MÓDULO 3

Marco normativo

Curso: Autoridades de Registro de Firma Digital Remota (AC MODERNIZACION PFDR)

Módulo 3: Marco Normativo

Introducción

Desde el año 2001, la Argentina reconoce la eficacia jurídica del empleo de la firma electrónica y de la firma digital en las condiciones que establece la Ley N° 25.506.

La Ley N° 25.506 de Firma Digital estableció una Infraestructura de Firma Digital de alcance nacional, aplicable tanto al Sector Público como al Sector Privado. Posteriormente, la Ley N° 27.446 amplió el alcance de la ley de firma digital y actualiza su contenido.

La SECRETARÍA DE INNOVACIÓN PÚBLICA es la Autoridad de Aplicación de la Ley N° 25.506. Como responsable de la Infraestructura de Firma Digital, administra la Autoridad Certificante Raíz de la República Argentina, licencia a los certificadores que emiten certificados de clave pública, y controla todo el sistema de firma digital.

A su vez, la SUBSECRETARÍA DE INNOVACION ADMINISTRATIVA dispone de dos certificadores o autoridades certificantes:

- La Autoridad Certificante de la Oficina Nacional de Tecnologías de Información (AC-ONTI) la cual emite certificados que se almacenan en tokens criptográficos.
- La Autoridad Certificante del Ministerio de Modernización para la Plataforma de Firma Digital Remota (AC MODERNIZACION-PFDR) la cual emite certificados que no requieren el uso de tokens criptográficos ya que estos se almacenan en la plataforma.

A los efectos legales, la Ley N° 25.506 y su Decreto Reglamentario establecen un sistema de licenciamiento. El organismo o empresa que desee emitir certificados digitales aptos para firmar digitalmente, deben solicitar su licenciamiento a la Secretaría de Innovación Pública. A tal fin, deberá cumplir con un procedimiento legal y técnico obligatorio, establecido en la Resolución N° 399/2016 del Ministerio de Modernización. El licenciamiento produce importantes consecuencias legales, puesto que solamente los certificados emitidos por un certificador licenciado serán válidos para producir los efectos que la ley otorga a la firma digital.

El sistema de confianza de la Infraestructura de Firma Digital reposa en la identificación fehaciente de las personas que solicitan un certificado. Esta identificación requiere constatar que la persona es quien dice ser, y para ello, es necesario que al solicitar su certificado se presente físicamente ante el Certificador Licenciado y éste constate su documento de identidad y capture datos biométricos y la fotografía de la persona, como requisitos ineludibles para emitir un certificado digital. Esta tarea crucial en el sistema de

firma digital la desarrollan las Autoridades de Registro, responsables del proceso de identificación de los solicitantes y tramitación de sus certificados.

Las Autoridades de Registro dependen de un Certificador Licenciado, y deben ser autorizadas para funcionar por la SubSecretaría de Innovación Administrativa, pueden operar en puestos fijos o móviles y son las encargadas de establecer la vinculación entre la clave pública y los datos de identificación del suscriptor del certificado y delegando en ellas otras funciones.

Ley N° 25.506 de Firma Digital: características de la normativa

La Ley N° 25.506 de Firma Digital (Boletín Oficial del 14/12/2001) establece la Infraestructura de Firma Digital de la República Argentina. Es una ley de alcance nacional la cual complementa al Código Civil y Comercial de la Nación, es aplicable tanto al sector público como al sector privado, y otorga validez a todas las transacciones en formato electrónico como ser comercio electrónico, gobierno digital, contratos electrónicos entre otras.

La ley de firma digital reconoce la validez jurídica del documento electrónico, la firma electrónica y la firma digital, además establecía a la Jefatura de Gabinete de Ministros como Autoridad de Aplicación del Régimen Normativo de Firma Digital, actualmente dicha autoridad de aplicación es la Secretaría de Innovación Pública.

Entre las principales características que posee esta normativa podemos mencionar:

Certificadores extranjeros: establece la posibilidad del reconocimiento de certificadores extranjeros, actualmente sólo existe un convenio de reconocimiento mutuo con la República de Chile.
Para mayor información sobre los certificadores habilitados consultar el siguiente enlace:

https://www.argentina.gob.ar/firmadigital/acraiz/certificadoreslicenciados

Neutralidad tecnológica: la ley es tecnológicamente neutra, ya que siguiendo tendencias de otras normativas internacionales sobre tecnología, no define una firma digital adoptando alguna tecnología en especial sino que, en lugar de ello, define conceptos generales y establece que cualquier tecnología que asegure las mismas funcionalidades que garantiza una firma hológrafa y que sea homologada por la Autoridad de Aplicación de la ley será válida como sustituto. De esta manera se evita que la normativa quede obsoleta con el paso del tiempo a medida que avanza la tecnología.

Despapelización: la ley establecía un plazo de cinco años para la despapelización de toda la Administración Pública Nacional.

Protección de datos: Por último la ley establece varios puntos sobre la protección de datos de los usuarios de certificados, tanto por parte de las Autoridades Certificantes como también de sus Autoridades de Registro en lo que relativo a la confidencialidad de toda la información de los mismos. Las Autoridades Certificantes y sus Autoridades de Registro no podrán requerir datos indiscriminadamente al usuario con el pretexto de emitir su certificado, tampoco podrán hacer uso de esa información con otros fines, como por ejemplo comerciales, o ceder los datos para que un tercero la explote comercialmente. La ley prevé la aplicación de multas e incluso la baja de la licencia de todo aquel certificador licenciado que no cumpla con este requisito. Esto punto es importante a tener en cuenta ya que las Autoridades de Registro gestionaran la información de todos sus usuarios.

Sistema de licenciamiento y sus características

La ley 25.506 establece dos tipos de Autoridades Certificantes o Certificadores: los **Certificadores Licenciados** y los **Certificadores No Licenciados**.

En cuanto a la características del sistema de licenciamiento, este régimen es opcional, esto quiere decir que un certificador puede optar por estar licenciado o no pero, en caso que decida licenciarse deberá cumplir con un procedimiento legal y técnico obligatorio el cual incluye una serie de auditorías, y sólo una vez cumplido la totalidad de dicho proceso, el Ente Licenciante de la República Argentina le otorgará la licencia al certificador la cual lo acreditará en su carácter de Certificador Licenciado.

Es importante remarcar que ser Certificador Licenciado produce importantes consecuencias legales, ya que los certificados emitidos por un certificador licenciado son los únicos que serán válidos para producir los efectos que la ley otorga a la firma digital, mientras que los de un certificador no licenciado no gozarán de tales efectos (en breve veremos la diferencia entre ambos efectos).

El listado actualizado de todos los Certificadores Licenciados se encuentra publicado en:

https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/acraiz

Normativa Complementaria

Como normativa complementaria podemos citar principalmente:

- **Decreto Nº 182/2019** del 11 de Marzo de 2019 (reemplaza al Decreto N°2628/02) y sus modificatorios reglamentan la Ley N° 25.506, es decir, regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, establece las funciones de la Autoridad de Aplicación, del Ente Licenciante encargado de otorgar licencias a los certificadores que se licencien, de los Certificadores Licenciados y de sus Autoridades de Registro. A su vez compila todas las modificaciones que estaban insertas en otros decretos y que se fueron introduciendo desde el año 2002 debido al avance de la tecnología y cambios institucionales.

- **Ley N° 27.446** del 18 de Junio de 2018 extiende el alcance de la ley 25.506 eliminando las restricciones que originalmente contemplaba la ley ampliando el uso de la firma digital a cualquier tipo de documento legal, además establece como Autoridad de Aplicación de la ley al ex Ministerio de Modernización (actualmente Secretaría de Innovación Pública).

- **Resolución N° 116-E/2017** de la ex Secretaría de Modernización Administrativa la cual incorpora el requisito de captura, identificación y archivo de datos biométricos, por medio de huella dactilar y fotografía digital de rostro al proceso de certificación de todos los Certificadores Licenciados.

- **Resolución Nº 399-E/2016** del ex MINISTERIO DE MODERNIZACIÓN (RESOL-2016-399-E-APN-MM) estableció los procedimientos y pautas técnicas complementarias del marco normativo de firma digital. Es decir, los procedimientos y políticas que los Certificadores Licenciados deben cumplir, como así también los requisitos para el proceso de licenciamiento. En su artículo 34 dispone que los certificadores licenciados deberán adecuar los procesos utilizados por sus autoridades de registro, a los cambios tecnológicos que imponga la Autoridad de Aplicación.

- **Decreto N° 561** del 6 de Abril de 2016 establece el sistema de Gestión Documental Electrónica (GDE) y realiza modificaciones al Decreto N° 2628 reglamentario de la ley. Este sistema implementa el expediente electrónico el cual utiliza firma digital con token, firma digital remota y firma con certificado de servidor.

Toda la normativa antes mencionada puede ser consultada y descargada a través del siguiente enlace:

https://www.argentina.gob.ar/modernizacion/firmadigital/normativa-de-firma-digital-remota

Firma Digital: definición legal y requisitos

La ley de firma digital, en su artículo 2°, define a la **firma digital** como “el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.”

Observemos que la ley, en forma similar a como se definió en el primer módulo, define la firma digital a partir de su equivalente funcional con la firma hológrafa; por lo tanto vamos a ver que la mayoría de los requisitos legales que debe cumplir una firma digital son idénticos a las propiedades enumeradas en el módulo uno, estos requisitos son:

- **Autenticidad:** poder identificar al autor del documento.
- **Integridad:** estar vinculada a los datos del documento digital poniendo en evidencia su alteración.
- **Exclusividad:** estar bajo el absoluto y exclusivo control del firmante.
- **No repudio:** ser susceptible de verificación por parte de terceros.
- **Validez:** de acuerdo con el artículo 9, una firma digital es válida si:

    1. ha sido creada durante el período de vigencia del certificado digital válido del firmante
    2. ha sido debidamente verificada
    3. ha sido producida con un certificado digital emitido por un Certificador Licenciado, o que haya sido reconocido en los términos del artículo 16 de la ley (certificadores extranjeros).

Cabe observar que la definición legal de firma digital hecha por la ley exige que la misma cumpla, no solamente los primero cuatro requisitos que técnicamente la equiparan con una firma hológrafa, sino que además también se debe cumplir el requisito de validez, es importante observar el último ítem de este requisito ya que lo que nos está diciendo es que:

Una firma digital es aquella que se verifica su validez mediante el uso de un certificado de clave pública emitido por un Certificador Licenciado.

Recordemos que, tal como vimos en el módulo 2, para que la computadora del receptor pueda verificar la firma del emisor, era necesario que la computadora utilizara el certificado de clave pública del emisor el cual estaba emitido por una Autoridad Certificante. Ahora bien el último ítem del requisito de validez me está diciendo que, si el certificado del emisor no fue emitido por una Autoridad Certificante Licenciada, entonces esa firma digital no posee el mismo valor legal que una firma hológrafa.

Esto a su vez nos revela la gran diferencia existente entre el término legal y el técnico, ya que muchas veces se puede ver en Internet por ejemplo, que se emplea el término firma digital para referirse exclusivamente a un esquema criptográfico asimétrico utilizado como método de autenticación e integridad, pero si este sistema no cumple con el requisito de validez, entonces esa firma digital (técnicamente hablando), no tiene la misma validez legal y probatoria que una firma hológrafa (de puño y letra) tal como recién observamos en el párrafo anterior.

En cambio otras veces se puede estar hablando de firma digital en términos legales, en este caso una firma digital cumple más requisitos que los exclusivamente técnicos, no sólo tiene mayor valor probatorio que la anterior al ser válida legalmente y estar equiparada con la firma hológrafa, sino que además se encuentra soportada por toda una infraestructura de firma digital.

Firma Digital: concepto, efectos y validez probatoria

Los efectos que la ley otorga a la firma digital se refieren a la presunción de autoría e integridad del documento digital.

La presunción de autoría es la que establece, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. Asimismo, si el procedimiento de verificación de la firma digital de un documento es correcto se presume, salvo prueba en contrario, que dicho documento digital no ha sido modificado desde el momento de su firma.

El esquema legal de la firma digital es el mismo que opera sobre la firma hológrafa.

Esto significa que cada vez que se recibe un documento firmado digitalmente, si el proceso de verificación de firma es correcto, entonces se presume que esa firma es válida y posee el mismo valor legal que una firma hológrafa. Asimismo la ley también establece un principio de equivalencia funcional entre la firma digital y la firma hológrafa, ya que cada vez que en un documento se requiera el uso de una firma hológrafa ese requisito quedará satisfecho con un documento digital firmado digitalmente.

Así por ejemplo, si entre dos partes se celebra un contrato donde ambas partes lo firman digitalmente, para la ley es equivalente a que el contrato se hubiese firmado hológrafamente y, si alguna de las partes alega la invalidez de alguna de las firmas digitales involucradas, le corresponderá a esa parte demostrar ante la ley por qué esa firma cuestionada es inválida. En caso de no poder demostrarlo, para la ley la firma cuestionada continuará siendo válida.

La firma digital y la firma hológrafa son equivalentes.

Por lo antes expuesto tenemos que una firma digital desde el punto de vista técnico de seguridad me garantiza las mismas características que una firma hológrafa, esto debido a que ambas cumplen los mismos requisitos de autoría, integridad, exclusividad y no repudio. Desde el punto de vista legal dijimos que la ley le otorga la misma carga probatoria a la firma digital y a la firma hológrafa, mientras que desde el punto de vista funcional también ya que la ley dice que cualquier documento que requiera una firma hológrafa se puede reemplazar con un documento digital firmado digitalmente.

Firma Electrónica: definición legal y validez probatoria

La firma electrónica está definida en el artículo 5° de la Ley N° 25.506, como “el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.”

La Ley N° 25.506 admite la validez de ambos tipos de firmas: la digital y la electrónica, pero asigna mayor valor probatorio a la firma digital, invirtiendo la carga de la prueba en el caso de la firma electrónica.

La firma electrónica tiene validez legal, pero no equivale a la firma hólografa, ya que se invierte la carga probatoria.

Esto quiere decir que si entre dos partes que celebran un contrato donde ambas partes lo firman electrónicamente, para la ley esas firmas serán válidas. Pero en caso de que alguna de las partes alegue la invalidez de alguna de las firmas electrónicas involucradas, corresponderá a la parte que reclama su validez demostrar ante la ley por qué la firma cuestionada es válida y, en caso de no poder demostrarlo, ante el mero alegato de alguna de las partes, esa firma pasará a ser inválida.

Infraestructura de Firma Digital de la República Argentina

El marco normativo de la República Argentina en materia de Firma Digital está constituido por la Ley Nº 25.506 (B.O. 14/12/2001), el Decreto Nº reglamentario y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos. De tal manera que los componentes de dicha infraestructura son:

Autoridad de Aplicación: Es la Secretaría de Innovación Pública, quien está facultada a establecer las normas y procedimientos técnicos necesarios para la efectiva implementación de la ley.

Ente Licenciante: Es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores, de revocarlas y de supervisar su actividad, esta función es realizada en conjunto por la Secretaría de Innovación Pública y la Subsecretaria de Innovación Administrativa.

Autoridad Certificante Raíz: Es la autoridad certificante administrada por el ente licenciante destinada a emitir certificados digitales a los certificadores licenciados conforme a sus políticas de certificación aprobadas.

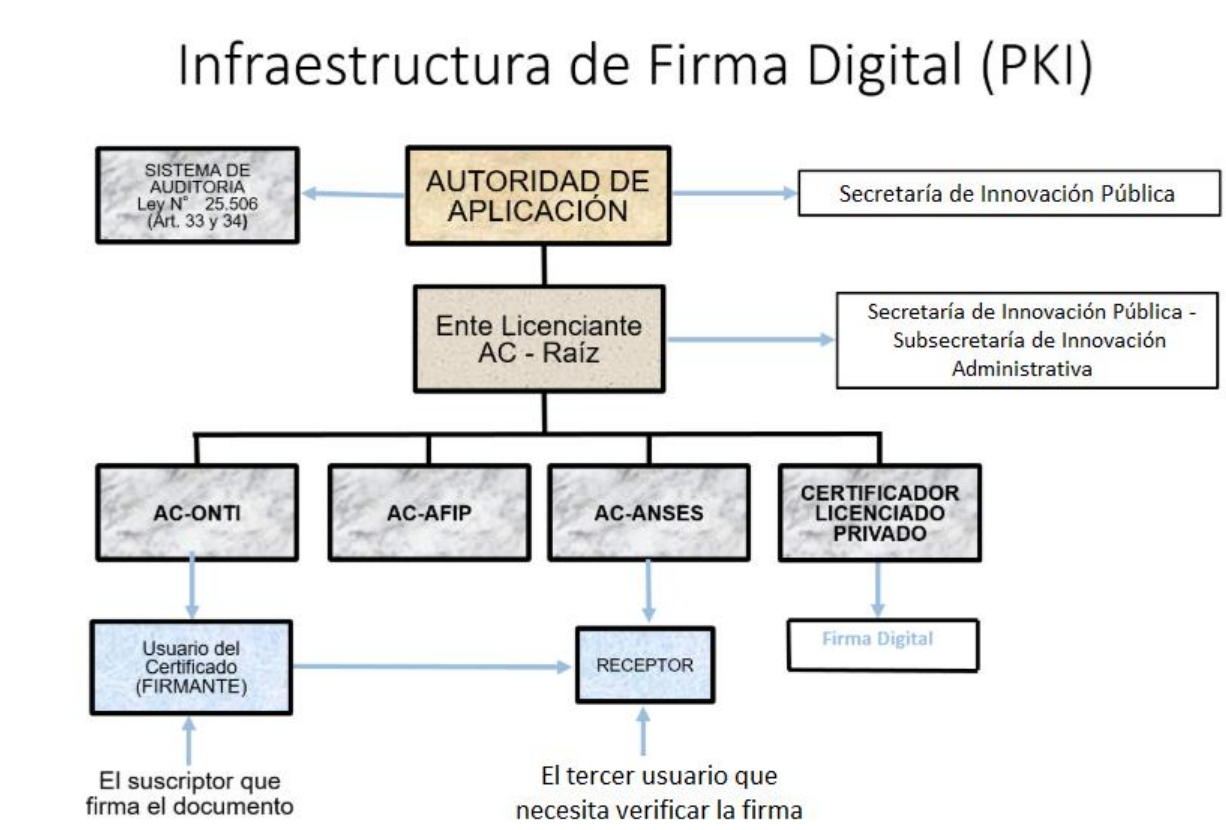
Certificadores licenciados o Autoridades Certificantes licenciadas: Son aquellas personas jurídicas, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello otorgada por el ente licenciante.

Autoridades de Registro: Son entidades que tienen a su cargo las funciones de validación de la identidad y titularidad de la clave pública, además de otros datos de los suscriptores de certificados. Toda Autoridad de Registro depende exclusivamente de una única autoridad certificante que es la que le delega sus funciones, y son autorizadas a funcionar por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

Sistema de Auditoria: Es el sistema de auditoría es realizado por la Sindicatura General de la Nación y la Auditoría General de la Nación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

Suscriptor de certificado de clave pública: es la persona o entidad incluida en el certificado, quien lo acepta y tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado.

Tercer Usuario: persona humana o jurídica que recibe un documento firmado digitalmente y que, a fin de verificar una firma digital, genera una consulta para verificar la validez del certificado digital correspondiente.



Si establecemos una comparación con la jerarquía de Autoridades Certificantes vista en el módulo anterior, el Ente Licenciante posee la Autoridad Certificante Raíz de la República Argentina que se encuentra en la cima de dicha jerarquía.

Cada vez que una autoridad certificante se licencia, luego de cumplir con los requisitos establecidos en la Resolución N° 399 E/2016, la Autoridad Certificante Raíz el emite su certificado de firma digital, o sea que los Certificadores Licenciados son aquellos que su certificado de clave pública está emitido por la raíz. Así los certificadores licenciados funcionarían como las autoridades certificantes de nivel medio, mientras que en el nivel inferior de la estructura podremos observar a los distintos usuarios de certificados que interactuarán entre sí intercambiando información firmada digitalmente.

Cabe observar que la Autoridad Certificante Raíz no puede emitir certificados a usuarios particulares, o sea no puede actuar como un certificador licenciado, sino que su única función es emitir licencias a los certificadores licenciados que así lo soliciten.

Por último cabe mencionar que de acuerdo con la Resolución N° 399 E/16 los certificados emitidos por los certificadores licenciados son interoperables, eso significa que pueden ser utilizados indistintamente para realizar trámites sin hacer distinción alguna sobre el certificador licenciado que lo emitió.

Marco Normativo de la Plataforma de Firma Digital Remota

A continuación veremos el marco normativo específico que rige para la Autoridad Certificante del MINISTERIO DE MODERNIZACIÓN y para la Plataforma de Firma Digital Remota las cuales en conjunto abreviamos como AC MODERNIZACION - PFDR.

Resolución Nº 399-E/2016 del exMINISTERIO DE MODERNIZACIÓN (RESOL-2016-399-E-APN-MM) estableció los procedimientos y pautas técnicas complementarias del marco normativo de firma digital. Es decir, los procedimientos y políticas que los Certificadores Licenciados deben cumplir, como así también los requisitos para el proceso de licenciamiento. En su artículo 34 dispone que los certificadores licenciados deberán adecuar los procesos utilizados por sus autoridades de registro, a los cambios tecnológicos que imponga la Autoridad de Aplicación.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266312/texact.htm

Decreto N° 892/2017: crea la Plataforma de Firma Digital Remota en la que se centraliza el uso de la firma digital y opera utilizando un sistema técnicamente confiable y seguro conforme los lineamientos de la Ley N° 25.506. Es administrada por la Secretaría de Innovación Pública a través de la Dirección Nacional de Sistemas de Administración y Firma Digital dependiente de la Subsecretaría de Innovación Administrativa.Cuenta con una Autoridad Certificante propia, la AC MODERNIZACION la cual es una Autoridad Certificante dedicada a emitir únicamente certificados de firma digital para ser utilizados en la mencionada plataforma.

La característica principal de esta plataforma es que no se necesita el uso de tokens para firmar digitalmente, los suscriptores disponiendo de una conexión internet a través de su celular o computadora pueden firmar digitalmente desde donde sea que estén.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266312/texact.htm

Resolución N° 213-E/2017 del ex Ministerio de Modernización actualiza los montos de auditorías, polizas de seguro de caución entre otras cosas.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/274575/norma.htm

Resolución N° 89/2018 de la ex Secretaría de Modernización Administrativa aprueba el procedimiento de solicitud por parte de los organismos o entidades que deseen constituirse como de Autoridad de Registro de la Autoridad Certificante del ex MINISTERIO DE MODERNIZACIÓN para la PLATAFORMA DE FIRMA DIGITAL REMOTA.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/314092/norma.htm

Resolución Nº 87/2018 de la ex Secretaría de Modernización Administrativa: establece en sus anexos las políticas y procedimientos que se aplicarán a la operatoria de la AC MODERNIZACION para la emisión de certificados que se utilizarán en la Plataforma de Firma Digital Remota,. En los módulos por venir veremos en detalle la Política Única de Certificación y el Manual de Procedimientos de Certificación, estos documentos son fundamentales para la operatoria de los Oficiales de Registro y en menor lugar del Responsable de Autoridad de Registro.

- Anexo 1: Política Única de Certificación v2.0 AC MODERNIZACION-PFDR
- Anexo 2: Manual de Procedimientos v2.0 AC MODERNIZACIÓN-PFDR
- Anexo 3: Acuerdo con Suscriptores v2.0 AC MODERNIZACIÓN-PFDR
- Anexo 4: Acuerdo Utilización Plataforma de Firma Digital Remota v2.0 AC MODERNIZACIÓN-PFDR
- Anexo 5: Política de Privacidad v2.0 AC MODERNIZACIÓN-PFDR
- Anexo 6: Términos y Condiciones con Terceros Usuarios v2.0 AC MODERNIZACIÓN-PFDR

Texto de la norma: http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/313978/norma.htm

Resolución N° 42/2019 de la ex Secretaría de Modernización Administrativa (RS-2019-39719259-APN-SECMA%JGM) la cual establece el procedimiento de captura, identificación y archivo de datos biométricos, por medio de huella dactilar y fotografía digital de rostro al proceso de certificación.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/322736/norma.htm

Anexo con procedimiento de captura biométrico:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/322736/res42.pdf