



FIRMA ELECTRÓNICA AVANZADA EN MÉXICO

2018





NORMATIVA SOBRE FIRMA ELECTRÓNICA AVANZADA

1

NORMATIVA SOBRE FIRMA ELECTRÓNICA AVANZADA

SECTOR PÚBLICO

- LEY de Firma Electrónica Avanzada.  Regular el uso de la firma electrónica avanzada y los servicios relacionados con la firma electrónica avanzada.
- REGLAMENTO de la Ley de Firma Electrónica Avanzada  Establece las normas reglamentarias para el uso de la Firma Electrónica Avanzada; los servicios relacionados con ésta, así como su homologación con otras firmas electrónicas avanzadas.
- DISPOSICIONES Generales de la Ley de Firma Electrónica Avanzada.  Los requisitos, características, estándares y mecanismos tecnológicos que deberán cumplir las Autoridades Certificadoras
- NORMA Oficial Mexicana NOM-151-SE-2016  Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos

NORMATIVA SOBRE FIRMA ELECTRÓNICA AVANZADA

SECTOR PRIVADO

- CÓDIGO de Comercio.  Regula el **comercio electrónico y Prestadores de Servicios de Certificación** (conforme a la adopción de la Ley Modelo de UNCITRAL)
- REGLAMENTO del Código de Comercio en materia de Prestadores de Servicios de Certificación (PSC).  **Normas reglamentarias** a las que deben sujetarse los PSC para la expedición de certificados.
- REGLAS GENERALES a las que deberán sujetarse los PSC  Reglas para **acreditarse como PSC y ofrecer los servicios** de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos, Digitalización de Documentos en Soporte Físico.
- DISPOSICIONES Generales de la Ley de Firma Electrónica Avanzada.  Los **requisitos, características, estándares y mecanismos tecnológicos** que deberán cumplir las Autoridades Certificadoras
- NORMA Oficial Mexicana NOM-151-SE-2016  Requisitos que deben observarse para la **conservación de mensajes de datos y digitalización de documentos**



REQUISITOS DE VALIDEZ DE LOS CERTIFICADOS

2

REQUISITOS DE VALIDEZ DE LOS CERTIFICADOS

Elementos Jurídicos

1. Nombre de la Autoridad Certificadora, razón social, nombre de dominio de internet, correo electrónico, datos de acreditación.
2. Código de identificación único del Certificado
3. Periodo de vigencia
4. Fecha y hora de la emisión, suspensión y revocación del Certificado
5. Referencia tecnológica empleada para la creación de la Firma Electrónica
6. Nombre de la unidad dentro de la organización
7. Correo electrónico
8. Calle, número y colonia
9. Código Postal
10. País
11. Entidad Federativa
12. Municipio o delación

REQUISITOS DE VALIDEZ DE LOS CERTIFICADOS

Elementos Técnicos

<p>Estructuras de certificados digitales y lista de revocación de certificados (CRL por sus siglas en inglés)</p>	<p><i>RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i></p> <p><i>ISO/IEC 9594-8 Information technology -- Open Systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks.</i></p> <p><i>Últimas versiones.</i></p>
<p>Algoritmo criptográfico para firma electrónica (SHA-256 con RSA)</p>	<p><i>FIPS PUB 186-4 Digital Signature Standard (DSS), Chapter 5.</i></p> <p><i>Última versión.</i></p>
<p>Algoritmo hash (SHA-256)</p>	<p><i>FIPS 180-4 Secure Hash Standard (SHS).</i></p> <p><i>Last versión.</i></p>
<p>OCSP service</p>	<p><i>RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.</i></p> <p><i>Última versión.</i></p>

REQUISITOS DE VALIDEZ DE LOS CERTIFICADOS

Elementos Técnicos

<i>Longitud de la clave</i>	<i>AC - 4096 bits.</i> <i>Usuarios - 2048 bits.</i>
<i>Política de certificados y declaración de práctica de certificación</i>	<i>ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.</i> <i>RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.</i> <i>Últimas versiones.</i>
<i>Plan de administración de claves</i>	<i>ETSI TS 102 042 - Sección 7.2.</i> <i>Última versión.</i>



RECONOCIMIENTO DE CERTIFICADOS DE FIRMA EMITIDOS POR PRESTADORES DE SERVICIOS EXTRANJEROS

3

RECONOCIMIENTO DE CERTIFICADOS EMITIDOS EN EL EXTRANJERO

SECTOR PÚBLICO (art. 30 LFEA)

Los certificados digitales expedidos fuera de la República Mexicana tendrán la misma validez y producirán los mismos efectos jurídicos



Siempre y cuando tales certificados **sean reconocidos por las autoridades certificadoras** y se garantice el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado.



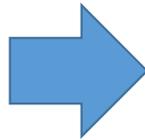
RECONOCIMIENTO DE CERTIFICADOS EMITIDOS EN EL EXTRANJERO

SECTOR PRIVADO (art. 114 CC)

REGLA GENERAL

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

Para determinar
grado de fiabilidad
equivalente



Se tomarán en consideración las **normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente**

3

RECONOCIMIENTO DE CERTIFICADOS EMITIDOS EN EL EXTRANJERO

SECTOR PRIVADO
(art. 114 CC)

ACUERDO DE RECONOCIMIENTO:



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



AUTORIDAD CERTIFICADORA

4

AUTORIDAD CERTIFICADORA



AUTORIDAD CERTIFICADORA

Armonización y homologación

Se emitieron las DISPOSICIONES Generales de la Ley de Firma Electrónica Avanzada., para establecer los **requisitos, características, estándares** y mecanismos tecnológicos que deberán cumplir las **Autoridades Certificadoras.**

Coordinación

Se firmaron bases de colaboración para favorecer el uso de la firma electrónica del SAT para procesos administrativos.



Prestadores de Servicios de Certificación

5

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Servicios

Certificado Digital

- Mensaje de datos que confirma el vínculo entre un firmante y la Firma Electrónica Avanzada.



Constancias de Conservación de Mensajes de Datos NOM-151-SCFI

- Garantizan la integridad de mensajes de datos en el transcurso de tiempo.



Sellos Digitales de Tiempo

- Son mensajes de datos que brindan certeza del momento en el que se realizó una transacción comercial electrónica.



Digitalización documentos

- Migración de documentos impresos a mensaje de datos



PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Requisitos

Elementos Humanos

- Un Profesional Jurídico.
- Un Profesional Informático.
- Cinco auxiliares de apoyo al Profesional Informático.

Elementos Materiales

- Espacio físico apropiado para la actividad.
- Controles de seguridad, accesos y perímetros de seguridad física.
- Medidas de protección.
- Políticas necesarias para garantizar la seguridad del área.

Elementos Económicos

- Seguro de Responsabilidad Civil.
- Una cuarta parte de la inversión requerida para cumplir con los elementos humanos, tecnológicos y materiales.
- Fianza.

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Requisitos

Elementos Tecnológicos

- Análisis y evaluación de riesgos y amenazas.
- Infraestructura informática.
- Equipo de cómputo y software.
- Política de seguridad de la información.
- Plan de continuidad del negocio y recuperación ante desastres.
- Plan de seguridad de sistemas.
- Estructura de certificados.
- Estructura de la lista de certificados revocados.
- Sitio electrónico.
- Procedimientos que informen de las características de los procesos de creación y verificación de Firma Electrónica Avanzada.
- Política de certificados.
- Declaración de prácticas de certificación.
- Modelos de operación de la Autoridad Certificadora (AC) y Autoridad Registratoras (AR).
- Plan de administración de claves.



Gracias!

2018

