¿Qué es un Certificado de Firma Digital?

Se entiende por Certificado de Firma Digital, al documento firmado digitalmente por un certificador licenciado (AC-Modernización-PFDR), que vincula los datos de validación de firma a su titular (datos previamente verificados por una AR) Las solicitudes de Certificados de Firma Digital deben ser aprobadas por una AR previamente autorizada por la Autoridad Certificante y el Ente Licenciante.

¿Quién es la Autoridad de Aplicación? (AC-RAÍZ)

- La Autoridad de Aplicación del régimen normativo que establece la infraestructura de firma digital estipulada por la Ley N° 25.506 es la Secretaría de innovación pública de la Jefatura de Gabinete de Ministros.
- La Autoridad Certificante Raíz es la Autoridad Certificante que reviste la mayor jerarquía de la infraestructura de Firma Digital de la REPÚBLICA ARGENTINA. Constituye la única instalación de su tipo y emite certificados digitales a las Autoridades Certificantes de los Certificadores Licenciados, una vez aprobados los requisitos de licenciamiento.
- Emite certificados digitales a las Autoridades Certificantes de los certificadores licenciados, una vez aprobados los requisitos de licenciamiento.

¿Quién es la Autoridad Certificante? (AC Modernización-PFDR)

La Secretaría de Innovación Pública de la JGM y la Subsecretaría de Innovación Administrativa.

¿Quiénes pueden ser "Suscriptores" / Titulares de certificados?

Toda persona humana que desee tener su Firma Digital.

¿Cuál es el período de validez de un Certificado de Firma Digital?

Plataforma Firma Digital Remota (Firma Remota) tienen un período de validez de CUATRO (4) años a partir de su fecha y hora de emisión.

ONTI (Firma en Token) tienen un período de validez de DOS (2) años a partir de su fecha y hora de emisión.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

Usos y responsabilidades

¿Qué se puede firmar digitalmente?

Desde la Plataforma de Firma Digital Remota- PFDR, se pueden firmar digitalmente archivos de tipo PDF.

Con la Firma en Token se puede firmar cualquier tipo de archivo.

¿Qué no es una Firma Digital?

- Una firma digitalizada (una firma manuscrita escaneada).
- Una contraseña o password.
- Un sistema biométrico.
- Un sistema de autenticación: este requisito sólo no alcanza.
- Una firma electrónica.
- Un documento encriptado (solo se garantiza la confidencialidad).

¿Quiénes son Terceros Usuarios?

Toda persona humana recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

Los Terceros Usuarios deben:

- Conocer los alcances de la Política Única de Certificación de la Autoridad Certificante de la Secretaría de Modernización que utiliza la Plataforma de Firma Digital Remota (AC MODERNIZACIÓN-PFDR) como así también la de la ONTI.
- Verificar la validez del certificado digital.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

Cuando recibo un documento ¿Qué necesito para verificar la validez de la firma?

Es requisito indispensable descargar y configurar el Adobe Acrobat Reader DC para visualizar el documento y para poder realizar la Validación de la integridad del Documento Firmado Digitalmente. Además hay que descargar los certificados AC-RAIZ.

¿Cuáles son las OBLIGACIONES del Suscriptor?

- Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación.
- Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable según determine el certificador.
- Solicitar la REVOCACIÓN de su certificado al Certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma.
- Informar sin demora al Certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.
- Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.
- Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la Política Única de Certificación
- Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

¿Dónde son válidos los certificados de firma digital emitidos por AC-MODERNIZACIÓN PFDR y por la ONTI?

- En todo el territorio argentino.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

- En Chile según lo establecido en la Resolución N° 436/2018. Apruébase el acuerdo de reconocimiento mutuo de certificados de firma digital suscripto con fecha 2 de noviembre de 2017 entre la República Argentina y la República de Chile.
- En Uruguay.

Técnicos y legales

Firma Digital. ¿Cómo funciona?

Funciona a través de la criptografía asimétrica. El objetivo principal de la criptografía siempre fue el secreto de la información, se buscaba proteger información sensible de la vista de terceros no deseados.

Podemos decir básicamente que los sistemas criptográficos pueden dividirse en dos categorías: Los Sistemas SIMÉTRICOS que utilizan la misma clave para encriptar y desencriptar la información y los sistemas ASIMÉTRICOS O DE CLAVE PÚBLICA que para encriptar y desencriptar se utilizan dos claves distintas en lugar de una, estas claves son dos claves numéricas y reciben el nombre de clave privada y clave pública.

¿Qué significa encriptar?

Encriptar significa ocultar datos mediante una clave para que no puedan ser interpretados por terceros no deseados. La encriptación de datos es una propiedad que permite otorgarle características de confidencialidad a la información, de manera tal que ésta solamente puede ser vista por el destinatario y si durante su transmisión la información es interceptada por un tercero, este no podrá interpretar su contenido ya que el mismo no será legible. Es importante aclarar que cuando firmamos digitalmente un documento electrónico su contenido NO se encripta, sino que solo agregamos una marca, que será la firma digital del documento y que se generará por medio de criptografía.

¿Encriptar y firmar es lo mismo?

NO. El proceso de firma y encriptación son procesos completamente distintos e independientes uno del otro. Teniendo en cuenta las características de seguridad que el documento requiera, se deberá evaluar la necesidad de solo firmarlo, o firmarlo y encriptarlo.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

En virtud de esto decimos que un documento electrónico puede:

- No estar ni firmado digitalmente ni encriptado: en ese caso el documento no posee ningún tipo de protección, como por ejemplo un correo electrónico.
- Estar firmado digitalmente pero no encriptado: en ese caso goza únicamente de las características de seguridad de la firma digital: autoría, exclusividad, integridad y no repudio. La información puede ser vista por terceros en caso de ser interceptada.
- Estar encriptado, pero no firmado digitalmente: en ese caso la información solamente goza de confidencialidad, pero no de las características antes mencionadas, por lo que si el documento fuera interceptado podría ser alterado sin que sea posible detectar la modificación.
- Estar firmado digitalmente y encriptado: en ese caso la información goza de confidencialidad junto con las propiedades otorgadas por la firma digital. En este caso la información no podrá ser revelada a terceros teniendo además certeza del autor y de la integridad del contenido del documento.

En función de lo expuesto podemos observar entonces, que firmar digitalmente un documento y encriptarlo son procesos completamente distintos e independientes uno del otro. Teniendo en cuenta las características de seguridad que el documento requiera, se deberá evaluar la necesidad de firmarlo, encriptarlo o de efectuar ambos procedimientos conjuntamente.

¿Qué diferencias hay entre la Firma Electrónica y la Firma Digital?

Tanto la Firma Electrónica como la Firma Digital, tienen Validez Jurídica. La Firma Electrónica NO reemplaza a la Firma Hológrafa (manuscrita) ya que no cumple con las propiedades necesarias como si lo hace la Firma Digital, además del Valor Probatorio que tiene esta última.

La Validez Probatoria de la Firma Digital la hace notoriamente superior a la Firma Electrónica, garantizando la legalidad y transparencia de los documentos firmados digitalmente como prueba legal. El valor probatorio de la firma digital se encuentra en la Ley 25.506 garantizando lo mencionado anteriormente.

Cabe destacar que la Firma Digital es validada por una Autoridad Certificante que nos asegura la Autenticidad de la misma.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

¿El documento firmado digitalmente tiene la misma validez al ser impreso?

NO. Un documento con Firma Digital Impreso NO posee Valor Legal ni Valor Probatorio, ya que en el documento impreso NO se visualiza ninguna marca que certifique el autor de la firma y tampoco se podría verificar la Integridad del mismo (la NO alteración del documento).

Seguridad

¿Por qué es segura mi Firma Digital?

Porque se basa en la generación de dos claves (una pública y una privada), que estarán relacionadas matemáticamente entre sí, donde se utiliza una de ellas para firmar y otra para verificar la misma. Este mecanismo matemático impide que sabida una de las claves se pueda calcular la otra clave. Este procedimiento es conocido como Criptación asimétrica o de clave pública.

¿Un documento firmado digitalmente es confidencial/secreto?

NO. La confidencialidad es una característica de seguridad complementaria, la cual no es satisfecha por la firma digital. Recuerde que el objetivo de la firma digital es reemplazar a la firma de puño y letra. Un papel firmado no es secreto ni confidencial, lo mismo sucede con un documento firmado digitalmente. Pero, así como se pueden tomar recaudos para transformar un papel en confidencial, lo mismo se puede hacer con un documento digital, procediendo a encriptarlo.

¿La AR se queda con alguna copia de mis claves?

NO. La Autoridad de Registro se obliga por normativa vigente a NO realizar bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados digitales.

¿Cómo una Autoridad de Registro te garantiza la seguridad?

El OR (Oficial de Registro) valida tu identidad, la titularidad de la clave pública y cualquier otro dato antes de emitir tu certificado. Su función de validar siempre la realiza cumpliendo las normas y recaudos establecidos para la protección de datos personales y cumpliendo las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador en la parte que resulte aplicable.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

Revocación

¿Dónde se puede consultar el listado de Certificados Revocados CRL?

El listado de Certificados revocados se podrá consultar en la web firmar.gob.ar. Cada lista de certificados revocados (CRL) emitida contendrá información sobre los números de serie de todos los certificados revocados anteriores al momento de la emisión de dicha CRL. Esta información estará firmada digitalmente por el Certificador.

Todos los servicios se encuentran disponibles SIETE POR VEINTICUATRO (7x24) horas, sujetos a un razonable calendario de mantenimiento.

¿Qué motivos causarían la REVOCACIÓN?

La AC MODERNIZACIÓN-PFDR procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

- A solicitud del titular del certificado digital.
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por Resolución de la Autoridad de Aplicación.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**

- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores y en el Acuerdo de Utilización de la Plataforma de Firma Digital Remota.
- Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02, la Resolución MM Nº 399-E/2016 y demás normativa sobre firma digital, como así también de acuerdo a lo establecido en la Política Única de Certificación y el Manual de Procedimientos del Certificador.
- Por revocación de su propio certificado digital. La AC MODERNIZACIÓN-PFDR o la AC ONTI, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

¿Quiénes están autorizados a solicitar la REVOCACIÓN del Certificado de Firma Digital?

- El suscriptor del Certificado de Firma Digital.
- Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización.
- La AC MODERNIZACIÓN-PFDR o alguna de sus ARs.
- La AC ONTI o alguna de sus ARs.
- El Ente Licenciante.
- La autoridad judicial competente.
- La Autoridad de Aplicación.

Referencias: **Preguntas frecuentes PFDR | Argentina.gob.ar**