INTRODUCCIÓN
A LA FIRMA DIGITAL

.01

1 QUÉ ES LA FIRMA DIGITAL

La firma digital es una herramienta tecnológica que permite asegurar la autoría de un documento o mensaje y verificar que su contenido no haya sido alterado. Es una secuencia única de letras y números que vincula al firmante con un documento electrónico. Se usa como identificación y autenticación en internet y sistemas informáticos. Un documento electrónico firmado digitalmente posee la misma validez jurídica que un documento en papel firmado de puño y letra.

Estas son las características de la firma digital:

Validez jurídica:
Tu firma digital te permite firmar documentos electrónicos digitalmente con la misma validez jurídica que una firma de puño y letra. La firma se encuentra bajo control del firmante en todo momento.

Autenticidad e integridad del documento:
Podrás identificar al autor fácilmente y verificar si el documento fue alterado, por lo cual se asegura su autoría e integridad.

Seguridad:
Se basa en la criptografía asimétrica. Instalaciones seguras para el almacenamiento de los datos, los roles definidos para cada proceso y el personal capacitado en todos los sectores garantizan la seguridad.

Múltiples usos:
Para hacer trámites con entidades privadas y públicas, tales como declaraciones impositivas y notificaciones judiciales, operaciones bancarias, contratos a distancia y documentos de comercio exterior. Se puede firmar digitalmente todo tipo de archivo.

INTRODUCCIÓN
A LA FIRMA DIGITAL

.01

2 NORMATIVA SOBRE LA FIRMA DIGITAL

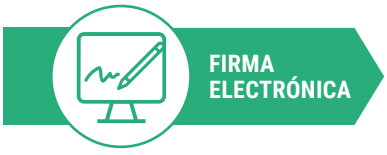
La Ley 25506 de Firma Digital (texto actualizado: https://www.argentina.gob.ar/normativa/nacional/70749/actualizacion) reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina (IFDRA).

Además, el artículo 288 del Código Civil y Comercial de la Nación sustenta la validez legal de la firma digital: «Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento».

Para ver toda la normativa referente a la firma digital, podés visitar el siguiente enlace: https://www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/innovacion/firma-digital/normativa-de-firma-digital.

3 COMPARACIÓN CON OTRO TIPO DE FIRMAS

Digital:
Es una cantidad determinada de algoritmos matemáticos, que se genera a través de un certificado digital emitido por una autoridad certificante licenciada por un órgano público. Se crea mediante una clave privada que se origina a través de un método de cifrado denominado criptografía asimétrica y utiliza una clave pública para verificar que dicha firma digital fue realmente generada mediante la clave privada correspondiente a la persona titular del certificado digital. Esta se plasma en un documento digital donde consta la voluntad del signatario y tiene la correspondiente validez jurídica.



Electrónica:
Es un conjunto de algoritmos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de algunos de los requisitos legales para considerarse firma digital. La firma electrónica puede ser simple (código, PIN o tilde) o avanzada (biometría, lápiz óptico).

Digitalizada:
Es la conversión del trazo de una firma en una imagen. Para obtener la propia firma digitalizada, hay que realizarla sobre un papel y escanearla, o bien mediante algún tipo de *hardware*, como pueden ser los *pads* de firma, que permiten guardar la imagen de la firma en la computadora, en formato JPG o PGN, y utilizarla cada vez que se la necesite. La firma digitalizada se considera firma electrónica simple, con lo cual es legal, pero no ofrece ninguna garantía respecto a la identidad del firmante.

4 CERTIFICADO DIGITAL

Para que el procedimiento de firma y autenticación sea confiable, hay que tener la seguridad de que la clave pública efectivamente pertenece al firmante. Por eso, el segundo elemento que sostiene el sistema de firma digital es la infraestructura de clave pública (PKI, *Public Key Infrastructure*), que regula cómo se emiten y distribuyen las claves. Para esto, se utilizan documentos llamados certificados de clave pública o, según nuestra normativa, certificados digitales.

Un certificado digital es simplemente un documento firmado digitalmente por una autoridad, en el cual se atestigua que una clave pública pertenece a determinado individuo o entidad. En general, contiene datos de identidad de la persona, su clave pública y el nombre de la autoridad que emitió el certificado. Todos los datos de identidad son previamente validados por esta autoridad, y el certificado se puede autenticar de la misma forma que cualquier otro documento con firma digital.

La infraestructura de clave pública es el conjunto de procedimientos, políticas y roles normados que definen cómo se generan y organizan esos certificados. Si el certificado es auténtico y se confía en la autoridad emisora, se puede asegurar la identidad del firmante. En nuestro país, esta regulación se conoce como Infraestructura de Firma Digital de la República Argentina o IFDRA.

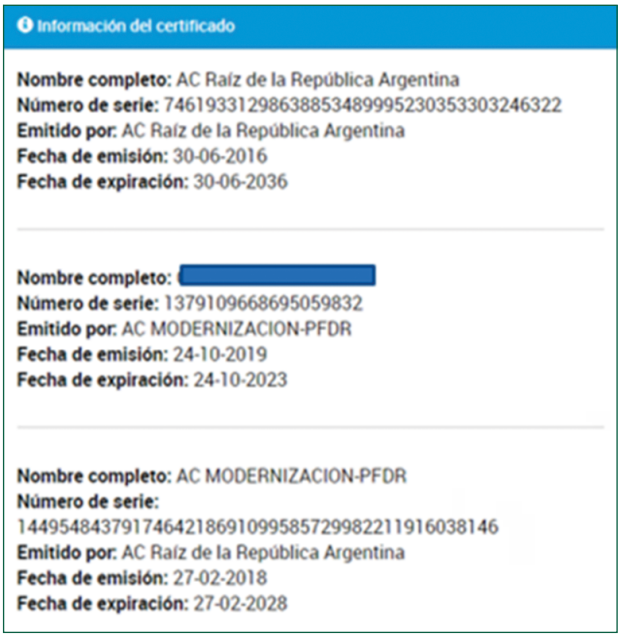
¿Quién regula?

Ley 25506
Firma Digital

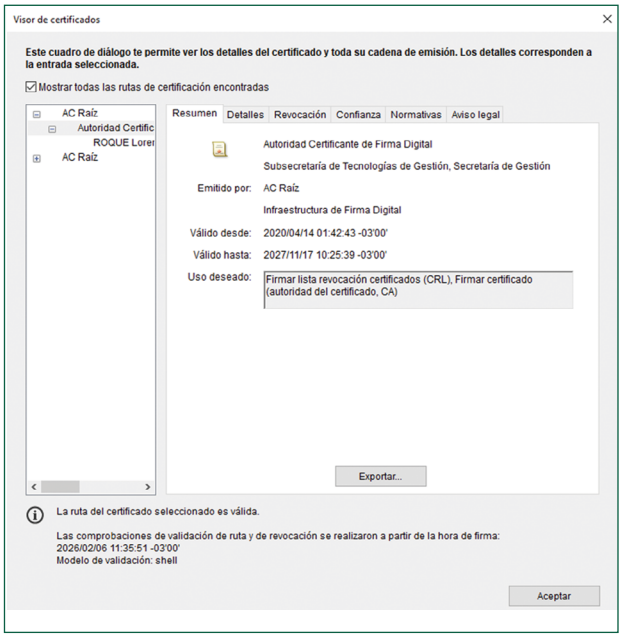
La autoridad de aplicación se establece en la Ley 25506 de Firma Digital. Actualmente, el rol lo desempeña la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros. Actúa como ente licenciante, que otorga, deniega o revoca las licencias de los certificadores licenciados. La autoridad certificante raíz (AC-Raíz), operada por el ente licenciante, es el primer nivel de jerarquía en la IFDRA. Emite certificados digitales a las autoridades certificantes de segundo nivel, una vez aprobados los requisitos de licenciamiento. Los certificadores licenciados son entidades públicas o privadas que se encuentran habilitadas por el ente licenciante para emitir certificados digitales a personas. Estos operan cada autoridad certificante de segundo nivel. Cada certificador licenciado delega en autoridades de registro las funciones de validación de la identidad y otros datos de los suscriptores de certificados.

5 CÓMO SE LEE UN CERTIFICADO DE FIRMAS

Desde la Plataforma de Firma Digital Remota (https://firmar.gob.ar/firmador/#/):



Desde Adobe:



Estos son los datos principales que vas a encontrar:

Titular del certificado (firmante): Nombre y apellido de la persona que firmó el documento. Es el dato central para identificar al firmante.

Entidad certificante (autoridad certificante): Indica quién emitió el certificado (por ejemplo, AC-ONTI/AC-Raíz). Garantiza que la identidad fue verificada por un organismo oficial.

Período de validez: Fecha de inicio y fecha de vencimiento. La firma es válida si fue utilizada dentro de este período.

Estado del certificado: Indica si el certificado está válido, revocado o expirado.

Algoritmo y clave criptográfica: Información técnica que asegura la integridad y seguridad de la firma.