernamental o corporativo.

Otro uso de la criptografía en la seguridad informática se da para proteger las comunicaciones privadas. Hay que recordar que en la actualidad las computadoras están conectadas entre sí por diversos medios alámbricos e inalámbricos. Por estos

[121] Fúster Sabater, Amparo y otros, *op. cit.,* p. 31.

medios viajan diariamente millones de datos transferidos entre diversos usuarios ubicados en distintos lugares, a veces separados de un escritorio a otro y a veces separados de un continente al otro. En este contexto resulta sumamente fácil interceptar en forma electrónica los datos de una comunicación privada. Sin embargo, mediante la criptografía se pueden cifrar los datos transferidos para hacerlos ininteligibles para cualquier intruso.

La forma de guardar la privacidad de estas comunicaciones es encriptándolas mediante un protocolo que –ejecutado automáticamente– hace que cada dispositivo transmisor cifre la información enviada y que cada dispositivo transmisor la descifre de manera casi instantánea e imperceptible. Lo único que ambos usuarios requieren es compartir una contraseña común con la que se conectaron previamente a la red de comunicación.

Finalmente mencionaremos otro uso que se la ha dado a la criptografía en el ámbito de la seguridad informática. Se trata de la autenticación de comunicaciones. Aquí se utilizan las dos funcionalidades de la criptografía que mencionábamos hace unos párrafos la identificación de las partes y la garantía de la integridad de sus comunicaciones. En este caso no sólo se trata de proteger la privacidad de los datos o las comunicaciones, sino de brindar certeza sobre sus autores y su contenido fiel.

Esto se puede dar si se parte de dos supuestos:

1. Que el conocimiento exclusivo del protocolo criptográfico y de los elementos para su funcionamiento (contraseñas, códigos, claves o llaves únicas e irrepetibles) por parte de los usuarios, hace concluir teóricamente que tienen el control absoluto e indudable de los mensajes que se comparten a tal grado que pueden garantizarse y validarse mutuamente su autoría.
2. Que la alta complejidad del método criptográfico utilizado hace teóricamente imposible la repetición de un mismo resultado criptográfico a partir del cifrado de dos mensajes distintos, por lo que es posible concluir que la reversión del método criptográfico, o al menos su replicación, permite validar la integridad del mensaje cifrado.

Esta funcionalidad de la criptografía en la seguridad informática es la que se conoce comúnmente como “firma electrónica” y se utiliza cada vez más en ámbitos como la comunicación entre entidades gubernamentales, la prestación de servicios públicos y, por supuesto, en el comercio electrónico.

En el siguiente apartado, analizaremos con mayor detenimiento cómo la criptografía y la seguridad informática hacen posible el uso de la firma electrónica en materia mercantil, así como la seguridad jurídica que brinda a las operaciones celebradas por este medio tecnológico.

3.-*Ventajas y desventajas*

La firma electrónica basada en métodos criptográficos es sumamente reciente frente al uso de los documentos firmados de manera autógrafa. Sin embargo, su uso ha aumentado de manera exponencial –y casi imperceptible– en los últimos años. La seguridad técnica de este método de contratación se ha reforzado a un grado que prácticamente podemos calificar de blindaje tecnológico. Pero debe reconocerse que es escaso el conocimiento técnico y jurídico de la firma electrónica, lo cual merma en cierto grado la confianza del público en general en este medio de contratación.

Tal como lo hicimos con el medio clásico de seguridad jurídica, el medio autógrafo, en este apartado analizaremos las ventajas y desventajas generales de la firma electrónica basada en métodos criptográficos.

En primer lugar, analizaremos las ventajas prácticas de esta firma electrónica:

1. Los documentos firmados electrónicamente son más fáciles de almacenar. Al generarse y conservarse en medios electrónicos, pueden ser almacenados en cantidades colosales en todo tipo de dispositivos, desde minúsculas tarjetas de memoria portátiles hasta computadores de cualquier capacidad, con todo tipo de medidas de seguridad. Esto es una importante

ventaja frente a los documentos impresos, que llegan a ocupar mucho espacio en los archivos físicos.

2. Los documentos electrónicos pueden transportarse de manera más rápida y práctica. Los mensajes de datos pueden transmitirse a cualquier lugar del planeta, por cualquier red informática –especialmente por internet–, en fracciones de segundos. Por su parte, los documentos físicos son difíciles de enviar de un lugar a otro, sobre todo cuando el traslado es internacional, el tiempo para su envío suele ser largo y siempre hay un alto riesgo de pérdida o daño.
3. Los mensajes de datos pueden reproducirse de manera íntegra e instantánea. Por medio de cualquier computadora se pueden generar, enviar y almacenar cuantas copias de un documento se desee sin pérdida de datos. Mientras tanto, los documentos físicos (sobre todo los extensos), requieren de mucho tiempo y recursos para ser reproducidos y siempre es probable que haya deficiencias en el copiado.
4. Los documentos electrónicos son más durables. Al no existir en forma física, pueden conservarse íntegramente sin afectaciones por el paso del tiempo, cuando se tienen las debidas precauciones de conservación. Esto es una importante ventaja frente a los documentos físicos, que invariablemente se degradan a lo largo del tiempo.
5. Los documentos electrónicos son más amigables con el medio ambiente, pues no requieren de papel para su conservación. Por su parte, los documentos físicos requieren de diversas cantidades de papel y típicamente han representado un fuerte desgaste de los recursos forestales a nivel mundial.
6. Los documentos electrónicos permiten el uso de una amplia gama de herramientas informáticas para su clasificación, búsqueda y análisis. Su uso resulta mucho más productivo que los documentos físicos, los cuales requieren siempre de un tratamiento físico para ser clasificados y solo pueden ser analizados por medio de los órganos sensoriales humanos.

7. Es técnicamente imposible la alteración de un documento electrónico. Cualquier intento de ello, se detecta fácil y automáticamente. En contraste, los documentos físicos pueden ser fácilmente alterados, por ejemplo: agregando o modificando el texto, adicionando o quitando páginas, y falsificando la firma autógrafa.

Ahora bien, no podemos omitir mencionar las desventajas que tienen los documentos electrónicos hoy en día:

1. Las personas en general están poco familiarizadas con los documentos electrónicos. Se conoce poco acerca de sus métodos de creación y de su seguridad técnica y jurídica. Aunque cabe mencionar que paulatinamente esta situación de ignorancia se está reduciendo.
2. Para la creación y uso de los documentos electrónicos se requiere de cierta infraestructura tecnológica que no está al alcance de todas las personas. Sin embargo, poco a poco estos elementos tecnológicos se están haciendo accesibles a una mayor parte de la población de nuestro país.

Después de este balance, resulta notorio que los documentos firmados electrónicamente son más seguros y prácticos que los típicos documentos autógrafos. Sin embargo, hace falta reducir el desconocimiento que existe sobre los documentos electrónicos, generando más información técnica y jurídica sobre los métodos de su creación, conservación y utilización.

Como se indicó desde el apartado introductorio, la presente investigación tiene como uno de sus principales objetivos aumentar el conocimiento técnico y jurídico sobre uno de los principales métodos de firma electrónica, con lo que se busca también consolidar una mayor confianza en dicho método.

Y en este contexto, procederemos en el siguiente capítulo a analizar la primera parte del método de firma electrónica objeto de este estudio: el resumen digital por medio del algoritmo *hash* seguro (SHA).

CAPÍTULO TERCERO
EL RESUMEN DIGITAL CON ALGORITMO *HASH* SEGURO (SHA)

En este capítulo analizaremos el primero de los elementos que integran el método de firma electrónica que se estudia en este trabajo. Este análisis lo iniciaremos conociendo qué son los procesos de resumen digital y cuáles son los principales que se han utilizado en la historia. Posteriormente nos adentraremos en el funcionamiento específico del algoritmo *hash* seguro (SHA, por sus siglas en inglés). Luego veremos algunos ejemplos prácticos del funcionamiento de este algoritmo. Y finalmente lo contrastaremos con las exigencias del Código de Comercio en materia de firma electrónica avanzada, para comprobar si cumple con éstas.

I.- Generalidades de los procesos de resumen digital

Los procesos de resumen digital son aquellos mecanismos criptográficos utilizados en la informática moderna que –además de codificar un mensaje–, tienen como característica principal el convertirlos a una cantidad específica y limitada de caracteres, con independencia de la longitud del texto original.

Estos métodos cifran el mensaje original. En decir, convierten en el texto original en una serie de caracteres ininteligibles a simple vista. Por ello podemos decir que se trata de mecanismos criptográficos. Sin embargo, tienen dos características peculiares que vale la pena analizar: son métodos que suelen efectuarse mediante un código o algoritmo abierto al público y son métodos criptográficos irreversibles.

1.- *Algoritmos abiertos al público*

Es importante inicialmente precisar qué son los algoritmos, pues vamos a utilizar dicho concepto de forma frecuente en los siguientes párrafos. Pues bien, la palabra algoritmo se define como un “conjunto ordenado y finito de operaciones que permite hallar la solución de un problema” y como un “método y notación en las distintas

formas del cálculo".[122] En el ámbito informático los algoritmos son elementos básicos de la programación, mediante los cuales se redactan las instrucciones precisas conforme a las cuales se ejecutará un programa de cómputo y se procesará la información en apego a las instrucciones del usuario y según se vayan dando las circunstancias previstas.

Volviendo a nuestro tema principal, hemos mencionado que los métodos de resumen digital suelen dejar abiertos al público los respectivos algoritmos que se utilizan para su generación. Como se verá en el apartado siguiente, desde hace muchos años se han divulgado en forma abierta estos algoritmos para su uso general.

La razón de esto es que, aunque son mecanismos criptográficos, la principal finalidad de los procesos de resumen digital no ha sido ocultar y transmitir mensajes a través de canales inseguros, sino servir como un paso previo, en el que se convierten los mensajes originales en un conjunto de caracteres de tamaño específico y limitado, para aplicar posteriormente un método criptográfico más sólido, utilizable de muchas maneras. Así pues, el principal uso de los métodos de resumen digital es como parte de procesos de autenticación de comunicaciones y no su simple ocultamiento.[123] Por lo tanto, no ha sido necesario ocultar el algoritmo mediante el cual se efectúan estos resúmenes digitales.

2.- *Procesos irreversibles*

Ahora veremos por qué decimos que los procesos de resumen digital son irreversibles. La irreversibilidad de estos mecanismos criptográficos estriba en el hecho de que solo pueden utilizarse para encriptar los mensajes, mas no para desencriptarlos. Esto los diferencia de otros mecanismos criptográficos que permiten ambas operaciones, tanto encriptación como desencriptación.

---

[122] Real Academia Española, *op. cit.*, voz: algoritmo.
[123] Como se recordará, en el apartado C del capítulo 2 de esta obra se habló de la criptografía moderna como mecanismo de autenticación de comunicaciones.

Un mecanismo criptográfico se vuelve irreversible debido a la imposibilidad técnica de volver atrás su algoritmo de cifrado para poder descifrar un mensaje. Esto puede suceder porque la reversión del algoritmo requiera de un cómputo de imposible realización con los métodos informáticos modernos o porque al momento de ejecutarse el algoritmo se pierda de forma irremediable cierta información, lo cual impide la recuperación íntegra del mensaje original.

Esto último es precisamente lo que sucede en el caso de los algoritmos de resumen digital, pues para convertir cualquier mensaje –independientemente de su longitud– en una cadena de caracteres de extensión específica, se pierde irremediablemente la mayor parte de la información necesaria para reintegrar el mensaje original.

A simple vista, pudiera parecer absurdo cifrar un mensaje de forma que no se pueda descifrar nunca y utilizar un método de encriptación que nos llevará a perder la mayor parte de la información integrante del mensaje original.

Sin embargo, estos mecanismos de cifrado son de mucha utilidad práctica. Lo explicaremos enseguida.

En la actualidad se generan documentos electrónicos de gran extensión o con una gran cantidad de datos incrustados[124]. Esta situación genera archivos informáticos de tamaño grande, que requieren de muchos *megabytes* de memoria. Y para cifrar documentos tan grandes se requiere de un proceso de cómputo muy lento.[125]

Así, los procesos de resumen digital se convierten en una solución para dicho problema, pues permiten reducir de manera segura el mensaje original a uno de tamaño mucho menor que, nuevamente puede ser rápidamente cifrado mediante algún otro método de encriptación.[126]

[124] Como pudieran ser tablas, imágenes, entre otras.
[125] León Tovar, Soyla H. *et al*, *op. cit.*, p. 221.
[126] *Idem.*

II.- El proceso de resumen digital mediante algoritmo *hash* seguro (SHA)

En este apartado efectuaremos el análisis del algoritmo *hash* seguro (SHA). Para ello, vamos a repasar brevemente la historia de algunos algoritmos desarrollados previamente. Enseguida conoceremos cuáles han sido las versiones históricas del algoritmo SHA, la literatura científica en la cual se encuentran descritos, así como sus principales características técnicas.

1.- *Los antecedentes: algoritmos MD*

Los primeros algoritmos de resumen digital que demostraron buena funcionalidad fueron los desarrollados por Ronald Rivest, reconocido criptógrafo y profesor del Instituto Tecnológico de Massachussets (MIT, por siglas en inglés).

Estos algoritmos se denominaron "*Message-Digest Algorithms*",[127] y son conocidos por el acrónimo MD que se acompaña con el respectivo número de versión. Los algoritmos más utilizados fueron MD2, MD4 y MD5.

Todos estos algoritmos fueron divulgados en abril de 1992 mediante diversos memorandos publicados por el Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés), aunque han sido actualizados en diversas ocasiones.

El algoritmo MD2 fue dado a conocer mediante el memorando RFC 1319[128] publicado por el. Este estándar ha sido actualizado en diversas ocasiones, siendo su última versión la que se ha descrito en el memorando RFC 6149[129] publicado por el IETF.

Por su parte, el algoritmo MD4 fue publicado originalmente en el memorando 1320 del IETF.[130] Su última actualización fue dada a conocer en el memorando 6150 del IETF.[131]

---

[127] En español: Algoritmos de resumen de mensajes.
[128] IETF, *memorando RFC 1319*, consultable en la página de internet de dicho organismo en la dirección https://datatracker.ietf.org/doc/rfc1319/.
[129] El memorando RFC 6149 se encuentra consultable en la página de internet del IETF, en la dirección https://datatracker.ietf.org/doc/rfc6149/.
[130] Consultable en el sitio de internet del IETF en la dirección https://datatracker.ietf.org/doc/rfc1320/.
[131] Consultable en el sitio de internet del IETF en la dirección https://datatracker.ietf.org/doc/rfc6150/.

Y finalmente tenemos el algoritmo MD5 que fue el que alcanzó más uso y popularidad entre los desarrollados por Ronald Rivest. Fue publicado en el memorando RFC 1321 del IETF[132] y su última actualización se publicó en el memorando RFC 6151.[133]

La seguridad de estos algoritmos la entendemos si pensamos en que para obtener dos mensajes que generen el mismo resumen digital se requieren 2^64,[134] operaciones y que para dar con un mensaje original a partir de un resumen digital dado se requieren efectuar 2^128[135] operaciones.[136] Esta seguridad era muy alta para la época en que se originaron estos algoritmos, pues resultaba imposible para una computadora de aquella época buscar obtener un mismo resumen digital a partir de un segundo mensaje. Actualmente los algoritmos MD2 y MD4 han quedado obsoletos, pues la computación actual permite que sean vulnerados de una manera relativamente fácil.

El algoritmo MD5 sigue siendo útil, pero su nivel de seguridad ha sido superado por algoritmos como el denominado “SHA”. Al respecto, resulta muy claro el comentario que hace Ariel Maiorano:

> En el año 1996, se descubrió un problema en el diseño de MD5. No se trataba de un problema o falla crítica, que volviese inseguras las implementaciones actuales, pero distintos expertos y criptógrafos propusieron la utilización de otros algoritmos de *hashing* criptográfico. Durante el año 2004, otros problemas más importantes fueron descubiertos y la seguridad del protocolo fue puesta en tela de juicio. Por último, un grupo de investigadores describió, en el año 2007, cómo es posible la confección de dos archivos distintos que generan el mismo *hashing* MD5.
>
> Ninguno de estos problemas citados implica que las implementaciones actuales de *checksums* o de registros de contraseñas mediante *hashes* (las dos aplicaciones más populares del algoritmo actualmente) se hayan vuelto vulnerables. Al menos por ahora, no se ha descubierto una técnica que perita obtener la entrada original a partir de *hash* o alterar a discreción un archivo (salvo en las pruebas citadas, sobre archivos de contenido particularmente seleccionados) y mantener su *checksum* o *hash* MD5 resultante. La recomendación de cualquier manera, es la de la implementación de otro algoritmo, como SHA-1, que veremos en el siguiente apartado.[137]

---

[132] Consultable en el sitio de internet del IETF en la dirección https://datatracker.ietf.org/doc/rfc1321/.
[133] Consultable en el sitio de internet del IETF en la dirección https://datatracker.ietf.org/doc/rfc6151/.
[134] Esta es una manera de describir cantidades muy grandes. En este caso significa elevar 2 a la 64 potencia, lo que da un resultado de 18,446,744,073,709,600,000.
[135] Es decir 340,282,366,920,938,000,000,000,000,000,000,000,000.
[136] Véase el memorando RFC 1319, parágrafo 4.
[137] Maiorano, Ariel, *op. cit.*, pp. 54 y 55.

2.- ***El proceso de resumen digital mediante algoritmos hash seguros (SHA)***

Tras el éxito de los algoritmos MD, en el año 1993 el Instituto Nacional de Normas y Tecnología de los Estados Unidos de Norteamérica (NIST, por sus siglas en inglés) desarrolló un algoritmo de resumen digital denominado "algoritmo *hash* seguro", mejor conocido como "SHA" por sus siglas en inglés. Este algoritmo se considera "más potente"[138] que el algoritmo MD.

En la actualidad se han hecho públicos cuatro algoritmos "SHA":

1. El algoritmo original, denominado SHA-0.
2. El algoritmo SHA-1.
3. El algoritmo SHA-2, que comprende los subalgoritmos SHA-224, SHA-256, SHA-384 y SHA-512, que a su vez incluye las especies SHA-512/224 y SHA-512/256.
4. El algoritmo SHA-3 que a su vez comprende los subalgoritmos SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 y SHAKE256.

La primera versión de este algoritmo, conocida como "SHA-0", ha quedado obsoleta, por lo que ha sido sustituida por las versiones posteriores.

Las versiones vigentes de este algoritmo son SHA-1, SHA-224, SHA-256, SHA-384 y SHA-256, mismas que se encuentran documentadas en el memorando "FIPS PUB 180-4" del Instituto Nacional de Normas y Tecnología de los Estados Unidos de Norteamérica.[139]

Cabe señalar que la versión SHA-1 también se encuentra documentada en el memorando RFC 3174 del IETF.[140] El resto de las versiones del algoritmo SHA

[138] León Tovar, Soyla H. y otros, *op. cit.*, p. 221.
[139] Consultable en el sitio de internet de dicho instituto en la dirección electrónica https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910977.
[140] Consultable en el sitio de internet de dicho organismo en la dirección electrónica https://datatracker.ietf.org/doc/rfc3174/.

se documentaron también en el memorando RFC 4634 del IETF.[141] La última actualización de ambos documentos la encontramos publicada en el memorando 6234 del IETF.[142]

Finalmente, tenemos que el estándar SHA-3 se publicó en el memorando "FIPS PUB 202" del Instituto Nacional de Normas y Tecnología de los Estados Unidos de Norteamérica.[143]

El proceso de resumen digital mediante los algoritmos SHA inicia tomando el mensaje original (texto en claro), mismo que debe estar forma de archivo informático y contenido en algún medio óptico, electrónico o de cualquier otra tecnología. La necesidad de que el mensaje se encuentre en estas formas se debe a que el proceso de resumen digital es altamente complejo y sólo se puede efectuar a través de algún dispositivo de cómputo moderno.

El mensaje original puede encontrarse en formato de texto, imagen, audio, video, o cualquier otro. Para efectos del algoritmo SHA, resulta indiferente el formato del mensaje original, pues éste se toma en su forma de archivo informático, es decir un conjunto de bits (dígitos binarios) que están almacenados en un dispositivo.

Los algoritmos SHA se desarrollan en dos etapas: la etapa de procesamiento y la etapa de cálculo *hash* o de resumen digital.

La etapa de preprocesamiento consiste en lo siguiente:

1. Rellenar el mensaje con los bits adicionales que sean necesarios para llegar a un múltiplo de un número previamente definido.
2. Una vez que se ha rellenado el mensaje y tiene la extensión adecuada, los bits que lo integran son agrupados en bloques de tamaño previamente definido.

[141] Consultable en el sitio de internet de dicho organismo en la dirección electrónica https://datatracker.ietf.org/doc/rfc4634/.
[142] Consultable en el sitio de internet de dicho organismo en la dirección electrónica https://datatracker.ietf.org/doc/rfc6234/.
[143] Consultable en el sitio de internet de dicho instituto en la dirección electrónica https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919061.

3. Se establecen valores de inicialización (como la longitud del mensaje, entre otros) que serán utilizados en el cálculo del resumen digital.
4. El resultado de esta etapa se denomina “mensaje relleno”, que es un conjunto de bloques de bits, bien definidos conforme al estándar SHA aplicado

La etapa del cálculo *hash* o de resumen digital consiste en aplicar al mensaje relleno complejísimas fórmulas matemáticas para obtener un nuevo y diferente mensaje, un resumen digital compuesto de un número previamente definido de bits. En cada estándar, el número de bits resultante siempre será el mismo.

Las características de estos resúmenes digitales son las siguientes:

a) La longitud del resumen digital siempre será de una longitud fija, sin importar cuál haya sido la longitud o las características del mensaje original.
b) En teoría, es prácticamente imposible encontrar otro texto en claro que dé como resultado un mismo resumen digital.[144]
c) Es imposible revertir el algoritmo para llegar al texto en claro a partir del resumen digital.

Las fórmulas matemáticas de cada uno de los estándares SHA se encuentran descritas de manera exacta y detallada en cada uno de los memorandos arriba referidos.

No es el objetivo de este trabajo describir ni comprobar dichas fórmulas, pero al respecto sí diremos que el diseño matemático de cada uno de estos algoritmos SHA tomó muchos años de investigación científica por parte de instituciones altamente calificadas. Por ello, la calidad científica de estos estándares informáticos está bien demostrada, es accesible a todo el público y es reconocida por la comunidad científica.

Desde el inicio de su desarrollo y hasta la fecha, los creadores de estos estándares y la comunidad científica en general se han ocupado en probar

[144] En informática, a esto se le conoce como un problema intratable, porque, aunque matemáticamente es viable llegar a un mismo resumen digital a partir de una mensaje diverso al original, esto no se puede lograr en la realidad práctica con los recursos informáticos de la época.

intensamente los algoritmos, para buscar posibles errores o vulnerabilidades informáticas. Estas pruebas se han hecho cada vez más robustas, debido al uso permanente de las más nuevas tecnologías informáticas que permiten realizar cálculos cada vez más avanzados y rápidos sobre los algoritmos SHA.

Con base en estas pruebas, sólo se han detectado vulnerabilidades graves en el primitivo algoritmo SHA-0, por lo que actualmente se desaconseja su uso.

El 23 de febrero de 2017, la empresa de informática Google y el CWI Institute in Amsterdam anunciaron que, como resultado de sus investigaciones, habían encontrado por primera vez una vulnerabilidad en el algoritmo SHA-1. Es significativo destacar que este hallazgo científico se dio hasta 20 años después de la presentación del algoritmo. Aunque esta vulnerabilidad es mínima y sólo podría ser explotada –con escasos o nulos beneficios– por las corporaciones más poderosas en tecnologías de la información, la comunidad científica, siempre prudente, ya empieza a aconsejar migrar del uso del algoritmo SHA-1 a otros más robustos como SHA-256 y SHA-3.[145]

III.- Ejemplo de un documento jurídico resumido digitalmente mediante algoritmo hash seguro (sha)

Para ejemplificar el uso del algoritmo “sha” podemos utilizar cualquier documento mercantil que típicamente se genere en forma impresa y se suscriba autógrafamente, como podría ser un contrato, un acta o un título de crédito. Pero, para mayor simplicidad y mejor entendimiento, utilizaremos como ejemplo un documento mercantil muy sencillo y con el que todos estamos familiarizados: un pagaré.

En la *ilustración 1* se muestra el un pagaré que es el mensaje original. A este pagaré le aplicaremos el algoritmo SHA-256, obteniendo como resultado el resumen digital que se muestra en la parte inferior la misma *ilustración*.

[145] Stevens, Marc *et al*, “Announcing the first SHA1 collision”, en *Google Securyty Blog*, 23 de febrero de 2017, consultable en la dirección electrónica https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html.

Como podemos ver, con independencia del tamaño del mensaje original, el resultado es un resumen digital de 64 bits.

Aun cuando se repita la operación informática varias veces, sobre el mismo mensaje original, y con el mismo algoritmo SHA-256, siempre resultará el mismo resumen digital.

Con esta utilidad, el algoritmo *hash* ayuda a comprobar la integridad del mensaje original, porque el destinatario puede aplicar el algoritmo al mensaje original, para verificar que el resultado sea precisamente el resumen digital que se le envía.

Para que esto quede más claro, podemos alterar intencionalmente el pagaré antes utilizado, para demostrar que será totalmente distinto el resumen digital resultante. Y como resultado tenemos un nuevo pagaré, cuya visualización se reproduce en la *ilustración 2*. La alteración consiste en cambiar el monto amparado por el pagaré de $5,000.00 a $15,000.00, así como modificar la tasa de intereses moratorios de un 1% a un 11% mensual.

Aunque estas modificaciones se pudieran apreciar solo como la adición de un dígito, respectivamente, al importe principal y a la tasa de interés previstos en el pagaré, al aplicarle el algoritmo SHA-256 a este nuevo pagaré obtenemos como resultado un diverso resumen digital, de la misma longitud de 64 bits, pero muy distinto al del primer pagaré. Este nuevo resumen digital también lo podemos apreciar en la parte inferior de la *ilustración 2*.

Esto nos demuestra como el algoritmo SHA-256 cumple con las características informáticas mencionadas en párrafos anteriores.

Y como lo adelantábamos hace un momento, estas funcionalidades del algoritmo *hash* analizado tienen una utilidad muy práctica en la seguridad informática, pues permiten verificar la integridad del mensaje original, ya que cualquier alteración en el mensaje de datos original implicaría la generación de un resumen digital muy distinto al resumen digital del mensaje original.

Sobre esto, debe insistirse que actualmente es técnicamente imposible encontrar de manera intencional un mensaje de datos diverso que arroje un

resumen digital idéntico al del mensaje original, por lo que el algoritmo SHA-256 resulta fiable.

Por supuesto que aún queda pendiente la verificación de la autoría del mensaje de datos, por lo que el uso simple del algoritmo *hash* no impide la posibilidad de que se generen y atribuyan dos mensajes en claro con sus respectivos resúmenes digitales, generando la confusión de cuál es el verdaderamente generado por el emisor. Sin embargo, esta problemática se resuelve con el uso del método RSA que se analizará en el siguiente capítulo.

Ilustración 1

MENSAJE ORIGINAL
PAGARÉ Número 1/2 Bueno por $5,000.00 Morelia, Michoacán, a 16 de agosto de 2018. Debo y pagaré incondicionalmente a la orden de MARÍA DE GUADALUPE RAMÍREZ GONZÁLEZ, en Morelia, Michoacán, el día 15 de diciembre de 2018, la cantidad de $5,000.00, valor recibido a mi entera satisfacción. Este pagaré forma parte de una serie numerada del 1 al 2 y todos están sujetos a la condición de que, al no pagarse cualquiera de ellos a su vencimiento, serán exigibles todos los que le sigan en número, además de los ya vencidos, desde la fecha de vencimiento de este documento hasta el día de su liquidación. Este pagaré causará intereses moratorios al tipo del 1 % mensual, pagaderos en esta ciudad juntamente con el principal. ACEPTO: JAVIER MARTÍN ESCAMILLA BÁEZ
RESUMEN CON SHA-256
D4CE329E4B9EDF5EDB43610A30D0CA222DBC4D1C80BA2E9317536F50EEBA2A90

Ilustración 2

MENSAJE ORIGINAL
PAGARÉ Número 1/2 Bueno por $15,000.00 Morelia, Michoacán, a 16 de agosto de 2018. Debo y pagaré incondicionalmente a la orden de MARÍA DE GUADALUPE RAMÍREZ GONZÁLEZ, en Morelia, Michoacán, el día 15 de diciembre de 2018, la cantidad de $15,000.00, valor recibido a mi entera satisfacción. Este pagaré forma parte de una serie numerada del 1 al 2 y todos están sujetos a la condición de que, al no pagarse cualquiera de ellos a su vencimiento, serán exigibles todos los que le sigan en número, además de los ya vencidos, desde la fecha de vencimiento de este documento hasta el día de su liquidación. Este pagaré causará intereses moratorios al tipo del 1 % mensual, pagaderos en esta ciudad juntamente con el principal. ACEPTO: JAVIER MARTÍN ESCAMILLA BÁEZ
RESUMEN CON SHA-256
B00096433264C656C8C3A4C66A9CEC77A9EF2A7D233D20EE5A24011710556FA9

CAPÍTULO CUARTO
EL MÉTODO DE ENCRIPTACIÓN “RSA”

En este capítulo analizaremos el método de encriptación con clave pública denominado “RSA”. Para poder entender este mecanismo criptográfico resultará necesario hacer un breve análisis sobre los métodos de criptografía con clave pública en general, incluyendo un repaso histórico de sus antecedentes. Posteriormente procederemos a revisar el estándar informático que describe este método criptográfico y ejemplificaremos su aplicación en un documento mercantil.

I.- Los métodos criptográficos de clave pública

En el capítulo 3 de este trabajo, ya analizábamos de manera básica los mecanismos informáticos de criptografía modernos y su uso para la seguridad informática. En este contexto, tenemos que los métodos informáticos más avanzados de criptografía son los que se basan en una infraestructura de clave pública.

Estos métodos se diseñaron con la finalidad de reforzar la secrecía en el intercambio de mensajes cifrados, resolviendo la añeja problemática que representaba la posibilidad del robo de la clave utilizada entre el emisor y el destinatario.

En efecto, durante siglos la fortaleza de todos los mecanismos tradicionales de cifrado era la clave que utilizarán para cifrar sus mensajes. Cuanto más compleja y dinámica fuera la clave acordada por el emisor y el destinatario, más difícil resultaba para un tercero extraño descifrar el documento. Sin embargo, en el momento en que el tercero se lograba apoderar de la clave, el mecanismo criptográfico quedaba inútil, pues todos los mensajes intercambiados conforme al mismo ya podían ser descifrados fácilmente por el intruso.

Esta problemática se empezó a resolver con la criptografía de clave pública, también llamada asimétrica, la cual utiliza una clave compuesta a su vez de dos claves, una pública y una privada. La clave pública es conocida por el emisor y por el destinatario –y eventualmente por cualquier otra persona– y sirve para cifrar

mensajes, sin poder descifrarlos. La clave privada es sólo conocida por el destinatario, que sirve para descifrar los mensajes.

Estas claves son únicas e irrepetibles, y se pueden generar cuantas sean necesarias. Las claves consisten en números de gran tamaño, generados en base a fórmulas matemáticas muy complejas, que no pueden ser revertidas ni con la más avanzada computación moderna. Así que técnicamente no es posible deducir las claves privadas de ninguna manera, ni siquiera a partir del mensaje cifrado, pues el mecanismo matemático para hacerlo se considera un problema intratable.

Enseguida analizaremos algunas de las características principales de este tipo de criptografía moderna.

1.- *Criptografía asimétrica*

Se dice que esta criptografía es asimétrica porque los procesos de encriptación y desencriptación requieren de sus respectivas y diversas claves o llaves.

En efecto, en la criptografía de clave pública, el emisor encripta el mensaje con una llave y el destinatario lo desencripta con una llave diversa, que solo él posee. Esta característica hace más seguro este método, pues la clave para desencriptar –desde su generación– solo la posee el destinatario.

Ello a diferencia de los métodos tradicionales de criptografía, llamados simétricos, que requieren de la misma clave para encriptar y desencriptar los mensajes.

2.- *Proceso reversible*

Contrario a lo que sucede en métodos criptográficos como el resumen digital analizado en el capítulo anterior, la criptografía con clave pública es un proceso reversible, ya que en este caso sí existe la posibilidad de desencriptar y recuperar íntegramente el mensaje original.

De ahí que este método sea muy útil para fines de conservación, transmisión y recuperación de mensajes confidenciales.

Sin embargo, debe tomarse en cuenta que, dada su complejidad, estos procesos de encriptación y desencriptación, suelen ser de ejecución muy prolongada, conforme se trate de archivos informáticos más grandes.

3.- *Estándar público*

Los más importantes métodos criptográficos de clave pública se encuentran descritos en documentos disponibles por el público en general, por lo que cualquier persona puede implementarlos libre y directamente con la tecnología adecuada.

Pero lo anterior no les resta efectividad como métodos criptográficos, ya que cada usuario genera de manera secreta su propia e irrepetible clave privada, que no puede ser deducida por ningún intruso aun cuando conozca el estándar en base al que fue generada.

II.- La firma electrónica avanzada basada en métodos criptográficos de clave pública

No obstante la notable aportación que han generado los métodos criptográficos de clave pública para la transmisión de mensajes confidenciales, probablemente su mayor utilidad se ha encontrado en el campo de la firma electrónica, como mecanismos para validar la autoría y la integridad de documentos e información de todo tipo: desde los documentos jurídicos más formales, programas informáticos de todo tipo, hasta los datos de transacciones financieras muy cuantiosas.

Sin haber sido el objetivo inicial, con algunas variantes, se vio que era posible utilizar los métodos de clave pública para que el emisor utilizará esta criptografía a fin de garantizarle al destinatario que él había generado el mensaje encriptado y estaba de acuerdo con lo plasmado en el mismo.

Como mecanismo de firma electrónica los métodos de clave pública funcionan también utilizando una clave compuesta a su vez de dos claves, una pública y una privada. En este caso la clave pública, conocida por el emisor y por el destinatario –y eventualmente por cualquier otra persona–, sirve para descifrar

mensajes, sin poder cifrarlos. La clave privada es sólo conocida por el emisor, y sirve para cifrar los mensajes.

Nuevamente las claves son únicas e irrepetibles, y se pueden generar cuantas sean necesarias, de la misma manera que se hace para fines de confidencialidad.

De igual manera, es técnicamente imposible deducir las claves privadas de ninguna manera, ni siquiera a partir del mensaje cifrado, pues el problema matemático implicado se considera intratable.

Como podemos ver, la firma electrónica de clave pública se basa en los mismos principios de la criptografía de clave pública, con una sola variante: la clave que se publica en los métodos de firma electrónica es la necesaria para encriptar y no la que se requiere para desencriptar. La razón es muy simple, pues en el caso de la firma electrónica no es prioritario el ocultamiento del mensaje, sino la garantía de que solo los puede encriptar el emisor. Esta garantía, fundada en el uso exclusivo de la clave privada de encriptación por parte del emisor, es la que genera la confianza de que es el autor del mensaje y está conforme con sus términos y consecuencias.[146]

Por supuesto que es posible combinar ambos usos de los métodos de clave pública: la validación y el ocultamiento de los mensajes. Ello mediante diversos esquemas de combinación e intercambio de las claves públicas y privadas entre las partes.

Enseguida revisaremos las principales características de este método avanzado de firma electrónica.

1.- *Correspondencia exclusiva de los datos de creación*

Como lo hemos mencionado, la firma electrónica basada en criptosistemas de clave pública funciona en base a archivos informáticos, llamados claves, que son únicos e irrepetibles, generados por las partes.

[146] Sobre esta variante del método criptográfico general, véase León Tovar, Soyla H. *et al*, *op. cit.*, México, Oxford, 2006, p. 219.

Por esta razón, se puede afirmar técnicamente que determinada clave privada corresponde única y exclusivamente a cada usuario, sin que exista la posibilidad técnica de que otro usuario cuente con una clave privada idéntica, generando confusión.

2.- Control exclusivo de los datos de creación

En estos criptosistemas las claves privadas de las partes se generan de manera totalmente secreta, sin dejar rastros en el programa informático que se utilizó para la generación. Además, en la actualidad es técnicamente imposible que una persona no autorizada descubra dichas claves privadas ni siquiera teniendo en su poder el mensaje transmitido o las claves públicas.

Tomando en cuenta esto, podemos decir que estos métodos de firma electrónica permiten que cada parte controle absolutamente los datos que requiere para encriptar y firmar sus mensajes.

Por supuesto que resulta necesario que el emisor implemente cuantas medidas de seguridad sean necesarias para que ninguna otra persona acceda a sus claves privadas. Por ello, la mayoría de estos sistemas de firma electrónica contemplan la posibilidad de que las partes revoquen sus claves privadas, dando aviso de ello a las demás partes, cuando ha perdido el control exclusivo sobre las mismas. Pero en caso de que no se tomen todas estas medidas preventivas o no se revoquen las claves privadas, el titular de las claves queda responsable de los posibles malos usos que se haga de las mismas.

Cabe señalar que para reforzar el control exclusivo sobre las claves privadas, en algunos de estos criptosistemas se incluye el uso de contraseñas privadas, generadas por los propios usuarios para poder utilizar las claves privadas. Ello permite que aún en el caso de que se pierda la clave privada, esta no pueda ser usada por terceras personas que no conozcan la correspondiente contraseña.

3.- *Garantía de integridad del mensaje y la firma*

Al ser reversible este método criptográfico de firma electrónica, es posible reconstruir el mensaje original desencriptándolo mediante el uso de la clave pública del emisor. Al llevar a cabo esta operación, el destinatario puede verificar cuál era el contenido del mensaje que firmó el destinatario y si efectivamente se trata del que se le está presentando.

Este método criptográfico descarta la posibilidad de que se haga pasar como bueno un mensaje alterado.

III.- El método de encriptación "RSA"

En este apartado analizaremos el estándar informático para encriptación llamado "RSA" y su especial aplicación práctica como mecanismo de firma electrónica. Para ello, haremos un breve repaso histórico de los antecedentes y el surgimiento del método "RSA". Posteriormente revisaremos los principales documentos en los que se describe el estándar "RSA". Y finalmente veremos cómo funciona este estándar en la práctica del derecho mercantil mexicano.

1.- *Nota histórica*

Es muy probable que los primeros métodos de encriptación con clave pública se diseñaran en el interior de los organismos militares o de inteligencia de los países más desarrollados de mediados del siglo XX. Esto debido a la necesidad en la época de contar con un sistema asimétrico que redujera el riesgo de interferencias en las comunicaciones a causa de la pérdida de la clave del sistema.[147] En tal caso, las investigaciones de estos métodos seguramente se mantuvieron en secreto por su propia naturaleza.

[147] Véase Ortega Triguero, Jesús J *et al*, *op. cit.*, p. 228.

Sin embargo, el primer trabajo que se conoció públicamente sobre el tema fue el de Whitfield Diffie y Martin Hellman, quienes expusieron por primera vez un método de criptografía asimétrica en el año 1976.[148] En este trabajo se introdujo por primera vez el concepto de un criptosistema de clave pública. Este criptosistema de conoció como el protocolo Diffie-Hellman.

En agosto de 1977 se publicó un artículo en la revista *Scientific American*, donde se reportaba el desarrollo de un nuevo criptosistema de clave pública por parte de Ronald L. Rivest. Adi Shamir y Leonard Adleman, científicos del *Massachusetts Institute of Technology* (MIT). Este sistema se basaba en el protocolo Diffie-Hellman, utilizando números primos para robustecerlo.[149] Tomando en cuenta los avances científicos de esa época, en este artículo se presentaba dicho criptosistema como "una nueva clase de cifrado que tomaría millones de años para ser roto".[150]

Este sistema, que a la postre se conocería como "RSA" por los nombres de sus creadores, fue patentado en los Estados Unidos de Norteamérica en el año de 1983.[151]

A partir de entonces, el sistema criptográfico de clave pública RSA se ha convertido en el más utilizado como método de cifrado de información de todo tipo y de firma electrónica. Como veremos en el siguiente apartado, el estándar RSA ha sufrido diversas actualizaciones y mejoras, que han quedado documentadas hasta las más modernas versiones. Las versiones vigentes, siguen siendo seguras, pues no existe en la actualidad ninguna computadora capaz de vulnerarlo, deduciendo las claves privadas a partir de los mensajes cifrados.

2.- *Descripción del estándar RSA*

---

[148] Diffie, Withfield y Hellman, Martin, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, volumen IT-22, número 6, Estados Unidos de Norteamérica, noviembre de 1976, pp. 644 a 654. Consultable en https://ee.stanford.edu/~hellman/publications/24.pdf.
[149] Gardner, Martin, "Mathematical Games", *Scientific American*, volumen 237, número 2, Estados Unidos de Norteamérica, agosto de 1977, pp. 122 a 124.
[150] *Ibidem*, p. 122.
[151] Rivest, Ronald L. y otros, *Patente de los Estados Unidos de Norteamérica número 4,405,829*, 20 de septiembre de 1983.

El estándar RSA se encuentra descrito básicamente en los siguientes documentos:

- En la patente número 4,405,829, registrada en los Estados Unidos de Norteamérica por los científicos Rivest, Shamir y Adleman.
- En el memorando RFC 8017 del Internet Engineering Task Force (IETF), relativo al estándar de criptografía de clave pública #1 (PKCS #1): especificaciones de criptografía RSA, versión 2.2.

En estos documentos se describe de manera general el funcionamiento técnico del criptosistema RSA, siendo la versión más actualizada la que se consigna en el memorando RFC 8017.

Siguiendo la descripción técnica RFC 8017, tenemos que el criptosistema RSA vigente se lleva a cabo en tres etapas generales: la generación de las claves, la generación de la firma electrónica y la verificación de la firma electrónica. Enseguida revisaremos cada una de ellas.

Como lo hemos mencionado anteriormente, el criptosistema requiere de dos claves: una privada y una pública.

La clave privada está integrada por componentes. Uno llamado módulo RSA y otro llamado exponente público RSA. El módulo RSA es un número entero que es el producto de multiplicar números primos muy grandes. Mientras que el exponente público RSA es un número entero entre 3 y el módulo RSA menos uno, debiendo satisfacer diversas condiciones matemáticas complejas.[152]

La clave pública se integra también por dos componentes: el módulo RSA y el exponente privado. El módulo RSA es el mismo que forma parte de la clave pública. El exponente privado es un número entero menor que el módulo RSA, debiendo satisfacer diversas condiciones matemáticas.[153]

---

[152] IETF, *Memorando RFC 8017 estándar de criptografía de clave pública #1 (PKCS #1): especificaciones de criptografía RSA, versión 2.2*, 2016, pp. 8 y 9, consultable en la página de internet de dicho organismo https://www.rfc-editor.org/pdfrfc/rfc8017.txt.pdf.
[153] *Ibidem*, pp. 9 y 10.

Con la clave pública y privada y mediante el uso de *hardware* y *software* apropiados, se pueden realizar los mecanismos criptográficos para la generación y verificación de la firma electrónica. No es posible efectuar estos procesos criptográficos sin ayuda de una computadora adecuada.[154]

La firma electrónica se genera cuando se cifra un mensaje mediante la correspondiente clave privada. Esta firma electrónica se puede validar descifrando el mensaje mediante la correspondiente clave pública. Ambos procesos informáticos implican la misma operación matemática, que principalmente es la exponenciación.[155]

[154] Véase *ibidem*, p. 12.
[155] *Ibidem*, pp. 12 a 17.

CAPÍTULO QUINTO
EL FUNCIONAMIENTO CONJUNTO DEL RESUMEN DIGITAL CON ALGORITMO HASH SEGURO (SHA) Y EL MÉTODO DE ENCRIPTACIÓN "RSA"

I.- Funcionamiento conjunto de los estándares SHA y RSA

Los estándares de seguridad informática analizados en los capítulos anteriores pueden utilizarse de manera complementaria. De hecho, su uso combinado genera el más efectivo y eficiente proceso de firma electrónica avanzada que existe en la actualidad. Enseguida analizaremos cómo se lleva a cabo la combinación de estos procesos informáticos y las ventajas que se obtienen frente a su uso individual.

El proceso se inicia ingresando el archivo informático que contiene el mansaje original, ya sea en formato de texto plano, en formato PDF o en cualquier otro formato. De cualquier manera, la computadora con la que se realiza el proceso sólo tomará el archivo como una serie de bits, sin analizarlos de ninguna manera.

Una vez ingresada la cadena de bits, la computadora aplica el proceso de resumen digital analizado en el capítulo 3 de este trabajo. Con el algoritmo seguro *hash* se genera como resultado una cadena de bits de longitud previamente determinada y que técnicamente es imposible de repetir a partir de un mensaje original diverso.

Al resumen digital obtenido, se le aplica el método de encriptación "RSA". Para ello, el firmante o emisor utiliza su llave privada. Con ello se obtiene como resultado un mensaje encriptado que puede ser desencriptado mediante la llave pública, que se distribuye previamente entre el o los destinatarios de los mensajes firmados. Como se explicó en el capítulo 4 de este trabajo, es técnicamente imposible deducir la llave privada a partir del mensaje encriptado de la llave pública, con lo que se garantiza que el titular de la llave pública es realmente el autor del mensaje, sin posibilidades de suplantación.

El mensaje encriptado, junto con el mensaje original se envía al destinatario.

Una vez recibido el mensaje encriptado, el destinatario utiliza la llave pública del emisor para desencriptar el mensaje. Como resultado obtendrá el resumen digital del mensaje original.

Asimismo, el destinatario procede a tomar el mensaje original recibido y le aplica el mismo algoritmo seguro *hash* que utilizó el emisor en su proceso. Como resultado obtendrá nuevamente un resumen digital.

Una vez hecho lo anterior. el emisor debe comparar ambos resúmenes digitales, y de ser idénticos queda validada la firma electrónica. Si los mensajes digitales fueran diferentes, se trata de una suplantación del emisor o de una alteración del documento firmado.

Al combinarse ambos estándares se suman sus utilidades y fortalezas informáticas, además de que se logra una mayor velocidad de procesamiento de la firma electrónica. Esto es así porque la aplicación directa del método RSA para encriptar y desencriptar los mensajes de datos requiere mayor tiempo de procesamiento en la medida en que se trata de mensajes con más bits de longitud. De hecho, los archivos que contienen documentos de muchas páginas llegan a requerir muchos minutos o hasta horas de procesamiento informático. Sin embargo, al resumirse digitalmente los mensajes de datos antes de encriptarlos, el proceso informático total de firma electrónica apenas toma unos segundos, aún tratándose de documentos muy grandes.

II.- Ejemplos de documentos jurídicos firmados electrónicamente con los estándares “SHA-256” y “RSA”

Para ejemplificar el funcionamiento conjunto de los métodos SHA-256 y RSA en documentos jurídicos, previamente se debe generar el par de claves, como se muestra en la *ilustración 3*.

Una vez obtenidas las claves privada y pública, es posible realizar los procesos de encriptación y desencriptación. Para ello, utilizaremos de ejemplo los mismos pagarés utilizados en el capítulo anterior. En la parte inferior de las

ilustraciones 4 y 5 se muestra el resultado de encriptar el resumen digital a través del método RSA con la llave privada que es siempre una cadena de 256 caracteres.

Al desencriptar el mensaje utilizando la clave pública, se regresa al resumen digital. Con lo que se puede comprobar le autoría y la integridad del mensaje de datos.

Cabe señalar que las ilustraciones incluidas en esta obra se generaron mediante los programas informáticos denominados “Hash Droid”[156] y “RSA in action”,[157] que son *software* gratuito y totalmente accesible. Como estos, existen muchos otros programas informáticos disponibles, algunos muy sencillos y otros muy complejos, para ejecutar los estándares SHA y RSA, por lo que se trata de tecnologías muy generalizadas y accesibles.

[156] Hash Droid versión 4.3, desarrollado por Christophe Bouyer (Hobby One), sin restricciones de uso, disponible en la tienda virtual “Google Play”, en la dirección de internet https://play.google.com/store/apps/details?id=com.hobbyone.HashDroid .

[157] *RSA in Action*, versión 1.0, desarrollado por Dinesh R, sin restricciones de uso, disponible en la tienda virtual “Google Play”, en el sitio de internet consultable en la siguiente dirección electrónica https://play.google.com/store/apps/details?id=com.dineshr.www.rsapublicprivatekeygenerator .

Ilustración 3

CLAVE PRIVADA
30819f300d06092a864886f70d010101050003818d0030818902818100b 761599996a151949f0cedaf19fc3015fe2de26c44108489e56ea8444402 1b05ac6ef5759ec9ee8ff58422e7f915a6c32e39439d7e6513fbbd0439a 6a6d79018f666177f4a483b8b23c8d0da77f157c6a95d2fc4f7e84a0640 3a3d625951c8a3c2dcd4f6d8eb6057f7fc0b4c5dc7ee89eb899c8cd1f57 89e98fa438cf6c51ecd0203010001

CLAVE PÚBLICA
30820275020100300d06092a864886f70d0101010500048202 5f3082025 b02010002818100b761599996a151949f0cedaf19fc3015fe2de26c4410 8489e56ea84444021b05ac6ef5759ec9ee8ff58422e7f915a6c32e39439 d7e6513fbbd0439a6a6d79018f666177f4a483b8b23c8d0da77f157c6a9 5d2fc4f7e84a06403a3d625951c8a3c2dcd4f6d8eb6057f7fc0b4c5dc7e e89eb899c8cd1f5789e98fa438cf6c51ecd020301000102818056108462 c705332a937317e24449cdafa4b99838c3c114d33b30b21c47e6cd13de9 7bcefd4f464d87f9be25e08d3168f28148c1d5082d3dc241be58ac76708 23430bac43765ea24b391b6619850bafb324a42febd6f46baba0697a17a 1a72f649d6ab24a32dc70104512639931b39134b1ea570cc4c092998464 4e36c1be2fe9024100ea99a0562b5fb8f149501810a6e941ea713ac5196 2dd7939a5b4c7222f6cd25316f774bc15aaba78eee1ee9c762e217df138 d8fa63186a96caa7bdd3fdc3b0a7024100c81ba3d4497cf44fc0040a18c 6a6aa96051a67bd84f5c0cd4d530525e1b18ce5ae2ea784697996228261 3c339d40c96eb2433d4321ff559fe05177f6cbeb8f6b02407f019ca409e 750a09028245f1f7db889cbb31d7198ec7dec8fa1470d62cf6f2e3c88cb 51e808fddaeab8b60d4e8dbae40bebd2cbfb4a04aa8e1c31d0cad95e910 2407edd2f1f6e3bbef4348b1b0f9c199bfaa25f9c3785ecfbffecaede8b a6ab96e52269c7a065f244a1ba410516bff28c02171813e5d4cef92cf3d d128e2fb836e302405719dd3355315273ecf6b92a106f4ffaaa8dc6103e 1679d14413ec9d44f8dd3c1810f7ada4d3196840df56d89dcb288353701 66e99c6697bdb2eea168d75c791

Ilustración 4

MENSAJE ORIGINAL
PAGARÉ Número 1/2 Bueno por $5,000.00 Morelia, Michoacán, a 16 de agosto de 2018. Debo y pagaré incondicionalmente a la orden de MARÍA DE GUADALUPE RAMÍREZ GONZÁLEZ, en Morelia, Michoacán, el día 15 de diciembre de 2018, la cantidad de $5,000.00, valor recibido a mi entera satisfacción. Este pagaré forma parte de una serie numerada del 1 al 2 y todos están sujetos a la condición de que, al no pagarse cualquiera de ellos a su vencimiento, serán exigibles todos los que le sigan en número, además de los ya vencidos, desde la fecha de vencimiento de este documento hasta el día de su liquidación. Este pagaré causará intereses moratorios al tipo del 1 % mensual, pagaderos en esta ciudad juntamente con el principal. ACEPTO: JAVIER MARTÍN ESCAMILLA BÁEZ
RESUMEN CON SHA-256
D4CE329E4B9EDF5EDB43610A30D0CA222DBC4D1C80BA2E9317536F50EEBA2A90
ENCRIPTADO RSA
5bca1107825a904bb5ecf2fc6ebdb2739154a9c36280950e4ea9c16a55dea2114afd8ff8674ad6e00fd87872d63a936d06ccaf5c76d87b8763ccbb50e90bf3119d890b56184d69783f08e0d6291f9133045c633fd054857a53be24204c87687dd01edaf28cf2a3aab032a9a460bb60598807391f90dd8a338e04e622b7396db5

Ilustración 5

MENSAJE ORIGINAL
PAGARÉ Número 1/2 Bueno por $15,000.00 Morelia, Michoacán, a 16 de agosto de 2018. Debo y pagaré incondicionalmente a la orden de MARÍA DE GUADALUPE RAMÍREZ GONZÁLEZ, en Morelia, Michoacán, el día 15 de diciembre de 2018, la cantidad de $15,000.00, valor recibido a mi entera satisfacción. Este pagaré forma parte de una serie numerada del 1 al 2 y todos están sujetos a la condición de que, al no pagarse cualquiera de ellos a su vencimiento, serán exigibles todos los que le sigan en número, además de los ya vencidos, desde la fecha de vencimiento de este documento hasta el día de su liquidación. Este pagaré causará intereses moratorios al tipo del 1 % mensual, pagaderos en esta ciudad juntamente con el principal. ACEPTO: JAVIER MARTÍN ESCAMILLA BÁEZ
RESUMEN CON SHA-256
D4CE329E4B9EDF5EDB43610A30D0CA222DBC4D1C80BA2E9317536F50EEBA2A90
ENCRIPTADO RSA
0be2f230633ae69643bdf3520e369434b57861f1ae821405143ac0a2beb9a60c8434ca064728a5bd435c10f6c2cc63a907d0d9d592ac7cca46c18900ba53ed5d4d9a4e9d19a17b1f157e4a22053517416a29814a181ad3274f356d88e42c6e03c44f070cefeb08a134c922a5fe9a667b860ad10da1a7a6f5c046981181f79754

Hay otros campos jurídicos de donde podemos tomar ejemplos de documentos firmados electrónicamente con los estándares informáticos analizados.

Uno de estos casos es el Juicio de Amparo, cuya normatividad permite el trámite en línea.[158] Hoy en día, el juicio de amparo en línea funciona con base en los estándares RSA y SHA-256.[159] Aunque el uso de la firma electrónica en el ámbito judicial excede de los límites de este trabajo, es interesante e ilustrativo conocer un documento firmado electrónicamente en un juicio de amparo, ya que en el mismo se utilizan los estándares SHA-256 y RSA de los que hemos venido hablando. En el *Anexo I* de este trabajo podemos ver una demanda de amparo firmada electrónicamente.[160] De este ejemplo, podemos destacar que, a pesar de la extensión de 39 páginas del documento original, el resultado es solo una cadena de 256 caracteres, al igual que en nuestro ejemplo anterior.

[158] Artículo 3º de la Ley Amparo.
[159] Incisos 1.6.2., 1.7.2, 6.6., 14.2.4, 14.3.5 de las Políticas para la obtención y uso de la Firma Electrónica Certificada del Poder judicial de la Federación (FIREL), así como para la operación de su infraestructura tecnológica, consultables en la página de internet del Poder Judicial de la Federación https://www.pjf.gob.mx/Docs/Politicas%20Firel%20con%20rubricas%20y%20firmas.pdf.
[160] Esta demanda se firmó electrónicamente a través del Portal de Servicios en Línea del Poder Judicial de la Federación, disponible en la dirección de internet siguiente: http://www.serviciosenlinea.pjf.gob.mx/juicioenlinea

CAPÍTULO SEXTO
CONCLUSIONES

Ahora corresponde consignar las diversas conclusiones a las que llegamos a partir del trabajo realizado en la presente obra.

I.- La superioridad teórica de la firma electrónica

Nos encontramos en una época caracterizada por una interrelación cada vez más grande, veloz y compleja entre las personas de la sociedad. En el ámbito privado, las telecomunicaciones están rompiendo todas las barreras geográficas y técnicas hasta ahora conocidas, con lo que se ha generado una generación y un intercambio de información que podemos calificar de explosivos, debido a su dinamismo, velocidad y crecimiento. No resulta raro entonces que las transacciones comerciales modernas se vean impulsadas por ese crecimiento explosivo.

Pero estas circunstancias modernas, implican un enorme reto jurídico: el de documentar, asegurar y ejecutar todas esas transacciones a la escala y velocidad que requieren las personas de hoy. Los medios tradicionales ya no permiten lograr ese cometido. No hay papel, tinta ni medios de transporte suficientes para documentar, firmar y transmitir oportunamente todos los convenios que se llevan a cabo en la nueva realidad mercantil mundial. Y, en cualquier caso, tampoco existe ningún poder judicial capaz de analizar y ejecutar todo el papeleo que se requeriría para documentar el volumen de transacciones mercantiles de la actualidad, ni siquiera a una escala nacional.

Y hablando del ámbito público, también nos encontramos con una demanda por parte de los gobernados, de inédita magnitud, para la realización de trámites necesarios para dar seguridad a la nueva y dinámica realidad social. Así que los trámites burocráticos administrativos y judiciales se suelen ver rebasados por la demanda social, cuando solo se basan en medios de documentación tradicionales, que por su costo y dificultad de procesamiento, ya resultan inconvenientes.

En suma: La dinámica social moderna requiere de mecanismos de seguridad jurídica a una velocidad y a una cantidad tan altas que no se pueden proporcionar a través de medios informáticos capaces de generar, procesar y almacenar información jurídica a gran escala, como los medios típicos no lo permiten ya.

De ahí que resulten también indispensables los mecanismos de firma electrónica, para brindar certeza jurídica a toda esta información electrónica.

Y vale la pena agregar que los mecanismos informáticos de los que hablamos, incluyendo los de firma electrónica, no solo son más rápidos y eficientes que los medios tradicionales, sino que también son más seguros. Al estar basados en los conocimientos matemáticos más sólidos de la época, se pueden calificar como técnicamente inquebrantables.

II.- La solidez técnica y jurídica de los estándares SHA y RSA

Tras conocer el funcionamiento técnico general de los estándares SHA y RSA hemos podido constatar que su diseño es el producto de un trabajo científico de muchas décadas, realizado por muchas personas y organizaciones calificadas, que actualmente sigue en marcha, buscando mejoras constantes.

Así que estos estándares se basan en principios matemáticos de la más alta complejidad, que sólo pueden ser ejecutados por computadoras, dotándolos de una seguridad informática insuperable el día de hoy, ya que no existe ni siquiera una posibilidad remota de vulnerarlos con ninguno de los equipos computacionales disponibles en nuestros días. Y no hay que olvidar que la comunidad científica ha trabajado en estándares informáticos superiores, para que estén disponibles al momento en que existan nuevos avances en la computación. [161]

No se trata pues de una moda pasajera carente de seriedad.

[161] Incluso ya existen ensayos sobre estándares criptográficos que serían aplicables al momento en que se encuentren disponibles las computadoras cuánticas, capaces de vulnerar el método RSA actual, pero al mismo tiempo capaces de ejecutar procedimientos criptográficos más avanzados. Véase Ekert, Artur y Renner, Renato, “Los límites físicos de la privacidad”, *Investigación y ciencia,* número 472, Barcelona, Prensa Científica, enero de 2016, pp. 18 a 25.

Muestra de la solidez técnica de estos estándares informáticos es que gran parte de los instrumentos reglamentarios en la materia los establecen como estándares obligatorios o como principales referencias para la ejecución de procesos de firma electrónica

Es por ello que esta investigación nos ha permitido reforzar la confianza en estos estándares de firma electrónica y avizorar los principales retos y oportunidades que existen en el horizonte futuro, como enseguida se comentará.

III.- Las dificultades prácticas de la firma electrónica

En la historia, todo avance tecnológico siempre se enfrenta al reto inicial de la asimilación por parte de los usuarios, quienes deben primero entenderlo, conociendo su funcionamiento, sus bondades, y sus inconvenientes, para luego aplicarlo. En esta fase inicial, muchos de los avances tecnológicos llegan a frenarse o a fracasar por distintos factores.

Inicialmente, el prejuicio de los usuarios que, por naturaleza se aferran a su cotidianeidad, y se suelen negar a los cambios tecnológicos. Asimismo, la mala información acerca de las características del avance tecnológico, con lo que se puede generar una mala valoración por parte de los usuarios, con su consecuente rechazo. Finalmente, la deficiente información sobre el funcionamiento de la nueva tecnología puede provocar la frustración del usuario o, peor aún, un mal uso de la tecnología.

Por ello es indispensable que en la fase de lanzamiento se redoblen esfuerzos de comunicación con los usuarios, para brindarles una mejor experiencia con la nueva tecnología. Sólo así tendrá éxito la innovación.

En el caso de las innovaciones tecnológicas lanzadas por empresas privadas, éstas cargan con toda la labor de comunicar a sus clientes las características y los beneficios de sus productos, para que éstos se consoliden con éxito en el mercado.

Tratándose de innovaciones tecnológicas de interés público, se requiere de un esfuerzo múltiple. Los diseñadores deben buscar, en la medida de lo posible,

que el producto tecnológico sea de fácil entendimiento y uso por parte de los usuarios, aún cuando esto no resulta tan fácil en tecnologías de alta complejidad. Los empresarios pueden apoyar elaborando aplicaciones comerciales específicas de la nueva tecnología, haciendo esfuerzos publicitarios, con lo cual se suele hacer más atractiva para sectores específicos de la población. Resulta crucial también el esfuerzo gubernamental para incorporar de manera decisiva la nueva tecnología a los procesos gubernamentales pertinentes, brindando la difusión oficial para el conocimiento de los gobernados.

Pero en estos casos requiere mención especial el papel de la comunidad académica, que debe avocarse al estudio de la novedad tecnológica, para conocerla de primera mano y a detalle, para exponer su funcionamiento a la comunidad, para proponer usos prácticos, para destacar sus ventajas y para evidenciar sus desventajas.

Tal es el caso de la firma electrónica, cuya licencia de uso es abierta para la comunidad en general,[162] y que requiere ser utilizada a gran escala para el interés común. Al ser un desarrollo tecnológico de relativamente reciente lanzamiento, se está enfrentando al enorme reto de consolidarse entre la población en general, necesitando del apoyo multilateral que hemos mencionado arriba. Así que, a pesar de su solidez teórica, la firma electrónica aún presenta muchas dificultades prácticas que deben resolverse para aprovechar todo su potencial.

El desconocimiento de la población general sobre la firma electrónica es profundo. La mayoría de las personas ignora su funcionamiento y teme que sea insegura. Se piensa que se trata de una invención débil, susceptible de ser vulnerada por medios informáticos. De ahí que la mayoría de la población se siga inclinando hacia la firma autógrafa.

[162] La firma electrónica como concepto tecnológico previsto en la ley, puede ser desarrollado de múltiples maneras por cualquier persona que desee crear mecanismos de firma electrónica en forma de aplicaciones informáticas públicas o comerciales. Incluso, como hemos visto en páginas anteriores, los desarrollos informáticos más importantes en materia de firma electrónica se han abierto a la disposición del público en general, en forma de estándares de licencia de uso abierto, para que cualquier persona los pueda utilizar para desarrollar nuevas tecnologías.

Incluso en el ámbito académico, nos resulta aún muy retador entender el derecho sin papel ni tinta, y conceptos como la “desmaterialización” y la “inmaterialización” de documentos jurídicos.[163]

Por otra parte, las autoridades gubernamentales, también por desconocimiento, han desaprovechado el potencial de la firma electrónica en los distintos procesos gubernamentales y han realizado apenas una pobre difusión sobre el tema entre el público. Apenas unos pocos trámites administrativos y judiciales utilizan la firma electrónica, con poco éxito entre los particulares, que siguen prefiriendo hacer sus trámites en papel impreso.

Aunque se ha legislado en materia de firma electrónica con un buen grado de avance, sigue faltando una regulación más práctica sobre la manera de presentar y valorar jurídicamente los documentos electrónicos. Esta oscuridad jurídica, sólo genera incertidumbre entre la población y desinhibe el uso de la firma electrónica, por temor de que no pueda ser jurídicamente exigible.[164]

Y ante todo este panorama, el medio empresarial se ha desincentivado, participando poco en el desarrollo de aplicaciones de firma electrónica.

Todo esto es indicativo de la gran labor que tenemos por delante los juristas para adentrarnos en la investigación de este tema, criticándolo y difundiéndolo, para proponer y promover mayores y mejores usos de las herramientas informáticas en el campo jurídico.[165]

---

[163] Véase Durán Díaz, Oscar Jorge, *Los títulos de crédito electrónicos y su desmaterialización*, México, Porrúa, 2009, paginas 91 a 96, 187 y 188.

[164] *Cfr.* Elías Azar, Edgar, *La contratación por medios electrónicos,* México, Porrúa, 2005, pp. 275 a 298.

[165] Véase Matjaž Perc *et al*, “Social and juristic challenges of artificial intelligence”, *Palgrave Comunications*, 29 de agosto de 2019, consultable en https://www.nature.com/articles/s41599-019-0278-x.pdf .

IV.- Las oportunidades de uso de la firma electrónica y otras tecnologías en el campo jurídico

Ya varios autores, como Richard Susskind, comienzan a visualizar cambios dramáticos en la actividad jurídica a nivel mundial, impulsados por la globalización y los cambios tecnológicos modernos.[166]

Estas predicciones ya no parecen ciencia ficción,[167] después de acercarnos, como lo hemos hecho en este trabajo, a las tecnologías informáticas que se diseñan para fines jurídicos.

Un vistazo por amplio catálogo de estándares informáticos internaciones, de alto nivel de seguridad y eficiencia, nos abren la imaginación hacia una serie de aplicaciones que pueden revolucionar realmente al mundo jurídico de los contratos, la solución de controversias y los procesos administrativos.

Ya en el mundo se empieza a hablar cada vez más de los contratos inteligentes, que son acuerdos jurídicos comerciales generados electrónicamente y cuyos términos pueden ser ejecutados automáticamente, por medio de un programa de cómputo con control sobre los bienes jurídicos en cuestión. Por ejemplo, un contrato de arrendamiento en el que se prevé que, ante la falta de pago del precio de la renta, se bloquee electrónicamente el uso del bien arrendado. O también un contrato de préstamos con garantía líquida, en el que se estipula que, en caso de falta de pago del préstamo, se haga automáticamente el cobro por medio de la garantía líquida.[168]

En estos casos, las controversias se resuelven automáticamente, sin la necesidad de acudir a ningún tribunal.

---

[166] Véase Susskind, Richard, *Tomorrow's lawyers. An introduction to your future*, 2ª ed., Reino Unido, Oxford, 2017, pp. 3 a 15.

[167] Ya en otras disciplinas se empiezan a utilizar con decisión los medios electrónicos para resolver los problemas propios de la modernidad. Por ejemplo, en el ámbito médico, donde resulta sumamente complejo y laborioso el manejo de los expedientes clínicos, se ve un amplio proceso de migración digital. Y ante ello, también surge la necesidad de seguridad jurídica en el manejo de dicha información. Al respecto véase Mareddu Gilbert, Mariana, *Regulación jurídica del expediente clínico electrónico,* México, Tirant lo Blanch, 2017, pp. 151 a 167.

[168] Sobre los medios de pago previstos en los contratos electrónicos, véase De Miguel Ascencio, Pedro Alberto, *Derecho del comercio electrónico*, México, Porrúa, 2005, pp. 91 a 95; y Ramírez Vieyra, Eréndira (coord.), "El pago electrónico", *Revista IDC edición especial sobre el mundo de comercio electrónico bajo la ley*, abril de 2017, pp. 41 a 47.

Pero también podemos imaginar juicios automáticos, en los que las partes actúen y se defiendan por medio de documentos electrónicos estandarizados, que puedan ser analizados directamente por una computadora que determine quién tiene la razón y resuelva lo conducente. Los juicios ejecutivos mercantiles, podrían estandarizarse de un modo relativamente fácil, para resolverse de manera automática, pues se basan en documentos sencillos, cuyo análisis se puede programar para cualquier computadora. Posteriormente, se podrían estandarizar más tipos de controversias. De lograrse esto, se podría apoyar de una manera muy significativa a los órganos jurisdiccionales del mundo, para descargarlos de las tareas de resolución de controversias mecánicas, para que puedan concentrarse en la resolución de asuntos abstractos.

De igual forma, con el mayor uso de herramientas informáticas, las autoridades podrían eliminar el uso de tantos formularios en papel que, además de mermar el medio ambiente, requieren el análisis humano. Si estos formularios de papel se sustituyen por formularios electrónicos, bien pensados y estandarizados, estaríamos en posibilidades de ver una multiplicidad de trámites burocráticos en línea y de resolución automática.

De notable relevancia será también la inteligencia artificial que se está desarrollando y que podrá aplicarse en distintos ámbitos de la vida jurídica.

Uno de estos ámbitos será la identificación de personas para fines de registro poblacional, civiles, fiscales y hasta penales. de gran utilidad para ello serán las tecnologías de identificación biométrica, que cada vez adquieren más características de inteligencia artificial, pues los dispositivos de reconocimiento biométrico están comenzando a aprender a identificar personas en muy diversas y dinámicas situaciones.[169]

Otro de los aspectos de la vida jurídica que pueden mejorar gracias a la inteligencia artificial es en general la productividad de los operadores jurídicos que, en cualquiera de sus trincheras, se enfrentan día a día a los retos de administrar

[169] Véase Schechter, Erik, “How to Make Guns Safer”, *Scientific American*, 1 de octubre de 2015, consultable en https://www.scientificamerican.com/article/how-to-make-guns-safer/

proyectos eficiente y eficazmente o de atender un gran cúmulo de trabajo rutinario. Para esto, se desarrollan continuamente herramientas informáticas inteligentes que ayudan a reconocer, analizar y procesar información automática y exactamente.[170]

Por supuesto que todas estas aplicaciones requieren de algunas adecuaciones legislativas, propias de cada país. Pero sobre todo, se requiere de juristas más abiertos al conocimiento y uso de estándares informáticos, capaces de crear vínculos entre el derecho y la informática, basados en la lógica jurídica,[171] para resolver la alta demanda de seguridad jurídica, ya inatendible con los medios tradicionales.

[170] Véase Lathan, Corina y Russel, Stuart, "Open AI Ecosystem Portends a Personal Assistant for Everyone", *Scientific American*, 23 de junio de 2016, consultable en la dirección de internet https://www.scientificamerican.com/article/open-ai-ecosystem-portends-a-personal-assistant-for-everyone/ ; y Susskind, Richard, *op. cit.*, pp. 101-110.
[171] Véase Flores Salgado, Lucerito, *Derecho informático*, México, Patria, 2009, p. 47.

ANEXO I

Juicio: Amparo indirecto.
Partes: Javier Martín Escamilla Báez contra actos del H. Congreso del Estado de Michoacán de Ocampo y otras autoridades.

HONORABLE JUEZ DE DISTRITO EN EL ESTADO DE MICHOACÁN, EN TURNO

PRESENTE.-

JAVIER MARTIN ESCAMILLA BAEZ
70.6a.66.20.63.6a.66.00.00.00.00.00.00.00.00.00.00.54.e5
16/01/2020 11:35:28

Licenciado en Derecho JAVIER MARTÍN ESCAMILLA BÁEZ, con cédula profesional número 6026850, por mi propio derecho; autorizando al Licenciado en Derecho OLIVER ALEJANDRO MURGUÍA ALCARAZ, únicamente para el efecto de que pueda oír y recibir todo tipo de notificaciones, imponerse de los autos, consultar el expediente electrónico y recoger documentos relativos al presente juicio; ante ustedes, con el debido respeto, comparezco y expongo:

Que inicialmente, con fundamento en el artículo 3°, 12° y demás relativos de la Ley de Amparo vigente, así como los artículos 78, 79 y 80 del Acuerdo General Conjunto 1/2015, de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal, que regula los servicios tecnológicos relativos a la tramitación electrónica del juicio de amparo, las comunicaciones oficiales y los procesos de oralidad penal en los centros de justicia penal federal, **solicito que se autorice al suscrito y al Licenciado en Derecho Oliver Alejandro Murguía Alcaraz, a efecto de que podamos consultar el expediente electrónico así como recibir todo tipo de notificaciones y documentos inherentes a la tramitación del presente juicio**, en el entendido de que ambos somos usuarios debidamente registrados en el Portal de Servicios en Línea del Poder Judicial de la Federación, como enseguida se detalla:

AUTORIZADO	NOMBRE DE USUARIO DEL PORTAL
JAVIER MARTÍN ESCAMILLA BÁEZ	jmareb
OLIVER ALEJANDRO MURGUÍA ALCARAZ	Alexmurguia

Que con el carácter antes mencionado, por medio del presente ocurso, **VENGO A DEMANDAR EL AMPARO Y LA PROTECCIÓN DE LA JUSTICIA FEDERAL** en contra de las autoridades y los actos de la autoridad que señalaré en el capítulo correspondiente.

Por lo que, para efecto de cumplir con lo dispuesto por el artículo 108 y demás relativos de la Ley de Amparo, manifiesto, **bajo protesta de decir verdad,** lo siguiente:

I. NOMBRE Y DOMICILIO DEL QUEJOSO:

Lo es JAVIER MARTÍN ESCAMILLA BÁEZ, con domicilio en [redacted].

II. NOMBRE Y DOMICILIO DEL TERCERO INTERESADO:

Bajo protesta de decir verdad, manifiesto que **no hay tercero interesado** en el presente juicio.

III.- AUTORIDADES RESPONSABLES:

Lo son las siguientes:

1. El HONORABLE CONGRESO DEL ESTADO DE MICHOACÁN DE OCAMPO.
2. El CIUDADANO GOBERNADOR DEL ESTADO DE MICHOACÁN DE OCAMPO.
3. El CIUDADANO TESORERO MUNICIPAL DEL MUNICIPIO DE MORELIA, MICHOACÁN.

IV.- NORMAS GENERALES Y ACTOS RECLAMADOS:

De las autoridades responsables se reclaman los siguientes actos:

1. Del **HONORABLE CONGRESO DEL ESTADO DE MICHOACÁN**, se reclama la **aprobación de los decretos legislativos** mediante los cuales se expidieron los **artículos 17 al 44 de la Ley de Hacienda Municipal del Estado de Michoacán de Ocampo**; los **artículos 8° y 9° de la Ley de Ingresos para el Municipio de Morelia, Michoacán, para el ejercicio fiscal 2019**; así como **los artículos 9°, 10, párrafos primero y segundo, 11 y 17 al 28 de la Ley de Catastro del Estado de Michoacán,** todos ellos vigentes actualmente y relativos al impuesto predial aplicable en el municipio de Morelia, Michoacán;

2. Del CIUDADANO GOBERNADOR DEL ESTADO DE MICHOACÁN DE OCAMPO, se reclama la promulgación y entrada en vigor de **los decretos legislativos** mediante los cuales se expidieron los **artículos 17 al 44 de la Ley de Hacienda Municipal del Estado de Michoacán de Ocampo**; los **artículos 8° y 9° de la Ley de Ingresos para el Municipio de Morelia, Michoacán, para el ejercicio fiscal 2019**; así como **los artículos 9°, 10, párrafos primero y segundo, 11 y 17 al 28 de la Ley de Catastro del Estado de Michoacán,** todos ellos vigentes actualmente y relativos al impuesto predial aplicable en el municipio de Morelia, Michoacán; y

3. Del CIUDADANO TESORERO MUNICIPAL DEL MUNICIPIO DE MORELIA, MICHOACÁN, se reclaman todos los actos tendientes a la ejecución de los **artículos 17 al 44 de la Ley de Hacienda Municipal del Estado de Michoacán de Ocampo**; los **artículos 8° y 9° de la Ley de Ingresos para el Municipio de Morelia, Michoacán, para el ejercicio fiscal 2019**; así como **los artículos 9°, 10, párrafos primero y segundo, 11 y 17 al 28 de la Ley de Catastro del Estado de Michoacán,** todos ellos vigentes actualmente y relativos al impuesto predial aplicable en el municipio de Morelia, Michoacán.

Cabe señalar las disposiciones legales impugnadas constituyen un sistema jurídico complejo que regula lo relativo al impuesto predial aplicable en el municipio de Morelia, Michoacán, en

perjuicio del quejoso, por lo que aquí se impugnan conjuntamente, de conformidad con lo previsto en la siguiente tesis de jurisprudencia por la Suprema Corte de Justicia de la Nación:

> **Novena Época**
> **Registro digital: 169558**
> **Instancia: Segunda Sala**
> **Jurisprudencia**
> **Fuente: Semanario Judicial de la Federación y su Gaceta**
> **Tomo XXVII, Junio de 2008**
> **Materia(s): Común**
> **Tesis: 2a./J. 100/2008**
> **Página: 400**
> **AMPARO CONTRA LEYES. PARA IMPUGNARLAS COMO SISTEMA NORMATIVO ES NECESARIO QUE CONSTITUYAN UNA VERDADERA UNIDAD.**
> La Suprema Corte de Justicia de la Nación ha sostenido que en vía de amparo pueden reclamarse disposiciones legales que guarden una íntima relación entre sí, aun cuando el quejoso sólo acredite el acto de aplicación de una de ellas o que se ubique en el supuesto jurídico de una sola, que lo legitima para controvertirlas de manera conjunta como un sistema normativo, al irrogarle un menoscabo en su esfera jurídica. Ahora bien, esta prerrogativa de impugnación de normas desde su sola vigencia o por virtud de un acto de aplicación de alguna de ellas, requiere que en su conjunto formen una verdadera unidad normativa, de modo que si se declara la inconstitucionalidad de una, se afecte a las demás en su sentido, alcance o aplicación; por tanto, no cualquier norma puede integrar junto con otras un sistema impugnable a través del juicio de amparo, ya que deben tener una relación directa entre sí, casi indisociable en cuanto a la materia, tema, objeto, causa, principio o fuente; de ahí que no pueda integrarse o abarcar normas que sólo hacen una mera referencia, mención o correlación con otras, sino que deban guardar correspondencia entre ellas, porque precisamente a partir de esa relación estrecha el particular puede controvertir disposiciones generales aunque no hayan sido aplicadas en su perjuicio, siendo heteroaplicativas, o desde su sola vigencia, las autoaplicativas.
>
> *Amparo en revisión 1834/2004. El Florido California, S.A. de C.V. 7 de mayo de 2008. Mayoría de tres votos en cuanto al sentido de la ejecutoria. Mayoría de cuatro votos respecto de este criterio. Disidentes: Sergio Salvador Aguirre Anguiano y Margarita Beatriz Luna Ramos. Ponente: Sergio Salvador Aguirre Anguiano. Secretarios: Martha Elba Hurtado Ferrer, Fabiana Estrada Tena e Israel Flores Rodríguez.*
>
> *Amparo en revisión 1207/2006. Inmuebles Gómez, S.A. de C.V. 7 de mayo de 2008. Mayoría de tres votos en cuanto al sentido de la ejecutoria. Mayoría de cuatro votos respecto de este criterio. Disidentes: Sergio Salvador Aguirre Anguiano y Margarita Beatriz*

Luna Ramos. Ponente: Mariano Azuela Güitrón. Secretarios: Martha Elba Hurtado Ferrer, Fabiana Estrada Tena e Israel Flores Rodríguez.

Amparo en revisión 1260/2006. Eduser Inmobiliaria, S.A. de C.V. 7 de mayo de 2008. Mayoría de tres votos en cuanto al sentido de la ejecutoria. Mayoría de cuatro votos respecto de este criterio. Disidentes: Sergio Salvador Aguirre Anguiano y Margarita Beatriz Luna Ramos. Ponente: Genaro David Góngora Pimentel. Secretarios: Martha Elba Hurtado Ferrer, Fabiana Estrada Tena e Israel Flores Rodríguez.

Amparo en revisión 1351/2006. Metalmec, S.A. de C.V. y otras. 7 de mayo de 2008. Mayoría de tres votos en cuanto al sentido de la ejecutoria. Mayoría de cuatro votos respecto de este criterio. Disidentes: Sergio Salvador Aguirre Anguiano y Margarita Beatriz Luna Ramos. Ponente: Margarita Beatriz Luna Ramos. Secretarios: Martha Elba Hurtado Ferrer, Fabiana Estrada Tena e Israel Flores Rodríguez.

Amparo en revisión 1700/2006. Integración de Servicios en Salud, S.A. de C.V. 7 de mayo de 2008. Mayoría de tres votos en cuanto al sentido de la ejecutoria. Mayoría de cuatro votos respecto de este criterio. Disidentes: Sergio Salvador Aguirre Anguiano y Margarita Beatriz Luna Ramos. Ponente: Genaro David Góngora Pimentel. Secretarios: Martha Elba Hurtado Ferrer, Fabiana Estrada Tena e Israel Flores Rodríguez.

Tesis de jurisprudencia 100/2008. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del cuatro de junio de dos mil ocho.

V.- ANTECEDENTES:

Enseguida narro, **bajo protesta de decir verdad**, los siguientes hechos y abstenciones constituyen los antecedentes de los actos reclamados y que sirven de fundamento a los conceptos de violación:

1. El día 16 de diciembre de 2014, el Honorable Congreso del Estado de Michoacán aprobó el decreto legislativo mediante el cual se expidió la Ley de Hacienda Municipal del Estado de Michoacán que incluía sus artículos **17 al 44,** vigentes hasta la fecha, y los cuales se atacan mediante la presente demanda de amparo.

2. El día 25 de diciembre de 2014, con el refrendo del Secretario de Gobierno de esta entidad federativa, el Ciudadano Gobernador del Estado de Michoacán de Ocampo promulgó el decreto legislativo mencionado en el párrafo anterior.

3. El mismo día 25 de diciembre de 2014 se publicó en el Periódico Oficial del Estado de Michoacán la nueva Ley de Hacienda Municipal del Estado de Michoacán, entrando en vigor al día 1° de enero de 2015, conforme a su artículo transitorio primero.

4. El día 23 de diciembre de 2014, el Honorable Congreso del Estado de Michoacán aprobó el decreto legislativo mediante el cual se expidió la **Ley de Catastro del Estado de Michoacán** que incluía sus artículos **9º, 10, párrafos primero y segundo, 11 y 17 al 28,** vigentes hasta la fecha, y que se atacan mediante la presente demanda de amparo.

5. El día 30 de diciembre de 2014, el Ciudadano Gobernador del Estado de Michoacán de Ocampo, con el refrendo del Secretario de Gobierno de esta entidad federativa, promulgó el decreto legislativo mencionado en el párrafo anterior.

6. El mismo día 30 de diciembre de 2014 se publicó en el Periódico Oficial del Estado de Michoacán la nueva Ley de Catastro del Estado de Michoacán de Ocampo, entrando en vigor al día siguiente de su publicación, conforme a su artículo transitorio primero.

7. El día 30 de diciembre de 2018, el Honorable Congreso del Estado de Michoacán aprobó el decreto legislativo mediante el cual se expidió la **Ley de Ingresos para el Municipio de Morelia, Michoacán para el Ejercicio Fiscal del año 2019**, que incluía sus artículos **8º y 9º,** vigentes hasta la fecha, y los cuales se atacan mediante la presente demanda de amparo.

8. El día 31 de diciembre de 2018, con el refrendo del Secretario de Gobierno de esta entidad federativa, el Ciudadano Gobernador del Estado de Michoacán de Ocampo promulgó el decreto legislativo mencionado en el párrafo anterior.

9. El mismo día 31 de diciembre de 2018 se publicó en el Periódico Oficial del Estado de Michoacán la nueva **Ley de Ingresos para el Municipio de Morelia, Michoacán para el Ejercicio Fiscal del año 2019**, entrando en vigor el

día 1° de enero de 2019, conforme a su artículo transitorio primero.

10. El quejoso es propietario de un bien inmueble ubicado en [redacted], el cual se encuentra empadronado bajo la cuenta predial número [redacted].

11. En este contexto cabe señalar que este año 2019, **por primera ocasión**, el quejoso se encontró obligado al pago del impuesto predial en la ciudad de Morelia, Michoacán en los términos de las normas reclamadas.

12. Es así que el día 28 de enero de 2019 el Tesorero Municipal de Morelia, Michoacán, determinó el correspondiente impuesto predial a cargo del quejoso, por la cantidad total de **$**[redacted] **(**[redacted] **PESOS Y CERO CENTAVOS, MONEDA NACIONAL),** tal como se detalla en la orden de pago que se expidió al quejoso por medio del sitio de internet oficial del ayuntamiento de Morelia, Michoacán, consultable en la dirección www.morelia.gob.mx , orden de pago que adjunto electrónicamente al presente libelo.

13. Atendiendo a tal orden de pago, el día **29 de enero de 2019** el quejoso procedió a realizar el pago del impuesto predial que le fue determinado por la autoridad municipal responsable, lo cual hizo también por medio de la misma página de internet oficial, tras lo cual se le expidió el comprobante de pago electrónico con **folio número** [redacted], mismo que se acompaña a la presente demanda.

14. El pago de este impuesto predial detona el interés jurídico del quejoso para promover el presente juicio de amparo, tal como lo ha determinado jurisprudencialmente la Segunda Sala de la Suprema Corte de Justicia de la Nación en la tesis **2a./J. 141/2012 (10a.)** que enseguida transcribo íntegramente:

Décima Época
Registro digital: 2002151
Instancia: Segunda Sala
Jurisprudencia
Fuente: Semanario Judicial de la Federación y su Gaceta
Libro XIV, Noviembre de 2012, Tomo 2
Materia(s): Común
Tesis: 2a./J. 141/2012 (10a.)
Página: 1305

IMPUESTO PREDIAL. EL RECIBO O CERTIFICADO DE PAGO ES SUFICIENTE PARA ACREDITAR EL INTERÉS JURÍDICO EN EL JUICIO DE AMPARO PROMOVIDO CONTRA LAS LEYES QUE LO ESTABLECEN.
El interés jurídico que le asiste a la parte quejosa para reclamar en el juicio de amparo las leyes que establecen o modifican el impuesto predial en aspectos generales, con motivo de un acto de aplicación, puede acreditarse con el recibo o certificado de pago del tributo a su nombre, correspondiente al ejercicio de vigencia de la ley, pues de tal prueba deriva que es contribuyente de aquél, en relación con el predio a que el recibo se refiere y que realizó el pago de la contribución, sin que deba exigirse la aportación de mayores elementos de prueba; salvo en los casos en que se impugnen, en lo particular, normas que regulen determinados supuestos que requieran de la demostración, con mayores pruebas, de que el particular se encuentra comprendido en ellos.

Contradicción de tesis 258/2012. Entre las sustentadas por los Tribunales Colegiados Primero en Materias Penal y Administrativa del Octavo Circuito y Segundo en Materias Penal y Administrativa del Décimo Séptimo Circuito. 19 de septiembre de 2012. Cinco votos. Ponente: Margarita Beatriz Luna Ramos. Secretaria: Guadalupe Margarita Ortiz Blanco.

Tesis de jurisprudencia 141/2012 (10a.). Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del veintiséis de septiembre de dos mil doce.

15. No omito señalar que, si bien es cierto que el quejoso realizó el pago del impuesto predial a su cargo con un descuento por pago anticipado, no menos cierto es que **dicho pago con descuento no puede considerarse como consentimiento expreso de las normas reclamadas**, tal como se desprende de la tesis de jurisprudencia **2a./J. 55/2010,** emitida por la Segunda sala de la Suprema Corte de Justicia de la Nación, la cual es del tenor literal siguiente:

Novena Época
Registro digital: 164615
Instancia: Segunda Sala
Jurisprudencia
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo XXXI, Mayo de 2010
Materia(s): Administrativa
Tesis: 2a./J. 55/2010
Página: 830

CONSENTIMIENTO EXPRESO COMO CAUSAL DE IMPROCEDENCIA DEL AMPARO. NO LO ACTUALIZA EL PAGO ANUAL ANTICIPADO DEL IMPUESTO PREDIAL PARA GOZAR DE LA REDUCCIÓN DE UN PORCENTAJE SOBRE SU MONTO.

El Tribunal en Pleno de la Suprema Corte de Justicia de la Nación, en la jurisprudencia P./J. 68/97, de rubro: "LEYES, AMPARO CONTRA. EL PAGO LISO Y LLANO DE UNA CONTRIBUCIÓN NO IMPLICA EL CONSENTIMIENTO EXPRESO DE LA LEY QUE LA ESTABLECE.", sostuvo que si el quejoso presenta demanda de amparo contra una ley tributaria dentro del plazo legal, computado a partir de que realizó el pago de la contribución en forma lisa y llana, tal proceder no constituye una manifestación de voluntad que entrañe el consentimiento de la norma que establece la contribución, pues dada la naturaleza fiscal de ésta, su cumplimiento por parte de los contribuyentes se impone como imperativo y conlleva la advertencia cierta de una coacción, por lo que la promoción del juicio de amparo correspondiente refleja la inconformidad del peticionario de garantías con el contenido de la ley impugnada. Ahora bien, la circunstancia de que algunas leyes fiscales ofrezcan a sus destinatarios alguna reducción en las cantidades a enterar por su pago anticipado, esto es, por cubrirlas con anterioridad a la fecha ordinariamente programada para su recaudación, no implica una inexorable sumisión que torne improcedente el juicio constitucional, ya que al adoptar ese beneficio el sujeto obligado exclusivamente acepta cumplir oportunamente sus cargas fiscales, y esa observancia puntual de la ley no puede sancionarse con la supresión del acceso al juicio de garantías, ya que la sumisión al pago de las contribuciones, sea porque pese sobre el contribuyente la amenaza del cobro coactivo o por el estímulo del beneficio de una disminución que premie su pago anticipado, constituyen dos formas de conminar al sujeto pasivo del tributo para cumplir con sus obligaciones tributarias, de manera que este actúa para evitar sanciones o para obtener adicionalmente disminuciones en sus pagos, pero no por voluntad propia. Consecuentemente, si el juicio de amparo se promueve en tiempo y forma legales, contra el pago anticipado del impuesto predial que el contribuyente se autoliquide, no se configura la causal de improcedencia prevista en la fracción XI del artículo 73 de la Ley de Amparo.

Contradicción de tesis 102/2010. Entre las sustentadas por los Tribunales Colegiados Tercero en Materia Administrativa del

Tercer Circuito y Tercero en Materia Administrativa del Cuarto Circuito. 21 de abril de 2010. Unanimidad de cuatro votos. Ausente: Sergio Salvador Aguirre Anguiano. Ponente: Margarita Beatriz Luna Ramos. Secretaria: Ma. de la Luz Pineda Pineda.

Tesis de jurisprudencia 55/2010. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del veintiocho de abril de dos mil diez.

Nota: La tesis P./J. 68/97 citada, aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo VI, septiembre de 1997, página 92.

16. Expuesto lo anterior, debe decirse que **todas las disposiciones reclamadas son violatorias de diversas disposiciones constitucionales y derechos fundamentales en perjuicio del quejoso**, tal como se expone en el capítulo de los Conceptos de Violación, por lo que **debe concederse el Amparo y la Protección de la Justicia Federal** que aquí se demanda.

VI.- PRECEPTOS CONSTITUCIONALES VIOLADOS:

Los actos reclamados violan en perjuicio de la parte quejosa los **artículos 1º, primer y tercer párrafo, 14, segundo párrafo, 16, primer párrafo, 31, fracción IV, 115, fracción IV, y 133**, todos ellos de **la Constitución Política de los Estados Unidos Mexicanos**.

VII.- CONCEPTOS DE VIOLACIÓN:

PRIMER CONCEPTO DE VIOLACIÓN

Los **artículos 17 al 44 de la Ley de Hacienda Municipal del Estado de Michoacán de Ocampo**; los **artículos 8º y 9º de la Ley de Ingresos para el Municipio de Morelia, Michoacán, para el ejercicio fiscal 2019**; así como los **artículos 9º, 10, párrafos primero y segundo, 11 y 17 al 28 de la Ley de Catastro del Estado de Michoacán,** todos ellos relativos al impuesto predial aplicable en el municipio de Morelia, Michoacán, **son violatorios del principio de legalidad tributaria** previsto en el artículo 31, fracción IV, y **el principio de seguridad jurídica en materia fiscal**, previsto en los artículos 14, segundo párrafo, y 16, primer párrafo, todos de la Constitución Política de los Estados Unidos Mexicanos.

Para explicar lo anterior, debemos inicialmente recordar que el artículo 31, fracción IV, de nuestra Carta Magna contiene los altos requisitos que deben cumplir los impuestos que establezca el Estado a cargo de los gobernados, siendo del tenor literal siguiente:

> **Artículo 31.** Son obligaciones de los mexicanos:
>
> (…)
>
> **IV.** Contribuir para los gastos públicos, así de la Federación, como de los Estados, de la Ciudad de México y del Municipio en que residan, de la manera proporcional y equitativa **que dispongan las leyes**.[1]

De la parte final de la disposición transcrita se desprende el **principio de legalidad tributaria**, que se traduce en la obligación de que todos los elementos del impuesto sean establecidos en normas de carácter general formalmente legislativas.

Sobre este tema precisamente se ha pronunciado el Pleno de la Suprema Corte de Justicia de la Nación en la siguiente tesis de jurisprudencia:

> **Séptima Época**
> **Registro digital: 232797**
> **Instancia: Pleno**
> **Jurisprudencia**
> **Fuente: Semanario Judicial de la Federación**
> **Volumen 91-96, Primera Parte**
> **Materia(s): Constitucional, Administrativa**
> **Página: 173**
> **Genealogía:**
> **Informe 1974, Primera Parte, Pleno, página 347.**
> **Apéndice 1917-1985, Primera Parte, Pleno, tesis 54, página 105.**
> **Apéndice 1917-1988, Primera Parte, Pleno, tesis 86, página 158.**
> **Apéndice 1917-1995, Tomo I, Primera Parte, tesis 168, página 169.**
>
> **IMPUESTOS, PRINCIPIO DE LEGALIDAD QUE EN MATERIA DE, CONSAGRA LA CONSTITUCION FEDERAL.**
> El principio de legalidad se encuentra claramente establecido por el artículo 31 constitucional, al expresar, en su fracción IV, que los mexicanos deben contribuir para los gastos públicos de la manera proporcional y equitativa que dispongan las leyes y está, además, minuciosamente reglamentado en su aspecto formal, por diversos preceptos que se refieren a la expedición de la Ley General de Ingresos, en la que se determinan los impuestos que se causarán y

[1] El énfasis en las citas es propio.

recaudarán durante el período que la misma abarca. Por otra parte, examinando atentamente este principio de legalidad, a la luz del sistema general que informa nuestras disposiciones constitucionales en materia impositiva y de explicación racional e histórica, se encuentra que la necesidad de que la carga tributaria de los gobernados esté establecida en una ley, no significa tan solo que el acto creador del impuesto deba emanar de aquel poder que, conforme a la Constitución del Estado, está encargado de la función legislativa, ya que así se satisface la exigencia de que sean los propios gobernados, a través de sus representantes, los que determinen las cargas fiscales que deben soportar, sino fundamentalmente que los caracteres esenciales del impuesto y la forma, contenido y alcance de la obligación tributaria, estén consignados de manera expresa en la ley, de tal modo que no quede margen para la arbitrariedad de las autoridades exactoras ni para el cobro de impuestos imprevisibles o a título particular, sino que el sujeto pasivo de la relación tributaria pueda, en todo momento, conocer la forma cierta de contribuir para los gastos públicos del Estado, y a la autoridad no queda otra cosa sino aplicar las disposiciones generales de observancia obligatoria, dictadas con anterioridad al caso concreto de cada causante. Esto, por lo demás, es consecuencia del principio general de legalidad, conforme al cual ningún órgano del Estado puede realizar actos individuales que no estén previstos y autorizados por disposición general anterior, y está reconocido por el artículo 14 de nuestra Ley Fundamental. Lo contrario, es decir, la arbitrariedad en la imposición, la imprevisibilidad en las cargas tributarias y los impuestos que no tengan un claro apoyo legal, deben considerarse absolutamente proscritos en el régimen constitucional mexicano, sea cual fuere el pretexto con que pretenda justificárseles.

Séptima Epoca, Primera Parte:
Volúmenes 91-96, página 92. Amparo en revisión 331/76. María de los Angeles Prendes de Vera. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Carlos del Río Rodríguez.

Volúmenes 91-96, página 92. Amparo en revisión 1008/76. Antonio Hernández Abarca. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Arturo Serrano Robles.

Volúmenes 91-96, página 92. Amparo en revisión 5332/75. Blanca Meyerberg de González. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Ramón Canedo Aldrete.

Volúmenes 91-96, página 92. Amparo en revisión 5464/75. Ignacio Rodríguez Treviño. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Arturo Serrano Robles.

Volúmenes 91-96, página 92. Amparo en revisión 5888/75. Inmobiliaria Havre, S.A. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Arturo Serrano Robles.

Observaciones:
Nota: En el Semanario Judicial de la Federación, Volúmenes 91-96, la referencia de la página 91 es incorrecta, por lo que se corrige, como se observa en este registro.

En consonancia con lo anterior, los artículos 14, segundo párrafo, y 16, primer párrafo, de la Constitución Política de los Estados Unidos Mexicanos estipulan lo siguiente:

> **Artículo 14.** (…)
>
> Nadie podrá ser privado de la libertad o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante los tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento y conforme a las Leyes expedidas con anterioridad al hecho.
>
> **Artículo 16.** Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

De esta manera, nuestra Carta Magna consagra **el principio de seguridad jurídica en materia tributaria**, que permite a los contribuyentes en todo momento tener certeza de sus derechos y obligaciones frente a las autoridades exactoras, conociendo con exactitud cuáles serán las consecuencias jurídicas de cualquiera de las hipótesis jurídicas en las que se lleguen a colocar.

Así lo confirma la **tesis de jurisprudencia 2a./J. 140/2017 (10a.)** emitida por la Segunda Sala de nuestro Más Alto Tribunal, que enseguida copio:

> **Décima Época**
> **Registro digital: 2015246**
> **Instancia: Segunda Sala**
> **Jurisprudencia**
> **Fuente: Gaceta del Semanario Judicial de la Federación**
> **Libro 47, Octubre de 2017, Tomo II**
> **Materia(s): Constitucional, Administrativa**
> **Tesis: 2a./J. 140/2017 (10a.)**
> **Página: 840**
> **PRINCIPIO DE SEGURIDAD JURÍDICA EN MATERIA FISCAL. SU CONTENIDO ESENCIAL.**

Dicho principio constituye uno de los pilares sobre el cual descansa el sistema fiscal mexicano y tutela que el gobernado no se encuentre en una situación de incertidumbre jurídica y, por tanto, en estado de indefensión. En ese sentido, el contenido esencial del principio de seguridad jurídica en materia fiscal radica en **poder tener pleno conocimiento sobre la regulación normativa prevista en la ley y sobre sus consecuencias**. De esta forma, las manifestaciones concretas del principio aludido se pueden compendiar en **la certeza en el derecho y en la interdicción de la arbitrariedad**; la primera, a su vez, en **la estabilidad del ordenamiento normativo, esto es, que tenga un desarrollo suficientemente claro, sin ambigüedades o antinomias, respecto de los elementos esenciales de la contribución** y la certidumbre sobre los remedios jurídicos a disposición del contribuyente, en caso de no cumplirse con las previsiones de las normas; y la segunda, principal, mas no exclusivamente, a través de los principios de proporcionalidad y jerarquía normativa.

Amparo en revisión 441/2015. Smart & Final del Noroeste, S.A. de C.V. y otra. 5 de octubre de 2016. Cinco votos de los Ministros Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán; votó en contra de consideraciones Margarita Beatriz Luna Ramos. Ponente: Javier Laynez Potisek. Secretario: Jorge Jiménez Jiménez.

Amparo en revisión 845/2015. Tiendas Aurrerá, S. de R.L. de C.V. 5 de octubre de 2016. Cinco votos de los Ministros Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán; votó en contra de consideraciones Margarita Beatriz Luna Ramos. Ponente: Javier Laynez Potisek. Secretario: Jorge Jiménez Jiménez.

Amparo en revisión 876/2015. Desarrollo Comercial Abarrotero, S.A. de C.V. y otras. 25 de enero de 2017. Cinco votos de los Ministros Alberto Pérez Dayán, Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Eduardo Medina Mora I.; votó en contra de consideraciones Margarita Beatriz Luna Ramos. Ponente: Javier Laynez Potisek. Secretario: Jorge Jiménez Jiménez.

Contradicción de tesis 59/2017. Entre las sustentadas por los Tribunales Colegiados Segundo en Materia Administrativa del Segundo Circuito, Primero de Circuito del Centro Auxiliar de la Novena Región, con residencia en Zacatecas, Zacatecas, Primero y Segundo del Trigésimo Circuito y Décimo Primero en Materia Administrativa del Primer Circuito. 12 de julio de 2017. Unanimidad de cuatro votos de los Ministros Alberto Pérez Dayán, Javier Laynez Potisek, José Fernando Franco González Salas y Eduardo Medina Mora I. Ausente: Margarita Beatriz Luna Ramos. Ponente: Alberto Pérez Dayán. Secretario: Jorge Jiménez Jiménez.

Amparo en revisión 478/2017. Patricia Guadalupe López Araujo. 30 de agosto de 2017. Cinco votos de los Ministros Alberto Pérez Dayán, Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Eduardo Medina Mora I.; votó con salvedad Javier Laynez Potisek. Ponente: Alberto Pérez Dayán. Secretario: Jorge Jiménez Jiménez.

Tesis de jurisprudencia 140/2017 (10a.). Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del trece de septiembre de dos mil diecisiete.

Esta tesis se publicó el viernes 06 de octubre de 2017 a las 10:16 horas en el Semanario Judicial de la Federación y, por ende, se considera de aplicación obligatoria a partir del lunes 09 de octubre de 2017, para los efectos previstos en el punto séptimo del Acuerdo General Plenario 19/2013.

Como podemos apreciar, los principios de legalidad tributaria y de seguridad jurídica en materia fiscal son dos pilares de nuestro Estado de derecho que se encuentran íntimamente relacionados y que **tienen como finalidad esencial impedir una actuación arbitraria e imprevisible por parte de las autoridades exactoras**.

No obstante lo anterior, **las normas reclamadas en este juicio regulan de manera deficiente los elementos esenciales del impuesto predial en el municipio de Morelia**, Michoacán, para el ejercicio fiscal del año 2019, dejando un **amplio e inadmisible margen de discrecionalidad a las autoridades** exactoras para afectar a los contribuyentes que están obligados al pago de esa contribución, configurándose así una violación a los referidos principios de legalidad tributaria y de seguridad jurídica en materia fiscal.

Para evidenciar la inconstitucionalidad del impuesto combatido, revisaremos enseguida como se encuentran regulados sus elementos esenciales del impuesto combatido.

Inicialmente, tenemos que **el objeto** del tributo en cuestión en esencia es toda clase de derechos de propiedad o posesión sobre los bienes inmuebles, incluyendo terrenos y construcciones de toda índole.[2]

[2] Al respecto, el artículo 17 de la Ley de Hacienda del Estado de Michoacán, establece textualmente lo siguiente: "**ARTÍCULO 17**. Es objeto del impuesto Predial: I. La propiedad o copropiedad de predios rústicos, urbanos y las construcciones adheridas a ellas, así como la propiedad de condominios; II. Los derechos sobre la propiedad o posesión de terrenos ejidales o comunales y de parcelamiento, así como la posesión de construcciones permanentes en zonas urbanas, ejidales o comunales; III. La posesión de predios rústicos o urbanos y las construcciones adheridas a ellos; IV. Cuando por cualquier título se tenga

Ahora bien, **los sujetos** del referido impuesto predial son precisamente todos los titulares de estos derechos de propiedad o posesión inmobiliarios.[3]

Con respecto a **la base** del controvertido impuesto predial, el artículo 20, primer párrafo, de la Ley de Hacienda Municipal del Estado de Michoacán establece literalmente lo siguiente:

> **"ARTÍCULO 20.** La base del impuesto predial tanto de predios urbanos como rústicos será el valor catastral registrado".

La tasa del impuesto predial en Morelia está contemplada en los artículos 8º y 9º de la Ley de Ingresos para el Municipio de Morelia, para el ejercicio fiscal del año 2019, siendo dicha tasa, en términos generales, del 0.3125% anual sobre el valor catastral que sirve como base del tributo.

Finalmente, la **forma de pago** del impuesto se encuentra regulada de manera general en los artículos 25 y 26 de la Ley de Hacienda Municipal del Estado de Michoacán, donde se estipula que la tesorería municipal determinará el impuesto anual a cargo del contribuyente, debiéndose este de pagar en una sola exhibición o bimestralmente en seis partes iguales.

Cabe señalar que es precisamente **la base del tributo** la que presenta **una deficiente regulación legal**, dejando al contribuyente en un completo estado de incertidumbre respecto a la forma en la que se determina el "valor catastral" de los inmuebles bajo su propiedad o posesión, y permitiendo un amplio margen de discrecionalidad y arbitrariedad a las autoridades que participan en la determinación y cobro del inconstitucional impuesto predial.

En efecto, como vimos en líneas anteriores, la base del impuesto predial es el valor catastral del inmueble que se encuentre

---

la concesión, uso o goce de predios rústicos o urbanos del dominio del Estado, Municipio o de la Federación; V. El usufructo; y, VI. La propiedad o concesión de plantas de beneficio y establecimientos mineros o metalúrgicos, en los términos de la Legislación Federal de la materia, comprendiendo: A) El terreno; y, B) Las construcciones y sus mejoras".

[3] Sobre este punto, el artículo 18 de la Ley de Hacienda Municipal del Estado de Michoacán establece lo siguiente "**ARTÍCULO 18**. Son sujetos del impuesto Predial: I. Los propietarios, copropietarios, condóminos y poseedores de predios; II. Los poseedores de predios; III. Los titulares de los derechos de propiedad o de posesión de los predios fideicomitidos; IV. Los titulares de derechos agrarios sobre la propiedad ejidal o comunal, así como los poseedores de construcciones permanentes en zonas urbanas ejidales o comunales; V. Los poseedores que por cualquier título tengan la concesión, uso o goce de predios del dominio del Estado, de sus Municipios o de la Federación; VI. Los usufructuarios; y, VII. Los propietarios de empresas mineras o metalúrgicas, en los términos de la Legislación Federal de la materia".

registrado ante las autoridades correspondientes. Al respecto, debemos precisar que –de conformidad con el artículo 9º de la Ley de Catastro del Estado de Michoacán– los valores catastrales de los inmuebles **se deben fijar con base en las tablas de valores unitarios de terreno y construcción** que apruebe el Congreso del Estado de Michoacán a propuesta del ayuntamiento correspondiente.

Estas tablas de valores unitarios deben contener el valor estandarizado por metro cuadrado de terreno –dependiendo de la zona de su ubicación– y por metro cuadrado de construcción –dependiendo de su calidad y condiciones–. Por lo tanto, estas tablas de valores unitarios se constituyen en el elemento medular para determinar los valores catastrales de todos los inmuebles en el municipio.

Sin embargo, a pesar de ser determinantes para conocer la base del impuesto predial controvertido, **dichas tablas de valores unitarios no han sido aprobadas ni publicadas oficialmente** para que los contribuyentes sepan con certeza cuáles son los valores unitarios que se tomarán en cuenta para determinar los valores catastrales base del impuesto predial que se cobrará en este ejercicio fiscal de 2019.

En efecto, **no existe ninguna evidencia oficial de que dichas tablas de valores unitarios hayan sido aprobadas por el Congreso del Estado de Michoacán**, como lo prevé el artículo 9º de la Ley de Catastro de nuestra entidad federativa.

Y –suponiendo sin conceder– que dichas tablas hubieran sido aprobadas por el órgano legislativo estatal, resulta patente que **dichas tablas no se han publicado por medio del Periódico Oficial del Estado de Michoacán** para el debido conocimiento de todos los contribuyentes.

Resulta obvio entonces que se está privando a los gobernados de la posibilidad de conocer todos los elementos del impuesto predial para este ejercicio fiscal del año 2019 –especialmente de la forma en la que se determina base de dicho tributo–, dejándolos así en un absoluto **estado de incertidumbre e indefensión jurídica**, a merced de la arbitraria actuación de la autoridad exactora, que determina entonces los correspondientes créditos fiscales de manera discrecional y oscura.

Por lo tanto, estamos ante una flagrante **violación al principio de legalidad tributaria**, ya que uno de los elementos del impuesto predial, específicamente las tablas de valores unitarios determinantes de la base del tributo, no se encuentra contemplado en una ley formal, debidamente aprobada y publicada, mediante la cual se otorgue certidumbre al contribuyente y se evite la actuación arbitraria de la autoridad exactora.

Sobre este tema se ha pronunciado el Pleno de nuestro Más Alto Tribunal en los términos siguientes:

> **Séptima Época**
> **Registro digital: 232795**
> **Instancia: Pleno**
> **Jurisprudencia**
> **Fuente: Semanario Judicial de la Federación**
> **Volumen 91-96, Primera Parte**
> **Materia(s): Constitucional, Administrativa**
> **Página: 172**
> **Genealogía:**
> **Informe 1973, Primera Parte, Pleno, página 348.**
> **Apéndice 1917-1985, Primera Parte, Pleno, tesis 49, página 94.**
> **Apéndice 1917-1988, Primera Parte, Pleno, tesis 79, página 144.**
> **Apéndice 1917-1995, Tomo I, Primera Parte, tesis 161, página 164.**
> **IMPUESTOS, BASES PARA DETERMINAR EL MONTO DE LOS. LA LEY DEBE SEÑALARLAS.**
> La determinación del monto de los impuestos **debe ser hecha en la misma ley** que los establece o, cuando menos, ésta debe fijar las bases generales necesarias para que las autoridades encargadas de su aplicación puedan hacer la fijación del monto del impuesto. De no ser así, se infringe el principio de proporcionalidad y equidad en materia impositiva que establece el artículo 31, fracción IV, de la Constitución Federal.
> *Séptima Epoca, Primera Parte:*
>
> *Volúmenes 91-96, página 90. Amparo en revisión 331/76. María de los Angeles Prendes de Vera. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Carlos del Río Rodríguez.*
>
> *Volúmenes 91-96, página 90. Amparo en revisión 1008/76. Antonio Hernández Abarca. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Arturo Serrano Robles.*
>
> *Volúmenes 91-96, página 90. Amparo en revisión 5332/75. Blanca Meyerberg de González. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Ramón Canedo Aldrete.*
>
> *Volúmenes 91-96, página 90. Amparo en revisión 5464/75. Ignacio Rodríguez Treviño. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Arturo Serrano Robles.*

Volúmenes 91-96, página 90. Amparo en revisión 5888/75. Inmobiliaria Havre, S.A. 31 de agosto de 1976. Unanimidad de quince votos. Ponente: Arturo Serrano Robles.

Al respecto, cobra también aplicación la tesis de jurisprudencia número **2a./J. 94/2017 (10a.)** emitida por la Segunda Sala de la Suprema Corte de Justicia de la Nación, de la que se desprende que la falta de ciertos detalles esenciales de las tablas de valores unitarios previstas en el artículo 115, fracción IV, de la Carta Magna conllevan una grave violación al principio de la legalidad tributaria; por lo que, en casos como el presente, dicha violación es más grave tomando en cuenta que no se han emitido ni publicado ninguno de los elementos que deberían contener las tablas de valores unitarios ordenadas en nuestra Constitución Federal. para mejor referencia, enseguida se copia de forma íntegra la jurisprudencia en comento:

Décima Época
Registro digital: 2014654
Instancia: Segunda Sala
Jurisprudencia
Fuente: Gaceta del Semanario Judicial de la Federación
Libro 43, Junio de 2017, Tomo II
Materia(s): Constitucional
Tesis: 2a./J. 94/2017 (10a.)
Página: 800

TABLAS DE VALORES UNITARIOS DE SUELO Y CONSTRUCCIÓN. RESULTAN VIOLATORIAS DEL PRINCIPIO DE LEGALIDAD TRIBUTARIA, CUANDO NO ESTABLECEN EL CRITERIO PARA CLASIFICAR LOS TIPOS DE CONSTRUCCIÓN, ATENDIENDO A SU CALIDAD DE LUJO, SUPERIOR, MEDIA O ECONÓMICA PARA EFECTOS DEL IMPUESTO SOBRE TRANSMISIONES PATRIMONIALES.

Conforme al antepenúltimo párrafo de la fracción IV del artículo 115 de la Constitución Política de los Estados Unidos Mexicanos los Ayuntamientos, en el ámbito de su competencia, propondrán a las Legislaturas Estatales las cuotas y tarifas aplicables a impuestos, derechos, contribuciones de mejoras y las tablas de valores unitarios de suelo y construcciones que sirvan de base para el cobro de las contribuciones sobre la propiedad inmobiliaria, las cuales revisten una importancia fundamental en la integración de los elementos que conforman el impuesto sobre transmisiones patrimoniales, ya que impactan la base gravable de la contribución, por lo que las normas que contengan dichas tablas deben respetar los principios de justicia tributaria contenidos en el numeral 31, fracción IV, constitucional. En ese sentido, si en las propias tablas de valores unitarios de suelo y construcción, se establece como elemento a considerar en la fijación de la base gravable del impuesto relativo la clasificación del inmueble en

atención a su calidad de construcción como de lujo, superior, media, económica y austera, definiendo lo que debe entenderse sólo por la última de ellas, es claro que **se permite un margen de arbitrariedad a favor de la autoridad administrativa en lo que respecta a la determinación de un elemento que incide en la base gravable del impuesto sobre transmisiones patrimoniales**, lo que **viola el principio de legalidad tributaria**. Cabe precisar que la inconstitucionalidad mencionada no implica que los contribuyentes dejen de pagar el impuesto sobre transmisiones patrimoniales, sino que atendiendo a que la violación constitucional se genera por virtud de la falta de certeza en cuanto a la base aplicable a un determinado inmueble, el efecto de la declaratoria referida consiste en que se aplique el monto de menor cuantía.

Amparo en revisión 323/2015. José Salomón Chidan Charur. 5 de agosto de 2015. Cinco votos de los Ministros Eduardo Medina Mora I., Juan N. Silva Meza, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán. Ponente: Margarita Beatriz Luna Ramos. Secretaria: Claudia Mendoza Polanco.

Amparo en revisión 569/2015. Grupo Constructor 321, S.A. de C.V. 26 de agosto de 2015. Cinco votos de los Ministros Eduardo Medina Mora I., Juan N. Silva Meza, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán. Ponente: Alberto Pérez Dayán. Secretaria: Guadalupe de la Paz Varela Domínguez.

Amparo en revisión 770/2015. Hostales de Occidente, S.A. de C.V. 25 de noviembre de 2015. Cinco votos de los Ministros Eduardo Medina Mora I., Juan N. Silva Meza, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán. Ponente: Eduardo Medina Mora I. Secretario: Miguel Ángel Burguete García.

Amparo en revisión 22/2016. Arturo Daniel Ramírez Cevallos, también conocido como Arturo Daniel Ramírez Ceballos, en su carácter de albacea de la sucesión testamentaria a bienes de Rebeca Ceballos García, también conocida como Rebeca Ceballos García de Ramírez y/o Rebeca Cevallos García. 4 de mayo de 2016. Cinco votos de los Ministros Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán. Ponente: Javier Laynez Potisek. Secretario: Jorge Jiménez Jiménez.

Amparo en revisión 1105/2016. Inversiones e Inmuebles Control, S.A. de C.V. 19 de abril de 2017. Cinco votos de los Ministros Alberto Pérez Dayán, Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Eduardo Medina Mora I. Ponente: Javier Laynez Potisek. Secretario: Ron Snipeliski Nischli.

Tesis de jurisprudencia 94/2017 (10a.). Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del veintiuno de junio de dos mil diecisiete.

Esta tesis se publicó el viernes 30 de junio de 2017 a las 10:36 horas en el Semanario Judicial de la Federación y, por ende, se considera de aplicación obligatoria a partir del lunes 03 de julio de 2017, para los efectos previstos en el punto séptimo del Acuerdo General Plenario 19/2013.

Y asimismo estamos ante una evidente **violación del principio de seguridad jurídica en materia fiscal**, puesto que la falta de una disposición legal en la que se puedan consultar con certeza los valores unitarios conforme a los que se determina la base del impuesto predial en Morelia, deja a los contribuyentes en completo estado de incertidumbre jurídica, porque no pueden conocer con detalle sus derechos y obligaciones fiscales, y en pleno estado de indefensión, pues no tienen acceso a los elementos mínimos requeridos para comprobar el respeto de sus derechos fundamentales y fiscales y, en su caso, ejercitar las acciones correspondientes para defenderlos.

Por ello, queda demostrado que, en perjuicio del quejoso, **las normas atacadas son violatorias de los artículos 14, segundo párrafo, 16, primer párrafo, y 31, fracción IV, todos de la Constitución Política de los Estados Unidos Mexicanos**, donde se reconocen **los principios de seguridad jurídica en materia fiscal y de legalidad tributaria**, por lo que debe concederse el amparo y la protección de la Justicia de la Unión que aquí se demanda.

SEGUNDO CONCEPTO DE VIOLACIÓN

Los **artículos 17 al 44 de la Ley de Hacienda Municipal del Estado de Michoacán de Ocampo**; los **artículos 8º y 9º de la Ley de Ingresos para el Municipio de Morelia, Michoacán, para el ejercicio fiscal 2019**; así como **los artículos 9º, 10, párrafos primero y segundo, 11 y 17 al 28 de la Ley de Catastro del Estado de Michoacán,** todos ellos relativos al impuesto predial aplicable en el municipio de Morelia, Michoacán, **son violatorios del artículo 115, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos**.

Sobre este particular debemos recordar que el **artículo 115, fracción IV,** de la **Constitución Política de los Estados Unidos Mexicanos**, es del tenor literal siguiente:

> **Artículo 115.** Los estados adoptarán, para su régimen interior, la forma de gobierno republicano, representativo, democrático, laico y popular, teniendo como base de su división territorial y de su organización política y administrativa, el municipio libre, conforme a las bases siguientes:
>
> (…)
>
> **IV.-** Los municipios administrarán libremente su hacienda, la cual se formará de los rendimientos de los bienes que les pertenezcan, así como de las contribuciones y otros ingresos que las legislaturas establezcan a su favor, y en todo caso:
>
> **a)** Percibirán **las contribuciones**, incluyendo tasas adicionales, **que establezcan los Estados sobre la propiedad inmobiliaria**, de su fraccionamiento, división, consolidación, traslación y mejora así como las que tengan por base el cambio de valor de los inmuebles.
>
> (…)
>
> **Los ayuntamientos**, en el ámbito de su competencia, **propondrán a las legislaturas estatales** las cuotas y tarifas aplicables a impuestos, derechos, contribuciones de mejoras **y las tablas de valores unitarios de suelo y construcciones que sirvan de base para el cobro de las contribuciones sobre la propiedad inmobiliaria**.

La redacción actual de esta disposición data del 23 de noviembre de 1999, fecha en que se publicó en el Diario Oficial de la Federación un Decreto por el que se declaró reformada y adicionada esa norma constitucional.[4]

De esta manera nuestra Carta Magna estableció un sistema claro y específico para establecer legalmente las tablas de valores unitarios de suelo y construcciones que sirvan como base para determinar los impuestos prediales a favor de los diversos municipios.

Dicho proceso debe iniciar cuando el respectivo **ayuntamiento** presente ante el congreso del estado **una propuesta de las tablas** de valores unitarios de suelo y construcciones.

[4] Conforme a su artículo primero transitorio, el mencionado decreto entró en vigor noventa días después de su publicación en el Diario Oficial de la Federación.

El congreso del estado debe entonces **analizar con detenimiento las tablas propuestas por el ayuntamiento**, pudiendo aprobarlas o modificarlas de manera razonada.

Al respecto el Pleno de la Suprema Corte de Justicia de la Nación ha emitido la tesis de jurisprudencia **P./J. 122/2004**, en la que ha delineado los parámetros generales que se deben respetar al momento de que los congresos locales decidan sobre las tablas de valores unitarios propuestas por los ayuntamientos. Enseguida se transcribe de forma íntegra dicha jurisprudencia:

> **Novena Época**
> **Registro digital: 179823**
> **Instancia: Pleno**
> **Jurisprudencia**
> **Fuente: Semanario Judicial de la Federación y su Gaceta**
> **Tomo XX, Diciembre de 2004**
> **Materia(s): Constitucional, Administrativa**
> **Tesis: P./J. 122/2004**
> **Página: 1124**
>
> **PREDIAL MUNICIPAL. CONDICIONES A LAS QUE DEBEN SUJETARSE LAS LEGISLATURAS LOCALES EN LA REGULACIÓN DEL IMPUESTO RELATIVO (INTERPRETACIÓN DE LA FRACCIÓN IV DEL ARTÍCULO 115 DE LA CONSTITUCIÓN FEDERAL).**
> La fracción IV del artículo 115 de la Constitución Política de los Estados Unidos Mexicanos, al disponer el proceso de regulación del impuesto predial, divide las atribuciones entre los Municipios y las Legislaturas Locales, pues mientras aquéllos tienen competencia constitucional para proponer las tablas de valores unitarios de suelo que servirán de base para el cobro del impuesto relativo, así como las cuotas o tarifas que deberán aplicarse sobre dichas tablas para el cálculo final de la cantidad a pagar por los contribuyentes; las Legislaturas Estatales, por su parte, son competentes para tomar la decisión final sobre estos aspectos cuando aprueban las leyes de ingresos de los Municipios. Ahora bien, el alcance exacto y la articulación mutua de las competencias señaladas debe derivarse de una interpretación sistemática de la citada fracción IV, la cual regula, entre otros aspectos, las relaciones entre los Estados y los Municipios en materia de hacienda y recursos económicos municipales, asimismo, establece diversas garantías a favor de los Municipios, como la libre administración de la hacienda municipal, la integridad de los recursos económicos municipales y la existencia de fuentes de ingreso reservadas a los Municipios, las cuales quedarían soslayadas si las Legislaturas Estatales pudieran determinar con absoluta libertad los elementos configuradores del mencionado impuesto, sin necesidad de considerar la propuesta municipal más allá de la simple obligación de recibirla y tenerla como punto de partida formal del proceso legislativo. Por ello, si se toma en cuenta que dicha atribución de propuesta tiene un rango

> constitucional equivalente a la facultad decisoria de las Legislaturas Locales, y que se trata de un impuesto reservado constitucionalmente a las haciendas municipales, es indudable que sólo pueden alejarse de las propuestas municipales si proveen para ello argumentos de los que derive una justificación objetiva y razonable; de ahí que cuando las legislaturas, al aprobar las leyes de ingresos municipales, modifiquen las propuestas de los Ayuntamientos referentes al impuesto predial, es necesario que las discusiones y constancias del proceso legislativo demuestren que dichos órganos colegiados no lo hicieron arbitrariamente, sino que la motivación objetiva en la cual apoyaron sus decisiones se refleje, fundamentalmente, en los debates llevados a cabo en la respectiva comisión de dictamen legislativo.
> Controversia constitucional 14/2004. Municipio de Guadalajara, Estado de Jalisco. 16 de noviembre de 2004. Unanimidad de once votos. Ponente: José Ramón Cossío Díaz. Secretario: Fernando A. Casasola Mendoza.
>
> El Tribunal Pleno, en su sesión privada celebrada hoy treinta de noviembre en curso, aprobó, con el número 122/2004, la tesis jurisprudencial que antecede. México, Distrito Federal, a treinta de noviembre de dos mil cuatro.

Nótese que la Constitución Política de los Estados Unidos Mexicanos **de ninguna manera permite que los ayuntamientos determinen unilateralmente las tablas de valores unitarios**. Nuestra Carta Magna **tampoco permite que el poder ejecutivo local intervenga de ninguna manera en la configuración de tales tablas de valores unitarios**. Por el contrario, nuestro Código Supremo –en armonía con el principio de legalidad tributaria– **confiere siempre a la legislatura local la responsabilidad de tomar la decisión definitiva sobre las tablas de valores unitarios** que deben imperar para efectos de la determinación de la base del impuesto predial.

Empero lo anterior, las normas reclamadas establecen un procedimiento para determinar las tablas de valores unitarios en el Estado de Michoacán que **es contrario al procedimiento previsto en la Constitución Política de los Estados Unidos Mexicanos** que acabamos de describir.

Para evidenciar esta inconstitucionalidad basta leer el contenido de los artículos 9, 10, párrafos primero y segundo, 11 de la Ley de Catastro del Estado de Michoacán, que son del tenor literal siguiente:

> **ARTÍCULO 9.** El Congreso del Estado, aprobará los valores unitarios de terreno y construcción que propongan los Ayuntamientos, los cuales tendrán como referencia los valores de mercado al

momento de elaborarse el estudio. Dichos valores servirán de base para determinar el valor catastral de los predios ubicados en el territorio del Estado.

Para lograr congruencia y homogeneidad en la forma de proponer los valores unitarios de terreno y construcción para aprobación del Congreso del Estado, **los Ayuntamientos procurarán sujetarse a los procedimientos que determine el Secretario de Finanzas y Administración, en la metodología que al efecto emita y publique**. A instancia del Congreso del Estado, la Secretaría de Finanzas y Administración podrá emitir su opinión técnica en relación con los proyectos de valores que presenten los Ayuntamientos.

ARTÍCULO 10. Hasta en tanto el Congreso del Estado, no apruebe nuevos valores unitarios de terreno y construcción, conforme al artículo 9 de esta Ley, **los aprobados se actualizarán para aplicarse en el año de que se trate, a lo que resulte de multiplicar los valores vigentes durante el año de calendario anterior, por el factor que se obtenga de dividir el Índice Nacional de Precios al Consumidor correspondiente al mes de noviembre de dicho año, entre el Índice Nacional de Precios al Consumidor del mismo mes del año precedente que publique el Banco de México**.

Cuando, como resultado de las operaciones a que se refiere el párrafo anterior, se obtengan cantidades en fracción monetaria, las mismas se ajustarán a la unidad monetaria más próxima.

(…)

ARTÍCULO 11. La Autoridad Municipal en su respectiva jurisdicción y mientras el Congreso del Estado, no apruebe nuevos valores unitarios de terreno conforme a lo establecido en el artículo 9 de esta Ley, **deberá asignar valor a las nuevas áreas de desarrollo urbano, tomando como base los valores aprobados por el Congreso del Estado, para áreas de desarrollo urbano equivalentes**.

Para efectos de realizar las acciones catastrales a que se refiere el artículo 31 de esta Ley en las nuevas áreas de desarrollo urbano y, **hasta en tanto la Autoridad Municipal realiza la asignación a que se refiere el párrafo que antecede, la Secretaría de Finanzas y Administración asignará los valores unitarios de terreno que corresponda a dichas áreas, considerando el valor determinado por el Congreso del Estado, a una zona de desarrollo urbano equivalente en cada población**.

De la lectura de estas normas legales, podemos ver varias irregularidades que atentan contra lo previsto en nuestra Carta Magna.

En primer lugar, las disposiciones legales transcritas **permiten abiertamente que los ayuntamientos y la legislatura local**

incumplan con sus respectivos deberes constitucionales de proponer y aprobar de manera regular las tablas de valores unitarios que sirven como base para determinar el impuesto predial a cargo de los contribuyentes.

Esto es así porque las disposiciones de la ley de catastro local transcritas establecen previsiones para el caso de que los ayuntamientos y el congreso local sean omisos en el cumplimiento de su deber, lo cual es totalmente inadmisible, pues en la práctica se está permitiendo y regulando una situación de hecho contraria a nuestra Carta Magna: **la inactividad legislativa**.

Además debe precisarse que estas normas legales son inconstitucionales porque **dan píe a que los ayuntamientos y la legislatura local prolonguen indefinidamente su omisión** de proponer y aprobar las multireferidas tablas, lo cual **es contrario al espíritu del artículo 115, fracción IV, constitucional**, cuyo fin primordial fue establecer un procedimiento razonable para que se emitan **de manera periódica regular** tablas de valores unitarios que reflejen de forma siempre actualizada la realidad económica de los inmuebles en el cada municipio, como fuente de riqueza que debe ser gravada siempre de manera proporcional y equitativa, en armonía con el artículo 31, fracción IV, de nuestro Código Supremo. La voluntad del Poder Revisor de la Constitución se desprende de la simple lectura del artículo transitorio quinto del Decreto por el que se declara reformado y adicionado el artículo 115 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el día 23 de diciembre de 1999 y que a la letra dice:

> **ARTICULO QUINTO.** Antes del inicio del ejercicio fiscal de 2002, las legislaturas de los estados, en coordinación con los municipios respectivos, adoptarán las medidas conducentes a fin de que los valores unitarios de suelo que sirven de base para el cobro de las contribuciones sobre la propiedad inmobiliaria sean equiparables a los valores de mercado de dicha propiedad y procederán, en su caso, a realizar las adecuaciones correspondientes a las tasas aplicables para el cobro de las mencionadas contribuciones, **a fin de garantizar su apego a los principios de proporcionalidad y equidad**.

Admitir lo que establece la Ley de Catastro del Estado de Michoacán, nos llevaría al extremo de **permitir que las tablas de valores unitarios se mantengan desactualizadas de manera**

indefinida hasta en tanto los ayuntamientos y las legislaturas decidan unilateralmente cumplir con sus obligaciones constitucionales.

Por otra parte, las citadas disposiciones de la Ley de Catastro local estipulan un mecanismo muy diverso al previsto por la Carta Magna para la emisión de las tablas de valores unitarios de suelo y construcción.

Podemos afirmar lo anterior porque las normas reclamadas prevén la posibilidad de que **los propios ayuntamientos establezcan sus tablas de valores unitarios sin la necesidad de la aprobación del congreso local** cuando se trata de zonas de nueva creación no previstas en las tablas de valores unitarios.

Sin embargo, debe hacerse énfasis en que nuestra Carta Magna fue clara al disponer en su artículo 115, fracción IV, que las tablas de valores unitarios **deben ser aprobadas única y exclusivamente por el correspondiente congreso local, sin que pueda delegarse dicha responsabilidad a los ayuntamientos locales**.

Por lo tanto, resulta inconstitucional el permiso que dan las normas reclamadas a los ayuntamientos locales. Y dicha irregularidad resulta inadmisible si tomamos en cuenta que con ello no solo se contraviene un claro procedimiento constitucional, sino que **se permite a los ayuntamientos un amplio margen de discrecionalidad y arbitrariedad** en el cobro del impuesto predial municipal, además de que se contraviene el principio de legalidad tributaria al permitir que un elemento esencial del impuesto –la base– se establezca mediante un proceso meramente administrativo y no legislativo.

Además, es reprochable y contrario a la constitución que las normas transcritas de la Ley de Catastro del Estado de Michoacán **permitan al Poder Ejecutivo del Estado de Michoacán, a través de su Secretaría de Finanzas y Administración, interferir en el proceso de propuesta y aprobación de las tablas de valores unitarios de suelo y construcciones**, mediante la imposición de lineamientos de procedimiento y metodología a los que deben sujetarse los ayuntamientos para la formulación de sus propuestas al poder legislativo local.

Esto resulta inadmisible si tomamos en cuenta que el artículo 115, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos también es claro al establecer un procedimiento en el que los ayuntamientos proponen y el Poder Legislativo local autoriza las tablas de valores unitarios **sin que el Poder Ejecutivo local sea de ninguna manera intermediario** en dicho procedimiento.

Por lo tanto, deben declararse inconstitucionales las normas reclamadas, máxime que admitirlas equivaldría a tolerar una vulneración a la clara esfera de atribuciones de los ayuntamientos y el poder legislativo michoacanos.

Por último, encontramos otro vicio de inconstitucionalidad en las normas reclamadas cuándo permiten qué se actualicen las tablas de valores unitarios conforme al fenómeno económico de la inflación, en base a un supuesto Índice Nacional de Precios al Consumidor emitido por el Banco de México.

Esta previsión contraviene nuevamente el claro proceso legislativo contemplado en el artículo 115, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos, pues permite la intervención del Banco de México en dicho proceso, aún cuando la responsabilidad constitucional de aprobar esas tablas corresponde en exclusiva a los congresos locales.

No es dable justificar la participación del Banco de México argumentando la necesidad de mantener actualizados conforme a la inflación los valores unitarios previstos en las tablas multireferidas, pues en todo caso los congresos locales podrían utilizar por su cuenta los índices inflacionarios de referencia cuando lo creyeran conveniente para actualizar los valores unitarios cada vez que aprobaran nuevas tablas conforme al claro procedimiento previsto en nuestro Código Supremo. Lo anterior, sobre todo si tomamos en cuenta que los valores inmobiliarios rara vez obedecen al fenómeno inflacionario general, ya que en realidad suelen aumentar o disminuir dinámicamente en base a fenómenos urbanísticos, comerciales, sociales y políticos imperantes en la zona de su ubicación. Así un inmueble puede subir o bajar drásticamente de valor dependiendo de factores ajenos a la simple inflación, como serían el acceso a servicios públicos, la seguridad pública, y la cercanía con centros de interés económico y social (centros comerciales, laborales, recreativos, etcétera).

Ello al margen de que el Banco de México actualmente no tiene facultades para publicar el Índice Nacional de Precios al Consumidor, pues dicha responsabilidad recae en el Instituto Nacional de Estadística y Geografía, conforme a los artículos 59, fracción III, inciso a) de la Ley del Sistema Nacional de Información Estadística y Geográfica, 20 y 20-bis del Código Fiscal de la Federación, y 23 fracción X del Reglamento Interior del Instituto Nacional de Estadística y Geografía.

En este sentido, resulta ilustrativa la siguiente tesis de jurisprudencia emitida por la Suprema Corte de Justicia de la Nación, de la que se desprende la inconstitucionalidad de las normas fiscales en las que se delega a autoridades diversas al poder legislativo la facultad de establecer elementos que se deban tomar en cuenta por los contribuyentes para calcular la base gravable, aun cuando dichas autoridades tengan cierta capacidad técnica ampliamente reconocida:

> **Novena Época**
> **Registro digital: 200283**
> **Instancia: Pleno**
> **Jurisprudencia**
> **Fuente: Semanario Judicial de la Federación y su Gaceta**
> **Tomo II, Octubre de 1995**
> **Materia(s): Constitucional, Administrativa**
> **Tesis: P./J. 27/95**
> **Página: 52**
> **INDICE NACIONAL DE PRECIOS AL CONSUMIDOR. EL ARTICULO 20 DEL CODIGO FISCAL DE LA FEDERACION ES INCONSTITUCIONAL POR VIOLAR LA GARANTIA DE LEGALIDAD TRIBUTARIA (TEXTO VIGENTE EN MIL NOVECIENTOS OCHENTA Y SIETE).**
> El segundo párrafo del artículo 20 del Código Fiscal de la Federación, según texto vigente en el año de mil novecientos ochenta y siete, al disponer que deberá aplicarse el Indice Nacional de Precios al Consumidor calculado por el Banco de México para determinar las contribuciones y sus accesorios, en los casos en que las leyes fiscales así lo establezcan, viola la garantía de legalidad tributaria consagrada en el artículo 31, fracción IV, constitucional, porque no precisa los componentes, bases, criterios o reglas que deberán considerarse para formular el citado índice, sino que deja en manos del Banco de México la determinación de uno de los elementos que los contribuyentes deben considerar para calcular la base gravable, con lo cual se quebranta la garantía ya citada que busca salvaguardar a los particulares de la actuación caprichosa de autoridades u órganos distintos del legislador, sin que obste a esta conclusión que el índice de que se trata puede ser un instrumento de medición económica confiable, por cuanto su elaboración se halla encomendada a un organismo capacitado técnicamente para detectar las variaciones inflacionarias, pues lo cierto es que la Constitución exige que sea

precisamente el legislador y no otro órgano u organismo diverso, quien precise todos los elementos de la contribución.

Amparo en revisión 1404/91. Hotel Condesa del Mar, S.A. de C.V. 6 de abril de 1995. Unanimidad de once votos. Ponente: Juan Díaz Romero. Secretaria: Adriana Campuzano de Ortiz.

Amparo en revisión 3075/89. Consultoría Directiva, S.A. de C.V. 26 de septiembre de 1995. Unanimidad de once votos. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Salvador Castro Zavaleta.

Amparo en revisión 1042/89. Cydsa, S.A. de C.V. 26 de septiembre de 1995. Unanimidad de once votos. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Homero Fernando Reed Ornelas.

Amparo en revisión 3710/89. Autos La Viga, S.A. de C.V. 26 de septiembre de 1995. Unanimidad de once votos. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Homero Fernando Reed Ornelas.

Amparo en revisión 3754/89. Compañía Inmobiliaria y de Inversiones Universidad, S.A. de C.V. 26 de septiembre de 1995. Unanimidad de once votos. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Homero Fernando Reed Ornelas.

El Tribunal Pleno en su sesión privada celebrada el dos de octubre en curso, por unanimidad de once votos de los ministros: presidente José Vicente Aguinaco Alemán, Sergio Salvador Aguirre Anguiano, Mariano Azuela Güitrón, Juventino V. Castro y Castro, Juan Díaz Romero, Genaro David Góngora Pimentel, José de Jesús Gudiño Pelayo, Guillermo I. Ortiz Mayagoitia, Humberto Román Palacios, Olga María Sánchez Cordero y Juan N. Silva Meza; aprobó, con el número 27/1995 (9a.) la tesis de jurisprudencia que antecede; y determinó que las votaciones de los precedentes son idóneas para integrarla. México, Distrito Federal, a dos de octubre de mil novecientos noventa y cinco.

Por lo tanto, resulta absolutamente inadmisible y contraria a la Constitución la previsión que hacen las normas reclamadas para que las tablas de valores unitarios de suelo y construcción se actualicen conforme a la inflación supuestamente reflejada en el Índice Nacional de Precios al Consumidor publicado por el Banco de México.

Todas estas irregularidades en las normas reclamadas constituyen en suma una clara violación el perjuicio del quejoso al **artículo 115, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos,** por lo que resulta dable conceder a la parte quejosa el amparo y la protección de la Justicia Federal que aquí se reclama.

TERCER CONCEPTO DE VIOLACIÓN

Los **artículos 17 al 44 de la Ley de Hacienda Municipal del Estado de Michoacán de Ocampo**; los **artículos 8º y 9º de la Ley de Ingresos para el Municipio de Morelia, Michoacán, para el ejercicio fiscal 2019**; así como **los artículos 9º, 10, párrafos primero y segundo, 11 y 17 al 28 de la Ley de Catastro del Estado de Michoacán,** todos ellos relativos al impuesto predial aplicable en el municipio de Morelia, Michoacán, **son violatorios de los principios de proporcionalidad y equidad tributarias** previstos en el artículo **31, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos**.

Sobre este tema, es oportuno recordar que el artículo 31, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos reconoce a favor de los gobernados **los principios de proporcionalidad y equidad tributarias,** en los siguientes términos:

> **Artículo 31.** Son obligaciones de los mexicanos:
>
> (…)
>
> **IV.** Contribuir para los gastos públicos, así de la Federación, como de los Estados, de la Ciudad de México y del Municipio en que residan, de **la manera proporcional y equitativa** que dispongan las leyes.

El principio de **proporcionalidad tributaria** implica que cada gobernado debe contribuir al gasto público en función de su respectiva capacidad contributiva, de tal forma que los contribuyentes que tengan más capacidad económica contribuyan en forma proporcionalmente mayor a los que tengan menor capacidad económica.

Por otro lado, el principio de **equidad tributaria** se traduce en que todos los contribuyentes que se sitúen en la misma hipótesis jurídicas contribuyan de la misma manera y que sólo los contribuyentes que se sitúen en hipótesis jurídicas distintas contribuyan de manera distinta al gasto público.

Estos principios constitucionales han quedado ampliamente explicados en diversas tesis de jurisprudencia expedidas por nuestro Más Alto Tribunal, como la que enseguida se transcribe:

Séptima Época
Registro digital: 232197
Instancia: Pleno
Jurisprudencia
Fuente: Semanario Judicial de la Federación
Volumen 199-204, Primera Parte
Materia(s): Constitucional, Administrativa
Página: 144
Genealogía:
Informe 1985, Primera Parte, Pleno, tesis 5, página 371.
Apéndice 1917-1995, Tomo I, Primera Parte, tesis 170, página 171.
IMPUESTOS, PROPORCIONALIDAD Y EQUIDAD DE LOS.

El artículo 31, fracción IV, de la Constitución, establece los principios de proporcionalidad y equidad en los tributos. La proporcionalidad radica, medularmente, en que los sujetos pasivos deben contribuir a los gastos públicos en función de su respectiva capacidad económica, debiendo aportar una parte justa y adecuada de sus ingresos, utilidades o rendimientos. Conforme a este principio los gravámenes deben fijarse de acuerdo con la capacidad económica de cada sujeto pasivo, de manera que las personas que obtengan ingresos elevados tributen en forma cualitativamente superior a los de medianos y reducidos recursos. El cumplimiento de este principio se realiza a través de tarifas progresivas, pues mediante ellas se consigue que cubran un impuesto en monto superior los contribuyentes de más elevados recursos y uno inferior los de menores ingresos, estableciéndose, además, una diferencia congruente entre los diversos niveles de ingresos. Expresado en otros términos, la proporcionalidad se encuentra vinculada con la capacidad económica de los contribuyentes que debe ser gravada diferencialmente conforme a tarifas progresivas, para que en cada caso el impacto sea distinto no sólo en cantidad sino en lo tocante al mayor o menor sacrificio, reflejado cualitativamente en la disminución patrimonial que proceda, y que debe encontrarse en proporción a los ingresos obtenidos. El principio de equidad radica medularmente en la igualdad ante la misma ley tributaria de todos los sujetos pasivos de un mismo tributo, los que en tales condiciones deben recibir un tratamiento idéntico en lo concerniente a hipótesis de causación, acumulación de ingresos gravables, deducciones permitidas, plazos de pago, etcétera, debiendo únicamente variar las tarifas tributarias aplicables de acuerdo con la capacidad económica de cada contribuyente, para respetar el principio de proporcionalidad antes mencionado. La equidad tributaria significa, en consecuencia, que los contribuyentes de un mismo impuesto deben guardar una situación de igualdad frente a la norma jurídica que lo establece y regula.

Séptima Epoca, Primera Parte:

Volúmenes 199-204, página 57. Amparo en revisión 2598/85. Alberto Manuel Ortega Venzor. 26 de noviembre de 1985. Unanimidad de diecisiete votos. Ponente: Mariano Azuela Güitrón. Secretaria: María del Carmen Sánchez Hidalgo.

Volúmenes 199-204, página 57. Amparo en revisión 2980/85. Jesús Farías Salcedo. 26 de noviembre de 1985. Unanimidad de diecisiete votos. Ponente: Luis Fernández Doblado. Secretario: Roberto Terrazas Salgado.

Volúmenes 199-204, página 57. Amparo en revisión 2982/85. Rubén Peña Arias. 26 de noviembre de 1985. Unanimidad de diecisiete votos. Ponente: Fausta Moreno Flores. Secretario: Herminio Huerta Díaz.

Volúmenes 199-204, página 57. Amparo en revisión 4292/85. Juan Carlos Francisco Díaz Ponce de León. 26 de noviembre de 1985. Unanimidad de diecisiete votos. Ponente: Mariano Azuela Güitrón. Secretaria: María del Carmen Sánchez Hidalgo.

Volúmenes 199-204, página 57. Amparo en revisión 4528/85. Jean Vandenhaute Longard. 26 de noviembre de 1985. Unanimidad de diecisiete votos. Ponente: Carlos de Silva Nava. Secretaria: Fátima Sámano Hernández.

Nota: En el Informe de 1985 y Apéndice 1917-1995, la tesis aparece bajo el rubro "IMPUESTOS. SU PROPORCIONALIDAD Y EQUIDAD.".

Observaciones:
Nota: En el Semanario Judicial de la Federación, la referencia de la página 58 de los precedentes es incorrecta, la cual se corrige, como se observa en este registro.

Sin embargo, las normas reclamadas en el presente juicio **no respetan los principios constitucionales de equidad y proporcionalidad tributarias,** tal como se explica enseguida.

Como se expuso en el segundo concepto de violación, los artículos 9, 10, párrafos primero y segundo, y 11 de la Ley de Catastro del Estado de Michoacán, permiten tres situaciones irregulares y contrarias a la Constitución General, a saber:

a) Que **se prolongue indefinidamente la omisión** de los ayuntamientos y del Congreso del Estado de Michoacán en cumplir con su obligación de proponer y aprobar, respectivamente, las tablas de valores unitarios del suelo y las construcciones que sirven como base para el cobro del impuesto predial;

b) Que mientras se aprueben nuevas tablas de valores unitarios, **las existentes se actualicen en proporción a la inflación nacional, tomando como referencia para tal efecto el supuesto Índice Nacional de Precios al Consumidor publicado por el Banco de México**; y

c) Que **los ayuntamientos aprueben unilateralmente valores** unitarios de suelo para las áreas "de desarrollo urbano equivalente", mientras no se aprueben nuevas tablas de valores unitarios.

Cada una de esas irregularidades conlleva también una violación a los principios de equidad y proporcionalidad tributarias.

En *primer lugar*, tenemos que el permiso legal para postergar indefinidamente la aprobación de nuevas tablas de valores unitarios genera una constante desactualización de las tablas pre-existentes, pues **estas dejan de reflejar paulatinamente la realidad de los valores de la tierra y los materiales de construcción**, que evolucionan constantemente con base en las cambiantes condiciones urbanas, sociales y económicas de cada municipio.

Al perder su precisión y actualización, las tablas de valores unitarios **dejan de ser confiables como parámetro** para determinar valores catastrales fieles a los valores reales de los inmuebles en el municipio. Por lo tanto, dichas tablas y valores catastrales **dejan de ser acordes a la verdadera capacidad contributiva de los gobernados**, generándose una violación al principio de proporcionalidad tributaria, debido a que estamos en presencia de un impuesto que no afecta a los contribuyentes en una proporción directa a su capacidad de contribuir al gasto público.

En este sentido, debe precisarse que no sirven como excusa las disposiciones que establece la norma catastral reclamada en el sentido de simplemente actualizar los valores unitarios preexistentes mediante la inflación reflejada por los supuestos índices de precios al consumidor, pues es obvio que los valores inmobiliarios no aumentan o disminuyen por el simple efecto de la inflación, sino por múltiples factores económicos como la urbanización de los municipios, la seguridad pública, la existencia de servicios públicos, y la cercanía con lugares de importancia económica, entre otros. Por lo tanto, el tratar de actualizar los valores unitarios con base a la inflación es una medida insuficiente –y hasta contraproducente– para que sean fieles a la siempre cambiante realidad inmobiliaria y para que sean armónicos con los principios de proporcionalidad y equidad tributarias.

En *segundo lugar*, la facultad que confieren las normas impugnadas para que los ayuntamientos aprueben unilateralmente valores unitarios de suelo para las nuevas zonas que supuestamente sean "de desarrollo urbano equivalente" a las previstas en las tablas aprobadas por el congreso local **se traduce en una clara violación a los principios de equidad y proporcionalidad tributarias**, pues esta intervención inconstitucional y discrecional de los ayuntamientos genera una distorsión en los valores unitarios del suelo de las diversas zonas del municipio, que impide brindar un tratamiento equitativo a los contribuyentes, basado en la particular y real capacidad contributiva de cada uno de ellos.

Ya se ha mencionado en páginas anteriores que la intervención de los ayuntamientos en la aprobación de valores unitarios del suelo de ciertas zonas es violatoria del principio de legalidad tributaria, al tratarse de autoridades administrativas. Por lo tanto, aquí es aplicable la jurisprudencia **P./J. 77/99,** emitida por el Pleno de nuestro Más Alto Tribunal, donde se estableció que **la violación al principio de equidad tributaria es *per se* una violación a los principios de equidad y proporcionalidad tributarias**. Dicha tesis jurisprudencial es del tenor literal siguiente:

> **Novena Época**
> **Registro digital: 193475**
> **Instancia: Pleno**
> **Jurisprudencia**
> **Fuente: Semanario Judicial de la Federación y su Gaceta**
> **Tomo X, Agosto de 1999**
> **Materia(s): Constitucional, Administrativa**
> **Tesis: P./J. 77/99**
> **Página: 20**
> **LEGALIDAD TRIBUTARIA. EL EXAMEN DE ESTA GARANTÍA EN EL JUICIO DE AMPARO, ES PREVIO AL DE LAS DEMÁS DE JUSTICIA FISCAL.**
> Las argumentaciones encaminadas a poner de manifiesto en el juicio de amparo, la existencia de una violación a la garantía de legalidad tributaria consagrada en el artículo 31, fracción IV, de la Constitución General de la República, deben examinarse previamente a las que también se esgriman respecto de la violación de las demás garantías de justicia fiscal de los tributos, dado que el principio general de legalidad constituye una exigencia de primer orden, conforme al cual ningún órgano del Estado puede realizar actos individuales que no estén previstos y autorizados por una disposición legal anterior, por lo que de no respetarse, no podría considerarse equitativa y proporcional una contribución cuyos elementos no estén expresamente previstos en una ley formal y material.

Amparo en revisión 1897/95. Calixto Villamar Jiménez. 13 de abril de 1999. Mayoría de ocho votos. Disidentes: Juan Díaz Romero, José Vicente Aguinaco Alemán y Olga María Sánchez Cordero. Ponente: Juan Díaz Romero. Encargado del engrose: Guillermo I. Ortiz Mayagoitia. Secretario: Armando Cortés Galván.

Amparo en revisión 1404/95. Carlos Alberto Hernández Pineda. 13 de abril de 1999. Mayoría de ocho votos. Disidentes: Juan Díaz Romero, José Vicente Aguinaco Alemán y Olga María Sánchez Cordero. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Francisco de Jesús Arreola Chávez.

Amparo en revisión 205/97. Fidel Enrique Navarro Espinoza. 13 de abril de 1999. Mayoría de ocho votos. Disidentes: Juan Díaz Romero, José Vicente Aguinaco Alemán y Olga María Sánchez Cordero. Ponente: Sergio Salvador Aguirre Anguiano. Secretaria: Alejandra de León González.

Amparo en revisión 146/97. J. Jesús Martínez Franco. 13 de abril de 1999. Mayoría de ocho votos. Disidentes: Juan Díaz Romero, José Vicente Aguinaco Alemán y Olga María Sánchez Cordero. Ponente: José de Jesús Gudiño Pelayo. Secretaria: Guadalupe M. Ortiz Blanco.

Amparo en revisión 3093/96. Beatriz Ramírez Ortiz. 13 de abril de 1999. Mayoría de ocho votos. Disidentes: Juan Díaz Romero, José Vicente Aguinaco Alemán y Olga María Sánchez Cordero. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: Lourdes Margarita García Galicia.

El Tribunal Pleno, en su sesión privada celebrada el trece de julio del año en curso, aprobó, con el número 77/1999, la tesis jurisprudencial que antecede. México, Distrito Federal, a catorce de julio de mil novecientos noventa y nueve.

En *tercer lugar*, tenemos que la intervención del Banco de México en la configuración de uno de los elementos de la base del impuesto predial constituye una violación más al principio de legalidad tributaria, como se ha visto en páginas anteriores. Así que nuevamente estamos en presencia de una violación a los principios de equidad y proporcionalidad tributarias, conforme al criterio de la Suprema Corte de Justicia de la Nación plasmado en la jurisprudencia **P./J. 77/99** arriba citada.

Además, la previsión que hacen las normas reclamadas en el sentido de actualizar los valores unitarios con base en la inflación anual genera una paulatina desactualización de las tablas de valores unitarios de suelo y construcciones, ya que en realidad las propiedades inmobiliarias cambian de valor de forma dinámica, dependiendo de diversas circunstancias de

índole comercial, urbanística, social y política. Por lo tanto, al apartarse de la realidad inmobiliaria, las tablas de valore unitarios dejan de reflejar la verdadera capacidad contributiva de los dueños o poseedores de los inmuebles, y dejan de ser un instrumento para determinar la base del impuesto predial de una manera confiable y respetuosa de los principios de equidad y proporcionalidad tributaria.

De todo esto, solo podemos concluir que las normas reclamadas **son violatorias**, en perjuicio del quejoso, **de los principios de legalidad y equidad tributarias, reconocidos en el artículo 31, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos,** por lo que se debe conceder a la parte quejosa el amparo y la protección de la Justicia de la Unión que aquí se reclama.

CUARTO CONCEPTO DE VIOLACIÓN

Como consecuencia de lo anterior, todas las normas reclamadas también son violatorias de los **artículos 1°, primer y tercer párrafo y 133**, todos ellos de **la Constitución Política de los Estados Unidos Mexicanos**, como enseguida se explica.

Como sabemos, el artículo 1°, primer y tercer párrafo, constitucional, entre otras cosas, contiene la obligación de todas las autoridades de respetar los derechos fundamentales reconocidos en nuestra Carta Magna, mientras que el artículo 133 constitucional contiene el principio de supremacía constitucional, conforme al cual ninguna de las normas secundarias puede contravenir a la Constitución Política de los Estados Unidos Mexicanos.

No obstante lo anterior, a lo largo de las páginas anteriores hemos expuesto cómo las normas reclamadas son violatorias de diversos derechos fundamentales del quejoso y son contrarias a diversas disposiciones constitucionales.

Por lo tanto, es obvio que las autoridades responsables no cumplieron con su obligación de respetar los derechos fundamentales del quejoso, en contravención del mandato de nuestro primer artículo constitucional.

Asimismo, es notorio que las autoridades responsables conculcaron el principio de supremacía constitucional al

establecer normas secundarias que –como se ha explicado– son contrarias a lo establecido en nuestra Carta Magna.

Por lo tanto, las normas atacadas son violatorias de los de los **artículos 1°, primer y tercer párrafo y 133**, todos ellos de **la Constitución Política de los Estados Unidos Mexicanos**, por lo que se debe conceder el amparo y la protección de la Justicia Federal que se demanda.

* * *

VIII.- PRUEBAS.

Para demostrar mi dicho, ofrezco desde ahora los siguientes medios de convicción, sin perjuicio de poder ofrecer más en caso de ser necesario en el momento procesal oportuno:

1. **DOCUMENTAL PÚBLICA**.- Consistente en la **orden electrónica de pago**, de fecha [redacted], emitida por la Tesorería Municipal de Morelia, Michoacán, a cargo del quejoso, con respecto al inmueble ubicado en [redacted], la cual se encuentra empadronada bajo la clave predial [redacted].

2. **DOCUMENTAL PÚBLICA**.- Consistente en el **comprobante electrónico de pago**, de fecha [redacted], emitido por la Tesorería Municipal de Morelia, Michoacán, a cargo del quejoso, con respecto al inmueble ubicado en el [redacted], la cual se encuentra empadronada bajo la cuenta predial [redacted].

3. **INSTRUMENTAL PÚBLICA DE ACTUACIONES**.- Consistente en todas las constancias y actuaciones que se acumulen en el expediente durante la tramitación del presente juicio de amparo, en todo lo que beneficie a la parte quejosa.

4. **PRESUNCIONAL LEGAL Y HUMANA**.- Consistente en el conocimiento a que llegue la ley o su Señoría de hechos nuevos mediante razonamientos efectuados con base en hechos previamente sabidos, en todo lo que beneficie a esta parte quejosa.

Por lo anteriormente expuesto y fundado, a usted, Honorable Juez, atentamente pido:

PRIMERO: Que, mediante el presente ocurso, así como los documentos y copias que se acompañan, se me tenga por **presentada en tiempo y forma demanda de amparo indirecto** contra las autoridades y actos que arriba se indican;

SEGUNDO: Que se **admita a trámite la presente demanda**, por encontrase totalmente ajustada a derecho;

TERCERO: Que se me tengan por **ofrecidas desde ahora las pruebas** que se indican en el cuerpo de la demanda, sirviéndose **admitirlas y proveer lo necesario para su legal desahogo**; y

CUARTO: Que, después de los trámites que correspondan, se declare la inconstitucionalidad de los actos reclamados y **se conceda a la parte quejosa el amparo y la protección de la Justicia Federal que aquí se demanda**.

Morelia, Michoacán, a 6 de febrero de 2019.

Licenciado en Derecho JAVIER MARTÍN ESCAMILLA BÁEZ
(Firmando mediante la Firma Electrónica Avanzada
del Poder Judicial de la Federación)

PODER JUDICIAL DE LA FEDERACIÓN

EVIDENCIA CRIPTOGRÁFICA - TRANSACCIÓN

Archivo Firmado:
08690010000000000002614548.p7m
Autoridad Certificadora:
Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal
Firmante(s): 1

FIRMANTE				
Nombre:	JAVIER MARTIN ESCAMILLA BAEZ	**Validez:**	BIEN	Vigente

FIRMA				
No. serie:	70.6a.66.20.63.6a.66.00.00.00.00.00.00.00.00.00.00.00.54.e5	**Revocación:**	Bien	No revocado
Fecha: (UTC/ Cd Mx)	06/02/2019 21:01:10 - 06/02/2019 15:01:10	**Status:**	Bien	Valida
Algoritmo:	RSA - SHA256			
Cadena de firma:	63 f3 47 ca 0b 16 35 6f 2c 0f 2e 89 ea 41 0f 7c 8f e7 11 40 32 c9 37 05 b7 fd 76 f7 42 fa 11 f8 b8 6e 04 ab cc 58 7d 4e 86 06 6b fd b3 44 f0 23 21 97 6b 7f d5 7b fc 90 43 56 33 f9 cb 54 84 88 03 a9 e1 60 d4 17 b9 c6 7d 32 a0 56 69 11 75 f1 0b e0 10 0c 1c 93 1a c4 55 41 9a a9 cc 03 b8 5a 1e 48 41 91 f0 a9 72 4f 96 65 c3 96 c1 54 cc 22 c5 51 8b cc b3 11 14 13 3a 47 56 f3 84 ea 8e 46 04 23 fd 99 0b 84 98 15 a7 e4 37 97 95 87 34 ac fe 5f 4b 35 73 17 56 ad cc c4 f1 82 55 ef 47 2d cd 1d 4a d7 2a 15 7d ee 10 64 b4 99 48 ae f4 15 62 26 a5 11 e7 d1 75 da e0 9d bd 77 b7 77 f9 03 2f a5 6a fa a5 c8 b6 70 26 ad 9d 05 67 4d fb 7f 34 ce 01 62 81 af 05 64 07 2f a2 f3 bb d3 5e a2 6f 27 5e 00 e4 8d 3f ac ce 6f 15 49 65 6b 07 99 31 47 23 f9 2e db b1 84 07 6e 41 0e c8 86 d6 c1			

OCSP	
Fecha: (UTC / Cd. Mx.)	06/02/2019 21:01:11 - 06/02/2019 15:01:11
Nombre del respondedor:	OCSP ACI del Consejo de la Judicatura Federal
Emisor del respondedor:	Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal
Número de serie:	70.6a.66.20.63.6a.66.00.00.00.00.00.00.00.00.00.00.00.00.02

TSP	
Fecha : (UTC / Cd Mx)	06/02/2019 21:01:11 - 06/02/2019 15:01:11
Nombre del emisor de la respuesta TSP:	Autoridad Emisora de Sellos de Tiempo del Consejo de la Judicatura Federal
Emisor del certificado TSP:	Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal
Identificador de la respuesta TSP:	7034531
Datos estampillados:	W3xXq5YvpmagXeLmLyREhNB+OUI=

FUENTES DE INFORMACIÓN

Fuentes bibliográficas

DURÁN DÍAZ, Oscar Jorge, *Los títulos de crédito electrónicos y su desmaterialización*, México, Porrúa, 2009.

ELÍAS AZAR, Edgar, *La contratación por medios electrónicos,* México, Porrúa, 2005.

FLORES SALGADO, Lucerito, *Derecho informático*, México, Patria, 2009

FÚSTER SABATER, Amparo y otros, *Criptografía, protección de datos y aplicaciones*. *Guía para estudiantes y profesionales*, México, Alfaomega, 2015.

INSTITUTO DE INVESTIGACIONES JURÍDICAS DE LA UNAM, *Diccionario Jurídico Mexicano*, edición histórica, México, Porrúa, 2011.

LEÓN TOVAR, Soyla H. *et al*, *La firma electrónica avanzada. Estudio teórico, práctico y técnico*, México, Oxford, 2005.

MAIORANO, Ariel, *Criptografía. Técnicas de desarrollo para profesionales*, Buenos Aires, Alfaomega, 2009.

MAREDDU GILBERT, Mariana, *Regulación jurídica del expediente clínico electrónico,* México, Tirant lo Blanch, 2017.

DE MIGUEL ASCENCIO, Pedro Alberto, *Derecho del comercio electrónico*, México, Porrúa, 2005.

ORTEGA TRIGUERO, Jesús J. y otros, *Introducción a la criptografía. Historia y actualidad*, Cuenca, Universidad de Castilla-La Mancha, 2006.

REAL ACADEMIA ESPAÑOLA, *Diccionario de la Lengua Española*, 23ª edición, Madrid, Espasa, 2014.

REYES KRAFFT, Alfredo Alejandro, en *La firma electrónica y las entidades de certificación*, 2ª edición, México, Porrúa, 2008.

SÁNCHEZ GÓMEZ, Narciso, *Primer curso de derecho administrativo*, 7ª ed., México, Porrúa, 2015.

SERRA ROJAS, Andrés, *Derecho administrativo*, *Primer curso*, 29ª ed, México, Porrúa, 2016.

SUSSKIND, Richard, *Tomorrow's lawyers. An introduction to your future*, 2ª ed., Reino Unido, Oxford, 2017

TÉLLEZ VALDÉS, Julio, *Derecho informático*, 4ª edición, México, Mc Graw Hill, 2009.

TÉLLEZ VALDÉS, Julio, Lex cloud computing*. Estudio jurídico del cómputo en la nube en México*, México, Instituto de Investigaciones Jurídicas-UNAM, 2013.

TENA, Felipe J., *Derecho mercantil mexicano,* 22ª edición, México, Porrúa, 2010.

Fuentes hemerográficas

EKERT, Artur y RENNER, Renato, "Los límites físicos de la privacidad", *Investigación y ciencia,* número 472, Barcelona, Prensa Científica, enero de 2016

GARDNER, Martin, “Mathematical Games”, *Scientific American*, volumen 237, número 2, Estados Unidos de Norteamérica, agosto de 1977.

RAMÍREZ VIEYRA, Eréndira (coord.), “El pago electrónico”, *Revista IDC edición especial sobre el mundo de comercio electrónico bajo la ley*, abril de 2017.

Fuentes electrónicas

DIFFIE, WITHFIELD y HELLMAN, Martin, “New Directions in Cryptography”, *IEEE Transactions on Information Theory*, volumen IT-22, número 6, Estados Unidos de Norteamérica, noviembre de 1976. Consultable en https://ee.stanford.edu/~hellman/publications/24.pdf.

CATANZARO, MICHEL *et al*, “Voice Analysis Should Be Used with Caution in Court”, *Scientific American*, 25 de enero de 2017, consultable en https://www.scientificamerican.com/article/voice-analysis-should-be-used-with-caution-in-court/

EDITORES DE *SCIENTIFIC AMERICAN*, “Biometric Security Poses Huge Privacy Risks”, *Scientific American*, enero 1 de 2014, consultable en https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/

HYUNG WOOK NOH *et al*, “Ratiometric impedance sensing of fingers for robust identity authentication”, *Scientific reports. Nature Research*, 19 de septiembre de 2019, consultable en https://www.nature.com/articles/s41598-019-49792-9.pdf

ETSI, *Estándar ETSI TS 102 042*, consultable en la dirección de internet de dicho organismo en la dirección https://www.etsi.org/.

LATHAN, CORINA y RUSSEL, STUART, “Open AI Ecosystem Portends a Personal Assistant for Everyone”, *Scientific American*, 23 de junio de 2016, consultable en la dirección de internet https://www.scientificamerican.com/article/open-ai-ecosystem-portends-a-personal-assistant-for-everyone/ .

MATJAŽ PERC *et al*, “Social and juristic challenges of artificial intelligence”, *Palgrave Comunications*, 29 de agosto de 2019, consultable en https://www.nature.com/articles/s41599-019-0278-x.pdf .

IETF, *memorando RFC 1319*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc1319/.

IETF, *memorando RFC 1320*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc1320/.

IETF, *memorando RFC 1321*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc1321/.

IETF, *memorando RFC 2314*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc2314/.

IETF, *memorando RFC 2986 estándar PKCS #10 sobre especificación de sintaxis de solicitud de certificación*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc2986/.

IETF, *Memorando RFC 3161 protocolo de internet X.509 de sellado de tiempo de infraestructura de clave pública*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc*3161*/.

IETF, *Memorando RFC 3174*, consultable en la dirección electrónica https://datatracker.ietf.org/doc/rfc3174/.

IETF, *Memorando RFC 3647 Infraestructura de clave pública de Internet X.509 Política de certificados y marco de prácticas de certificación*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc*3647*/.

IETF, *memorando RFC 4634*, consultable en la dirección electrónica https://datatracker.ietf.org/doc/rfc4634/.

IETF, *memorando RFC 5208*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc5208/.

IETF, *memorando RFC 5280 estándar de internet X.509 sobre certificado de infraestructura de clave pública y perfil de lista de revocación de certificados*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc5280/.

IETF, *memorando RFC 5652 sintaxis de mensaje criptográfico*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc5652/.

IETF, *memorando RFC 5816*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc*5816*/.

IETF, *memorando RFC 5958 paquete de llaves asimétricas (estándar antes conocido como PKCS#8)*, consultable en la dirección de internet de internet https://datatracker.ietf.org/doc/rfc5958/.

IETF, *memorando RFC 5967 tipo de medio para aplicación PKCS #10*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc5967/.

IETF, *memorando RFC 6149*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc6149/.

IETF, *memorando RFC 6150*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc6150/.

IETF, *memorando RFC 6151*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc6151/.

IETF, *memorando RFC 6234*, consultable en la dirección electrónica https://datatracker.ietf.org/doc/rfc6234/.

IETF, *memorando RFC 6818*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc6818/.

IETF, *memorando RFC 6960 protocolo X.509 de estado de certificado en línea de infraestructura de clave pública de Internet*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc6960/.

IETF, *Memorando RFC 8017 estándar de criptografía de clave pública #1 (PKCS #1): especificaciones de criptografía RSA, versión 2.2*, 2016, consultable en la dirección de internet https://www.rfc-editor.org/pdfrfc/rfc8017.txt.pdf

IETF, *memorando RFC 8398*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc8398/.

IETF, *memorando RFC 8399*, consultable en la dirección de internet https://datatracker.ietf.org/doc/rfc8399/.

ISO e IEC, *estándar ISO/IEC 7810:2003*, consultable en la página de internet http://www.iso.org.

ISO e IEC, *estándar ISO/IEC 7811-1:2014*, consultable en la página de internet http://www.iso.org.

ISO e IEC, *estándar ISO/IEC 7816-1:2011*, consultable en la página de internet http://www.iso.org.

ISO e IEC, *estándar ISO/IEC 10373:2006*, consultable en la página de internet http://www.iso.org.

NITS, *Estándar FIPS PUB 180-4*, consultable en la dirección de internet https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910977 .

NITS, *Estándar FIPS PUB 202*, consultable en la dirección de internet https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919061 .

MERCADO LIBRE ®, página de internet consultable en la dirección electrónica http://www.mercadolibre.com.mx/.

PAY PAL ®, página de internet consultable en la dirección electrónica https://www.paypal.com/mx/home.

SCHECHTER, ERIK, “How to Make Guns Safer”, *Scientific American*, 1 de octubre de 2015, consultable en https://www.scientificamerican.com/article/how-to-make-guns-safer/

STEVENS, Marc *et al*, “Announcing the first SHA1 collision”, en *Google Securyty Blog*, 23 de febrero de 2017, consultable en la dirección electrónica https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

Normatividad

Constitución Política de los Estados Unidos Mexicanos.

Código Civil Federal.

Código de Comercio.

Código Fiscal de la Federación.

Declaratoria de entrada en vigor de la Norma Oficial Mexicana NOM-151-SCFI-2002, publicada el 19 de diciembre de 2005 en el Diario Oficial de la Federación.

Ley de Amparo

Ley de Firma Electrónica Avanzada.

Norma Oficial Mexicana NOM-151-SCFI-2002 relativa a las prácticas comerciales-requisitos que deben observarse para la conservación de mensajes de datos publicada en el Diario Oficial de la Federación el 4 de junio de 2002.

Norma Oficial Mexicana NOM-151-SCFI-2016, relativa a los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos que sustituyó la Norma Oficial Mexicana NOM-151-SCFI-2002, publicada el 30 de marzo de 2017 en el Diario Oficial de la Federación.

Políticas para la obtención y uso de la Firma Electrónica Certificada del Poder judicial de la Federación (FIREL), así como para la operación de su infraestructura tecnológica.

Resolución Miscelánea Fiscal para 2009.

Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación, publicadas en Diario Oficial de la Federación el 10 de agosto de 2014.

Reglas Generales a las que Deberán Sujetarse los Prestadores de Servicios de Certificación, publicadas en Diario Oficial de la Federación el 14 de mayo de 2018.

Segunda Resolución de Modificaciones a la Resolución Miscelánea Fiscal para 2017 y sus anexos 1, 1-A, 3, 7, 9, 11, 14, 15, 16, 18, 20, 23, 25 y 25-Bis, publicada en el Diario Oficial de la Federación del 18 de julio de 2017.

Jurisprudencia

PLENO DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, “Tesis de jurisprudencia P./J. 125/2004” rubro: “FIRMA AUTÓGRAFA. TRATÁNDOSE DE ACTOS O RESOLUCIONES ADMINISTRATIVAS LA ANULACIÓN POR CARECER DE AQUÉLLA PUEDE SER CON O SIN DETERMINACIÓN DE EFECTOS”*, Semanario Judicial de la Federación y su Gaceta*, Novena Época, Tomo XXI, enero de 2005, Materia(s): Administrativa, p. 5. Registro: 179578.

SEGUNDA SALA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, “Tesis de jurisprudencia 2a./J. 2/92”, rubro: “FIRMA FACSIMILAR. DOCUMENTOS PARA LA NOTIFICACION DE CREDITOS FISCALES”, *Gaceta del Semanario Judicial de la Federación*, Octava Época, núm. 56, agosto de 1992, Materia(s): Administrativa, p. 15, Registro: 206419.

SEGUNDA SALA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, “Tesis de jurisprudencia: 2a./J. 148/2016 (10a.)”, rubro: “CONTABILIDAD ELECTRÓNICA. EL ANEXO 24 DE LA RESOLUCIÓN MISCELÁNEA FISCAL PARA 2015, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 5 DE ENERO DE 2015, VIOLA LOS DERECHOS A LA LEGALIDAD Y A LA SEGURIDAD JURÍDICA”, *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 35, octubre de 2016, Tomo I, p. 699, Materia(s): Constitucional, Registro digital: 2012921.

SEGUNDA SALA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, “Tesis aislada 2a. XXIV/2018 (10a.)”, rubro: “CONTABILIDAD ELECTRÓNICA. EL ANEXO 24 DE LA RESOLUCIÓN MISCELÁNEA FISCAL PARA 2017, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 6 DE ENERO DE 2017, ACTUALIZA LOS SUPUESTOS A LOS QUE ESTABA SUJETA LA CONCESIÓN DEL AMPARO CONTRA DICHO ANEXO PARA 2015” *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 53, Abril de 2018, Tomo I, p.: 853, Materia(s): Administrativa, Común, Registro digital: 2016592.

Otras fuentes

CÁMARA DE DIPUTADOS, “Dictamen de las comisiones Unidas de Justicia y de Comercio, con proyecto de decreto por el que se dictaminan diversas reformas y adiciones al Código Civil Federal, al Código de Comercio y a la Ley Federal de Protección al Consumidor en materia de comercio electrónico”, *Gaceta Parlamentaria de la Cámara de Diputados*, año III, número 500, miércoles 26 de abril de 2000.

CÁMARA DE DIPUTADOS, “Dictamen de las comisiones unidas de la función pública, y de economía de la Cámara de Diputados, relativa al proyecto de

decreto que expide la Ley de Firma Electrónica Avanzada", *Gaceta Parlamentaria de la Cámara de Diputados*, 24 de noviembre de 2011.

DIRECCIÓN GENERAL DE NORMAS DE LA SECRETARÍA DE ECONOMÍA, *Respuesta a solicitudes de información con folios 0001000189019, 0001000189119 y 0001000189219*, Oficio No. DGN.312.01.2019.3365 despachado el 13 de septiembre de 2019

ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su Incorporación al Derecho Interno*, recomendada por resolución de la Asamblea General aprobada en la 85ª sesión plenaria el 12 de diciembre de 2001.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su Incorporación al Derecho Interno*, recomendada por resolución de la Asamblea General aprobada en la 85ª sesión plenaria el 16 de diciembre de 1996.

PODER EJECUTIVO DE LOS ESTADOS UNIDOS MEXICANOS, *Iniciativa de decreto por el que se expide la Ley de Firma Electrónica Avanzada*, presentada ante el Senado de la República en sesión de fecha 9 de diciembre de 2010.

RIVEST, Ronald L. y otros, *Patente de los Estados Unidos de Norteamérica número 4,405,829*, 20 de septiembre de 1983.

SENADO DE LA REPÚBLICA, "Dictamen de las comisiones unidas de gobernación y de estudios legislativos con opinión de la comisión de ciencia y tecnología, todas ellas del Senado de la República, con respecto a iniciativa presentada por el Poder Ejecutivo de decreto que expide la Ley de Firma Electrónica

Avanzada", *Gaceta del Senado*, 22 de marzo de 2011, Consideración Primera.

Software utilizado

Hash Droid versión 4.3, desarrollado por Christophe Bouyer (Hobby One), sin restricciones de uso, disponible en la tienda virtual "Google Play", en la página de internet consultable en la siguiente dirección electrónica: https://play.google.com/store/apps/details?id=com.hobbyone.HashDroid .

Portal de Servicios en Línea del Poder Judicial de la Federación, disponible en la página de internet siguiente: http://www.serviciosenlinea.pjf.gob.mx/juicioenlinea

RSA in Action, versión 1.0, desarrollado por Dinesh R, sin restricciones de uso, disponible en la tienda virtual "Google Play", en la siguiente dirección: https://play.google.com/store/apps/details?id=com.dineshr.www.rsapublicprivatekeygenerator .