

LEY 25.506 DE FIRMA DIGITAL

La Ley 25.506 de Firma Digital regula en Argentina:

- la firma digital,
- los certificados digitales,
- la infraestructura de confianza electrónica,
- la validez jurídica de documentos electrónicos.

Su objetivo principal es otorgar:

- seguridad,
- autenticidad,
- eficacia probatoria,

a las operaciones realizadas en entornos digitales.

CONTEXTO

Tradicionalmente:

- los documentos en papel,
- con firma manuscrita,

eran el principal medio de acreditar autoría y consentimiento.

Con la digitalización surgió la necesidad de crear mecanismos tecnológicos capaces de brindar:

- identificación del firmante,
- integridad del documento,
- seguridad jurídica.

PRINCIPIOS FUNDAMENTALES

1. AUTENTICIDAD

Permite verificar:

quién firmó el documento.

La firma digital vincula técnicamente el documento con el titular del certificado digital.

Objetivo

Evitar:

- suplantación de identidad,
 - falsificación,
 - adulteración.
-

2. INTEGRIDAD

Garantiza que:

el documento no fue modificado luego de firmado.

Si el contenido cambia:

- la firma pierde validez,
 - el sistema detecta alteración.
-

Funcionamiento técnico

Se utiliza una función criptográfica denominada:

- hash,
 - huella digital.
-

3. NO REPUDIO

Implica que:

el firmante no puede negar válidamente haber firmado.

Esto otorga:

- fuerza probatoria,
 - seguridad contractual,
 - confianza jurídica.
-

BASE TECNOLÓGICA

La ley se basa en criptografía asimétrica.

PKI — Public Key Infrastructure

Infraestructura de clave pública.

Funciona mediante:

- clave privada,
 - clave pública,
 - certificados digitales.
-

FUNCIONAMIENTO SIMPLIFICADO

Paso 1

El usuario posee:

- una clave privada (secreta),
 - una clave pública.
-

Paso 2

Firma digitalmente el documento utilizando su clave privada.

Paso 3

El sistema genera una huella criptográfica.

Paso 4

El receptor verifica:

- autenticidad,
 - integridad,
 - vigencia del certificado.
-

CERTIFICADO DIGITAL

Concepto

Documento electrónico emitido por una entidad confiable que:

- acredita identidad,
 - vincula persona y clave pública.
-

CONTIENE

- nombre del titular,
 - clave pública,
 - período de vigencia,
 - autoridad certificante,
 - firma de la entidad emisora.
-

AUTORIDADES CERTIFICANTES

Son entidades habilitadas para emitir certificados digitales válidos.

FUNCIÓN

Verifican la identidad del solicitante antes de emitir el certificado.

Actúan como:

terceros de confianza.

EJEMPLO EN ARGENTINA

SIGEN

(Sindicatura General de la Nación)

OTRAS ENTIDADES RELACIONADAS

También intervienen:

- ONTI,
 - Autoridad Certificante Raíz,
 - organismos públicos habilitados.
-

EFFECTOS JURÍDICOS

Presunción legal

La firma digital presume:

- autoría,
- integridad,
- autenticidad.

CÓDIGO CIVIL Y COMERCIAL

Arts. 286 a 288 CCCN

Arts. 286 a 288 CCCNArts. \ 286 \ a \ 288 \ CCCNArts. 286 a 288 CCCN

DIFERENCIA CON FIRMA ELECTRÓNICA

Firma Electrónica	Firma Digital
Menor seguridad	Mayor seguridad

No tiene presunción legal automática	Sí tiene presunción legal
Puede probarse por cualquier medio	Basada en certificado digital
Más simple	Criptográficamente robusta

APLICACIONES PRÁCTICAS

En Argentina se utiliza en:

- expedientes judiciales electrónicos,
 - AFIP,
 - facturación electrónica,
 - trámites administrativos,
 - banca digital,
 - contratos electrónicos,
 - firma remota estatal.
-

EJEMPLO COTIDIANO

Cuando un abogado firma un escrito judicial digitalmente:

- el sistema verifica identidad,
 - garantiza integridad,
 - registra fecha y hora,
 - genera trazabilidad.
-

IMPORTANCIA JURÍDICA

La firma digital permite:

- despapelización,
 - modernización estatal,
 - contratación remota,
 - seguridad en transacciones,
 - agilización procesal.
-

La firma digital busca cumplir en el mundo electrónico la misma función que la firma manuscrita en el papel, pero utilizando herramientas criptográficas que aportan mayor seguridad técnica y jurídica.