

## HOMOLOGACIÓN DE LA REGULACIÓN Y OPERACIÓN DE FIRMA ELECTRÓNICA AVANZADA EN MÉXICO Y PROPUESTA DE REFORMA LEGAL QUE INCLUYE ADEMÁS LA MATERIA DE CONSERVACIÓN DE MENSAJES DE DATOS Y DIGITALIZACIÓN DE DOCUMENTOS EN PAPEL

Por: Dr. Alfredo Alejandro Reyes Krafft<sup>1</sup>

**SUMARIO:** I. La firma electrónica. II. Cuestiones a tomar en cuenta para establecer los lineamientos de digitalización por tercero legalmente autorizado. III. Cuestiones a tomar en cuenta para establecer los lineamientos de preservación de evidencia digital. IV. Facultades del Congreso de la Unión. V. Regulación en actos competencia de los Estados. VI. Facultad del Congreso para vincular a la administración pública federal. VII. Facultad del Congreso para vincular a la administración pública estatal y municipal. VIII. Propuestas y reforma a la ley. IX. Anexos.

**RESUMEN:** En el presente trabajo se realiza un estudio de la legislación mexicana, federal, estatal y municipal, de cómo a través de éstas se definieron ciertos actos jurídicos celebrados mediante medios ópticos y/o electrónicos en la evolución de nuestro marco jurídico, reconociéndose así a los medios tecnológicos dentro de dicha legislación, lo cual sirve como base para definir lo que hoy es la Ley de Firma Electrónica Avanzada y debido a la pluralidad de legislaciones que sientan diferentes métodos de tratamiento para los documentos generados por medios electrónicos, el autor propone la homologación de los procesos con el establecimiento de reglas para el reconocimiento de los certificados digitales entre las entidades y las dependencias nacionales, y así se logre mejorar los controles de certificación de la firma electrónica y de los procesos que requieren de ésta.

**PALABRAS CLAVES:** firma electrónica avanzada; homologación normativa; digitalización, evidencia digital; firma digital, certificados digitales.

**ABSTRACT:** On this document a study of Mexican State, Federal and Local legislation is made, and of how through this legislations certain legal acts were defined. This acts were held through optic and/or electronic means on the evolution of our jurisdictional framework, recognizing technological means inside such legislation which nowadays works as a base for defining what today is The Advanced Electronic Signature. Due to the diversity of legislations that state different methods of treatment for the documents that were generated by electronic means, the author proposes the standarization of the processes with the established rules for the recognition of digital certificates among the entities and national premises and by doing so being able to improve the certification control on the Electronic Signature and of the processes that require it.

---

<sup>1</sup>Doctor en derecho, con mención Cum Laude, por la Universidad Panamericana; Director de Negocios Digitales e Industria Bancaria en Grupo Financiero BBVA Bancomer y Coordinador del Advisory Board de la Asociación Mexicana de Internet (AMIPCI), Coordinador del Grupo de Trabajo de Banca y Comercio Electrónico de la Asociación de Banqueros de México, Secretario del Consejo Directivo de GS1 México (Asociación Mexicana de Estándares para el Comercio Electrónico AMECE). Es investigador nacional nivel 1 del Sistema Nacional de Investigadores. Profesor de la Universidad Panamericana (posgrado en derecho), del posgrado en derecho de la Universidad Nacional Autónoma de México -UNAM- y del Tecnológico de Monterrey -ITESM- (Campus Estado de México y Santa Fé).

**KEY WORDS:** Advanced Electronic Signature, Regulatory Standardization; Scanned Documents; Digital Evidence; Digital Signature; Digital Certificates.

## **I.- LA FIRMA ELECTRÓNICA<sup>2</sup>**

La regulación de la firma electrónica en México no es nueva, la contratación entre ausentes usando medios tecnológicos se encuentra en nuestra legislación desde el siglo antepasado, ya el Código de Comercio de 1889 regulaba las operaciones por telégrafo<sup>3</sup> y el Código Civil de 1928 aquellas que se realizaban utilizando el teléfono<sup>4</sup>. La legislación existente desde esa fecha y hasta el 29 de mayo del 2000, requería para la validez del acto o contrato del soporte de la forma escrita y la firma autógrafa, para vincular a las partes en forma obligatoria.

El 29 de mayo del año 2000, se publicó en el Diario Oficial de la Federación el Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal (ahora Código Civil Federal), del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor:<sup>5</sup>

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

Se reconoció en el CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador: La fiabilidad del método para generar, comunicar, recibir o archivar la información (que pueda conservarse sin cambio), su atribución a las personas obligadas y la posibilidad de acceder a ella en

---

<sup>2</sup>Para este tema confrontar: REYES KRAFFT, Alfredo; *La Firma Electrónica y las Entidades de Certificación*; Porrúa; México 2008

NAVARRO ISLA, Jorge (Coordinador): *Tecnologías de la Información y Comunicaciones, Aspectos Legales*; Porrúa-ITAM; México; 2005

ELÍAS AZAR, Edgar: *Contratación por Medios Electrónicos*, México, Porrúa, 2005

NAVA GARCÉS, Alberto Enrique; *La prueba electrónica en materia penal*, México, Porrúa 2011.

<sup>3</sup>Artículo 80 del Código de Comercio en <http://www.diputados.gob.mx/LeyesBiblio/pdf/3.pdf> consultado el 13 de abril del 2012

<sup>4</sup>Art. 1805 del Código Civil <http://www.diputados.gob.mx/LeyesBiblio/pdf/2.pdf> consultado el 13 de abril del 2012

<sup>5</sup>[http://www.diputados.gob.mx/LeyesBiblio/ref/cfpc/CFPC\\_ref03\\_29may00.pdf](http://www.diputados.gob.mx/LeyesBiblio/ref/cfpc/CFPC_ref03_29may00.pdf) consultado el 13 de abril del 2012

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

En el CÓDIGO DE COMERCIO se definió el concepto “Mensaje de Datos” como la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

Respecto de la obligación a los comerciantes de conservar por un plazo mínimo de 10 años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignan contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, en el caso de mensajes de datos se requerirá que el contenido de la información se haya mantenido íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Economía emitió una Norma Oficial Mexicana que establece los requisitos que deberán observarse para la conservación de mensajes de datos.

Se estableció una presunción en materia mercantil, salvo pacto en contrario, de que el mensaje proviene del emisor (atribución a la persona obligada) si ha sido enviado: i) Usando medios de identificación, tales como claves o contraseñas de él (para lo que se requerirá de un previo acuerdo entre las partes), o ii) Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

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

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

Se reformó también la LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR para reconocer la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones (confidencialidad, certeza, seguridad en la información proporcionada al consumidor, etc.), previendo

sanciones administrativas para el caso de que los proveedores no cumplan con dichas disposiciones.

El 30 de mayo del 2000 se publican reformas a la Ley Federal de Procedimiento Administrativo<sup>6</sup> que habilita el empleo optativo para el ciudadano de medios electrónicos para llevar a cabo algunos procedimientos administrativos de gestión.

La entonces Secretaría de Contraloría y Desarrollo Administrativo emitió disposiciones generales el 17 de enero del 2002 con el objeto de certificar el medio de identificación electrónica de los particulares frente a la autoridad en los trámites electrónicos que se realicen.<sup>7</sup>

El 4 de junio del 2002 se publica la NOM- 151- SCFI-2002.- REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACIÓN DE MENSAJES DE DATOS,<sup>8</sup> la cual establece dos métodos; uno para la conservación de mensajes de datos, con fundamento en lo dispuesto por el art. 49 del Código de Comercio y otro para digitalizar archivos soportados en medio físico. El 19 de diciembre del 2005 se publica en el Diario Oficial la resolución por la que se da a conocer la fecha de entrada en vigor.<sup>9</sup> El 13 de julio del 2011, por cuestiones de forma la cuarta Sala Regional Metropolitana del Tribunal Federal de Justicia Fiscal y Administrativa declara la nulidad de la NOM 151.

El 29 de agosto del 2003 se publica un Decreto de Reformas al Código de Comercio en materia de firma electrónica<sup>10</sup> que básicamente adopta la Ley Modelo sobre Firma Electrónica de UNCITRAL), introduce el concepto de firma electrónica fiable o avanzada y complementa la parte relativa a mensaje de datos detallando conceptos como intermediario, acuse de recibo, copia, error, etc. Da reconocimiento y validez de los certificados extranjeros e incorpora además la figura del prestador de servicios de certificación, quien como tercero confiable estará investido de la facultad de validar, por su probidad y su tecnología (no fe pública), el proceso de emisión, identificación y atribución de certificados digitales:

Notarios o Corredores Públicos

Empresas Privadas

Instituciones Públicas

---

<sup>6</sup> [www.diputados.gob.mx/LeyesBiblio/decre/LFPAdm\\_30may00.doc](http://www.diputados.gob.mx/LeyesBiblio/decre/LFPAdm_30may00.doc) consultado el 13 de abril del 2012

<sup>7</sup> <http://www.funcionpublica.gob.mx/index.php/acuerdo-edod-de-menu-legislacion.html> consultado el 13 de abril del 2012

<sup>8</sup> [http://acedicom.edicomgroup.com/archivos/pdf/MX\\_NOM\\_151\\_SCFI.pdf](http://acedicom.edicomgroup.com/archivos/pdf/MX_NOM_151_SCFI.pdf) consultado el 13 de abril del 2012

<sup>9</sup> [http://www.profeco.gob.mx/juridico/normas/resol\\_nom151scfi2002.pdf](http://www.profeco.gob.mx/juridico/normas/resol_nom151scfi2002.pdf) consultado el 13 de abril del 2012

<sup>10</sup> [http://www.diputados.gob.mx/LeyesBiblio/ref/ccom/CCom\\_ref29\\_29ago03.pdf](http://www.diputados.gob.mx/LeyesBiblio/ref/ccom/CCom_ref29_29ago03.pdf) consultado el 13 de abril del 2012

Con fecha 19 de julio del 2004 se publica el reglamento respectivo y el 10 de agosto del 2004 las Reglas Generales que fueron modificadas el 5 de marzo del 2007.<sup>11</sup>

Por acuerdo presidencial publicado en el Diario Oficial el 9 de diciembre del 2005, se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico<sup>12</sup> y se publican posteriormente los Lineamientos para la implementación, homologación, operación y reconocimiento de FEA en la Administración Pública Federal.(DOF 24 de agosto 2006) y los Lineamientos para la operación de dichos sistemas; así como los requerimientos mínimos de funcionalidad y seguridad que garanticen la validez, autenticidad, confidencialidad, integridad y disponibilidad de los documentos electrónicos gubernamentales. (Oficio Circular No. SP/100/0315/2006, firmado por el Secretario de la Función Pública el 19 de mayo del 2006, en vigor a partir del 1 de junio del 2006). Asimismo el 6 de septiembre del 2011 se publica el ACUERDO que establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.

Y el DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Procedimiento Contencioso Administrativo y de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa,<sup>13</sup> DOF 12 de junio del 2009 reformado posteriormente el 3 de junio del 2011 que establece el denominado juicio en línea.

Algunos Estados de la República emiten disposiciones relacionadas con el uso de la firma electrónica avanzada (se anexa cuadro comparativo):

- Aguascalientes: Decreto 468.- Se reforma el Código Civil, Artículos 2873, 2874 BIS, 2875. (otorgación de poder, Registro Público de la Propiedad -firma electrónica, responsabilidad de los servidores públicos del Registro, impugnación de actos de la Dirección del RPP. (20 septiembre 2010) –Ámbito Notarial-
- Baja California: Ley de Firma Electrónica para el Estado de Baja California de 15 de octubre del 2009.
- Chiapas: Ley de Firma Electrónica Avanzada para el Estado de Chiapas (21 de octubre 2009).
- Colima: Ley sobre el Uso de Medios Electrónicos y Firmas Electrónicas para el Estado de Colima de 30 de mayo de 2009.
- Distrito Federal: “Ley de Firma Electrónica del Distrito Federal” (4 Nov 2009).
- Durango: Ley de Firma Electrónica Avanzada para el Estado de Durango de 26 de mayo de 2010.

---

<sup>11</sup> <http://www.firmadigital.gob.mx/marcolegal.html> consultado el 13 de abril del 2012

<sup>12</sup> [www.cidge.gob.mx](http://www.cidge.gob.mx) consultado el 13 de abril del 2012

<sup>13</sup> [https://www.juicioenlinea.gob.mx/portalexterno/faces/pages/seguridad/login2.jspx?\\_adf.ctrl-state=1dh69owqcz\\_4](https://www.juicioenlinea.gob.mx/portalexterno/faces/pages/seguridad/login2.jspx?_adf.ctrl-state=1dh69owqcz_4) consultado el 13 de abril del 2012

- Estado de México: “Ley para el Uso de Medios Electrónicos del Estado de México” (3 Sept 2010).
- Guanajuato: “Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios” (1° Nov. 2004).
- Guerrero: Ley n° 874 que regula el Uso de la Firma Electrónica Certificada del Estado de Guerrero, del 30 de diciembre de 2008 y su Reglamento el 22 de diciembre de 2009.
- Hidalgo: “Ley sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada para el Estado de Hidalgo” (10 marzo 2008)
- Jalisco: Ley de Firma Electrónica Certificada para el Estado de Jalisco y sus Municipios. (enero 2007) y su Reglamento el 28 de noviembre del 2008.
- Morelos: Ley de Firma Electrónica del Estado Libre y Soberano de Morelos de 26 de octubre 2010.
- Quintana Roo: Ley sobre el Uso de Medios Electrónicos, Mensajes de Datos y Firma Electrónica Avanzada para el Estado de Quintana Roo, de 22 junio 2010.
- Sonora: “Ley sobre el Uso de Firma Electrónica Avanzada para el Estado de Sonora”. (6 julio 2006) y su Reglamento 19 de mayo del 2008.
- Yucatán: Ley sobre el Uso de Medios Electrónicos y Firma Electrónica del Estado de Yucatán, abril 2009.

A todo lo anterior habría que adicionar las disposiciones que regulan la firma electrónica en el ámbito financiero y fiscal.

No podemos dejar de considerar las disposiciones relativas a la firma electrónica emitidas por Acuerdo General 21/2007 del Pleno del Consejo de la Judicatura Federal, que establece la firma electrónica para el seguimiento de expedientes (FESE).<sup>14</sup>

Acuerdo de la Comisión de Administración del Consejo de la Judicatura Federal, que establece el procedimiento de asignación, certificación y uso de la Firma Electrónica para el Seguimiento de Expedientes (FESE).

Acuerdo de la Comisión de Administración del Consejo de la Judicatura Federal, mediante el cual se modifican diversas disposiciones al Acuerdo de la propia Comisión, que establece el procedimiento de asignación, certificación y uso de la Firma Electrónica para el Seguimiento de Expedientes (FESE).

La Unidad para el Control de Certificación de Firmas estará a cargo de la Dirección General de Estadística y Planeación Judicial y se auxiliará de los secretarios autorizados de los Juzgados de Distrito, y Tribunales de Circuito.

<sup>14</sup> Consultar la voz: FESE en [http://w3.cjf.gob.mx/sevie\\_page/normativa/Default.asp](http://w3.cjf.gob.mx/sevie_page/normativa/Default.asp) consultado el 13 de abril del 2012

El pasado 11 de enero del 2012 se promulgó la Ley de Firma Electrónica Avanzada,<sup>15</sup> que de acuerdo con su artículo primero transitorio entrará en vigor a los 120 días hábiles siguientes a su publicación en el Diario Oficial de la Federación, es decir, en junio del 2012.

Por otro lado están las disposiciones generales que deberán emitir y publicar en el Diario Oficial la Secretaría de la Función Pública, la Secretaría de Economía y el SAT, en términos de lo dispuesto por el art. 5 de la ley, en los siguientes 90 días hábiles a la entrada en vigor de la ley (octubre del 2012).

Se acordó también, en el tercero transitorio, la emisión de un reglamento en un plazo de 180 días hábiles siguientes a la entrada en vigor de la ley (febrero del 2013).

La regulación tan dispersa de la firma electrónica avanzada en nuestro país ocasiona la coexistencia de varias autoridades (Secretaría de Economía, Secretaría de la Función Pública, Instituto Mexicano del Seguro Social, Servicio de Administración Tributaria, Banco de México, Comisión Nacional de Seguros y Fianzas, Tribunales Federales, así como poderes locales) y por ende distintos prestadores de servicios de certificación que emiten certificados digitales bajo diversa regulación, proceso, vigencia, ámbito de validez, etc. Lo que de principio genera un alto costo al duplicar procesos y al no permitir compartir o centralizar infraestructura, y dificulta su uso a los ciudadanos ya que para cada gestión con autoridad distinta requiere de un certificado diferente, complicando su operación (ya que debe de administrar múltiples certificados, con el consecuente riesgo que ello implica).

Es por ello particularmente importante el establecimiento de reglas para el reconocimiento de certificados digitales entre los distintos estados de la república y las distintas dependencias y entidades federales, de tal forma que permitan su homologación. La forma idónea de realizar esta homologación es mediante el establecimiento en la normativa federal de criterios de homologación de certificados digitales entre la normativa federal, estatal y municipal, lo anterior dará como consecuencia el reconocimiento implícito de certificados, de tal suerte que con un certificado municipal pudieran realizarse trámites federales y viceversa.

Esto dará mucho mayor cobertura al proceso de enrolamiento y certificación digital, pues en lugar de que pocos ciudadanos cuenten con muchos certificados podemos mejor dar un solo certificado digital que le sirva para muchas cosas a muchos ciudadanos.

---

<sup>15</sup> [http://dof.gob.mx/nota\\_detalle.php?codigo=5228864&fecha=11/01/2012](http://dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012) consultado el 13 de abril del 2012

## **II. CUESTIONES A TOMAR EN CUENTA PARA ESTABLECER LOS LINEAMIENTOS DE DIGITALIZACIÓN POR TERCERO LEGALMENTE AUTORIZADO**

Lineamientos para la migración de información soportada en un medio físico a una forma digital.

El documento contempla lineamientos que permitan establecer los requisitos mínimos para proceder a la migración o digitalización de los documentos que se conservan en medios físicos que tengan el carácter de originales y que la ley no tenga disposición en contrario, a través de un cotejo del proceso de migración, por la figura de un Tercero Legalmente Autorizado por la autoridad (TLA), obteniendo como consecuencia que los documentos migrados a mensajes de datos tengan el mismo valor probatorio que los originales en papel que les sirvieron de base.

Se entiende por Tercero Legalmente Autorizado a la persona física o moral que cumple con los requisitos establecidos y es facultada por la autoridad en la materia para verificar y acreditar que un Proceso de Migración de información de un medio físico a una forma digital garantiza que es posible detectar si existe alguna alteración en dicha información, desde el momento en que se generó por primera vez en su forma definitiva, entendida ésta como el resultado de la migración.

Con el objeto de mitigar los riesgos de digitalizar un documento alterado, el propietario de la información en razón de la criticidad y volumen de la información a migrar, deberá, por medio de procesos, elementos humanos y tecnológicos que considere convenientes, aplicar controles con el objetivo de validar que el documento a digitalizar no ha sufrido alteración y que se encuentra íntegro en su estructura física. El TLA será responsable de verificar dentro de su proceso de auditoría la existencia de dichos controles evaluando su efectividad.

### 1. Generalidades

- 1.1. Las personas que opten por migrar información de un medio físico a una forma digital deberán sujetarse a lineamientos, su cumplimiento deberá ser cotejado por el tercero legalmente autorizado al momento de la verificación del proceso de migración, así como auditorías periódicas para brindar mayor certeza al proceso.
- 1.2. Se podrá migrar información de un medio físico a una forma digital a través de terceros prestadores de servicios siempre y cuando los procesos de dichos prestadores de servicios cumplan con lo establecido por los lineamientos aplicables.
- 1.3. Se podrá migrar información que se encuentre soportada en un medio físico a una forma digital, siempre y cuando esté permitido por la legislación vigente y además el proceso de migración haya sido verificado por un tercero legalmente

autorizado y observen para su conservación las disposiciones a la conservación de mensajes de datos.

- 1.4. Se deberá contar con los mecanismos necesarios que permitan detectar si existe alguna alteración en la información migrada, desde el momento en que se generó por primera vez en su forma definitiva, esto es al momento de la migración, mediante los procedimientos y tecnologías de información que utilicen como parte de su proceso de migración.
- 1.5. Se podrán aplicar las tecnologías de información existente en el mercado para el proceso de migración, siempre que dicha tecnología permita cumplir con lo que se establezca en los lineamientos aplicables.
- 1.6. Se debe garantizar que el proceso de migración permita que la información migrada sea accesible para su ulterior consulta, implementando mecanismos de respaldo y recuperación de la información, y permita ser verificada su integridad e inalterabilidad, sin importar el formato en el que se encuentre.
- 1.7. El tercero legalmente autorizado deberá informar a las personas que realicen actos de comercio los límites de responsabilidad de sus servicios.

## 2. Lineamientos Generales del Proceso

El proceso de migración deberá cumplir como mínimo los siguientes requisitos, los cuales deberán estar documentados y deberán ser cotejados por el tercero legalmente autorizado:

- 2.1 Contar con una aplicación que asegure la legibilidad del documento migrado y la futura validación de la inalterabilidad e integridad del documento digitalizado, así como su disponibilidad y accesibilidad para su ulterior consulta. En ningún caso un tercero legalmente autorizado podrá llevar a cabo la prestación de los servicios de digitalización, retención, conservación y almacenamiento de información, de los cuales hubiere verificado y acreditado su proceso de migración.
- 2.2 Que un tercero legalmente autorizado verifique que el proceso de migración se encuentre correctamente documentado y cumple dependiendo del volumen y criticidad de la información, con los niveles de seguridad, controles y aplicaciones habituales o requeridos para asegurar la integridad, inalterabilidad, accesibilidad de la información migrada desde el momento que se generó por primera vez en su forma digital, entendiéndose por ésta su forma definitiva. Se entenderán cumplidos los requisitos de integridad e inalterabilidad del documento migrado salvo prueba en contrario cuando se cuente con procesos y tecnología que permita verificar dicha integridad e inalterabilidad, como es el caso de la firma electrónica avanzada, y surtirá plenos efectos jurídicos a partir del momento de su conservación.

- 2.3 Los mecanismos para la digitalización utilizados deberán garantizar la obtención de un mensaje de datos que pueda representar visualmente de forma fiel e íntegra de cada documento original.
- 2.4 Para los casos en que sea utilizada la firma electrónica avanzada, el certificado usado para la firma de las imágenes debe corresponder al funcionario designado por el propietario de la información, recayendo en quien firme, la responsabilidad de la verificación de la legibilidad, así como la integridad e inalteración del documento antes del proceso de migración.
- 2.5 El resultado del proceso de digitalización deberá organizarse en torno a una base de datos documental, esto es por cada documento digitalizado se deberá conservar un registro con los datos principales del documento, además de un campo en el que se contenga el documento migrado o que enlace al archivo que la contenga. Asimismo, la base de datos creada debe permitir la consulta de los metadatos de referencia identificativa del tercero legalmente autorizado que acreditó el proceso de migración, así como la del sello digital de tiempo y cuando estén incluidos: los datos de la firma electrónica del documento migrado o cualquier otro metadato señalado en el propio proceso de migración.
- 2.6 Se debe disponer de la tecnología y aplicaciones de digitalización con las siguientes funcionalidades:
  - 2.6.1 Se garantice que los datos, imágenes y la base de datos sean íntegros e inalterables de forma automática y a través del tiempo. Se entenderán cumplidos los requisitos de integridad e inalterabilidad del documento migrado digital salvo prueba en contrario cuando se cuente con procesos y tecnología que permita verificar dicha integridad e inalterabilidad, como es el caso de la firma electrónica avanzada, y surtirá plenos efectos jurídicos a partir del momento de su conservación.
  - 2.6.2 Las representaciones visuales deberán proporcionar un nivel de resolución espacial mínimo de 200 ppp (píxeles por pulgada), tanto para imágenes obtenidas en blanco y negro, color o escala de grises. La representación visual obtenida debe respetar la geometría del original en tamaños y proporciones.
  - 2.6.3 Permita acceso completo y sin demora injustificada a la base de datos y los documentos migrados, la copia o descarga en línea en los formatos a los cuales se hayan migrado los documentos y la impresión a papel cuando sea necesario. Para garantizar la independencia de la plataforma tecnológica y evitar su obsolescencia, los formatos a los que se pretenda migrar deben ser autodocumentados y autosuficientes en contenido para asegurar el acceso a las imágenes.

- 2.7 Para que el documento migrado se considere fiel e íntegro ha de ser obtenido en un proceso de migración en el que sin intervención en momento alguno del operador se realicen como mínimo las siguientes tareas:
  - 2.7.1 Digitalización del documento por un medio fotoeléctrico, de modo que se obtenga un mensaje de datos en memoria del sistema asociado al dispositivo.
  - 2.7.2 Optimización de la representación visual del documento migrado para garantizar su legibilidad, de modo que todo el contenido del documento original pueda apreciarse y sea válido para su gestión.
  - 2.7.3 Introducir en el documento migrado, como metadatos, la referencia identificativa del tercero legalmente autorizado que acreditó el proceso, una marca de tiempo. Para la representación de metadatos podrá ser utilizada la especificación estándar denominada XMP (Extensible MetadataPlatform).
  - 2.7.4 Un procedimiento de conciliación para verificar la calidad y legibilidad del documento migrado.

Las personas que deseen que un tercero legalmente autorizado verifique su proceso de migración deberá aportar el proceso documentado en todas sus etapas, las normas técnicas en las que se base el procedimiento de migración, así como los protocolos o normas y procedimientos de seguridad, de control y de explotación referidos a la creación y consulta de la base de datos documental que contenga las imágenes digitalizadas de los documentos originales en papel y en su caso los mecanismos de firma electrónica utilizados.

Las personas que realicen actos de comercio deberán contar con elementos humanos, materiales, tecnológicos y sus procedimientos necesarios para un proceso de migración confiable.

### **III. CUESTIONES A TOMAR EN CUENTA PARA ESTABLECER LOS LINEAMIENTOS DE PRESERVACIÓN DE EVIDENCIA DIGITAL**

#### **PRESERVACIÓN DE PRUEBA DIGITAL**

---

##### **1. TÉRMINOS Y DEFINICIONES**

- Adquisición.- Proceso de creación de una copia de los datos dentro de un conjunto definido.
- Expoliación.- Puede tener una doble connotación. La informática se refiere a la alteración o destrucción de la prueba que puede resultar por degradación

magnética, degradación eléctrica, calor, exposición a alta o baja humedad, así como golpes o vibraciones. Desde la perspectiva legal, se puede referir a la destrucción de una cosa por el acto de un extraño, como, la supresión o alteración de un escrito. Es un acto que provoca que las posibles pruebas en un juicio sean consideradas no válidas, ya sea intencionalmente o por negligencia. En el caso de un documento, por ejemplo, destruir, alterar u ocultar todo se considera “expolio” si el documento era relevante para un litigio en curso.

- Dispositivo Digital.- Equipo electrónico usado para procesar o almacenar información digital.
- Especialista de Prueba Digital (EPD).- Un individuo que puede llevar a cabo las tareas de un PRPD y tiene conocimiento especializado, habilidades y destrezas para manejar una amplia gama de problemas técnicos. Un EPD puede tener habilidades adicionales de nicho, tales como adquisición de redes, de RAM, Linux, etc.
- Identificación.- Proceso que involucra la búsqueda, reconocimiento y documentación de una prueba digital potencial.
- Primer Respondiente de Prueba Digital (PRPD).- Individuo que está autorizado, capacitado y calificado para actuar primero en una escena de un incidente para realizar recolección y adquisición de prueba digital con la responsabilidad del manejo de dicha prueba.
- Preservación.- Proceso para mantener y salvaguardar la integridad y/o condición de original de la prueba digital potencial.
- Prueba digital.- Información o datos, almacenados o transmitidos en forma binaria, que pueden ser considerados como prueba de manera confiable.
- Recolección.- Proceso de recolección de los artículos físicos que contienen la prueba digital potencial.

## 2. PRINCIPIOS PARA EL TRATAMIENTO DE PRUEBA DIGITAL

Un PRPD y EPD deben adquirir la potencial prueba digital en la manera menos intrusiva para evitar introducir cambios cuando sea posible. Mientras se lleve a cabo este proceso, un PRPD debe considerar el método más apropiado para usar. Si introducir cambios no puede ser evitado dadas las circunstancias, los pasos tomados deben ser documentados

para dar cuenta de los cambios introducidos. Los métodos usados deben ser claramente documentados en detalle, y tan práctico como sea posible, también deben ser reproducibles y verificables por un PRPD competente.

La prueba digital es gobernada por tres principios: relevancia, confiabilidad y suficiencia. La prueba digital es relevante cuando se va a probar o refutar un elemento del caso concreto objeto de investigación. La confiabilidad significa generalmente el poder asegurar que la prueba digital es lo que pretende ser. El concepto de suficiencia significa que el PRPD necesita recolectar suficiente evidencia para permitir que los elementos del asunto sean adecuadamente examinados o investigados.

Todas las herramientas de un PRPD deben ser validadas antes de usarlas. El PRPD también debe:

- Documentar todas sus actividades;
- Determinar y aplicar un método para establecer la precisión y confiabilidad de la copia de la prueba digital comparada con la fuente original; y
- Reconocer que el acto de preservación de la potencial prueba digital no siempre puede ser no intrusivo.

### 3. REQUERIMIENTOS PARA EL MANEJO DE PRUEBA DIGITAL

Los principios que gobiernan la prueba digital pueden ser satisfechos de la siguiente manera:

- Relevancia.- Debe ser posible demostrar que el material adquirido es relevante para la investigación; que contiene información valiosa para asistir la investigación de determinado incidente y que hay buenas razones para haber adquirido dicho material.
- Confiabilidad.- Todos los procesos usados en el manejo de una prueba digital potencial deben ser auditables y repetibles. Los resultados de aplicar dichos procesos deben ser reproducibles.
- Suficiencia.- Durante la adquisición, el PRPD deberá haber tomado precaución para asegurar que suficiente material ha sido recolectado para permitir el desarrollo de una adecuada investigación. El PRPD deberá tener la capacidad, a través de auditoría y justificación, de indicar qué tanto material, en total, fue considerado y los procesos usados para decidir qué tanto y cuál material adquirir.

Existen cuatro requisitos para el efectivo manejo de prueba digital. Estos requerimientos son auditabilidad, repetibilidad, reproducibilidad y justificación.

- **Auditabilidad.-** Debe ser posible para un asesor independiente u otra parte autorizada interesada, evaluar los pasos tomados por un PRPD y EPD. Esto será posible mediante la apropiada documentación de todas las acciones tomadas. Un PRPD y EPD deben ser capaces de justificar su proceso de toma de decisiones al seleccionar determinado curso de acción. Los procesos realizados por un PRPD y EPD deben estar disponibles para una valoración independiente para determinar si un procedimiento, técnica o método científico apropiado fue seguido.
- **Repetibilidad.-** Repetibilidad es una propiedad de un proceso usando los mismos instrumentos en el mismo artículo (material), bajo las mismas condiciones para llegar a los mismos resultados. Un PRPD debidamente capacitado y experimentado debe ser capaz de llevar a cabo todos los procesos descritos en la documentación y llegar a los mismos resultados, sin una guía o interpretación. Repetibilidad se establece cuando los mismos resultados de prueba son producidos bajo las siguientes condiciones:
  - o Usando el mismo procedimiento y método de medición;
  - o Usando los mismos instrumentos y bajo las mismas condiciones; y
  - o Puede ser repetido en cualquier momento después de la prueba original.

Un PRPD debe asegurar que el proceso de adquisición es confiable. Para lograr repetibilidad, deben implementarse métodos de control de calidad y documentación del proceso.

- **Reproducibilidad.-** Reproducibilidad es una propiedad del proceso que consiste en usar diferentes procesos en el mismo artículo (material) para llegar al mismo resultado.
- **Justificación.-** El PRPD debe ser capaz de justificar todas las acciones y métodos usados para el manejo de la prueba digital. La justificación puede ser lograda mediante la demostración de que la decisión fue la mejor opción para obtener toda la potencial prueba digital.

#### 4. PASOS EN EL MANEJO DE LA PRESERVACIÓN DE PRUEBA DIGITAL

Toda prueba digital potencial debe ser preservada para asegurar su utilidad en la investigación. Es importante proteger la integridad de la prueba. El proceso de preservación involucra la salvaguarda de potencial prueba digital y dispositivos digitales que puedan

contener potencial prueba digital contra manipulación, alteración y expoliación. El proceso de preservación debe ser iniciado y mantenido a través de los pasos de manejo de prueba digital, comenzando por la identificación de dispositivos digitales que pueden contener prueba digital potencial. Un PRPD debe tener la capacidad de demostrar que la prueba no ha sido modificada desde que fue recolectada o adquirida. Cuando sea requerido por ley, la prueba digital debe ser preservada de manera que asegure la confidencialidad de la información.

## 5. COMPONENTES CLAVE EN LA CADENA DE CUSTODIA Y PRESERVACIÓN DE PRUEBA DIGITAL

- Cadena de Custodia

Un PRPD debe ser capaz de dar cuenta de todos los datos adquiridos y dispositivos en todo momento durante la investigación. El registro de cadena de custodia es un documento que identifica la cronología del movimiento y manejo de la prueba potencial. Esto típicamente puede ser logrado mediante el rastreo de la historia del artículo (material) desde el momento en que fue identificado, recolectado o adquirido por el equipo investigador hasta su estado y ubicación presente.

El registro de cadena de custodia es un documento o serie de documentos relacionados que detallan la cadena de custodia y registra quién fue responsable por el manejo de prueba digital potencial, ya sea en la forma de datos digitales u otros formatos (tales como notas en papel). El propósito de mantener un registro de cadena de custodia es permitir la identificación de acceso y movimientos de prueba potencial en cualquier momento del tiempo. El registro de cadena de custodia puede por sí mismo estar compuesto por más de un documento.

Un registro de cadena de custodia debe contener al menos la siguiente información:

- o Identificador único de prueba;
- o Quién accedió a la prueba, la fecha y ubicación en que tuvo lugar el acceso;
- o Quién y cuándo ingresó y sacó la prueba de las instalaciones de preservación de pruebas;
- o Por qué la prueba fue retirada (qué caso y el propósito) y la autoridad relevante, si fuese aplicable; y
- o Cualquier cambio inevitable a la prueba digital potencial, así como el nombre del individuo responsable y la justificación del por qué se realizó el cambio.

La cadena de custodia debe mantenerse durante todo el ciclo de vida de la prueba y preservado por un cierto período después del fin del ciclo de vida de la prueba. Debe

establecerse desde el momento en que el dispositivo digital o prueba digital potencial es adquirida y no debe comprometerse.

- Preservación de la prueba digital potencial

En la preservación de prueba digital potencial adquirida y dispositivos digitales recolectados durante el empaquetado, es importante asegurar estos artículos (materiales) en una manera que elimine la expoliación o manipulación. La manipulación puede resultar de un acto intencional de hacer o permitir cambios a la prueba digital. Es entonces crucial proteger la prueba digital lo mejor que sea posible, y usar el dato original tan poco como sea posible.

Todo dispositivo digital recolectado y prueba digital potencial adquirida debe ser protegida tanto como sea posible en contra de pérdida, manipulación o expoliación. La actividad más importante en el proceso de preservación es mantener la integridad y autenticidad de la prueba digital potencial y su cadena de custodia.

El dispositivo digital recolectado y prueba digital potencial adquirida deben ser almacenados en una instalación de preservación de prueba que aplique controles físicos de seguridad, tales como sistemas de control de acceso, sistemas de vigilancia, sistemas de detección de intrusos o cualquier otro ambiente controlado para la preservación de prueba digital. Los objetivos principales de la seguridad física son la protección y prevención de pérdida y manipulación, así como permitir la auditabilidad.

## 6. INSTANCIAS EN LA PRESERVACIÓN DE PRUEBA DIGITAL

Después de que el proceso de adquisición ha sido completado, el PRPD debe sellar la información adquirida mediante el uso de funciones de verificación o firmas electrónicas avanzadas. Esto es necesario para confirmar que los contenidos de la imagen copiada no han sido expoliados o manipulados desde que la imagen fue creada. Además, el aspecto de la seguridad de los pasos de manejo de la prueba es importante. El PRPD debe de asegurarse de lo siguiente:

- Usar una función apropiada de verificación para proveer evidencia de que los archivos copiados son equivalentes a los originales.
- Puede ser apropiado asociar al PRPD con la prueba digital potencial adquirida, usando firmas electrónicas avanzadas, sistemas biométricos y fotografías.

Todos los dispositivos digitales que fueron recolectados deben ser adecuadamente preservados. Como una alternativa a sellar la información adquirida con funciones de verificación o firmas electrónicas avanzadas, el PRDP puede usar también sistemas o características biométricas. Al adjuntar características biométricas a la prueba adquirida, se puede asegurar que la prueba no sea manipulada sin comprometer la característica biométrica.

#### **IV. FACULTADES DEL CONGRESO DE LA UNIÓN**

A) La facultad del Congreso de la Unión para legislar en materia mercantil de conformidad con la fracción X del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos ha sido materia de estudios. No se tiene conocimiento de objeción respecto del ejercicio de dichas atribuciones mediante las reformas a la legislación federal que se aprobaron en mayo de 2000 y agosto del 2003, por lo que en el presente análisis se prescinde de la materia comercial por no representar problema alguno.

B) En cuanto a la promulgación de una “Ley de Firma Electrónica Avanzada”, de aplicación en la administración pública federal, el Congreso de la Unión tiene facultad para expedirla con fundamento en el artículo 90, en relación con el artículo 73, fracción XXX de la Constitución Política de los Estados Unidos Mexicanos. Lo anterior es así, en virtud de lo siguiente:

El artículo 90 constitucional, reformado en abril de 1981, faculta al Congreso de la Unión para expedir una Ley Orgánica para la Administración Pública Federal, mientras que la fracción XXX del artículo 73 constitucional, sirve de fundamento a efecto de que el mismo órgano legislativo emita cualquier ley que sea necesaria a objeto de hacer efectivas las facultades del propio Congreso.

En efecto, la fracción XXX de dicha disposición contiene las llamadas facultades implícitas, las que se entienden conferidas al Congreso de la Unión, a efecto de legislar en aquellas materias que si bien no se encuentran expresamente establecidas en el artículo 73 u otros preceptos, sí se requieren para hacer efectivas las atribuciones de la Federación. (Ver tesis en la parte final).

En tal virtud, debe observarse que la ley se encuentra dirigida a regular y atribuir valor jurídico a determinados actos que se llevarían a cabo en situaciones cuya regulación corresponde al Gobierno Federal, bien sea porque se traduzcan en cuestiones mercantiles, porque referan a actos jurídicamente realizados ante o por las dependencias o autoridades federales, etc.

Por otra parte, la fracción XXIX-F del artículo 73 constitucional, establece que el Congreso se encuentra facultado para expedir leyes tendientes a la generación, difusión y aplicación de los conocimientos científicos y tecnológicos que requiere el desarrollo nacional. De lo anterior se desprende que la ley en análisis, está difundiendo y aplicando los conocimientos tecnológicos que requieren el desarrollo nacional, en virtud de que se facilitaría el uso de los modernos sistemas de comunicación e informáticos y se impulsaría el uso de los mismos por los diversos sectores de la sociedad y del gobierno, generando con ello el consecuente desarrollo nacional en esta materia y evitando el rezago con respecto a otros estados más avanzados tecnológicamente en materia informática. Debe entenderse que si bien este precepto no constituye el fundamento directo para el ejercicio de tales atribuciones por parte de la Federación, la legislación es desde luego compatible con el mismo.

Finalmente, la fracción XVII del artículo 73 constitucional, establece competencia al Congreso de la Unión para legislar sobre vías generales de comunicación. En estricto tenor, debe observarse que el objeto de la ley es otorgar validez jurídica a los mensajes de datos y firmas electrónicas (entre otros), lo cual no constituye una vía general de comunicación. No obstante, si dichos datos y firmas serán transmitidos en virtud de comunicación informática por diversos medios como el servicio de internet, que constituye jurídicamente un servicio de valor agregado que opera a través de vías generales de comunicación, es de observarse que, de existir implicaciones técnicas por la trasmisión de dicha información que afecten las comunicaciones de competencia federal, no habría problema alguno para legislar al respecto, por tratarse en ambos casos de funciones propias de las autoridades federales.

Lo anterior no implica que los estados carezcan de competencia para emitir leyes similares, puesto que los mismos podrán dar de igual forma validez jurídica a actos de similar naturaleza, sin pronunciarse respecto a las características o requisitos que deben tener dichas vías generales de comunicación.

Así pues, la permisión de llevar a cabo actos jurídicos por medios informáticos será objeto de la legislación federal, en la medida en que transforman los requisitos y características de los actos jurídicos que son materia de regulación federal, tales como la celebración de un contrato administrativo con el gobierno federal, el cumplimiento de trámites o presentación de promociones o solicitudes ante el gobierno indicado, la celebración de actos de comercio, la participación en procedimientos administrativos federales, etc. Obviamente, en el ámbito de la administración pública local, la competencia normativa se surte a favor de las legislaturas de los estados y del D.F.

## **V. REGULACIÓN EN ACTOS COMPETENCIA DE LOS ESTADOS**

Como acertadamente se aprecia de la lectura del artículo 3 de la ley, la norma jurídica, tendrá aplicación en el ámbito federal, puesto que el Congreso de la Unión no cuenta con facultades para dar validez jurídica a los mensajes de datos o a las firmas electrónicas en relación con actos que son materia de legislaciones locales, a menos que dichas normas se encuentren contenidas en la legislación local.

En efecto, debe observarse que existen determinados actos jurídicos que son materia de legislación por parte de los Estados, por lo que sin modificar las características y requisitos de dichos actos jurídicos, podrían establecerse reglas para el reconocimiento de certificados digitales en los distintos estados de la república y las distintas dependencias y entidades federales, de tal forma que permitan su homologación.

## **VI. FACULTAD DEL CONGRESO PARA VINCULAR A LA ADMINISTRACIÓN PÚBLICA FEDERAL**

Aun y cuando la ley en estudio es contundente respecto a la obligación de utilización de las firmas electrónicas y mensajes de datos por parte del gobierno federal, así como respecto a la certificación, debe indicarse que se puede establecer la obligación a cargo de las diversas entidades o dependencias de los Poderes de la Unión a efecto de que lleven a cabo las medidas tendientes a la utilización de dichos instrumentos informáticos como actos jurídicamente válidos, mediante la expedición de las normas respectivas con las disposiciones transitorias pertinentes para determinar su *vacatio legis* en cada momento.

En efecto, no hay vulneración constitucional alguna, si, como es el caso, el Congreso de la Unión, en el contenido y alcance de la ley, obliga al gobierno federal (en forma total o parcial) a la utilización de los mensajes de datos y de las firmas electrónicas, es precisamente a través de la legislación (entre otras normas jurídicas) como se encausa y determina la forma de actuación gubernamental, y las diversas autoridades deberán por lo mismo apegar sus actos a las disposiciones legislativas respectivas, sin que lo anterior pueda ser considerado como una invasión de facultades o una vulneración al principio de división de poderes.

Lo anterior, se hizo sin que eliminaran las formas actuales de realización de actos jurídicos, principalmente por lo que hace a la relación entre gobierno y gobernados, puesto que en caso de establecer dichos medios como los únicos jurídicamente válidos, se estaría imposibilitando o dificultando el acceso de los particulares a la administración, desventaja que, seguramente, sería considerada inconstitucional por parte de los tribunales del Poder Judicial de la Federación.

Similares consideraciones cabrían hacerse respecto de determinados actos de autoridad sujetos a regulación constitucional con formas determinadas, como el caso del derecho de petición consignado en el artículo 8° de la Constitución General de la República, toda vez que si bien es de esperar que la interpretación de nuestros tribunales federales sea en el sentido de considerar que la admisión voluntaria de diversas modalidades de comunicación electrónica entre los particulares y la administración es una forma de ampliar y no de restringir los derechos fundamentales, no podemos estar a salvo de una interpretación rígida y literal de dicho precepto que generase inseguridad jurídica al respecto.

## **VII. FACULTAD DEL CONGRESO PARA VINCULAR A LA ADMINISTRACIÓN PÚBLICA ESTATAL Y MUNICIPAL**

Como comentamos, la norma jurídica, tendrá originariamente aplicación en el ámbito federal, puesto que el Congreso de la Unión no cuenta con facultades para dar validez jurídica a los mensajes de datos o a las firmas electrónicas en relación con actos que son materia de legislaciones locales.

Pero ello no obsta a que cuente con facultades para establecer reglas que permitan la homologación normativa de las disposiciones relacionadas con el reconocimiento de certificados digitales entre los Estados y las dependencias y entidades de la administración pública federal, sin modificar en forma alguna las características o requisitos que el congreso local respectivo previó para los actos materia de regulaciones locales.

Por lo anterior se recomienda establecer una disposición transitoria en la que se otorgue un plazo razonable a efecto de que los distintos Estados implementen las reformas legales requeridas.

Lo anterior es así en virtud de que, en caso de ser una obligación establecida por el legislador, debe establecerse un plazo perentorio para cumplir con la misma, o en su caso el establecimiento de las reglas para la entrada gradual, puesto que de lo contrario, al considerar que no existe plazo para la instrumentación necesaria a efectos de aplicación de la ley, dicha obligación encontraría una excusa jurídicamente válida para evitar su cumplimiento, y por otra parte, no se podría establecer que dicha obligación se cumpliera con la entrada en vigor de la ley, puesto que sería materialmente imposible cumplir con la misma.

## VIII. PROPUESTAS Y REFORMA A LA LEY

Proponemos algunas adecuaciones a la Ley de Firma Electrónica Avanzada:

1. Homologación conceptual de normativas (diferentes y nuevos conceptos que se contraponen con otra regulación, confusión de principios normativos).

La ley contempla en su artículo segundo un cúmulo de definiciones que no son acordes con otra normativa como el Código de Comercio, la Ley Modelo de Firmas Electrónicas de la UNCITRAL, entre otras, cuando la base teórica y práctica de las firmas electrónicas es la misma sin importar el ámbito en que se aplique. Así mismo, se agregan definiciones que en vez de apoyar a la interpretación de la ley la dificultan. Como ejemplo, tenemos la definición de mensaje de datos junto con la de documento electrónico, el mantenimiento de ambas crea confusión. Otro ejemplo es la definición de acto que no es muy clara y por tanto no se tiene una certeza del alcance de dicha definición, que es donde deberá aplicarse la firma electrónica avanzada.

Así mismo, en el artículo 8, donde se establecen los principios rectores, en la mayoría de los casos se confunden los principios con las características, englobando ambos como principios. Los principios conforme se deben interpretar y aplicar las leyes de firma electrónica son los siguientes de acuerdo a nuestra regulación actual (Código de Comercio), a las prácticas internacionales y a la Ley Modelo de Firma Electrónica Avanzada de la UNCITRAL: a) neutralidad tecnológica, b) compatibilidad internacional c) autonomía de las partes y d) equivalencia funcional.

Por otro lado, las características que deberán considerarse para que la firma electrónica sea considerada avanzada y por tanto con la misma validez legal que la autógrafa son: autenticidad, integridad y no repudio. La confidencialidad no es ni un principio ni una característica propia de la firma, es una ventaja del uso del cifrado de documentos.

Por lo anterior, consideramos que en dichos artículos se agregan y/o mezclan los conceptos, características o requisitos relativos a la FEA, lo cual generaría confusión, yendo hacia una mayor diversidad de regulación con conceptos y contenidos diferentes, más que hacia una regulación federal homologada y acorde a las prácticas internacionales, lo que impediría un uso más común y habitual de la firma electrónica avanzada.

Esta situación puede acarrear controversias judiciales derivado de las múltiples interpretaciones que se le podría dar a diferentes regulaciones relacionadas con la firma electrónica, por lo que recomendamos que sean homologados los conceptos, principios y características, a lo contenido en la experiencia internacional y nuestra regulación actual.

2. Aceptación en ámbitos, fiscal, administrativo y fiscal, de los certificados sin importar la autoridad de emisión (SE, SAT o SFP).

Si bien existen varios ámbitos y varias autoridades que emiten certificados digitales de firma electrónica avanzada, tres son las principales: Secretaría de Economía, Secretaría de la Función Pública y el Servicio de Administración Tributaria, cada una para un sector: comercial, administrativo y fiscal respectivamente.

A pesar de lo anterior, y aun siendo uno de los objetivos de la ley la homologación de las firmas y los certificados, no se establecen las bases conforme a las cuales se reconocerán los certificados digitales de estas Autoridades entre sí, ni los posibles escenarios en los que se puede llegar a una homologación, ni qué se entiende por este proceso.

Así mismo, excluye expresamente de su aplicación a los ámbitos: fiscal, aduanero, financiero y comercial, lo que de nueva cuenta produce un impedimento para el uso generalizado de estos medios electrónicos, necesitando contar con uno de ellos para cada sector en específico.

Cabe señalar, que la tecnología actual utilizada para la generación de firmas electrónicas avanzadas es la misma, se utiliza una estructura de par de llaves (PKI), por lo que debieran ser aceptados conforme al principio de neutralidad tecnológica, que está incluido en la propia iniciativa, cualquier certificado y cualquier firma electrónica avanzada que cumpla con los requisitos en ella contenidos y no dependiendo de la autoridad que lo emita.

Aunado a ello, si la aplicación de la ley solo fuera en la administración pública federal, dejando fuera el reconocimiento de otros certificados (lo cual no recomendamos), el título y los objetivos resultarían demasiado extensos. Por ello recomendamos que se abarque expresamente en esta ley a demás sectores.

3. Apego al objetivo y nombre de la ley (ampliar objetivos o limitar contenido).

El título de la ley es LEY FEDERAL DE FIRMA ELECTRÓNICA AVANZADA y entre sus objetivos sólo encontramos los relacionados con la propia firma, sin embargo, a partir del artículo 11 hasta el 16, se establecen requisitos y procedimientos que no tiene que ver con firma electrónica, sino con el procedimiento administrativo. Temas como: notificación electrónica, tableros electrónicos, pruebas electrónicas, comunicaciones electrónicas, conservación de mensajes de datos, entre otros son establecidas a lo largo de los artículos antes mencionados.

Todos ellos no son temas relacionados con la firma electrónica avanzada ni acorde con los objetivos de la ley en cuestión, lo que podría llevar consigo, de nueva cuenta, procesos judiciales porque el contenido va más allá de los objetivos de la ley. Por ello, recomendamos llevar este contenido a la regulación específica (Ley Federal de Procedimiento Administrativo, que ya contempla algunos de estos elementos) o deberán expandirse los objetivos y el nombre de la ley.

Cabe señalar que estos temas ya fueron analizados y se encuentran en vigor por los “Lineamientos para la Operación, Funcionalidad, Comunicación y Seguridad de los Sistemas Automatizados de Control de Gestión de la Administración Pública Federal” y por las “Disposiciones que deberán observar las dependencias y los organismos descentralizados de la Administración Pública Federal, para la recepción de promociones que formulen los particulares en los procedimientos administrativos a través de medios de comunicación electrónica, así como para las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones administrativas definitivas que se emitan por esa misma vía”.

#### 4. Aceptación como prueba del documento digitalizado

Los artículos 15 y 16 establecen diversas reglas y criterios relacionados con la conservación, digitalización y/o migración de documentos físicos a mensajes de datos, sin embargo, conforme está redactada hoy en día la iniciativa, esto es un proceso que no ayuda en materia de migración de prueba física a prueba electrónica porque desde la fracción I se obliga a mantener el original físico.

La fracción II no ayuda en el tema de eliminación de archivos muertos; debiera establecerse la salvedad de que la autoridad deberá aceptar el mensaje de datos si el oferente puede acreditar que siguió, para su digitalización un proceso fiable que permite validar su integridad y autenticidad.

Lo más recomendable es legislar respecto de la posibilidad de digitalizar la documentación si se tienen los elementos suficientes para comprobar que su contenido es íntegro y auténtico, permitiendo que el documento digitalizado sea aceptado en juicio con plena validez jurídica. Lo anterior, ayudaría a potencializar muchas industrias en México al no tener que conservar físicamente un cúmulo de documentos, lo cual actualmente genera altos costos y riesgos de administración, almacenamiento y conservación.

## PROPUESTA DE REFORMA LEGAL

(En la columna izquierda, aparece en cursivas y color rojo el texto de las correcciones y adiciones propuestas por el autor. Asimismo, en cursivas y color verde aparecen los textos que en opinión del autor –antes de ser aceptados definitivamente-, debieran ser sometidos a un examen más detenido.)

TÍTULO PRIMERO	TEXTO PROPUESTO
DISPOSICIONES GENERALES	
CAPÍTULO ÚNICO	
<b>Artículo 1.</b> La presente Ley es de orden e interés público y tiene por objeto regular:	
I. El uso de la firma electrónica avanzada en los actos previstos en esta Ley y la expedición de certificados digitales a personas físicas;	
II. Los servicios relacionados con la firma electrónica avanzada, y	
III. La homologación de la firma electrónica avanzada con las firmas electrónicas avanzadas reguladas por otros ordenamientos legales, en los términos establecidos en esta Ley.	
Artículo 2. Para los efectos de la presente Ley se entenderá por:	
I. Actos: las comunicaciones, trámites, servicios, actos jurídicos y administrativos, así como procedimientos administrativos en los cuales los particulares y los servidores públicos de las dependencias y entidades de la Administración Pública Federal, de la Procuraduría General de la República y de las unidades administrativas de la Presidencia de la República, utilicen la firma electrónica avanzada;	<i>I. Actos: las comunicaciones, trámites, servicios, actos jurídicos y administrativos, así como procedimientos administrativos entre particulares y los servidores públicos de las dependencias y entidades de la Administración Pública Federal, de la Procuraduría General de la República y de las unidades administrativas de la Presidencia de la República, que utilicen la firma electrónica avanzada;</i>
II. Actuaciones Electrónicas: las notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes o documentos y, en su caso, las resoluciones administrativas definitivas que se emitan en los actos a que se refiere esta Ley que sean comunicadas por medios electrónicos;	

<p>III. Acuse de Recibo Electrónico: el mensaje de datos que se emite o genera a través de medios de comunicación electrónica para acreditar de manera fehaciente la fecha y hora de recepción de documentos electrónicos relacionados con los actos establecidos por esta Ley;</p>	
<p>IV. Autoridad Certificadora: las dependencias y entidades de la Administración Pública Federal y los prestadores de servicios de certificación que conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos;</p>	<p><i>IV. Agencia Certificadora: las dependencias y entidades de la Administración Pública Federal y los prestadores de servicios de certificación que conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos y con la firma electrónica;</i></p>
<p>V. Certificado Digital: el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada;</p>	<p><i>V. Certificado Digital: el mensaje de datos u otro registro, emitido por una Agencia Certificadora que permita confirmar el vínculo entre un firmante y su clave privada;</i></p>
<p>VI. Clave Privada: los datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante;</p>	<p><i>Clave Privada: los datos que el firmante genera de manera secreta, mantiene bajo su exclusivo control y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante;</i></p>
<p>VII. Clave Pública: los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante;</p>	<p><i>VII. Clave Pública: los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante ya que se encuentran matemáticamente asociados a su clave privada;</i></p>
<p>IX. Dependencias: las secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como las unidades administrativas de la Presidencia de la República, conforme a lo dispuesto en la Ley Orgánica de la Administración Pública Federal. La Procuraduría General de la República será considerada con este carácter para efectos de los actos administrativos que realice en términos de esta Ley;</p>	
<p>X. Documento Electrónico: aquél que es generado, consultado, modificado o procesado por medios electrónicos;</p>	<p><i>X. Documento Electrónico: aquél mensaje de datos firmado electrónicamente;</i></p>

<p>XI. Dirección de Correo Electrónico: la dirección en Internet señalada por los servidores públicos y particulares para enviar y recibir mensajes de datos y documentos electrónicos relacionados con los actos a que se refiere la presente Ley, a través de los medios de comunicación electrónica;</p>	
<p>XII. Entidades: los organismos públicos descentralizados, empresas de participación estatal mayoritaria y 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;</p>	
<p>XIII. Firma Electrónica Avanzada: 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;</p>	<p><i>XIII. Firma Electrónica Avanzada: el conjunto de datos y caracteres consignados en forma electrónica en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información en él contenida que permite la identificación del firmante, creada creados por medios electrónicos utilizando una clave privada que mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa;</i></p>
<p>XIV. Firmante: toda persona que utiliza su firma electrónica avanzada para suscribir documentos electrónicos y, en su caso, mensajes de datos;</p>	<p><i>XIV. Firmante: toda persona que utiliza su firma electrónica avanzada para suscribir documentos electrónicos y, en su caso, mensajes de datos;</i></p>
<p>XV. Medios de Comunicación Electrónica: los dispositivos tecnológicos que permiten efectuar la transmisión y recepción de mensajes de datos y documentos electrónicos;</p>	
<p>XVI. Medios Electrónicos: los dispositivos tecnológicos para el procesamiento, impresión, despliegue, conservación y, en su caso, modificación de información;</p>	
<p>XVII. Mensaje de Datos: la información generada, enviada, recibida, archivada o comunicada a través de medios de comunicación electrónica, que puede contener documentos electrónicos;</p>	<p><i>XVII. Mensaje de Datos: la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología de comunicación electrónica, que puede contener documentos electrónicos;</i></p>

<p>XVIII. Página Web: el sitio en Internet que contiene información, aplicaciones y, en su caso, vínculos a otras páginas;</p>	<p><i>XVIII. Página Web: Información electrónica contenida en un servidor conectado a Internet que contiene además de Mensajes de Datos, aplicaciones y, en su caso, vínculos a otras páginas; El conjunto de páginas web interrelacionadas entre sí y con otras páginas toma el nombre de Sitio Web</i></p>
<p>XIX. Prestador de Servicios de Certificación: las instituciones públicas conforme a las leyes que les son aplicables, así como los notarios y corredores públicos y las personas morales de carácter privado que de acuerdo a lo establecido en el Código de Comercio sean reconocidas con tal carácter para prestar servicios relacionados con la firma electrónica avanzada y, en su caso, expedir certificados digitales;</p>	
<p>XX. Secretaría: la Secretaría de la Función Pública;</p>	
<p>XXI. Servicios relacionados con la Firma Electrónica Avanzada: los servicios de firmado de documentos electrónicos, de verificación de la vigencia de certificados digitales, de verificación y validación de la unicidad de la clave pública, así como de consulta de certificados digitales revocados, entre otros, que en términos de las disposiciones jurídicas aplicables pueden ser proporcionados por la Autoridad certificadora;</p>	<p><i>XXI. Servicios relacionados con la Firma Electrónica Avanzada: los servicios de firmado de documentos electrónicos, de verificación de la vigencia de certificados digitales, de verificación y validación de la unicidad de la clave pública, de sellado de tiempo así como de consulta de certificados digitales revocados, entre otros, que en términos de las disposiciones jurídicas aplicables pueden ser proporcionados por la agencia certificadora;</i></p>
<p>XXII. Sistema de Trámites Electrónicos: el sitio desarrollado por la dependencia o entidad y contenido en su página Web, para el envío y recepción de documentos, notificaciones y comunicaciones, así como para la consulta de información relacionada con los actos a que se refiere esta Ley;</p>	
<p>XXIII. Sujetos Obligados: los servidores públicos y particulares que utilicen la firma electrónica avanzada, en términos de lo previsto en las fracciones II y III del artículo 3 de esta Ley, y</p>	
<p>XXIV. Tablero Electrónico: el medio electrónico a través del cual se ponen a disposición de los particulares que utilicen la firma electrónica avanzada en términos de esta Ley, las actuaciones electrónicas que emitan las dependencias y entidades, y que genera un acuse de recibo electrónico. Este medio electrónico estará ubicado en el sistema de trámites electrónicos de las propias dependencias y entidades.</p>	

<b>Artículo 3.</b> Están sujetos a las disposiciones de la presente Ley:	
I. Las dependencias y entidades;	
II. Los servidores públicos de las dependencias y entidades que en la realización de los actos a que se refiere esta Ley utilicen la firma electrónica avanzada, y	
III. Los particulares, en los casos en que utilicen la firma electrónica avanzada en términos de esta Ley.	
<b>Artículo 4.</b> Las disposiciones de esta Ley no serán aplicables a los actos en que no sea factible el uso de la firma electrónica avanzada por disposición de ley o aquéllos en que exista previo dictamen de la Secretaría. Tampoco serán aplicables a las materias fiscal, aduanera y financiera.	<i>Artículo 4. Las disposiciones de esta Ley no serán aplicables a los actos en que no sea factible el uso de la firma electrónica avanzada por disposición de ley o aquéllos en que exista previo dictamen de la Secretaría. Y solo serán aplicables a las materias fiscal, aduanera y financiera en los términos y bajo las condiciones que se establezcan por La Secretaría, La Secretaría de Economía y el Servicio de Administración Tributaria de manera conjunta en Disposiciones de Carácter General que deberán publicarse en el Diario Oficial de la Federación.</i>
En los actos de comercio e inscripciones en el Registro Público de Comercio, el uso de la firma electrónica avanzada se regirá de conformidad con lo previsto en el Código de Comercio y demás ordenamientos aplicables en la materia, sin perjuicio de la aplicación de lo dispuesto en esta Ley en lo que resulte procedente.	
<b>Artículo 5.</b> La Secretaría, en el ámbito de su competencia, estará facultada para interpretar las disposiciones de esta Ley para efectos administrativos.	
La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria dictarán, de manera conjunta, las disposiciones generales para el adecuado cumplimiento de esta Ley, mismas que deberán publicarse en el Diario Oficial de la Federación.	
<b>Artículo 6.</b> A falta de disposición expresa en esta Ley o en las demás disposiciones que de ella deriven, se aplicarán supletoriamente la Ley Federal de Procedimiento Administrativo, el Código Civil Federal y el Código Federal de Procedimientos Civiles.	<i>Artículo 6. A falta de disposición expresa en esta Ley o en las demás disposiciones que de ella deriven, se aplicarán supletoriamente la Ley Federal de Procedimiento Administrativo, el Código Civil Federal, el Código de Comercio y el Código Federal de Procedimientos Civiles.</i>

<b>TÍTULO SEGUNDO</b>	
<b>DE LA FIRMA ELECTRÓNICA AVANZADA</b>	
<b>CAPÍTULO I</b>	
Del uso y validez de la firma electrónica avanzada	
<b>Artículo 7.</b> La firma electrónica avanzada podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos.	
Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.	
<b>Artículo 8.</b> Para efectos del artículo 7 de esta Ley, la firma electrónica avanzada deberá cumplir con los principios rectores siguientes:	
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;	<i>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;</i>
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;	<i>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;</i>
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 electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;	<i>IV. Neutralidad Tecnológica: Consiste en que la Regulación y Supervisión tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;</i>

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	<i>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</i>
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.	<i>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.</i>
	<i>VII.- Compatibilidad Nacional e Internacional, en términos de lo dispuesto por los artículos 29 y 30.</i>
<b>Artículo 9.</b> Para que los sujetos obligados puedan utilizar la firma electrónica avanzada en los actos a que se refiere esta Ley deberán contar con:	
I. Un certificado digital vigente, emitido u homologado en términos de la presente Ley, y	
II. Una clave privada, generada bajo su exclusivo control.	
<b>CAPÍTULO II</b>	
<b>De los documentos electrónicos y de los mensajes de datos</b>	
<b>Artículo 10.</b> Las dependencias y entidades en las comunicaciones y, en su caso, actos jurídicos que realicen entre las mismas, harán uso de mensajes de datos y aceptarán la presentación de documentos electrónicos, los cuales deberán contar, cuando así se requiera, con la firma electrónica avanzada del servidor público facultado para ello.	
<b>Artículo 11.</b> Las dependencias y entidades en la realización de los actos a que se refiere esta Ley, deberán aceptar el uso de mensajes de datos y la presentación de documentos electrónicos cuando las mismas ofrezcan esta posibilidad, siempre que los particulares por sí o, en su caso, a través de las personas autorizadas por los mismos en términos del artículo 19 de la Ley Federal de Procedimiento Administrativo, manifiesten expresamente su conformidad para que dichos actos se efectúen, desde su inicio hasta su conclusión, a través de medios de comunicación electrónica.	

<p>La manifestación a que se refiere el párrafo anterior deberá señalar adicionalmente:</p>	
<p>I. Que aceptan consultar el tablero electrónico, al menos, los días quince y último de cada mes o bien, el día hábil siguiente si alguno de éstos fuere inhábil; y en caso de no hacerlo, se tendrá por hecha la notificación en el día hábil que corresponda;</p>	
<p>II. Que aceptan darse por notificados de las actuaciones electrónicas que emita la dependencia o entidad que corresponda, en el mismo día en que consulten el tablero electrónico, y</p>	
<p>III. Que en el supuesto de que por causas imputables a la dependencia o entidad se encuentren imposibilitados para consultar el tablero electrónico o abrir los documentos electrónicos que contengan la información depositada en el mismo, en los días señalados en la fracción I de este artículo, lo harán del conocimiento de la propia dependencia o entidad a más tardar dentro de los tres días hábiles siguientes a aquél en que ocurra dicho impedimento, por medios de comunicación electrónica o cualquier otro previsto en el Reglamento de esta Ley, para que sean notificados por alguna otra forma de las establecidas en la Ley Federal de Procedimiento Administrativo.</p>	
<p><b>Artículo 12.</b> Los sujetos obligados deberán contar con una dirección de correo electrónico para recibir, cuando corresponda, mensajes de datos y documentos electrónicos en la realización de los actos previstos en esta Ley.</p>	
<p><b>Artículo 13.</b> Cada dependencia y entidad creará y administrará un sistema de trámites electrónicos que establezca el control de accesos, los respaldos y la recuperación de información, con mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia.</p>	
<p>La Secretaría emitirá los lineamientos conducentes a efecto de dar cumplimiento a lo dispuesto en este artículo.</p>	

<p><b>Artículo 14.</b> La información contenida en los mensajes de datos y en los documentos electrónicos será pública, salvo que la misma esté clasificada como reservada o confidencial en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.</p>	
<p>Los mensajes de datos y los documentos electrónicos que contengan datos personales estarán sujetos a las disposiciones aplicables al manejo, seguridad y protección de los mismos.</p>	
<p style="text-align: center;"><b>CAPÍTULO II</b></p>	
<p style="text-align: center;"><b>De los documentos electrónicos y de los mensajes de datos</b></p>	
<p><b>Artículo 15.</b> Las dependencias y entidades, así como los sujetos obligados deberán conservar en medios electrónicos, los mensajes de datos y los documentos electrónicos con firma electrónica avanzada derivados de los actos a que se refiere esta Ley, durante los plazos de conservación previstos en los ordenamientos aplicables, según la naturaleza de la información.</p>	
<p>Mediante disposiciones generales se establecerá lo relativo a la conservación de los mensajes de datos y de los documentos electrónicos con firma electrónica avanzada, para lo cual se tomarán en cuenta, entre otros requisitos, los previstos en la Norma Oficial Mexicana a que se refiere el artículo 49 del Código de Comercio.</p>	<p><i>Para garantizar la integridad de los documentos que se pretendan conservar en el tiempo, además de la firma electrónica avanzada se utilizarán procesos de sellado de tiempo, conforme a estándares internacionales llevados a cabo por una Agencia Certificadora o un Prestador de Servicios de Certificación debidamente acreditado.</i></p>
<p><b>Artículo 16.</b> Cuando se requiera que un documento impreso y con firma autógrafa, sea presentado o conservado en su forma original, tal requisito quedará satisfecho si la copia se genera en un documento electrónico, y se cumple con lo siguiente:</p>	
<p>I. Que la migración a una forma digital 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;</p>	<p><i>I. Que la migración a una forma digital haya sido realizada o supervisada por un servidor público que cuente con facultades de certificación de documentos en términos de las disposiciones aplicables, por un Tercero Legalmente Acreditado 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;</i></p>

<p>II. Cuando exista duda sobre la autenticidad del documento electrónico remitido, la dependencia o entidad podrá solicitar que el documento impreso le sea presentado directamente o bien, que este último se le envíe por correo certificado con acuse de recibo.</p>	<p><i>II. Cuando exista duda sobre la autenticidad del documento electrónico remitido, solo en el caso de que el documento hubiere sido digitalizado por el particular interesado sin la supervisión de un servidor público con facultades de certificación o de un Tercero Legalmente Autorizado, la dependencia o entidad podrá solicitar que el documento impreso le sea presentado directamente o bien, que este último se le envíe por correo certificado con acuse de recibo.</i></p>
<p>En el supuesto de que se opte por el envío del documento impreso a través de correo certificado, será necesario que adicionalmente se envíe dentro de los tres días hábiles siguientes, mediante un mensaje de datos, la guía que compruebe que el referido documento fue depositado en una oficina de correos;</p>	
<p>III. Que la información contenida en el documento electrónico se mantenga 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;</p>	
<p>IV. Que el documento electrónico permita conservar el formato del documento impreso y reproducirlo con exactitud, y</p>	
<p>V. Que se observe lo previsto en las disposiciones generales en materia de conservación de mensajes de datos y de los documentos electrónicos con firma electrónica avanzada.</p>	
<p>Lo establecido en este artículo se aplicará sin perjuicio de que las dependencias y entidades observen, conforme a la naturaleza de la información contenida en el documento impreso de que se trate, los plazos de conservación previstos en los ordenamientos aplicables.</p>	
<p style="text-align: center;"><b>TÍTULO TERCERO</b></p>	
<p style="text-align: center;"><b>DEL CERTIFICADO DIGITAL</b></p>	
<p style="text-align: center;"><b>CAPÍTULO I</b></p>	
<p style="text-align: center;"><b>De la estructura y procedimientos del certificado digital</b></p>	
<p><b>Artículo 17.</b> El certificado digital deberá contener lo siguiente:</p>	

I. Número de serie;	
II. Autoridad certificadora que lo emitió;	<i>II. Agencia certificadora que lo emitió;</i>
III. Algoritmo de firma;	
IV. Vigencia;	
V. Nombre del titular del certificado digital;	
VI. Dirección de correo electrónico del titular del certificado digital;	
VII. Clave Única del Registro de Población (CURP) del titular del certificado digital;	
VIII. Clave pública, y	
IX. Los demás requisitos que, en su caso, se establezcan en las disposiciones generales que se emitan en términos de esta Ley.	
<b>Artículo 18.</b> Para obtener un certificado digital el interesado accederá a la página Web de la Autoridad certificadora y llenará el formato de solicitud con los datos siguientes:	
I. Nombre completo del solicitante;	
II. Domicilio del solicitante;	
III. Dirección de correo electrónico para recibir mensajes de datos y documentos electrónicos;	
IV. Clave Única del Registro de Población (CURP) del solicitante, salvo que se trate de extranjeros, quienes deberán asentar los datos del documento que acredite su legal estadía en territorio nacional, y	
V. Nombre de la Autoridad certificadora a quien va dirigida la solicitud. Posteriormente, el interesado deberá acudir ante la Autoridad Certificadora correspondiente y entregar su solicitud con firma autógrafa, acompañada de:	<i>V. Nombre de la Agencia certificadora a quien va dirigida la solicitud. Posteriormente, el interesado deberá acudir ante la Agencia Certificadora correspondiente y entregar su solicitud con firma autógrafa, acompañada de...</i>
a) El documento que compruebe el domicilio a que se refiere la fracción II;	
b) El documento de identificación oficial expedido por Autoridad competente, y	
c) El documento probatorio de nacionalidad mexicana, y tratándose de extranjeros, el documento que acredite su legal estadía en territorio nacional.	

La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria establecerán de manera conjunta, en términos de las disposiciones aplicables, los procedimientos para el registro de datos y verificación de elementos de identificación, emisión, renovación y revocación de certificados digitales, los cuales darán a conocer a través de sus respectivas páginas Web.	
<b>Artículo 19.</b> El certificado digital quedará sin efectos o será revocado por la Autoridad certificadora que lo emitió, cuando se actualice alguno de los supuestos siguientes:	<i>Artículo 19. El certificado digital quedará sin efectos o será revocado por la Agencia certificadora que lo emitió, cuando se actualice alguno de los supuestos siguientes:</i>
I. Por expiración de su vigencia;	
II. Cuando se compruebe que los documentos que presentó el titular del certificado digital para acreditar su identidad son falsos;	
III. Cuando así lo solicite el titular del certificado digital a la Autoridad certificadora que lo emitió;	<i>III. Cuando así lo solicite el titular del certificado digital a la Agencia certificadora que lo emitió;</i>
IV. Por fallecimiento del titular del certificado digital;	
V. Cuando se extravíe o inutilice por daños el medio electrónico que contenga los certificados digitales;	<i>V. Cuando se extravíe o inutilice por daños el medio electrónico que contenga los certificados digitales;</i>
VI. Cuando se ponga en riesgo la confidencialidad, integridad o seguridad de los datos de creación de la firma electrónica avanzada, y	<i>VI. Cuando se ponga en riesgo la confidencialidad, integridad o seguridad de la Clave Privada del Titular del Certificado, y...</i>
VII. Por resolución de Autoridad judicial o administrativa que así lo determine.	
En los casos a que se refiere la fracción IV de este artículo, la revocación procederá a solicitud de un tercero legalmente autorizado, quien deberá acompañar el acta de defunción del titular del certificado digital.	
<b>Artículo 20.</b> La vigencia del certificado digital será de cuatro años como máximo, la cual iniciará a partir del momento de su emisión y expirará el día y en la hora señalada en el mismo.	
<b>CAPÍTULO II</b>	
<b>Derechos y obligaciones del titular del certificado digital</b>	
<b>Artículo 21.</b> El titular de un certificado digital tendrá los derechos siguientes:	

I. A ser informado por la Autoridad certificadora que lo emita sobre:	
a) Las características y condiciones precisas para la utilización del certificado digital, así como los límites de su uso;	
b) Las características generales de los procedimientos para la generación y emisión del certificado digital y la creación de la clave privada, y	
c) La revocación del certificado digital;	
II. A que los datos e información que proporcione a la Autoridad certificadora sean tratados de manera confidencial, en términos de las disposiciones jurídicas aplicables, y	
III. A solicitar la modificación de datos y elementos del certificado digital, mediante la revocación de éste, cuando así convenga a sus intereses.	
<b>Artículo 22.</b> El titular de un certificado digital estará obligado a lo siguiente:	
I. Hacer declaraciones veraces y completas en relación con los datos y documentos que proporcione para su identificación personal;	
II. Custodiar adecuadamente sus datos de creación de firma y la clave privada vinculada con ellos, a fin de mantenerlos en secreto;	<i>II. Custodiar adecuadamente sus datos de creación de firma y la su clave privada vinculada con ellos, a fin de mantenerla en secreto;</i>
III. Solicitar a la Autoridad certificadora la revocación de su certificado digital en caso de que la integridad o confidencialidad de sus datos de creación de firma o su frase de seguridad hayan sido comprometidos y presuma que su clave privada pudiera ser utilizada indebidamente, y	<i>III. Solicitar a la Agencia certificadora la revocación de su certificado digital en caso de que la integridad o confidencialidad de su clave privada o su frase de seguridad hayan sido comprometidos y presuma que su clave privada pudiera ser utilizada indebidamente, y</i>
IV. Dar aviso a la Autoridad certificadora respectiva de cualquier modificación de los datos que haya proporcionado para su identificación personal, a fin de que ésta incorpore las modificaciones en los registros correspondientes y emita un nuevo certificado digital.	<i>IV. Dar aviso a la Agencia certificadora respectiva de cualquier modificación de los datos que haya proporcionado para su identificación personal, a fin de que ésta incorpore las modificaciones en los registros correspondientes y emita un nuevo certificado digital.</i>
<b>CAPÍTULO III</b>	
<b>De las Autoridades certificadoras</b>	<i>De las Agencias certificadoras</i>
<b>Artículo 23.</b> La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria son consideradas Autoridades certificadoras para emitir certificados digitales en términos de esta Ley.	<i>Artículo 23. La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria son consideradas Autoridades certificadoras para autorizar a Agencias Certificadoras a emitir certificados digitales en términos de esta Ley.</i>

<p><b>Artículo 24.</b> Las dependencias y entidades, distintas a las mencionadas en el artículo anterior, así como los prestadores de servicios de certificación que estén interesados en tener el carácter de Autoridad certificadora en términos de la presente Ley, deberán:</p>	<p><i>Artículo 24. Las dependencias y entidades, distintas a las mencionadas en el artículo anterior, así como los prestadores de servicios de certificación que estén interesados en tener el carácter de Agencia certificadora en términos de la presente Ley, deberán:...</i></p>
<p>I. Contar con el dictamen favorable de la Secretaría, y</p>	
<p>II. Cumplir con los demás requisitos que se establezcan en las disposiciones generales que se emitan en los términos de esta Ley.</p>	
<p>Adicionalmente, los notarios y corredores públicos y las personas morales de carácter privado deberán presentar el documento emitido por la Secretaría de Economía que los acredite como prestadores de servicios de certificación, en virtud de haber cumplido con los requisitos establecidos en el Código de Comercio y su Reglamento.</p>	<p><i>Adicionalmente, los notarios y corredores públicos, y las personas morales de carácter privado y los demás prestadores de servicios de certificación legalmente acreditados deberán presentar el documento emitido por la Secretaría de Economía que los acredite como prestadores de servicios de certificación, en virtud de haber cumplido con los requisitos establecidos en la normatividad respectiva</i></p>
<p><b>Artículo 25.</b> Las Autoridades certificadoras tendrán las atribuciones y obligaciones siguientes:</p>	<p><i>Artículo 25. Las Agencias certificadoras tendrán las atribuciones y obligaciones siguientes:</i></p>
<p>I. Emitir, administrar y registrar certificados digitales, así como prestar servicios relacionados con la firma electrónica avanzada;</p>	
<p>II. Llevar un registro de los certificados digitales que emitan y de los que revoken, así como proveer los servicios de consulta a los interesados;</p>	
<p>III. Adoptar las medidas necesarias para evitar la falsificación, alteración o uso indebido de certificados digitales, así como de los servicios relacionados con la firma electrónica avanzada;</p>	
<p>IV. Revocar los certificados de firma electrónica avanzada, cuando se actualice alguno de los supuestos previstos en el artículo 19 de esta Ley conforme a los procedimientos a que se refiere el artículo 18 de la misma;</p>	
<p>V. Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada, así como de los servicios relacionados con la misma;</p>	<p><i>V. Garantizar la autenticidad, integridad, conservación y confidencialidad y confiabilidad de la firma electrónica avanzada generada con base en los certificados digitales que emitan, así como de los servicios relacionados con la misma;</i></p>

<p>VI. Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, y</p>	
<p>VII. Las demás que les confieran las disposiciones jurídicas aplicables.</p>	
<p>Lo anterior, sin perjuicio de las atribuciones que, en su carácter de Autoridad certificadora, corresponden al Servicio de Administración Tributaria en términos de la legislación fiscal y aduanera.</p>	
<p><b>Artículo 26.</b> Las Autoridades certificadoras que sean reconocidas como tales en términos del artículo 24 de esta Ley, podrán dejar de tener ese carácter cuando incumplan las obligaciones previstas en la presente Ley o se ubiquen en alguno de los supuestos previstos en el Reglamento de esta Ley.</p>	<p><i>Artículo 26. Las Agencias certificadoras que sean reconocidas como tales en términos del artículo 24 de esta Ley, podrán dejar de tener ese carácter cuando incumplan las obligaciones previstas en la presente Ley o se ubiquen en alguno de los supuestos previstos en el Reglamento de esta Ley.</i></p>
<p>Cuando la Autoridad certificadora sea un prestador de servicios de certificación, el procedimiento para revocar el instrumento que le reconozca tal carácter, tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.</p>	<p><i>Cuando la Agencia certificadora sea un prestador de servicios de certificación, el procedimiento para revocar el instrumento que le reconozca tal carácter, tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.</i></p>
<p><b>Artículo 27.</b> La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria podrán coordinarse para acordar y definir los estándares, características y requerimientos tecnológicos a que se deberán sujetar las Autoridades certificadoras referidas en el artículo 24 de esta Ley para garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada.</p>	<p><i>Artículo 27. La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria podrán coordinarse para acordar y definir los estándares, características y requerimientos tecnológicos a que se deberán sujetar las Autoridades certificadoras referidas en el artículo 24 de esta Ley para garantizar la autenticidad, integridad y conservación, confidencialidad y confiabilidad de la firma electrónica avanzada.</i></p>
<p style="text-align: center;"><b>CAPÍTULO IV</b></p>	
<p style="text-align: center;"><b>Del reconocimiento de certificados digitales y de la celebración de bases de colaboración y convenios de colaboración o coordinación</b></p>	
<p><b>Artículo 28.</b> La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria y demás Autoridades certificadoras a que se refiere el artículo 24 podrán celebrar bases o convenios de colaboración, según corresponda para la prestación de servicios relacionados con la firma electrónica avanzada.</p>	<p><i>Artículo 28. La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria y demás Autoridades certificadoras a que se refiere el artículo 24 podrán celebrar bases o convenios de colaboración, según corresponda para la prestación de servicios relacionados con la firma electrónica avanzada..</i></p>

<p><b>Artículo 29.</b> El Ejecutivo Federal, por conducto de la Secretaría, de la Secretaría de Economía o el Servicio de Administración Tributaria, a solicitud de cualquier Autoridad certificadora, podrá suscribir previa opinión de las otras dos, convenios de coordinación para el reconocimiento de certificados digitales homologados en términos de lo previsto en esta Ley, con:</p>	<p><i>Artículo 29. El Ejecutivo Federal, por conducto de la Secretaría, de la Secretaría de Economía o el Servicio de Administración Tributaria, a solicitud de cualquier Agencia certificadora, podrá suscribir previa opinión de las otras dos, convenios de coordinación para el reconocimiento de certificados digitales homologados en términos de lo previsto en esta Ley, con:</i></p>
<p>I. Los poderes Legislativo y Judicial, federales;</p>	
<p>II. Los órganos constitucionales autónomos, y</p>	
<p>III. Los gobiernos de las entidades federativas, los municipios y los órganos político-administrativos del Distrito Federal.</p>	
<p>Los convenios de coordinación que se suscriban deberán darse a conocer a las demás Autoridades certificadoras, a través de la página Web de la Secretaría.</p>	
<p><b>Artículo 30.</b> Los certificados digitales expedidos fuera de la República Mexicana tendrán la misma validez y producirán los mismos efectos jurídicos reconocidos en la presente Ley, siempre y cuando tales certificados sean reconocidos por las Autoridades certificadoras a que se refiere el artículo 23 de la propia Ley y se garanticen, en la misma forma que lo hacen con sus propios certificados, el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado.</p>	
<p><b>TÍTULO CUARTO</b></p>	
<p><b>DE LAS RESPONSABILIDADES Y SANCIONES</b></p>	
<p><b>CAPÍTULO ÚNICO</b></p>	
<p><b>Artículo 31.</b> Las conductas de los servidores públicos que impliquen el incumplimiento a los preceptos establecidos en la presente Ley, dará lugar al procedimiento y a las sanciones que correspondan en términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.</p>	
<p>Cuando las infracciones a la presente Ley impliquen la posible comisión de una conducta sancionada en los términos de la legislación civil, penal o de cualquier otra naturaleza, las dependencias y entidades lo harán del conocimiento de las Autoridades competentes.</p>	

## IX. Anexos

### TESIS JURISPRUDENCIALES EN RELACIÓN CON LAS FACULTADES IMPLÍCITAS

Quinta Época

Instancia: Segunda Sala

Fuente: Semanario Judicial de la Federación

Tomo: LXXXV

Página: 211

**LEY FORESTAL, CONSTITUCIONALIDAD DE LA.-** Es indudable que conforme al artículo 27 constitucional, la nación tiene la obligación de dictar las medidas de utilidad pública necesarias para la conservación, restauración y propagación (natural o artificial) de la vegetación forestal del territorio de la República, regulando su aprovechamiento. La facultad que para dictar aquellas medidas otorgó el Constituyente a la nación, la ejerce por medio de su órgano legislador que es el Congreso de la Unión, quien, a su vez, obra con facultades implícitas que le otorga la fracción XXIX del artículo 73 de la Carta Magna. En consecuencia, el Congreso de la Unión estuvo en aptitud de expedir la Ley Forestal en vigor, puesto que constitucionalmente está autorizado para expedir las leyes que sean necesarias para hacer efectivas las facultades concedidas por la Constitución, a los Poderes de la Unión.

Amparo administrativo en revisión 6213/43. Compañía del Ferrocarril Sud-Pacífico de México. 11 de julio de 1945. Unanimidad de cuatro votos. El Ministro Franco Carreño no votó por las razones que constan en el acta del día. La publicación no menciona el nombre del ponente.

---

Sexta Época

Instancia: Pleno

Fuente: Semanario Judicial de la Federación

Tomo: Primera Parte, XXXV

Página: 101

**LEY ORGÁNICA DEL PODER JUDICIAL DE LA FEDERACIÓN, CONSTITUCIONALIDAD DE LA.-** El Congreso de la Unión expidió la Ley Orgánica del Poder Judicial de la Federación, que rige la estructura y funcionamiento del propio poder, para que el mismo pueda ejercer de modo efectivo las facultades que le otorga la Constitución General de la República, e introdujo en dicha ley las disposiciones que atribuyen a los

tribunales de los Estados la función de órganos auxiliares de los federales, por estimar que sin el auxilio de la justicia común, la administración de la justicia federal se vería en muchos casos retardada y entorpecida. Tal es la razón en que se inspiran dichas disposiciones, cuya constitucionalidad, por ende, no puede desconocerse, ya que si el Congreso de la Unión las consideró necesarias para hacer efectivas las facultades constitucionales del Poder Judicial de la Federación, se sigue de ello que fueron expedidas en uso de las facultades implícitas que a aquél concede la fracción XXX del artículo 73 de la Carta Fundamental.

Varios 331/54. Queja formulada por el C. Gobernador Sustituto Constitucional del Estado de Sinaloa en contra del Juez de Distrito en el propio Estado. 17 de enero de 1961. Unanimidad de dieciséis votos. La publicación no menciona el nombre del ponente.

---

Séptima Época

Instancia: Pleno

Fuente: Semanario Judicial de la Federación

Tomo: 52 Primera Parte

Página: 13

**AGRARIO. PERMUTA DE BIENES EJIDALES. CONSTITUCIONALIDAD DE LOS PRECEPTOS DEL CÓDIGO AGRARIO QUE LA REGLAMENTAN.-** La facultad del Congreso de la Unión para legislar en materia agraria se funda en las diversas fracciones de los artículos 27 y 73, fracción XXX, ambos de la Constitución Federal. Del primer precepto son relevantes, para sostener la facultad del Congreso de la Unión de dictar normas generales en materia agraria, las fracciones VII a la XVI, en cuanto establecen un conjunto de reglas respecto a la organización ejidal. Si el Congreso de la Unión tiene facultad general en materia agraria, también tiene las facultades implícitas para dictar las medidas necesarias a fin de cumplir con las facultades expresas, de donde resulta la facultad implícita de crear disposiciones de carácter general sobre permuta de bienes ejidales. No es necesario que algún precepto constitucional conceda al Poder Legislativo Federal en forma expresa facultades para legislar sobre permuta de tierras ejidales, pues el artículo 27 constitucional autoriza a la nación, representada en el caso por el Poder Legislativo Federal, para legislar en materia agraria y en uso de tales facultades el Poder Legislativo estableció en los artículos 138, 139 y 140 del Código Agrario que tales tierras son inalienables, imprescriptibles, inembargables e intransmisibles, pero en el artículo 141 fijó las excepciones de la regla general, entre las que se encuentra la permuta de los bienes ejidales por otras tierras, pues no existe ningún principio o disposición constitucional que establezca o de la que pudiera deducirse la prohibición de tal permuta. En consecuencia, no son inconstitucionales los artículos 146 y del 278 al 281 del Código Agrario que regulan las permutas de tierras ejidales.

Amparo en revisión 8192/62. Isabel Vázquez viuda de Jiménez y coagraviados. 3 de abril de 1973. Unanimidad de diecisiete votos. Ponente: Rafael Rojina Villegas.

Nota: En el Informe de 1973, la tesis aparece bajo el rubro “BIENES EJIDALES, PERMUTA DE, CONSTITUCIONALIDAD DE LOS PRECEPTOS DEL CÓDIGO AGRARIO QUE LO REGLAMENTAN. NO VIOLAN LOS ARTÍCULOS 27 Y 73 DE LA CONSTITUCIÓN FEDERAL.”.

---

Séptima Época

Instancia: PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Fuente: Semanario Judicial de la Federación

Tomo: 145-150 Sexta Parte

Página: 119

**FACULTADES IMPLÍCITAS Y EXPLÍCITAS. MULTAS.-** En un sistema constitucional como el nuestro, de facultades específicamente otorgadas a las Autoridades, de manera que sólo pueden hacer lo que la ley les permite, a diferencia del particular, que puede hacer todo lo que la ley no le prohíbe, se debe estimar que las Autoridades, para actuar con competencia en términos del artículo 16 constitucional al causar perjuicios o molestias a los particulares, deben actuar con facultades legales que les hayan sido otorgadas en la Constitución o en alguna ley. Por una parte, si hay cierto tipo de facultades que se otorgan en forma genérica, de manera que las Autoridades no pueden actuar fuera de los fines, objetivos y materia que se les señalan, pero que al mismo tiempo, por la naturaleza misma de la facultad otorgada, resulta imposible que la propia Constitución contenga todos los elementos y matices de la facultad otorgada, y en estos casos, se deben estimar constitucionalmente otorgadas todas las facultades implícitas en las expresamente otorgadas, entendiendo por implícitas aquellas facultades sin las cuales sería nugatorio, o estéril, o se vería sustancialmente mermada la facultad que expresamente se otorgó. Y, aun tratándose de las facultades legislativas del Congreso, por ejemplo, que están sólo sucintamente enunciadas en el artículo 73 constitucional, la doctrina ha dicho que si el fin de la ley es legítimo, y si está dentro de los objetivos señalados en la Constitución, y los medios escogidos en la ley son claramente adecuados para alcanzar esos objetivos, y además no sólo no están prohibidos, sino que son compatibles con la letra y el espíritu de la Constitución, esa ley es constitucional. Pero hay otros campos en los que las facultades se otorgan en forma restrictiva, de manera que no puede hablarse ahí de facultades implícitas, y sólo se puede admitir que se ejerciten las facultades expresas y limitativamente otorgadas. Es el caso de las normas que imponen cargas fiscales, reconocido en el artículo

11 del Código Fiscal de la Federación y emanado primordialmente de la fracción IV del artículo 31 constitucional, conforme a la cual ningún cobro se puede hacer por la vía económico-coactiva ni aplicarse ninguna otra sanción a un particular, sin acudir a los tribunales previamente establecidos (como excepción a lo dispuesto en el artículo 14 constitucional), si no está claramente determinado en una ley, sin que las Autoridades administrativas puedan ampliarse sus facultades al respecto por razones de interés público, o de conveniencia en el ejercicio de sus facultades, ni por ningunas otras. En el caso de las multas y sanciones administrativas se está, evidentemente en la segunda hipótesis de las examinadas, y las facultades para imponer sanciones, así como las sanciones mismas y las hipótesis en que procede su aplicación, deben estar expresa y explícitamente enunciadas en la ley, sin que se pueda ampliar ni facultades, ni sanciones, ni hipótesis de infracción, ni por analogía, ni por mayoría de razón, ni porque indebidamente se estime que el que puede lo más debe poder lo menos. Luego, para imponer las sanciones a que restrictivamente se refiere el artículo 23, fracción VI, del Reglamento Interior de la Secretaría de Agricultura y Recursos Hidráulicos (sin analizar aquí si es el Congreso el que debe fijar las facultades de los órganos de Autoridad del Ejecutivo, o si éste puede por sí y ante sí ampliarlas, otorgarlas o modificarlas), con base en ese precepto sólo tiene facultades el director general de Control y Vigilancia Forestal, sin que pueda asumirlas el secretario del ramo por analogía ni por mayoría de razón, ni por poder lo más, como superior de quien puede lo menos, porque esto violaría el sistema de facultades restringidas para imponer sanciones cobrables por la vía económico-coactiva, o imponibles sin acudir a los tribunales previamente establecidos.

#### PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO.

Amparo directo 1110/80. Doddoli Hermanos, S. de R.L. 1o. de abril de 1981. Unanimidad de votos. Ponente: Guillermo Guzmán Orozco.

---

Séptima Época

Instancia: Pleno

Fuente: Semanario Judicial de la Federación

Tomo: 187-192 Primera Parte

Página: 14

**AGRARIO. COMISIONES AGRARIAS MIXTAS Y COMISARIADOS EJIDALES. COMPETENCIA Y ATRIBUCIONES. SON CONSTITUCIONALES LOS PRECEPTOS DE LA LEY DE REFORMA AGRARIA QUE LAS REGLAMENTAN.-** Este Tribunal

Pleno ha establecido que es facultad exclusiva del Congreso de la Unión el legislar en materia agraria, haciendo derivar dicha atribución de las diversas fracciones del artículo 27 constitucional, particularmente de su fracción XI, en concordancia con la fracción XXX del artículo 73 de la misma Ley Fundamental, y ha afirmado también que si el Poder Legislativo detenta la mencionada facultad, también posee las facultades implícitas necesarias para realizar aquéllas que le son expresas. El artículo 27 constitucional en su fracción XI, incisos c) y e), establece la existencia de las comisiones agrarias mixtas y de los comisariados ejidales y otorga al Congreso de la Unión la facultad de reglamentar la competencia y atribuciones de esos organismos, todo lo cual conlleva a concluir que los artículos 434 al 440 de la Ley Federal de Reforma Agraria no son contrarios a los artículos 27 y 133 de la Constitución Federal, sino que se encuentran apegados a dichos preceptos de la Carta Fundamental.

Amparo en revisión 1177/79. Juliana Domínguez Cuendia. 4 de septiembre de 1984. Unanimidad de dieciocho votos. Ponente: J. Ramón Palacios Vargas.

Séptima Época, Primera Parte:

Volúmenes 175-180, página 29. Amparo en revisión 5193/79. Ana Segundo viuda de Zuriaga. 19 de julio de 1983. Unanimidad de diecinueve votos. Ponente: David Franco Rodríguez.

Véase: Semanario Judicial de la Federación, Séptima Época, Primera Parte:

Volumen 43, página 82, bajo el rubro “AGRARIO. FACULTAD LEGISLATIVA PRIVATIVA DEL CONGRESO DE LA UNION EN LA MATERIA, INCLUSIVE EN EL ASPECTO FISCAL.”.

Volumen 52, página 13, bajo el rubro “AGRARIO. PERMUTA DE BIENES EJIDALES. CONSTITUCIONALIDAD DE LOS PRECEPTOS DEL CÓDIGO AGRARIO QUE LA REGLAMENTAN.”.