ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

TSJCDMX

Firma Electrónica y Prueba Electrónica

Joel A. Gómez Treviño

Presidente Fundador de AMDI. Coordinador del Comité de Derecho de las Tecnologías de Información de ANADE.
Profesor del ITESM, INFOTEC, UDLAP Jenkins Graduate School y Universidad Panamericana Campus Guadalajara.
Socio Director de Lex Informática Abogados, S.C.

¿CUÁLES SON LOS PRINCIPALES PROBLEMAS O RETOS DE LOS CONTRATOS ELECTRÓNICOS?

@JoelGomezMX

Jurídicos

- ¿Cómo **manifestar la voluntad** a través de medios electrónicos?
- ¿Cómo se **perfecciona** un contrato electrónico?
- ¿Qué pasa cuando la ley te pide como **formalidad** celebrar los contratos por escrito y firmarlos si se celebran por internet?
- ¿Cómo **probamos la existencia de un contrato** (su oferta y aceptación) si se celebra mediante un medio electrónico?

Tecnológicos

- **Confidencialidad:** Si así lo acuerdan las partes, solo el emisor y el receptor pueden tener acceso al mensaje.
- **Identificación:** ¿Cómo garantizar que el mensaje proviene del emisor?
- **Autenticidad:** ¿Cómo garantizar que la persona que firma el contrato es quien dice ser?
- **Integridad:** ¿Cómo garantizamos que el contenido del mensaje y la firma no han sido alterados?
- **No repudio:** Innegable autoría y recepción del mensaje.

ANTECEDENTES INTERNACIONALES

- Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).
- Ley Modelo de la CNUDMI sobre Firma Electrónica (2001).
- Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2005).
- La Directiva de firma electrónica (1999/93/CE).
- La Directiva de comercio electrónico (2000/31/CE).
- Reglamento No 910/2014 del Parlamento Europeo Y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Cronología de Reformas más Relevantes

Mayo 29, 2000.-	Reformas al CCF, al CFPC, al CC y a la LFPC.
Junio 4, 2002.-	NOM-151-SCFI-2002, Requisitos que deben observarse para la conservación de mensajes de datos.
Agosto 29, 2003.-	Reforma al Código de Comercio para regular la firma electrónica.
Julio 19, 2004.-	Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación.
Enero 11, 2012.-	Ley de Firma Electrónica Avanzada.
Marzo 21, 2014.-	Reglamento de la Ley de Firma Electrónica Avanzada.
Abril 7, 2016.-	Reforma al Código de Comercio para regular la digitalización de documentos.
Marzo 30, 2017.-	NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002).

Regulación del Comercio Electrónico y la Prueba Electrónica

Código Civil Federal

- Art. 1803.- Se puede manifestar la **voluntad** por medios electrónicos.
- Art. 1834.- Cuando se exija la **forma escrita** para el contrato, **los documentos** relativos **deben ser firmados** por todas las personas a las cuales se imponga esa obligación.
- Art. 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma **íntegra**, a través de dichos medios sea **atribuible** a las personas obligadas y **accesibles** para su ulterior consulta.

Código Federal de Procedimientos Civiles

- Art. 210-A.- **Se reconoce como prueba** la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
- **Para valorar la fuerza probatoria** de la información a que se refiere el párrafo anterior, se estimará primordialmente la **fiabilidad** del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible **atribuir** a las personas obligadas el contenido de la información relativa y ser **accesible** para su ulterior consulta.
- Cuando la **ley requiera que un documento sea conservado y presentado en su forma original**, ese requisito quedará satisfecho **si se acredita que la información** generada, comunicada, recibida o archivada por **medios electrónicos**, **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**.

Regulación del Comercio Electrónico y la Prueba Electrónica

Código de Comercio

- Art. 89.- **Se adoptan principios** de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos.
- Art. 89 bis.- **No se negarán efectos jurídicos**, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.
- Por tanto, ante autoridad legalmente reconocida, **dichos mensajes podrán ser utilizados como medio probatorio en cualquier diligencia** y surtirán los mismos efectos jurídicos que la documentación impresa.
- Arts. 95 bis 1 al 99.- Regulación de la firma electrónica y la digitalización de documentos.

NOM-151-SCFI-2016

- **Es de observancia general para los comerciantes que conserven mensajes de datos** (art. 49 CC), así como los requisitos a cumplir en la digitalización de toda o parte de la documentación relacionada con sus negocios en soporte papel a un mensaje de datos.
- Esta NOM permite que los comerciantes conserven por el plazo establecido en el CC (10 años), el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones; y **cuyo contenido debe mantenerse íntegro e inalterado** a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta.

Código de Comercio: forma escrita, firma, forma original, integridad

Art. 93.- Cuando la ley exija la **forma escrita** para los contratos, 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, sin importar el formato en el que se encuentre o represente. Cuando adicionalmente la ley exija la **firma de las partes**, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.	Art. 93 bis.- Cuando la ley requiera que la información sea presentada y conservada en su **forma original**, ese requisito quedará satisfecho respecto a un Mensaje de Datos: • **I.** Si existe garantía confiable de que se ha **conservado la integridad de la información**, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y • **II.** De requerirse que la información sea presentada, si **dicha información puede ser mostrada a la persona** a la que se deba presentar.	Art. 93 bis (continuación).- Se considerará que el contenido de un Mensaje de Datos es **íntegro**, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Regulación del Comercio Electrónico

Ley Federal de Protección al Consumidor

- Art. 76 bis.- Requisitos (catálogo de obligaciones) que deben cumplir los comerciantes que oferten bienes o servicios por Internet:
  - Confidencialidad
  - Seguridad
  - Teléfono y domicilio
  - Términos y condiciones
  - No enviar “avisos comerciales”
  - Evitar prácticas com. engañosas

NMX-COE-001-SCFI-2018

- Disposiciones a las que se sujetarán todas aquellas personas físicas o morales que en forma habitual o profesional ofrezcan, comercialicen o vendan bienes, productos o servicios, mediante el uso de medios electrónicos, con la finalidad de garantizar los derechos de los consumidores que realicen transacciones a través de dichos medios.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

TSJCDMX

FIRMA ELECTRÓNICA Y FIRMA ELECTRÓNICA AVANZADA

Joel A. Gómez Treviño

Presidente Fundador de AMDI. Coordinador del Comité de Derecho de las Tecnologías de Información de ANADE.
Profesor del ITESM, INFOTEC, UDLAP Jenkins Graduate School y Universidad Panamericana Campus Guadalajara.
Socio Director de Lex Informática Abogados, S.C.

Clases de Criptografía

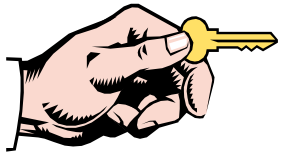
¿Qué es la Criptografía?

Es el proceso o habilidad de usar o descifrar escrituras secretas.

Clases de Criptografía

☑ Tradicional o Simétrica
☑ De Llave Pública o Asimétrica

Criptografía Tradicional



Aquella en la que la llave de cifrado es la misma de descifrado.

Criptografía de Llave Pública (PKI)

Cada persona tiene un par de llaves, una pública que todos conocen, y la otra privada que sólo su propietario conoce.

CRIPTOGRAFÍA.- DEFINICIONES BÁSICAS

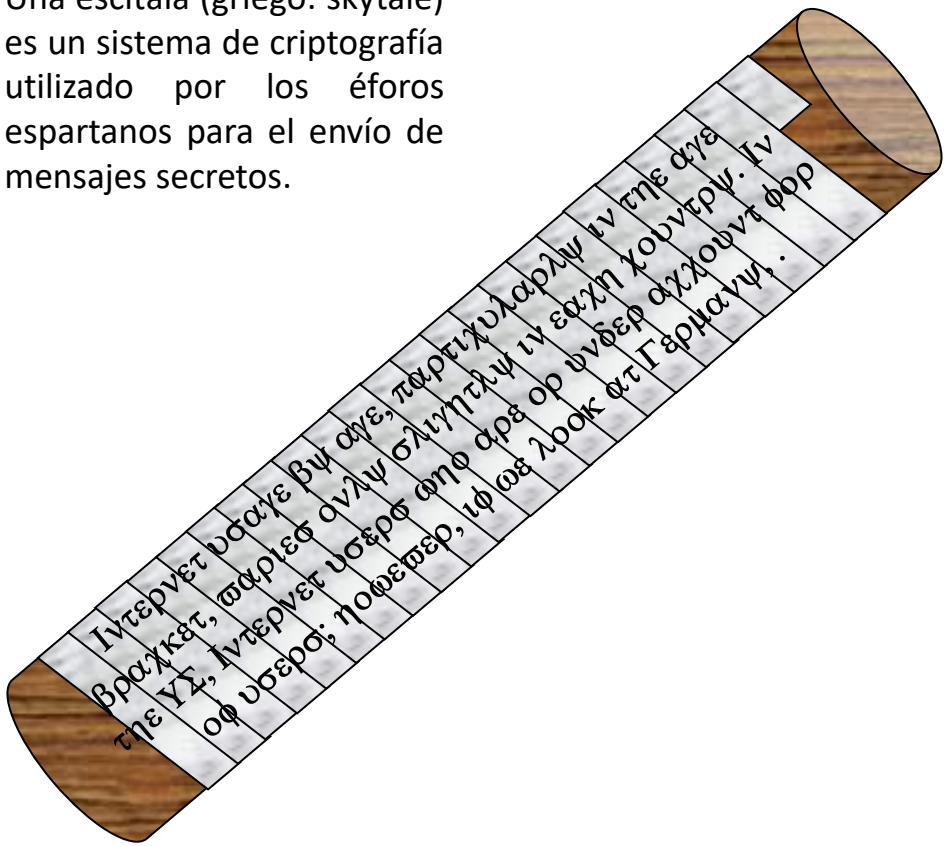
- Criptografía es la ciencia de mantener en secreto los mensajes.
- El texto original, o texto puro es convertido en un equivalente en código, llamado criptotexto (*ciphertext*) via un algoritmo de encripción.
- El criptotexto es decodificado al momento de su recepción y vuelve a su forma de texto original.

Antecedentes de la Criptografía

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

- En la Grecia antigua los militares utilizaban la criptografía, que aunque de manera rudimentaria, sus efectos eran los mismos: **Esconder un mensaje importante.**
- Ellos utilizaron un sistema llamado **SCYTALE**, el cual se basaba en un báculo pequeño.
- En este instrumento enredaban un listón delgado, de tal manera que quedara forrado.
- Finalmente, sobre el báculo forrado por el listón, escribían el mensaje a ser enviado al ejército aliado.

Una escítala (griego: skytálē) es un sistema de criptografía utilizado por los éforos espartanos para el envío de mensajes secretos.



Antecedentes de la Criptografía

- Posteriormente, este listón era desenrollado y en él quedaba escrito un mensaje indescifrable a simple vista.
- Ahora podía enviarse este mensaje de manera “segura”.

Antecedentes de la Criptografía

- Cuando el listón era enrollado en un báculo con las mismas dimensiones, se podía entender el mensaje.

- De esta forma sólo los ejércitos amigos tenían una réplica exacta del instrumento para “cifrar” y “descifrar” los mensajes importantes.

ESCÍTALA (GRIEGO: SKYTÁLĒ)

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

@JoelGomezMX

TEXTO ORIGINAL => CRIPTOTEXTO

Parameters

Word:

No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Determine

```
Input data (CMS):
4e6f207365206e65676172e16e2065666563746f73206a7572ed6469636f732c2076616c6964657a206f20667565727a61206f626c69
6761746f726961206120637 5616c7175696572207469706f20646520696e666f726d616369f36e20706f72206c6120736f6c61207261
7af36e20646520717565206574e920636f6e74656e69646120656e20756e204d656e73616a65206465204461746f732e030303

Cipher (ECB):
7e65ae819a4b62159be2205c46b650a08512990594c7e014009b6981d90ee1015545d59f5ed067e4e340781278b039d848e6bb014d36
fd79c4b3672e21c3d373fe0b59a809df8bf90969a94598f6dcaf0639a3bf664c03c79b95c424d054946774587c8dbd22046614722d0b
f96c902ddc2f2b9d72a64fb30c6a86db5c927093b2e65c3075de83ddb506a2cc15602f90ce09c0a9b3b176a854d83aac15fd7b82

Cipher to plain:        FEAR NUN JAKE POE MAIN CAW HUED EGO GIL GLUT CHAD AWAY FORK HAUL TOM MOS FAST CAL AD
SHUT BUOY LONG TOOT FINE BEEF OFF CLOG MOLE BE URGE STAG ASH AVE TURN ART TINA ADDS PUT MULE HOOF DASH MITE
NINE HOUR RAFT VAT SOB MEET WORN BODY COLT FIB WAYS WIRE BUS ANTE BALE PAN CURD BILE BAT RAYS TRIO RARE MUFF
STEW HOWL LIED BUM JAVA AFRO PIE DIVE NEWT LAY EDGE JIM PET FLY GURU UN UTAH ONUS GIG SILL EARN TALK SUNK
CERN SEWN CUE BAWL MALT MEAL MAN AHEM LOSS PEN COY TILE TEAM TRAG LYLE PRO LOST NAP APT OMIT REEK ARGO NAB
CLAW GOT BAWD BEAR NAME LATE NIL SCAT MYRA


Reverse:        2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

  decrypt: No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por
la sola razón de que esté contenida en un Mensaje de Datos.
```

MUCHOS TÉRMINOS

Universo del Consentimiento
Énfasis en consentimiento expreso

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

@JoelGomezMX

Consenti-miento verbal

Consentimiento tácito

FIRMAS

Consenti-miento por escrito

Firma autógrafa

Firma electrónica

Username + Password

Firma digital (Firma Electrónica Avanzada o Fiable)

Criptografía, llave pública, llave privada, certificado digital…

Firma biométrica

Click Wrap

Opt-In Opt-Out

Reconoci-miento de voz

Huella digital

NIP bancario

Consenti-miento por medios electrónicos

¿PARA QUÉ SIRVE UNA FIRMA?

@JoelGomezMX

- Declarar el consentimiento
- Declarar autoría
- Confirmar la relación que tiene el autor con el contenido del texto firmado
- Para demostrar la autenticidad y/o integridad de un documento

EJEMPLO DE UN MENSAJE DE DATOS FIRMADO DIGITALMENTE

<Firmado FirID=1>

Aceptación de Oferta de Compraventa

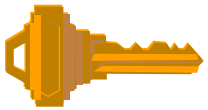
Estimado Pedro López, acepto tu oferta para comprarte 100 computadoras modelo ZX-99 por un precio total de $25,000 dólares, pagaderos al tipo de cambio de la fecha de entrega del pedido.

Juan Pérez

El Comprador

</Firmado>

<Firma FirID=1PsnID=perez082>2AB3764 578CC18946A29870F40198B240CD2302B2349 802DE002342B212990BA5330249CID</Firma>



POR CONFIDENCIALIDAD se usan las dos llaves del receptor:

Todo el documento es cifrado con la LLAVE PÚBLICA del receptor del mensaje (Pedro López). Entonces, sólo Pedro López, con su LLAVE PRIVADA puede descifrarlo (abrirlo para su lectura).

PARA AUTENTICARLO se usan las dos llaves del emisor:

El emisor (Juan Pérez) firma la aceptación con su LLAVE PRIVADA. Pedro López verificará la identidad de Juan Pérez comparando su LLAVE PRIVADA con su LLAVE PÚBLICA.

EJEMPLO REAL DE LLAVE PÚBLICA (3072 K)

Estimado Juan, te anexo el Contrato de Compraventa firmado digitalmente.

Joel A. Gómez Treviño

abogado@joelgomez.com

Llave pública generada por el sistema criptográfico asimétrico “PGP”

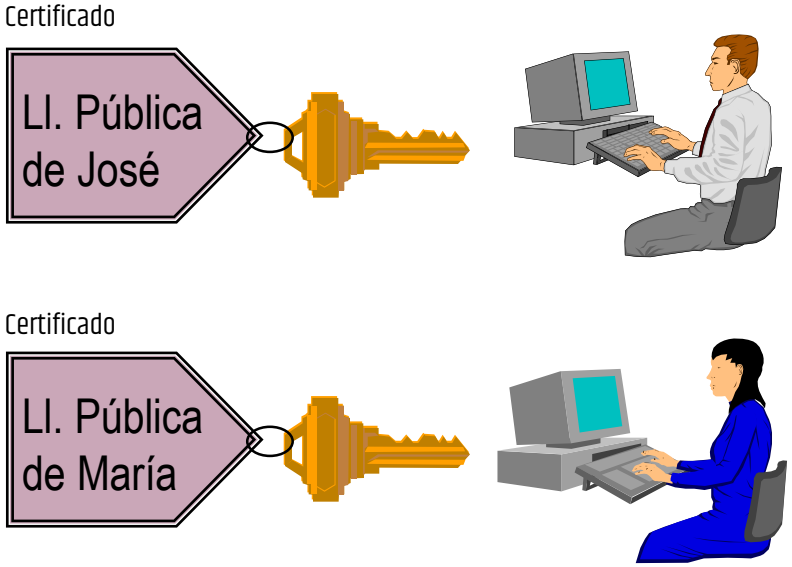
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com
mQGiBD9iEkIRBAD3RtpqZxsqYBcwJ4VTj5NsmkUiBZQ2HpY1oNpyRh7Wh7dYaioq0qWkFNQI5UJMPCm6hjPR2bo2PqhIChwLKJOMaiD1MlgxWBeMsz4GbTKgeS2wnaytQgWaQ/eQjVCUQ4mQg9RdS60
B7m7pOLd6ZtspYBXiqa9l2Q6YmgNnjEqScQCg/1iZrfVAFSqGN8IMkvsHGCKyUDMD/ReyBgrV3Ma7J66JXzapTUrFZ8NZJoa4GqRf+LBwDq7NLsENyzd5ofR77vsGFxguJ4D8rVRwq5PA7vjk4H7Oag7YPJH
k1W8kg84pYDHYdTaRMtzwfXksdraSsC/beDfP52PcpIrjmP1b9b5F5FT7wtKSzv6am7/+MmE1wcrtCbEvBADPnSyZ0EhUZpXi6Vi/gSBADXSwUR4GkRE9vktbXSfvI0fZwf8RMO5CVIFrjGI7nmUP809FUxRrSJ
2XuswGMzvoYpuiKh2p4x0NixlkyEZvDulA5BkkCDhuyf45nkIXQ6ZFOqN8hby/24muMU1IVUD8Y0VT77sSJa693fdDiAyhXbQ1Sm9lbCBBbGVqYW5kcm8gR8OzbWV6IFRyZXZpw7FvIDxqb2VsZ29tZXpAbG
F3eWVyLmNvbT6JAFcEEBECABcFAj9iEkMHCwkIBwMCCgIZAQUbAwAAAAAKCRAJgUzvMKbZ9HAUAJ9YTgGV+ruvM8Jadc7SPwixIOuY6QCfVNA10fJRJziyMdUKYRRee1XpI6a5Aw0EP2ISQxAMAMw
dd1ckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHIdOHX79sFzxIMRJitDYMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZCLQI2wSbLaF6dfJgJCo1+Le3kXXn11JJPmxi
O/CqnS3wy9kJXtwh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq01
uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmWn6vQCIC
bAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6UwybwACAgv9Hfeii/rSqOextybASEXJ/51sF3gQ7CAD9MQMX76NvS86USH6k2+XdOIZcF5Jg1U9bL8Kxk7pAlIRH/0gsTySBobhr/aUUyJYj1EI3Sp/QYAHrC/Jw4It
6Jo7tITYkLhIEWRkpfLiTt2HJJD/4a5uMMfQCghzYKJkxvCA3R5cxRvAkt4DgTUyn1/gZbgwjHg4qMWohQ8NnXxCyMcYxsH6kwYLR4auze5CpHQqS4Em92L6fKvSKkadjpNB9ZsmjhAVxAu3u39lWst41F4zzx
MnXLovXuAssZbM9nvj/f44K+7eABiWHDHQ178brPn2lMU4x4Z9smEbRjzVS2EbhxIB+8A1YbfczFjYzLmpMU7rJTYTkQQ5k8Rh4Tyd5d21S08n/nzENKUke0U7BpIJCA/VJaM7xMIFtgH4LNkXXsUljZUZVS12
3kuCkEEf+1eKZfrJmIop40VG7WWoMn9CxWwnxj+isyow0gqrdOehI8v/M6+mlr3IGhGluOlDgqZ/OSxiQBMBBgRAgAMBQI/YhJDBRsMAAAAAAoJEAmBTO8wptn0bHsAoL+KBJxC0712bw+phvkmGfB4eqOU
AJ9l8Sw845sr/W7xtiBcnoD+j3F62g===t9tQ
-----END PGP PUBLIC KEY BLOCK-----

CERTIFICADOS DIGITALES

Pero ¿cómo sabemos que José y María tienen asignadas las llaves públicas que dicen tener? Mediante un instrumento llamado **Certificado Digital**, emitido por un Prestador de Servicios de Certificación. El Certificado Digital es el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada.

CERTIFICADO DIGITAL

La identidad del titular.
Datos de filiación del titular.
La clave publica del titular.
Datos del certificado: número de serie, fecha de caducidad.
La identidad de la autoridad de certificación que lo ha emitido.
La firma de la autoridad de certificación.



- Firma Electrónica:
  - Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

II. Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

III. Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma, y

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

Lo anterior se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una firma electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

- **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**;

Otras definiciones de la Ley de Firma Electrónica Avanzada

- **Certificado Digital:** el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada;
- **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;
- **Clave Pública:** los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante;
- **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;

Objeto de la Ley de Firma Electrónica Avanzada

- Artículo 1. 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.

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

TSJCDMX

La Prueba Electrónica y Algunas Tesis Relevantes

Joel A. Gómez Treviño

Presidente Fundador de AMDI. Coordinador del Comité de Derecho de las Tecnologías de Información de ANADE.
Profesor del ITESM, INFOTEC, UDLAP Jenkins Graduate School y Universidad Panamericana Campus Guadalajara.
Socio Director de Lex Informática Abogados, S.C.

Prueba Pericial Científica
Su Objeto y Finalidad

- **El objeto de la prueba pericial es el auxilio en la administración de justicia**, consistente en que un experto en determinada ciencia, técnica o arte aporte al juzgador conocimientos propios de su pericia y de los que el juzgador carece, porque escapan al cúmulo de los que posee una persona de nivel cultural promedio, los cuales, además, resultan esenciales para resolver determinada controversia.

- Así, **el uso de la pericial**, y con ella de los métodos científicos, **implica el aprovechamiento de conocimientos especializados, indispensables para apreciar y calificar ciertos hechos o evidencias** y poderles atribuir o negar significado respecto a una cierta práctica, hipótesis o conjetura que pretende acreditarse.

Tesis Aislada: I.1o.A.E.45 K (10a.)

Prueba Electrónica Civil vs. Mercantil

210-A CFPC: **Se reconoce como prueba** la información generada o comunicada que conste en **medios electrónicos**, ópticos o en cualquier otra tecnología. Para la **valoración de la fuerza probatoria** se estimara primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

- Artículo 1205.- **Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador** acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas {los} mensajes de datos ...
- 1298-A CC: **Se reconoce como pruebas los mensajes de datos** y establece que **valorar la fuerza probatoria** de los mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.
- 1061 BIS CC (DOF: 13/06/2014): **En los juicios mercantiles se reconoce como prueba la información generada o comunicada en medios digitales, ópticos o en cualquier otra tecnología** se llevará a cabo conforme a lo establecido en ese ordenamiento. Su valor probatorio se regirá conforme a lo previsto por el articulo 210-A del CFPC.

TRANSFERENCIAS ELECTRÓNICAS. NO ES DOCUMENTO PRIVADO CUYO VALOR SEA EQUIPARABLE AL DE UNA COPIA SIMPLE.

Tesis: I.3o.C.220 C (10a.)

- **La impresión de internet de una transferencia electrónica** no puede ser valorada como una copia simple de un documento privado, toda vez que no puede imputársele a persona alguna su elaboración o materialización ante la falta de firma autógrafa para efectos de su reconocimiento, sino que en términos de los artículos 1237, 1238, 1242 y 1245 del Código de Comercio, así como del diverso 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria al de Comercio, **goza de la naturaleza de descubrimiento de la ciencia, por lo que queda al prudente arbitrio del juzgador la valoración de la información recabada de medios electrónicos**.

- Así, **en aras de crear seguridad jurídica en los usuarios de los servicios electrónicos**, el legislador estableció reglas específicas para la valoración de la documental electrónica, de tal suerte que no puede valorarse como si se tratara de una copia simple de documentos privados, sino que queda a la prudencia del juzgador, en la inteligencia de que **debe atenderse preponderantemente a la fiabilidad del método** en que haya sido generada, comunicada, recibida o archivada la información contenida en los medios electrónicos, como son el código de captura, la cadena de caracteres generada con motivo de la transacción electrónica, sello digital o **cualquiera que permita autenticar el contenido de ese documento digital** y no elementos ajenos a la naturaleza de los documentos electrónicos; […]

DOCUMENTOS Y CORREOS ELECTRÓNICOS. SU VALORACIÓN EN MATERIA MERCANTIL.

Tesis: I.4o.C.19 C (10a.)

- **En varios sistemas jurídicos se han equiparado totalmente los documentos multimedia o informáticos, a efectos de valoración**. Esa equivalencia es, básicamente, con los privados, y su admisión y valoración se sujeta a requisitos, sobre todo técnicos, como la firma electrónica, debido a los problemas de fiabilidad de tales documentos, incluyendo los correos electrónicos, ya que es posible falsificarlos e interceptarlos, lo cual exige cautela en su ponderación, pero sin desestimarlos sólo por esa factibilidad.
- **Para evitar una pericial en informática que demuestre la fiabilidad del documento electrónico, pero complique su ágil recepción procesal, el juzgador puede consultar los datos técnicos reveladores de alguna modificación señalados en el documento**, aunque de no existir éstos, atenderá a la posibilidad de alteración y acudirá a la experticia, pues el documento electrónico puede quedar en la memoria RAM o en el disco duro, y podrán expedirse copias, por lo que para comprobar el original deberán exhibirse documentos asistidos de peritos para su lectura.
- Así es, dado que **la impresión de un documento electrónico sólo es una copia de su original**.
- **Mayor confiabilidad merece el documento que tiene firma electrónica**, aunque entre esa clase de firmas existe una gradación de la más sencilla a la que posee mayores garantías técnicas, e igual escala sigue su fiabilidad, ergo, su valor probatorio.

DOCUMENTOS Y CORREOS ELECTRÓNICOS. SU VALORACIÓN EN MATERIA MERCANTIL.

Tesis: I.4o.C.19 C (10a.)

- Así, **la firma electrónica avanzada prevalece frente a la firma electrónica simple**, ya que los requisitos de producción de la primera la dotan de más seguridad que la segunda, y derivan de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre las Firmas Electrónicas. Esta propuesta de normatividad, al igual que la diversa Ley Modelo sobre Comercio Electrónico, fue adoptada en el Código de Comercio, **el cual sigue el criterio de equivalencia funcional que busca equiparar los documentos electrónicos a los tradicionales elaborados en soporte de papel, mediante la satisfacción de requisitos que giran en torno a la fiabilidad y trascienden a la fuerza probatoria de los mensajes de datos**. Por ende, conforme a la interpretación de los artículos 89 a 94, 97 y 1298-A del Código de Comercio, **en caso de que los documentos electrónicos reúnan los requisitos de fiabilidad** legalmente previstos, **incluyendo la existencia de una firma electrónica avanzada**, **podrá aplicarse el criterio de equivalente funcional con los documentos que tienen soporte de papel**, de manera que **su valor probatorio será equivalente al de estos últimos**.

- **En caso de carecer de esa firma y haberse objetado su autenticidad, no podrá concedérseles dicho valor similar**, aunque su estimación como prueba irá en aumento si en el contenido de los documentos electrónicos se encuentran elementos técnicos bastantes, a juicio del juzgador, para estimar altamente probable su autenticidad e inalterabilidad, o bien se complementan con otras probanzas, como la pericial en informática que evidencie tal fiabilidad. Por el contrario, **decrecerá su valor probatorio a la calidad indiciaria si se trata de una impresión en papel del documento electrónico**, que como copia del original recibirá el tratamiento procesal de esa clase de documentos simples, y se valorará en conjunto con las restantes pruebas aportadas al juicio para, en función de las circunstancias específicas, determinar su alcance demostrativo.

INFORMACIÓN PROVENIENTE DE INTERNET. VALOR PROBATORIO.

- El artículo 188 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, en términos de lo previsto en el diverso artículo 2o. de este ordenamiento legal, dispone: "**Para acreditar hechos o circunstancias en relación con el negocio que se ventila, pueden las partes presentar fotografías, escritos o notas taquigráficas, y, en general, toda clase de elementos aportados por los descubrimientos de la ciencia**."; asimismo, el diverso artículo 210-A, párrafo primero, de la legislación que se comenta, en lo conducente, **reconoce como prueba la información generada o comunicada que conste en medios electrónicos**, ópticos o en cualquiera otra tecnología; ahora bien, entre los medios de comunicación electrónicos se encuentra "internet", que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos y, dependiendo de esto último, puede determinarse el carácter oficial o extraoficial de la noticia que al efecto se recabe, y como constituye un adelanto de la ciencia, procede, en el aspecto normativo, otorgarle valor probatorio idóneo.

Tesis: V.3o.10 C

PRESUNCIONES LEGALES PREVISTAS EN LOS ARTÍCULOS 90, 90 BIS Y 95 DEL CÓDIGO DE COMERCIO. PARA QUE OPEREN A FAVOR DE LAS INSTITUCIONES BANCARIAS Y SE ARROJE LA CARGA DE LA PRUEBA A LOS USUARIOS, DEBEN ACREDITAR PREVIAMENTE QUE LA PLATAFORMA DONDE SE EJECUTÓ LA OPERACIÓN ES FIABLE Y SEGURA.

- Las instituciones de crédito pueden pactar con sus cuentahabientes que determinadas operaciones bancarias se realicen vía Internet por computadora; mediante teléfono celular inteligente (smartphone); o en cajeros automáticos, para lo cual deben proporcionar datos únicos y exclusivos que pueden consistir en usuarios, claves, contraseñas (como el NIP) e, incluso, contraseñas dinámicas (token).
- Entonces, **cuando una transacción electrónica se ejecuta con éxito**, de conformidad con los artículos 90, 90 Bis y 95 del Código de Comercio **surge la presunción de que se realizó, porque el cuentahabiente ingresó la información correcta para ese efecto, sea que lo haya efectuado personalmente, por conducto de su autorizado o mediante un sistema de información programado para actuar en su nombre automáticamente**; sin embargo, para que esta presunción opere a favor de la institución de crédito, de conformidad con el artículo 90 Bis citado, debe acreditar previamente que la plataforma donde se ejecutó la operación es fiable y segura, y que existe certeza de que una transacción sólo se realizará si se ingresan los datos correctos, y no pueda tratarse de un fraude electrónico, **de ese modo se revertirá la carga de la prueba al usuario bancario para que acredite que los mensajes de datos de la operación que se controvierta no fueron realizados por él**; por su autorizado o por un sistema de información que programó para actuar en su nombre automáticamente.
- **Lo anterior, puede demostrarse**, por ejemplo, **con el dictamen de un experto en materia informática que dirima si la plataforma donde se realizó la operación bancaria es fiable y segura** por contar con un procedimiento que única e invariablemente autorizará una transacción cuando se ingresen los datos correctos requeridos (usuarios, claves, NIP, contraseñas dinámicas, etcétera), y no por diversas intervenciones informáticas.

Tesis: (IV Región)1o. J/13 (10a.)

TARJETAS BANCARIAS. EL NÚMERO DE IDENTIFICACIÓN PERSONAL (NIP) MEDIANTE EL CUAL SE AUTORIZAN OPERACIONES COMERCIALES, TIENE EL CARÁCTER DE UNA FIRMA ELECTRÓNICA.

- El Banco de México, en atención al desarrollo del sistema financiero y la protección de los intereses de los usuarios, incentivó a las instituciones financieras emisoras de tarjetas bancarias para que adoptaran las medidas adicionales a fin de reducir riesgos derivados del uso de tales instrumentos en transacciones comerciales. Por tanto, **la gran mayoría de dichas instituciones optaron por sustituir la firma autógrafa de sus clientes, con el uso obligatorio de un número de identificación personal (NIP), como herramienta de autenticación en las operaciones comerciales de los tarjetahabientes**.
- Ahora bien, de conformidad con lo dispuesto por el artículo 89 del Código de Comercio, la firma electrónica se constituye por los datos aparejados a un mensaje de datos, […], y entre tales medios se encuentra el intercambio de información estructurada bajo alguna norma técnica o formato convenido; la cual sirve para identificar al firmante y vincular su consentimiento con el acto comercial que se realiza.
- Por tanto, **la naturaleza jurídica del NIP es la de una firma electrónica simple, de conformidad con el precepto legal aludido, en atención a que se trata de datos consignados, adjuntados o asociados en un mensaje de datos, los cuales sirven tanto para identificar al firmante, como para indicar que éste aprueba la información contendida en el mensaje de datos**.

Tesis: 1a. XLIX/2019 (10a.)

TSJCDMX

SOBRE LA MISCELÁNEA DE COMERCIO ELECTRÓNICO

¿ES LEGAL CONTRATAR POR INTERNET?

@JoelGomezMX

- **¡Sí!** Tanto en materia **civil** como **mercantil** nuestra legislación se ha reformado para que tanto particulares como comerciantes puedan expresar su voluntad (consentimiento) por medios electrónicos.
  - Reformas del año 2000 al Código Civil Federal y Código de Comercio.

¿ES LEGAL CONTRATAR POR INTERNET?

- Art. 1803 CCF: El consentimiento puede ser expreso o tácito. Será expreso cuando se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología {…}
- Art. 89 CC.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará **mensaje de datos**.

Consentimiento Electrónico

¿SON VÁLIDAS LAS PRUEBAS DIGITALES?

@JoelGomezMX

- **¡Sí!** Nuestra legislación **procesal civil** como **mercantil** fue modificada para aceptarlas:
  - Art. 210-A CFPC.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
  - Art. 89bis CC.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un mensaje de datos.
  - Art. 1298-A CC.- Se reconoce como prueba los mensajes de datos.

¿CÓMO PRESERVAMOS DATOS DIGITALES?

- **Conservación de Mensajes de Datos**
  - La NOM-151-SCFI-2016 permite el cumplimiento de la obligación a cargo de los comerciantes (Art. 49 del Código de Comercio) que utilicen mensajes de datos para realizar actos de comercio, de conservar por el plazo establecido en dicho Código (10 años), el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones; y cuyo contenido debe mantenerse íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta.

CONCLUSIONES SOBRE EL MENSAJE DE DATOS Y/O DOCUMENTO ELECTRÓNICO

- Está reconocido legalmente. Se puede usar para:
  - Evidencia en un juicio.
  - Contratar electrónicamente.
  - Presentar un documento original.
  - Conservar un documento en su formato original.
  - Archivar documentos.
- Tiene el mismo peso legal que un documento físico:
  - No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.
- Está protegido en diversos contextos:
  - Para brindar seguridad, confidencialidad y disponibilidad de la información.
  - Delitos informáticos.
  - Protección de datos personales.
  - Propiedad intelectual.
- Goza de protección y reconocimiento a nivel internacional.

GRACIAS

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

@JoelGomezMX

Joel A. Gómez Treviño
LEX INFORMÁTICA ABOGADOS, S.C.
ACADEMIA MEXICANA DE DERECHO INFORMÁTICO, A.C.

- www.LexInformatica.com
- www.JoelGomez.Abogado
- www.amdi.org.mx
- www.AbogadoDigital.tv
- www.Abogado.Digital

Boulevard Anillo Periférico Adolfo López Mateos No.4293, Piso 3, Int. 300.
Col. Jardines de la Montaña. C.P. 14210.
Ciudad de México.

Conmutador.- (55) 4774-0597

joelgomez@lexinformatica.com

abogado@joelgomez.com

Sobre el Autor

Joel Gómez Treviño

- Es Abogado egresado del Tecnológico de Monterrey y tiene una Maestría en Derecho Internacional por la Universidad de Arizona. Es Doctor Honoris Causa. Cuenta con 24 de años de trayectoria como especialista en derecho de las tecnologías de la información, privacidad y propiedad intelectual.
- Es Presidente fundador de la Academia Mexicana de Derecho Informático y Coordinador del Comité de Derecho de las TIC y Datos Personales de la Asociación Nacional de Abogados de Empresa, Colegio de Abogados (ANADE).
- Ha recibido 18 reconocimientos (nacionales e internacionales) debido a su desempeño profesional y su contribución al crecimiento de la industria de Internet en México.
- Ha sido invitado a impartir más de 450 conferencias y cursos en programas profesionales y académicos de Brasil, Canadá, Colombia, Costa Rica, Ecuador, España, Estados Unidos, Guatemala, Italia, Panamá, México y Asia.
- Es profesor del ITESM, Universidad Panamericana, INFOTEC y UDLAP.

Derechos de Autor

TSJCDMX

Joel Alejandro Gómez Treviño es el autor de estos materiales, los cuales en su versión original datan del año 1998 y su última actualización es del año 2019. Para su difusión y conocimiento, el autor desea ponerlos en libre circulación. Las únicas restricciones para el uso de estos materiales son las siguientes:

- No se pueden editar de ninguna manera.
- No se puede comercializar ni lucrar (directa o indirectamente) con ellos.
- En caso de utilizarlos (total o parcialmente), deberá citarse al autor.