República Argentina - Poder Ejecutivo Nacional
2018 - Año del Centenario de la Reforma Universitaria

Anexo

Número: IF-2018-41580610-APN-DNTEID#MM

CIUDAD DE BUENOS AIRES
Lunes 27 de Agosto de 2018

Referencia: Política Única de Certificación v2.0 AC MODERNIZACIÓN-PFDR

INFRAESTRUCTURA DE FIRMA DIGITAL – REPÚBLICA ARGENTINA

LEY Nº 25.506

POLÍTICA ÚNICA DE CERTIFICACIÓN

AUTORIDAD CERTIFICANTE del MINISTERIO DE MODERNIZACIÓN

Plataforma de Firma Digital Remota (AC MODERNIZACIÓN-PFDR)

DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA

SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA

SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA

MINISTERIO DE MODERNIZACIÓN

Versión 2.0 – DOCUMENTO PÚBLICO

Agosto 2018

1. – INTRODUCCIÓN.

1.1. - Descripción general.

El presente documento establece las políticas que se aplican a la relación entre la Autoridad Certificante del MINISTERIO DE MODERNIZACIÓN que utiliza la Plataforma de Firma Digital Remota – AC MODERNIZACIÓN-PFDR, en el marco de la Infraestructura de Firma Digital establecida por la Ley N° 25.506 y los solicitantes, suscriptores y terceros usuarios de los certificados que ésta emita. Un certificado vincula los datos de verificación de firma digital de una persona humana a un conjunto de datos que permiten identificar a dicha persona, conocida como suscriptor del certificado.

La autoridad de aplicación de la Infraestructura de Firma Digital antes mencionada es el MINISTERIO DE MODERNIZACIÓN, siendo dicho organismo y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA quienes entienden en las funciones de Ente Licenciante.

A fin de garantizar que estas firmas digitales cumplan con las exigencias de la Ley N° 25.506 de firma digital, y en virtud de lo establecido por el Decreto N° 892 del 1° de Noviembre de 2017, la Plataforma de Firma Digital Remota es administrada exclusivamente por el MINISTERIO DE MODERNIZACIÓN, a través de la DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACIÓN Y FIRMA DIGITAL dependiente de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA en la que se centralizará el uso de firma digital.

Dicha plataforma aplica procedimientos de seguridad de gestión tecnológica y administrativa específicos, incluidos canales de comunicación electrónica seguros, para garantizar que el entorno de creación de firmas digitales sea fiable y se utilice bajo el control exclusivo del firmante.

1.2. - Nombre e Identificación del Documento.

Nombre: Política Única de Certificación de la Autoridad Certificante del MINISTERIO DE MODERNIZACIÓN que utiliza la Plataforma de Firma Digital Remota.

Versión: 2.0

Fecha de aplicación:

Sitio de publicación: http://firmar.gob.ar/cps/cps.pdf

OID:

Lugar: Ciudad Autónoma de Buenos Aires, República Argentina.

1.3. – Participantes.

Integran la infraestructura del Certificador las siguientes entidades:

1.3.1. – Certificador.

La Autoridad Certificante del MINISTERIO DE MODERNIZACIÓN que utiliza la Plataforma de Firma Digital Remota (en adelante AC MODERNIZACIÓN-PFDR) cuyas funciones son administradas por la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA de la

SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN (en adelante, DNTEID), presta los servicios de certificación, de acuerdo con los términos de la presente Política Única de Certificación.

Correo electrónico: firmadigital@modernizacion.gob.ar

1.3.2. - Autoridad de Registro.

La AC MODERNIZACIÓN-PFDR posee una estructura de Autoridades de Registro (en adelante AR), delegando en ellas las funciones de:

1. Recepción de las solicitudes de certificados.

2. Validación de la identidad y de la titularidad de la clave pública de los solicitantes o suscriptores de certificados que se presenten ante ella.

3. Verificación de cualquier otro dato de los solicitantes o suscriptores.

4. Remisión de las solicitudes aprobadas al Certificador.

5. Recepción y validación de las solicitudes de revocación de certificados y su remisión al Certificador.

6. Identificación y autenticación de los solicitantes de revocación de certificados.

7. Archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el Certificador.

8. Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

9. Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador en la parte que resulte aplicable.

10. Captura de fotografía y datos biométricos determinados por la reglamentación.

La AC MODERNIZACIÓN-PFDR conformará sus Autoridades de Registro en:

a) Entidades o jurisdicciones pertenecientes al SECTOR PÚBLICO NACIONAL, PROVINCIAL, MUNICIPAL, en cualquiera de sus tres Poderes, organismos binacionales, organismos tripartitos, el BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, y otras organizaciones públicas.

b) Personas jurídicas del SECTOR PRIVADO y ENTES PÚBLICOS NO ESTATALES.

c) Personas jurídicas del SECTOR PRIVADO que cuenten con Políticas y áreas de Compliance (Cumplimiento) para los casos de aplicaciones de firma digital de recibos de sueldo

En todos los casos, la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA se reserva el derecho de autorizar la incorporación de las nuevas Autoridades de Registro.

La AC MODERNIZACIÓN – PFDR se reserva el derecho de dar de baja aquellas Autoridades de Registro que en un plazo de SEIS (6) meses no aprueben ninguna solicitud de emisión de certificado digital.

Las entidades públicas y privadas que tengan interés en constituirse como Autoridades de Registro de la AC MODERNIZACIÓN-PFDR, deberán solicitarlo por intermedio de su máxima autoridad, a la AC

MODERNIZACIÓN-PFDR, a través de los procedimientos electrónicos que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, en el sistema de Gestión Documental Electrónica – GDE o en la Plataforma de Trámites a Distancia (TAD), según el caso, informando la modalidad (fija o móvil).

Con dicha solicitud, la AR deberá proporcionar determinada información y acompañar documentación con carácter de Declaración Jurada, en los términos de los Artículos 109 y 110 del Reglamento de Procedimientos Administrativos Decreto 1759/72 T.O. 2017 aprobado por el Decreto N° 894/2017.

La AC MODERNIZACIÓN-PFDR en un primer análisis de la información y documentación que acompaña la solicitud, podrá, a su criterio, determinar su admisibilidad, solicitar ampliación de la información o documentación o desestimar la solicitud. Una vez admitido el trámite de solicitud de conformación de AR, asignará vacantes para el curso de Oficiales de Registro y Responsables de Soporte Técnico, y evaluará el cumplimiento de los requisitos establecidos para las AR, entre los que se cuenta la capacitación de sus OFICIALES DE REGISTRO y de los RESPONSABLES DE SOPORTE TÉCNICO, la disponibilidad de los recursos tecnológicos necesarios para la captura de datos biométricos y fotografía del suscriptor, así como la presentación de un seguro de caución cuando correspondiere, entre otros. Cumplidos los requisitos mencionados, la AC MODERNIZACIÓN-PFDR elevará un informe y solicitará autorización a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

Las ARs serán autorizadas a funcionar como tales mediante acto administrativo de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

Las ARs serán notificadas de dicha Resolución en su cuenta de usuario TAD, en caso de corresponder, o en su cuenta de usuario GDE.

Las Autoridades de Registro deben abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales emitidos.

La conservación de la documentación respaldatoria de los certificados digitales emitidos por 10 (DIEZ) años a partir de la fecha de vencimiento o revocación se realizará por los medios establecidos por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

Las Autoridades de Registro pueden desempeñar sus funciones en una instalación fija o en modalidad móvil.

Las Autoridades de Registro de la AC MODERNIZACIÓN-PFDR deberán asistirse mutuamente para expedirse sobre solicitudes de certificados digitales.

Toda la información vinculada a las AR conformadas en la AC MODERNIZACIÓN-PFDR, se encuentra disponible en el sitio web del Certificador: https://firmar.gob.ar/

Toda documentación relacionada con cualquier trámite que efectúe una Autoridad de Registro ante la AC MODERNIZACIÓN-PFDR (tal como solicitudes de altas y bajas de ARs, designaciones de personal que cumple roles propios de la AR, presentación de pólizas de seguros de caución, etc.) debe ser presentada por los interesados únicamente a través de la plataforma de Trámites a Distancia (TAD), o del sistema de Gestión Documental Electrónica – GDE en caso de corresponder. A tal fin, la Autoridad de Registro debe constituir una cuenta de usuario en la Plataforma de Trámites a Distancia (TAD) como requisito previo a su autorización para operar en tal carácter, en el caso de no disponer de un usuario en el sistema de Gestión Documental Electrónica - GDE.

1.3.3. - Suscriptores de certificados.

Podrán ser suscriptores de los certificados emitidos por la AC MODERNIZACIÓN-PFDR las personas humanas que requieran un certificado digital para firmar digitalmente cualquier documento o transacción,

pudiendo ser utilizados para cualquier uso o aplicación, como así también para autenticación o cifrado.

La AC MODERNIZACIÓN-PFDR emite también un certificado para ser usado en relación con el servicio On Line Certificate Status Protocol (en adelante, OCSP) de consulta sobre el estado de un certificado.

Los suscriptores de certificados de la AC MODERNIZACIÓN-PFDR generan sus claves en la Plataforma de Firma Digital Remota (en adelante, PFDR). En el caso de los Oficiales de Registro, las claves son generadas en dispositivos que cumplan con certificación "Overall" FIPS 140 (versión 2) Nivel 2 o superior. Estos certificados deberán ser emitidos por alguna de las AUTORIDADES CERTIFICANTES pertenecientes al MINISTERIO DE MODERNIZACIÓN.

1.3.4. - Terceros Usuarios.

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación, toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente

1.4. - Uso de los certificados.

Los certificados digitales que se emitan bajo la presente Política Única de Certificación podrán ser utilizados en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado.

1.5. - Administración de la Política.

1.5.1. - Responsable del documento.

Será responsable de la presente Política Única de Certificación la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA del MINISTERIO DE MODERNIZACIÓN, con los siguientes datos:

Correo electrónico: firmardigital@modernizacion.gob.ar

1.5.2. – Contacto.

La presente Política Única de Certificación es administrada por el máximo responsable de la AC MODERNIZACIÓN-PFDR cuyos datos de contacto figuran en el apartado anterior.

1.5.3. - Procedimiento de aprobación de la Política Única de Certificación.

Esta Política Única de Certificación ha sido presentada ante la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN y ha sido aprobada por el correspondiente Acto Administrativo.

1.6. - Definiciones y Acrónimos.

1.6.1. – Definiciones.

ACUERDO CON SUSCRIPTORES: Establece los derechos y obligaciones de las partes con respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política de Única de Certificación.

ACUERDO DE UTILIZACIÓN DE LA PLATAFORMA DE FIRMA DIGITAL REMOTA: Establece los derechos y obligaciones de las partes con respecto a la utilización de los servicios de almacenamiento y custodia de las claves privadas de los suscriptores que interactúan con la AC MODERNIZACIÓN-PFDR.

AUTORIDAD DE APLICACIÓN: El MINISTERIO DE MODERNIZACIÓN es la Autoridad de

Aplicación de la Infraestructura de Firma Digital establecida por la Ley N° 25.506.

AUTORIDAD DE REGISTRO: Es la entidad que tiene a su cargo las funciones indicadas en artículo 35 del Decreto Nº 2628/02.

CERTIFICADO DIGITAL: Se entiende por certificado digital al documento digital firmado digitalmente por un Certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).

CERTIFICADOR LICENCIADO: Se entiende por Certificador Licenciado a toda persona jurídica, 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.

ENTE LICENCIANTE: El MINISTERIO DE MODERNIZACIÓN y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA constituyen el ente licenciante.

LISTA DE CERTIFICADOS REVOCADOS: Lista de certificados que han sido dejados sin efecto en forma permanente por la AC MODERNIZACIÓN-PFDR, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL) (Anexo I, Decreto N° 2628/02).

MANUAL DE PROCEDIMIENTOS: Conjunto de prácticas utilizadas por la AC MODERNIZACIÓN-PFDR en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS) (Anexo I, Decreto N° 2628/02).

PLAN DE CESE DE ACTIVIDADES: Conjunto de actividades a desarrollar por la AC MODERNIZACIÓN-PFDR en caso de finalizar la prestación de sus servicios (Anexo I, Decreto N° 2628/02).

PLAN DE CONTINGENCIA: Conjunto de procedimientos a seguir por la AC MODERNIZACIÓN-PFDR ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones (Anexo I, Decreto N° 2628/02)

PLAN DE SEGURIDAD: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos de la AC MODERNIZACIÓN-PFDR (Anexo I, Decreto N° 2628/02).

POLÍTICA DE PRIVACIDAD: Conjunto de declaraciones que la AC MODERNIZACIÓN-PFDR se compromete a cumplir de manera tal de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

SERVICIO OCSP (PROTOCOLO EN LÍNEA DEL ESTADO DE UN CERTIFICADO – "ONLINE CERTIFICATE STATUS PROTOCOL"): Servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el Certificador que brinda el servicio.

SUSCRIPTOR O TITULAR DE CERTIFICADO DIGITAL: Persona humana a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.

TERCERO USUARIO: Persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

1.6.2. – Acrónimos.

ACR-RA – Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.

AC MODERNIZACIÓN-PFDR - Autoridad Certificante del MINISTERIO DE MODERNIZACIÓN que utiliza la Plataforma de Firma Digital Remota.

AR – Autoridad de Registro.

CDI – Clave de Identificación.

CRL - Lista de Certificados Revocados (“Certificate Revocation List”).

CUIL – Clave Única de Identificación Laboral.

CUIT - Clave Única de Identificación Tributaria.

DNTEID - Dirección Nacional de Tramitación e Identificación a Distancia

DNSAyFD – Dirección Nacional de Sistemas de Administración y Firma Digital

FIPS - Estándares Federales de Procesamiento de la Información (“Federal Information Processing Standard”).

HSM – Módulo de Seguridad de Hardware (“Hardware Security Module”).

IEC - International Electrotechnical Commission.

IETF - Internet Engineering Task Force.

MM - MINISTERIO DE MODERNIZACIÓN.

NIST - Instituto Nacional de Normas y Tecnología (“National Institute of Standards and Technology”).

OCSP - Protocolo en línea del estado de un certificado (“On line Certificate Status Protocol”).

OID - Identificador de Objeto (“Object Identifier”).

OR - Oficial de Registro.

OTP – Segundo factor de autenticación (One Time Password)

PFDR – Plataforma de Firma Digital Remota.

PIN – Contraseña que protege la clave privada del suscriptor, deberá contener como mínimo un largo de 8 caracteres requiriendo utilizar mayúsculas, minúsculas y números.

PKCS #10 - Estándar de solicitud de certificación (“Public-Key Cryptography Standards”).

RFC – “Request for Comments”.

RSA - Sistema Criptográfico de Clave Pública (“Rivest, Shamir y Adleman”).

SHA-256 - Algoritmo de Hash Seguro (“Secure Hash Algorithm”).

SMA - SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN

X.509 - Estándar UIT-T para infraestructuras de claves públicas.

2.- RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS.

Conforme a lo dispuesto por la Ley N° 25.506, la relación entre el Certificador que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la citada ley y demás legislación vigente (Art. 37). Dicha relación contractual quedará encuadrada dentro del ámbito de responsabilidad civil.

Asimismo, el artículo 38 de la citada ley dispone que "El Certificador que emita un certificado digital (…) es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al Certificador demostrar que actuó con la debida diligencia".

El artículo 36 del Decreto N° 2628/02 y sus modificatorios, establece la responsabilidad del Certificador Licenciado respecto de las Autoridades de Registro.

En ese sentido prescribe que una AR puede constituirse como única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo delegar su operatoria en otras Autoridades de Registro, siempre que medie la aprobación del Certificador Licenciado.

El Certificador es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en AR, sin perjuicio del derecho del Certificador de reclamar a la AR las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

Del mismo modo, las Autoridades de Registro pertenecientes al sector privado que serán conformadas en la AC MODERNIZACIÓN-PFDR, previa autorización de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, deberán constituir una garantía mediante un seguro de caución a fin de garantizar el cumplimiento de las obligaciones establecidas en la normativa vigente, sin perjuicio de otros requisitos que puedan ser exigidos con posterioridad a la aprobación de la presente Política Única de Certificación.

Por otra parte, el artículo 39 de la Ley N° 25.506 establece que el Certificador Licenciado no es responsable en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados digitales y que no estén expresamente previstos en la Ley N° 25.506;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el Certificador pueda demostrar que ha tomado todas las medidas razonables.

Los criterios de valoración que seguirá la AR sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán los normalmente aceptados en Derecho. La Autoridad de Registro siempre exigirá la presencia física del suscriptor.

Todos los trámites realizados por las ARs son firmados digitalmente por los oficiales de registro y

operadores que los realizan, asumiendo así su plena responsabilidad en el proceso.

Los alcances de la responsabilidad de la AC MODERNIZACIÓN-PFDR se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en la Política Única de Certificación en relación a la emisión y revocación de certificados.

Asimismo, la responsabilidad de la AC MODERNIZACIÓN-PFDR se limita a los ámbitos de su incumbencia directa, en ningún momento será responsable por el mal uso que pudiera hacerse de los certificados, tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.

La AC MODERNIZACIÓN-PFDR no garantiza el acceso a la información cuando mediaran razones de fuerza mayor (catástrofes naturales, cortes masivos de luz por períodos indeterminados, destrucción debido a eventos no previstos, etc.) ni asume responsabilidad por los daños o perjuicios que se deriven en forma directa o indirecta como consecuencia de estos casos.

La AC MODERNIZACIÓN - PFDR no asume responsabilidad:

a) en los casos no establecidos expresamente en la legislación aplicable,

b) en aquellos casos de utilización no autorizada de un certificado cuya descripción se encuentra establecida en esta Política Única de Certificación,

c) en aquellos casos de eventuales inexactitudes en los datos contenidos en el certificado que resulten de información facilitada por el suscriptor del certificado y que hubieran sido objeto de verificación de acuerdo con los procedimientos establecidos en la Política Única de Certificación y en el Manual de Procedimientos

d) en los supuestos de falta de cumplimiento de los procedimientos establecidos para la emisión y revocación de certificados por parte de las Autoridades de Registro y/o sus Oficiales de Registro.

2.1. – Repositorios.

El servicio de repositorio de información, la publicación de la Lista de Certificados Revocados y su servicio de OCSP son administrados en forma directa por la AC MODERNIZACIÓN - PFDR.

2.2. - Publicación de información de la AC MODERNIZACIÓN - PFDR.

La AC MODERNIZACIÓN - PFDR garantiza el acceso a la información actualizada y vigente publicada en su repositorio, en cumplimiento con lo dispuesto en el artículo 20 de la Resolución MM Nº 399-E/2016.

Adicionalmente a lo indicado, la AC MODERNIZACIÓN - PFDR mantiene en el mismo repositorio en línea de acceso público:

a) Su certificado OCSP.

b) Las versiones anteriores del Manual de Procedimientos.

c) Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.

d) Las versiones anteriores de certificados de la ACR-RA.

El servicio de repositorio se encuentra disponible para uso público durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento, en el sitio web de la AC MODERNIZACIÓN - PFDR https://firmar.gob.ar/

La AC MODERNIZACIÓN - PFDR se encuentra obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en el artículo 21, inc. k) de la Ley N° 25.506, el artículo 34 inc. g), h) y m) del Decreto N° 2628/02 y sus modificatorios, y en la presente Política Única de Certificación.

2.3. - Frecuencia de publicación.

El procedimiento de emisión y publicación de la CRL y de las delta CRL se ejecuta en forma automática por la aplicación de la AC MODERNIZACIÓN-PFDR. Se emitirá cada VEINTICUATRO (24) horas la CRL completa y se emitirán delta CRL con frecuencia horaria.

Se garantiza la actualización inmediata del repositorio cada vez que cualquiera de los documentos publicados sea modificado.

2.4. - Controles de acceso a la información.

Se garantizan los controles de los accesos al certificado de la AC MODERNIZACIÓN - PFDR, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política Única de Certificación y a su Manual de Procedimientos (excepto en sus aspectos confidenciales).

Solo se revelará información confidencial o privada, si es requerida judicialmente o en el marco de los procedimientos administrativos que resulten aplicables.

En virtud de lo dispuesto por la Ley de Protección de Datos Personales N° 25.326 y por el inciso h) del artículo 21 de la Ley N° 25.506, el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a las tramitaciones realizadas.

3. - IDENTIFICACIÓN Y AUTENTICACIÓN.

En esta sección se describen los procedimientos empleados para autenticar la identidad de los solicitantes de certificados digitales utilizados por la AC MODERNIZACIÓN-PFDR o sus AR como prerrequisito para su emisión. También se describen los pasos para la autenticación de los solicitantes de revocación de certificados.

3.1.- Asignación de nombres de suscriptores.

3.1.1. - Tipos de Nombres.

El nombre a utilizar es el que surge de la documentación presentada por el solicitante, de acuerdo al apartado que sigue.

3.1.2. - Necesidad de Nombres Distintivos.

Para los certificados de Personas Humanas:

- “commonName” (OID 2.5.4.3: Nombre común): se corresponde con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.

- “serialNumber” (OID 2.5.4.5: Nro. de serie): contiene el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: “[tipo de documento]” “[nro. de documento]”

Los valores posibles para el campo [tipo de documento] son:

- En caso de ciudadanos argentinos o residentes: “CUIT/CUIL”: Clave Única de Identificación Tributaria o Laboral.

- En caso de extranjeros:

- “PA” [país]: Número de Pasaporte y código de país emisor. El atributo [país] está codificado según el estándar [ISO3166] de DOS (2) caracteres.

- “EX” [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] está codificado según el estándar [ISO3166] de DOS (2) caracteres.

- “countryName” (OID 2.5.4.6: Código de país): representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

3.1.3. - Anonimato o uso de seudónimos.

No se emitirán certificados anónimos o cuyo Nombre Distintivo contenga UN (1) seudónimo.

3.1.4. - Reglas para la interpretación de nombres.

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política Única de Certificación coinciden con los correspondientes al documento de identidad del suscriptor. Las discrepancias o conflictos que pudieran generarse cuando los datos de los solicitantes o suscriptores contengan caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

3.1.5. - Unicidad de nombres.

El nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias se basa en la utilización del número de CUIL / CUIT.

Si se suscribiera más de UN (1) certificado con el mismo CUIL / CUIT, los certificados se diferenciarían por el número de serie.

3.1.6. - Reconocimiento, autenticación y rol de las marcas registradas.

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados,

La AC MODERNIZACIÓN - PFDR se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite el certificado debe demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2. - Registro inicial.

Se describen los procedimientos a utilizar para autenticar, como paso previo a la emisión de un certificado, la identidad y demás atributos del solicitante que se presente ante la AC MODERNIZACIÓN - PFDR o ante la Autoridad de Registro. Se establecen los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

La AC MODERNIZACIÓN - PFDR cumple con lo establecido en:

a) El artículo 21, inciso a) de la Ley de Firma Digital Nº 25.506 y el artículo 34, inciso e) del Decreto Nº 2628/02, relativos a la información a brindar a los solicitantes.

b) El artículo 14, inciso b) de la Ley de Firma Digital Nº 25.506 relativo a los contenidos mínimos de los certificados.

3.2.1 - Métodos para comprobar la posesión de la clave privada.

Las claves siempre son generadas por el solicitante utilizando la PFDR; la clave privada del solicitante se protegerá con el PIN establecido por este durante el proceso de solicitud, el cual deberá contener como mínimo un largo de OCHO (8) caracteres requiriendo utilizar mayúsculas, minúsculas y números y que se encuentra asociada a la cuenta de usuario del sistema. Adicionalmente se requerirá al solicitante un segundo factor de autenticación por medio de la introducción del código OTP correspondiente, el cual es conocido únicamente por el solicitante y que se encuentra asociado a la cuenta de usuario que fue previamente autenticada por el Oficial de Registro.

La AC MODERNIZACIÓN-PFDR por su parte utilizará técnicas de "prueba de posesión" para determinar que el solicitante se encuentra en posesión de la clave privada asociada a dicha clave pública.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión"; la PFDR remitirá los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

El procedimiento descripto asegura que:

a) La clave pública no pueda ser cambiada durante la transferencia.

b) Los datos recibidos por la AC MODERNIZACIÓN - PFDR se encuentran vinculados a dicha clave pública.

c) El remitente posee la clave privada que corresponde a la clave pública transferida.

De esta manera se garantiza, por los métodos de autenticación antes mencionados, que el solicitante es el titular de la clave privada asociada a la clave pública generada a través de la PFDR. El PIN establecido por el solicitante no es persistente en la aplicación de la PFDR lo cual garantiza que en ningún caso la AC MODERNIZACIÓN-PFDR ni sus Autoridades de Registro, podrán tomar conocimiento o acceder bajo ninguna circunstancia a los datos de creación de firma digital de los titulares de los certificados, conforme el artículo 21, inciso b) de la Ley N° 25.506.

3.2.2 - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

No aplicable

3.2.3. - Autenticación de la identidad de Personas Humanas.

Se describen los procedimientos de autenticación de la identidad de los suscriptores de los certificados de Personas Humanas.

Se exige la presencia física del solicitante o suscriptor del certificado ante la AC MODERNIZACIÓN-PFDR o la AR. La verificación se efectúa mediante la presentación de los siguientes documentos:

- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.

- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

Se consideran obligatorias las exigencias reglamentarias impuestas por:

a) El artículo 21 de la Ley Nº 25.506 incisos f), i) relativo a la recolección de datos personales y a la

conservación de la documentación de respaldo de los certificados emitidos, respectivamente.

b) El artículo 34 del Decreto Nº 2628/02 incisos i), m) relativo a abstenerse de generar, exigir, tomar conocimiento o acceder a la clave privada del suscriptor y a la protección de datos personales, respectivamente.

Adicionalmente, el Certificador celebra un acuerdo con el solicitante o suscriptor, conforme el Anexo IV de la Resolución MM N° 399-E/2016, del que surge su conformidad respecto de la veracidad de la información incluida en el certificado.

3.2.4. - Información no verificada del suscriptor.

Se conserva la información referida al solicitante que no hubiera sido verificada. Adicionalmente, se cumple con lo establecido en el apartado 3 del inciso b) del artículo 14 de la Ley N° 25.506.

3.2.5. - Validación de autoridad.

No aplicable

3.2.6. - Criterios para la interoperabilidad.

Los certificados emitidos pueden ser utilizados por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, así como para autenticación o cifrado.

3.3. - Identificación y autenticación para la generación de nuevo par de claves (Rutina de Re Key).

3.3.1. - Renovación con generación de nuevo par de claves (Rutina de Re Key).

No aplicable.

3.3.2. - Generación de un certificado con el mismo par de claves.

No aplicable.

3.4. - Requerimiento de revocación.

El requerimiento de revocación deberá ser efectuado por el suscriptor, utilizando cualquiera de los siguientes métodos:

a) A través de la aplicación de la AC MODERNIZACIÓN-PFDR (https://firmar.gob.ar/RA) que se encuentra disponible VEINTICUATRO (24) horas, utilizando su contraseña de usuario y el código de revocación que le fuera informado al momento de la emisión de su certificado.

b) Presentándose ante la AR correspondiente con documento que permita acreditar su identidad.

Asimismo, el requerimiento de revocación podrá ser solicitado por quienes se encuentren legitimados en el punto “4.9.2. – Autorizados a solicitar la revocación” de la presente Política Única de Certificación

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1. - Solicitud de certificado.

4.1.1. - Solicitantes de certificados.

Los solicitantes de certificados cumplen con lo establecido en el apartado 1.3.3 - suscriptores de certificados.

4.1.2. - Solicitud de certificado.

Las solicitudes sólo podrán ser iniciadas por el solicitante, quien deberá presentar su documento de identidad, según lo establecido en el apartado 3.2.3. Asimismo, el solicitante deberá contar con un celular inteligente (smartphone), Tablet o computadora port y poseer instalada en dicho dispositivo alguna aplicación que le permita generar códigos OTP (One Time Password).

El proceso de solicitud de certificado comprende los siguientes pasos:

a.- Registro del solicitante: validación de identidad, captura de huella dactilar y de fotografía.

b.- Confirmación de datos por el solicitante y aceptación de los términos de uso.

c.- Creación de la contraseña de usuario y Segundo factor de Autenticación (OTP)

d.- Creación de PIN de firma y Solicitud de Certificado

Los procedimientos utilizados para el registro de los solicitantes y la generación de las solicitudes de certificados se encuentran descriptos en el apartado 4.1.2. del Manual de Procedimientos asociado a esta Política Única de Certificación.

4.2. - Procesamiento de la solicitud del certificado.

El procesamiento de la solicitud finaliza con su aprobación o rechazo por parte de la AR.

Los procedimientos utilizados para la aprobación o rechazo de las solicitudes se encuentran definidos en el apartado 4.2. del Manual de Procedimientos asociado a esta Política Única de Certificación.

4.3. - Emisión del certificado.

4.3.1. - Proceso de emisión del certificado.

Cumplidos los recaudos del proceso enunciado en el apartado 4.1.2 y una vez aprobada la solicitud de certificado por la AR, la AC MODERNIZACIÓN-PFDR emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor.

El período de vigencia del certificado emitido se encuentra establecido en el apartado 7.1.

4.3.2. - Notificación de emisión.

La notificación de la emisión del certificado se efectúa a través de un correo electrónico remitido por la aplicación de la AC MODERNIZACIÓN-PFDR a la cuenta de correo declarada por el solicitante al momento de iniciar el trámite. En dicho correo se indicará la URL a la que deberá acceder para descargar el certificado emitido.

4.4. - Aceptación del certificado.

Un certificado emitido por la AC MODERNIZACIÓN-PFDR se considera aceptado por su titular una vez que éste haya sido puesto a su disposición por los medios indicados en el apartado anterior.

4.5. - Uso del par de claves y del certificado.

4.5.1. - Uso de la clave privada y del certificado por parte del suscriptor.

Según lo establecido en la Ley Nº 25.506, en su artículo 25, el suscriptor debe:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable según determine el certificador.

c) Solicitar la revocación de su certificado al Certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al Certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

De acuerdo con lo establecido en la Resolución MM N° 399-E/2016, el suscriptor debe:

a) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.

b) Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la presente Política Única de Certificación.

c) 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, del Acuerdo de Utilización de la Plataforma de Firma Digital Remota y de cualquier otro documento aplicable.

4.5.2. - Uso de la clave pública y del certificado por parte de Terceros Usuarios.

Los Terceros Usuarios deben:

a) Conocer los alcances de la presente Política Única de Certificación.

b) Verificar la validez del certificado digital.

4.6. - Renovación del certificado sin generación de un nuevo par de claves.

No aplicable.

4.7. - Renovación del certificado con generación de un nuevo par de claves.

No aplicable

4.8. - Modificación del certificado.

El suscriptor se encuentra obligado a notificar a la AC MODERNIZACIÓN-PFDR cualquier cambio en alguno de los datos contenidos en el certificado digital, que hubiera sido objeto de verificación, de acuerdo a lo dispuesto en el inciso d) del artículo 25 de la Ley N° 25.506. En cualquier caso, procede la revocación de dicho certificado y de ser requerido, la solicitud de uno nuevo.

4.9. - Suspensión y Revocación de Certificados.

Los certificados serán revocados de manera oportuna y sobre la base de una solicitud de revocación de certificado válida.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.9.1. - Causas de revocación.

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

a) A solicitud del titular del certificado digital.

b) Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.

c) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por Resolución Judicial.

e) Por Resolución de la Autoridad de Aplicación.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

i) Si se determina que la información contenida en el certificado ha dejado de ser válida.

j) Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.

k) 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.

l) 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.

ll) Por revocación de su propio certificado digital.

La AC MODERNIZACIÓN-PFDR, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

4.9.2. - Autorizados a solicitar la revocación.

Se encuentran autorizados a solicitar la revocación de un certificado emitido por la AC MODERNIZACIÓN-PFDR:

a) El suscriptor del certificado.

b) Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización.

c) La AC MODERNIZACIÓN-PFDR o alguna de sus ARs

d) El ente licenciante.

e) La autoridad judicial competente.

f) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación.

La AC MODERNIZACIÓN-PFDR garantiza que:

a) Se identifica debidamente al solicitante de la revocación según se establece en el apartado 3.4.

b) Las solicitudes de revocación, así como toda acción efectuada por la AC MODERNIZACIÓN-PFDR o la Autoridad de Registro en el proceso, están documentadas y conservadas en sus archivos.

c) Se documentan y archivan las justificaciones de las revocaciones.

d) Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se incluye en la próxima lista de certificados revocados a ser emitida.

e) El suscriptor del certificado revocado es informado del cambio de estado de su certificado.

Un suscriptor podrá revocar su certificado digital utilizando los procedimientos establecidos en el apartado 3.4. - Requerimiento de revocación de la presente Política Única de Certificación.

Los suscriptores serán notificados del cumplimiento del proceso de revocación, en sus respectivas direcciones de correo electrónico o en la aplicación de la AC MODERNIZACIÓN-PFDR.

4.9.4. - Plazo para la solicitud de revocación.

El titular de un certificado debe requerir su revocación en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1.

El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas cumpliendo con lo establecido en el artículo 34, inciso f) del Decreto Nº 2628/02 a través de la aplicación web de la AC MODERNIZACIÓN-PFDR.

4.9.5. - Plazo para el procesamiento de la solicitud de revocación.

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado indicando que la revocación ha sido puesta a disposición de los Terceros Usuarios, no superará en ningún caso las VEINTICUATRO (24) horas.

4.9.6. - Requisitos para la verificación de la lista de certificados revocados.

Los Terceros Usuarios están obligados a verificar el estado de validez de los certificados mediante el control de la lista de certificados revocados o en su defecto, mediante el servicio de consultas en línea sobre el estado de los certificados (OCSP), que la AC MODERNIZACIÓN-PFDR pondrá a su disposición.

Los Terceros Usuarios están obligados a confirmar la autenticidad y validez de las listas de certificados revocados mediante la verificación de la firma digital de la AC MODERNIZACIÓN-PFDR y de su período de validez.

La AC MODERNIZACIÓN-PFDR cumple con lo establecido en el artículo 34, inciso g) del Decreto Nº 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la Resolución MM N° 399-E/2016 y sus correspondientes Anexos.

4.9.7. - Frecuencia de emisión de listas de certificados revocados.

La AC MODERNIZACIÓN-PFDR genera y publica una Lista de Certificados Revocados (CRL) asociada a esta Política Única de Certificación con una frecuencia diaria. Asimismo, la AC MODERNIZACIÓN-PFDR genera y publica listas de certificados revocados complementarias (delta CRL) en modo horario.

4.9.8.- Vigencia de la lista de certificados revocados.

La lista de certificados revocados indicará su fecha de efectiva vigencia, así como la fecha de su próxima actualización.

4.9.9. - Disponibilidad del servicio de consulta sobre revocación y de estado del certificado.

La AC MODERNIZACIÓN-PFDR pone a disposición de los interesados la posibilidad de verificar el estado de un certificado por medio del acceso a la lista de certificados revocados y mediante el servicio de consultas en línea sobre el estado de los certificados (OCSP).

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

La CRL puede ser descargada del sitio web de la AC MODERNIZACIÓN-PFDR disponible en: http://firmar.gob.ar/crl/FD.crl

Las deltas CRL pueden ser descargadas del sitio web de la AC MODERNIZACIÓN-PFDR disponible en:

http://firmar.gob.ar/crl/FD+.crl

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital de acuerdo con las características enunciadas en el apartado 4.9.10, el mismo representa un método alternativo de consulta a la CRL.

El servicio OCSP se provee por medio del sitio web de la AC MODERNIZACIÓN-PFDR disponible en http://firmar.gob.ar/ocsp

La AC MODERNIZACIÓN-PFDR posee servicios de alta disponibilidad para la consulta del estado de verificación de los certificados.

4.9.10. - Requisitos para la verificación en línea del estado de revocación.

Para la correcta verificación en línea del estado de revocación de un certificado, el tercero usuario deberá disponer de un sistema operativo que implemente el protocolo OCSP. En su defecto, el protocolo debe ser implementado por la aplicación que pretenda validar la firma digital. Asimismo, los certificados de la ACR-RA y de la AC MODERNIZACIÓN-PFDR deberán encontrarse instalados en el almacén de certificados de confianza del sistema operativo y/o de la aplicación utilizada.

4.9.11. - Otras formas disponibles para la divulgación de la revocación.

La AC MODERNIZACIÓN-PFDR a través de su servicio de búsqueda y consulta de certificados emitidos, permite buscar un certificado y consultar su estado a ese instante; el mismo se encuentra disponible en el sitio web de la AC MODERNIZACIÓN-PFDR: https://firmar.gob.ar. Para disponer de este servicio el tercero usuario deberá poseer una computadora conectada a Internet y un navegador web a fin de poder acceder al sitio web de la AC MODERNIZACIÓN-PFDR.

4.9.12. - Requisitos específicos para casos de compromiso de claves.

En caso de compromiso de alguno de los factores de autenticación (PIN, contraseña de usuario, OTP), el titular del certificado correspondiente se encuentra obligado a comunicar inmediatamente dicha

circunstancia a la AC MODERNIZACIÓN-PFDR mediante alguno de los mecanismos previstos en el apartado 4.9.3. - Procedimientos para la solicitud de revocación.

4.9.13. - Causas de suspensión.

El estado de suspensión no se encuentra contemplado en el marco de la Ley Nº 25.506.

4.9.14. - Autorizados a solicitar la suspensión.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.9.15. - Procedimientos para la solicitud de suspensión.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.9.16. - Límites del período de suspensión de un certificado.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.10. – Estado del certificado.

4.10.1. – Características técnicas.

Los servicios disponibles para la verificación del estado de los certificados emitidos por el Certificador son:

a) Lista de certificados revocados (CRL).

b) Servicio OCSP.

c) Servicio de búsqueda y consulta de certificados emitidos.

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 la AC MODERNIZACIÓN-PFDR.

Cada lista de certificados revocados complementaria (delta CRL) contendrá los números de serie de los certificados que fueron revocados durante el período que abarca desde la emisión de la última CRL hasta el momento de emisión de dicha delta CRL; dicho período nunca superará las VEINTICUATRO (24) horas. Esta información se encontrará firmada digitalmente por el Certificador.

El servicio OCSP permitirá consultar el estado de revocación en línea de un certificado contra la información contenida en las últimas CRL y delta CRL emitidas; la información del estado de revocación de dicho certificado estará firmada digitalmente por el Certificador.

El servicio de búsqueda y consulta de certificados emitidos, permite buscar un certificado y a la vez consultar su estado a ese instante; la información sobre el estado del certificado no estará firmada digitalmente por la AC MODERNIZACIÓN-PFDR.

4.10.2. – Disponibilidad del servicio.

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

4.10.3. – Aspectos operativos.

No existen otros aspectos a mencionar.

4.11. – Desvinculación del suscriptor.

Una vez expirado el certificado o si este fuera revocado, su titular se considera desvinculado de los servicios de la AC MODERNIZACIÓN-PFDR, salvo que efectuara la tramitación de un nuevo certificado.

De igual forma se producirá la desvinculación, ante el cese de las operaciones de la AC MODERNIZACIÓN-PFDR.

4.12. – Recuperación y custodia de claves privadas.

En virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 25.506, la AC MODERNIZACIÓN-PFDR se obliga a no realizar bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados digitales. Asimismo, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley citada, el suscriptor de un certificado emitido en el marco de esta Política Única de Certificación se encuentra obligado a mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos e impedir su divulgación.

5. - CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN.

Se describen a continuación los procedimientos referidos a los controles de seguridad física, de gestión y operativos implementados por la AC MODERNIZACIÓN-PFDR. La descripción detallada de los mismos se encuentra en el Plan de Seguridad.

5.1. - Controles de seguridad física.

Se cuenta con controles de seguridad relativos a:

a) Construcción y ubicación de instalaciones.

b) Niveles de acceso físico.

c) Comunicaciones, energía y ambientación.

d) Exposición al agua.

e) Prevención y protección contra incendios.

f) Medios de almacenamiento.

g) Disposición de material de descarte.

h) Instalaciones de seguridad externas.

5.2. - Controles de Gestión.

Se cuenta con controles de seguridad relativos a:

a) Definición de roles afectados al proceso de certificación.

b) Número de personas requeridas por función.

c) Identificación y autenticación para cada rol.

d) Separación de funciones

5.3. - Controles de seguridad del personal.

Se cuenta con controles de seguridad relativos a:

a) Calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, de seguridad, limpieza, etcétera.

b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.

d) Frecuencia de procesos de actualización técnica.

e) Frecuencia de rotación de cargos.

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

h) Documentación provista al personal, incluidas tarjetas y otros elementos de identificación personal.

5.4. - Procedimientos de Auditoría de Seguridad.

Se cuenta con procedimientos de auditoría de seguridad sobre los siguientes aspectos:

a) Tipo de eventos registrados: se cumple con lo establecido en el Anexo I Sección 3 de la Resolución MM N° 399-E/2016.

b) Frecuencia de procesamiento de registros.

c) Período de guarda de los registros: se cumple con lo establecido en el inciso i) del artículo 21 de la Ley N° 25.506 respecto a los certificados emitidos.

d) Medidas de protección de los registros, incluyendo privilegios de acceso.

e) Procedimientos de resguardo de los registros.

f) Sistemas de recolección y análisis de registros (internos vs. externos).

g) Notificaciones del sistema de recolección y análisis de registros.

h) Evaluación de vulnerabilidades.

5.5. - Conservación de registros de eventos.

Se han desarrollado e implementado políticas de conservación de registros, cuyos procedimientos se encuentran desarrollados en el Manual de Procedimientos.

Los procedimientos cumplen con lo establecido por el artículo 21, inciso i) de la Ley Nº 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

Se respeta lo establecido en el Anexo I Sección 3 de la Resolución MM N° 399-E/2016 respecto del

registro de eventos.

Existen procedimientos de conservación y guarda de registros en los siguientes aspectos, que se encuentran detallados en el Manual de Procedimientos:

a) Tipo de registro archivado: se cumple con lo establecido en el Anexo I Sección 3 de la Resolución MM N° 399-E/2016.

b) Período de guarda de los registros.

c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso.

d) Procedimientos de resguardo de los registros.

e) Requerimientos para los registros de certificados de fecha y hora.

f) Sistemas de recolección y análisis de registros (internos vs. externos).

g) Procedimientos para obtener y verificar la información archivada.

5.6. - Cambio de claves criptográficas.

El par de claves de la AC MODERNIZACIÓN-PFDR ha sido generado con motivo del licenciamiento y tiene una vigencia de DIEZ (10) años. Por su parte, la licencia tiene una vigencia de CINCO (5) años.

En todos los casos el cambio de claves criptográficas de la AC MODERNIZACIÓN-PFDR implica la emisión de un nuevo certificado por parte de la AC-Raíz. Si la clave privada de la AC MODERNIZACIÓN-PFDR se encontrase comprometida, se procederá a la revocación de su certificado y esa clave ya no podrá ser usada en el proceso de emisión de certificados.

La AC MODERNIZACIÓN-PFDR tomará los recaudos necesarios para efectuar con suficiente antelación la renovación de su licencia y la obtención del certificado, si correspondiese.

5.7. - Plan de respuesta a incidentes y recuperación ante desastres

Se describen los requerimientos relativos a la recuperación de los recursos de la AC MODERNIZACIÓN-PFDR en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Continuidad de las Operaciones.

Se han desarrollado procedimientos referidos a:

a) Identificación, registro, reporte y gestión de incidentes.

b) Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.

c) Recuperación ante compromiso o sospecha de compromiso de la clave privada de la AC MODERNIZACIÓN-PFDR.

d) Continuidad de las operaciones en un entorno seguro luego de desastres.

Los procedimientos cumplen con lo establecido por el artículo 33 del Decreto Nº 2628/02 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8. - Plan de Cese de Actividades.

Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del

Certificador o de una o varias de sus Autoridades Certificantes o de Registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, suscriptores, terceros usuarios, otros Certificadores y otros usuarios vinculados.

b) Revocación del certificado de la AC MODERNIZACIÓN-PFDR y de los certificados emitidos.

c) Transferencia de la custodia de archivos y documentación e identificación de su custodio.

En relación a la custodia de archivos y documentación, se cumple con idénticas exigencias de seguridad que las previstas para el Certificador o su Autoridad Certificante o de Registro que cesó.

Se contempla lo establecido por el artículo 44 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el artículo 33 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la Resolución MM N ° 399-E/2016 y sus correspondientes Anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA.

Se describen las medidas de seguridad implementadas por la AC MODERNIZACIÓN-PFDR para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además, se incluyen los controles técnicos que se implementarán sobre las funciones operativas de la AC MODERNIZACIÓN-PFDR, AR, repositorios, suscriptores, etc.

6.1. - Generación e instalación del par de claves criptográficas.

6.1.1. - Generación del par de claves criptográficas.

El Certificador, luego del otorgamiento de su licencia, genera el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos (HSM) FIPS 140-2 Nivel 3.

En el caso de las AR, cada Oficial de Registro genera y almacena su par de claves utilizando un dispositivo criptográfico con certificación “Overall” FIPS 140 Versión 2 Nivel 2 o superior. Los correspondientes certificados serán ser emitidos por alguna de las AUTORIDADES CERTIFICANTES pertenecientes al MINISTERIO DE MODERNIZACIÓN.

Excepto en el caso de los ORs, los suscriptores utilizarán la Plataforma de Firma Digital Remota para el almacenamiento de los datos de creación de firma.

6.1.2. - Entrega de la clave privada.

En todos los casos, el certificador cumple con la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firmas de los suscriptores (incluyendo los roles vinculados a las actividades de registro), establecido por la Ley Nº 25.506, artículo 21, inciso b) y el Decreto Nº 2628/02, artículo 34, inciso i).

En el caso de los Oficiales de Registro, la clave privada es almacenada en un dispositivo criptográfico y queda protegida a través de DOS (2) factores:

a) La posesión personal e intransferible del dispositivo criptográfico por parte del suscriptor.

b) La generación de un pin o contraseña creada por el suscriptor y que sólo él conoce para acceder a la clave privada alojada en el dispositivo.

En el caso del resto de los suscriptores, la clave privada es almacenada en forma centralizada, a través de la Plataforma de Firma Digital Remota.

6.1.3. - Entrega de la clave pública al emisor del certificado.

Todo solicitante de un certificado emitido bajo la presente Política Única de Certificación entrega su clave pública a la AC MODERNIZACIÓN-PFDR, a través de la PFDR, durante el proceso de solicitud de su certificado. La AC MODERNIZACIÓN-PFDR por su parte utilizará técnicas de "prueba de posesión" para determinar que el solicitante se encuentra en posesión de la clave privada asociada a dicha clave pública.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión", remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

El procedimiento descripto asegura que:

a) La clave pública no pueda ser cambiada durante la transferencia.

b) Los datos recibidos por el Certificador se encuentran vinculados a dicha clave pública.

c) El remitente posee la clave privada que corresponde a la clave pública transferida.

6.1.4. - Disponibilidad de la clave pública del Certificador.

El certificado de la AC MODERNIZACIÓN-PFDR y el de la ACR-RA se encuentran a disposición de los suscriptores y terceros usuarios en un repositorio en línea de acceso público a través de Internet en https://firmar.gob.ar/

6.1.5. - Tamaño de claves.

El Certificador genera su par de claves criptográficas utilizando el algoritmo RSA de 4096 bits.

Los suscriptores, incluyendo las AR, generan sus claves mediante el algoritmo RSA con un tamaño de clave 2048 bits.

6.1.6. - Generación de parámetros de claves asimétricas.

No se establecen condiciones especiales para la generación de parámetros de claves asimétricas más allá de las que se indican en el punto 6.1.5.

6.1.7. - Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v.3).

Las claves criptográficas de los suscriptores de los certificados pueden ser utilizados para firmar digitalmente, para funciones de autenticación y para cifrado.

6.2. - Protección de la clave privada y controles sobre los dispositivos criptográficos.

La protección de la clave privada es considerada desde la perspectiva del Certificador, de los repositorios, de las AR y de los suscriptores, siempre que sea aplicable. Para cada una de estas entidades se abordan los siguientes temas:

a) Estándares utilizados para la generación del par de claves.

b) Número de personas involucradas en el control de la clave privada.

c) Procedimiento de almacenamiento de la clave privada en forma centralizada o en un dispositivo criptográfico, según corresponda.

d) Responsable de activación de la clave privada y acciones a realizar para su activación.

e) Duración del período de activación de la clave privada y procedimiento a utilizar para su desactivación.

f) Procedimiento de destrucción de la clave privada.

g) Requisitos aplicables al dispositivo criptográfico utilizado para el almacenamiento de las claves privadas, en el caso de los certificados de Oficiales de Registro.

6.2.1. – Controles y estándares para dispositivos criptográficos.

Para la generación y el almacenamiento de las claves criptográficas, el Certificador, los suscriptores y los Oficiales de Registro, utilizan, en cada caso, los medios y los dispositivos referidos en el apartado 6.1.1.

6.2.2. - Control “M de N” de clave privada.

Los controles empleados para la activación de las claves se basan en la presencia de M de N con M mayor a 2.

6.2.3. - Recuperación de clave privada.

Ante una situación que requiera recuperar su clave privada, y siempre que no se encuentre comprometida, el Certificador cuenta con procedimientos para su recuperación. Esta sólo puede ser realizada por personal autorizado, sobre dispositivos criptográficos seguros y con el mismo nivel de seguridad que aquel en el que se realicen las operaciones críticas de la AC MODERNIZACIÓN-PFDR.

No se implementan mecanismos de resguardo y recuperación de las claves privadas de los OR y de los suscriptores. Estos deberán proceder a la revocación del certificado y a tramitar una nueva solicitud de emisión de certificado, si así correspondiere.

6.2.4. - Copia de seguridad de clave privada.

El Certificador genera una copia de seguridad de la clave privada a través de un procedimiento que garantiza su integridad y confidencialidad.

No se mantienen copias de las claves privadas de los suscriptores de certificados ni de los Oficiales de Registro.

6.2.5. - Archivo de clave privada.

El Certificador almacena la copia de reguardo de su clave privada a través de un procedimiento que garantiza su integridad, disponibilidad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación, de acuerdo a lo dispuesto por la Resolución MM N° 399-E/2016 en cuanto a los niveles de resguardo de claves.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

El par de claves criptográficas del Certificador se genera y almacena en dispositivos criptográficos conforme a lo establecido en la presente Política Única de Certificación, salvo en el caso de las copias de

resguardo que también están soportados en dispositivos criptográficos (HSM) homologados FIPS 140-2 nivel 3.

El par de claves criptográficas de los suscriptores de certificados deberá ser generada y almacenada en forma centralizada en un dispositivo seguro, salvo el caso de los Oficiales de Registro, quienes generan y almacenan su par de claves en un dispositivo criptográfico con certificación “Overall” FIPS 140 Versión 2 nivel 2 o superior, no permitiendo su exportación.

6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos.

El almacenamiento de las claves criptográficas del Certificador se realiza en el mismo dispositivo de generación (HSM), que brinda un alto nivel de seguridad de acuerdo a la certificación FIPS 140-2 nivel 3, y en cuanto a seguridad física en un nivel 4, de acuerdo a lo establecido en el Anexo I de la Resolución MM N° 399-E/2016.

Las claves criptográficas de los suscriptores de certificados de los Oficiales de Registro deberán ser generadas y almacenadas en un dispositivo criptográfico con certificación “Overall” FIPS 140 Versión 2 Nivel 2 o superior, no permitiendo su exportación.

6.2.8. - Método de activación de claves privadas.

Para la activación de la clave privada de la AC MODERNIZACIÓN-PFDR se aplican procedimientos que requieren la participación de los poseedores de claves de activación según el control M de N descripto más arriba. Estos participantes son autenticados utilizando métodos adecuados de identificación.

6.2.9. - Método de desactivación de claves privadas.

Para la desactivación de la clave privada de la AC MODERNIZACIÓN-PFDR se aplican procedimientos que requieren la participación de los poseedores de las claves, según el control M de N. Para desarrollar esta actividad, los participantes son autenticados utilizando métodos adecuados de identificación.

6.2.10. - Método de destrucción de claves privadas.

Las claves privadas de la AC MODERNIZACIÓN-PFDR se destruyen mediante procedimientos que imposibilitan su posterior recuperación o uso, bajo las mismas medidas de seguridad física que se emplearon para su creación.

6.2.11. – Requisitos de los dispositivos criptográficos.

La AC MODERNIZACIÓN-PFDR utiliza un dispositivo criptográfico (HSM) con la certificación FIPS 140-2 Nivel 3 para la generación y almacenamiento de sus claves.

En el caso de los OR se utilizan dispositivos criptográficos con certificación “Overall” FIPS 140 Versión 2 Nivel 2 o superior.

6.3. - Otros aspectos de administración de claves.

6.3.1. - Archivo permanente de la clave pública.

Los certificados emitidos a los suscriptores, como así también el certificado de la AC MODERNIZACIÓN-PFDR, que contienen las correspondientes claves públicas, son almacenados bajo un esquema de redundancia y respaldados en forma periódica sobre dispositivos de solo lectura, lo cual, sumado a la firma de los mismos, garantiza su integridad.

Los certificados se almacenan en formato estándar bajo codificación internacional DER.

6.3.2. - Período de uso de clave pública y privada.

Las claves privadas correspondientes a los certificados emitidos por el Certificador son utilizadas por los suscriptores únicamente durante el período de validez de los certificados.

Las correspondientes claves públicas son utilizadas durante el período establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su período de validez.

6.4. - Datos de activación.

Se entiende por datos de activación, a diferencia de las claves, a los valores requeridos para la operatoria de los dispositivos criptográficos y que necesitan estar protegidos.

Se establecen medidas suficientes de seguridad para proteger los datos de activación requeridos para la operación de los dispositivos criptográficos de los usuarios de certificados.

6.4.1. - Generación e instalación de datos de activación.

Los datos de activación del dispositivo criptográfico del Certificador tienen un control “M de N” en base a “M” Poseedores de claves de activación, que deben estar presentes de un total de “N” Poseedores posibles.

Ni el Certificador, ni las AR implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores o a sus dispositivos criptográficos.

6.4.2. - Protección de los datos de activación.

El Certificador establece medidas de seguridad para proteger adecuadamente los datos de activación de su clave privada contra usos no autorizados. En este sentido, instruirá a los poseedores de las claves de activación para el uso seguro y resguardo de los dispositivos correspondientes.

6.4.3. - Otros aspectos referidos a los datos de activación.

Es responsabilidad de las AR, de los proveedores de otros servicios relacionados con la firma digital y demás suscriptores de certificados emitidos por la AC MODERNIZACIÓN-PFDR, la elección de contraseñas fuertes para la protección de sus claves privadas y para el acceso a los dispositivos criptográficos que utilicen.

6.5. - Controles de seguridad informática.

6.5.1. - Requisitos Técnicos específicos.

El Certificador establece requisitos de seguridad referidos al equipamiento y al software de certificación vinculados con los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación.

b) Separación de funciones entre los roles afectados al proceso de certificación.

c) Identificación y autenticación de los roles afectados al proceso de certificación.

d) Utilización de criptografía para las sesiones de comunicación y bases de datos.

e) Archivo de datos históricos y de auditoría del Certificador y usuarios.

f) Registro de eventos de seguridad.

g) Prueba de seguridad relativa a servicios de certificación.

h) Mecanismos confiables para identificación de roles afectados al proceso de certificación.

i) Mecanismos de recuperación para claves y sistema de certificación.

Las funcionalidades mencionadas son provistas a través de una combinación del sistema operativo, software de certificación y controles físicos.

6.5.2. - Requisitos de seguridad computacional.

El Certificador cumple con calificaciones de seguridad certificadas PP Compliant y/o EAL4+ sobre los productos en los que se basa la implementación, según corresponda.

El dispositivo criptográfico (HSM) utilizado por el Certificador está certificado por NIST (National Institute of Standards and Technology) y cumple la homologación FIPS 140-2 Nivel 3 o superior.

Los dispositivos criptográficos utilizados por los OR están certificados por NIST (National Institute of Standards and Technology) y cumplen la homologación “Overall” FIPS 140 Versión 2 Nivel 2 o superior.

6.6. - Controles Técnicos del ciclo de vida de los sistemas.

Se implementan procedimientos de control técnico para el ciclo de vida de los sistemas. Asimismo, se contemplan controles para el desarrollo, administración de cambios y gestión de la seguridad, en lo relacionado directa o indirectamente con las actividades de certificación.

6.6.1. - Controles de desarrollo de sistemas.

El Certificador cumple con procedimientos específicos para el diseño, desarrollo y prueba de los sistemas entre los que se encuentran:

a) Separación de ambientes de desarrollo, prueba y producción.

b) Control de versiones para los componentes desarrollados.

c) Pruebas con casos de uso.

6.6.2. – Controles de gestión de seguridad.

Se documenta y controla la configuración del sistema, así como toda modificación o actualización, habiéndose implementado un método de detección de modificaciones no autorizadas.

6.6.3. - Controles de seguridad del ciclo de vida del software.

No aplicable.

6.7. - Controles de seguridad de red.

Los controles de seguridad de la red interna y externa de la AC MODERNIZACIÓN-PFDR se encuentran a cargo de la DIRECCIÓN NACIONAL DE INFRAESTRUCTURA TECNOLÓGICA Y CIBERSEGURIDAD dependiente de la SECRETARÍA DE INFRAESTRUCTURA TECNOLÓGICA Y PAÍS DIGITAL del MINISTERIO DE MODERNIZACIÓN.

6.8. – Certificación de fecha y hora.

No aplicable.

7. - PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS.

7.1. - Perfil del certificado.

Todos los certificados son emitidos conforme con lo establecido en la especificación ITU X.509 versión 3, y cumplen con las indicaciones establecidas en la sección 2 “Perfil de certificados digitales” del Anexo III “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución MM N° 399–E/2016.

Perfil del certificado de PERSONA HUMANA.

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	Serial Number 2.5.4.5	(Número de serie del certificado) (entero positivo asignado unívocamente por la AC MODERNIZACIÓN-PFDR a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgoritm	sha256RSA (1.2.840.113549.1.1.11)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=AC MODERNIZACIÓN-PFDR
	organizationName - 2.5.4.10	O=MINISTERIO DE MODERNIZACIÓN
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30715117564
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	(fecha y hora de emisión UTC) yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	(fecha y hora de emisión UTC+ 4 años) yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN= [NOMBRES] [APELLIDOS]
	serialNumber - 2.5.4.5	SERIALNUMBER= CUIL (CUIL_NUMBER)
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	public key algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	(Clave pública del suscriptor)

Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectkeyIdentifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://firmar.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.11 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://firmar.gob.ar/cps/cps.pdf User notice = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = (Identificador de la clave de la AC) (Contiene un hash de 20 bytes del atributo clave pública de la AC MODERNIZACIÓN-PFDR)
Uso Extendido de Clave	ExtendedKeyUsage 2.5.29.37	No Aplica
Nombres Alternativos del Suscriptor	SubjectAltName 2.5.29.17	RFC 822 Name = (e-mail address)
Información	authorityInfoAccess	URL OCSP= http://firmar.gob.ar/ocsp

de Acceso de la AC	1.3.6.1.5.5.7.1.1	URL Certificado= http://firmar.gob.ar/aia/acmodernizacionpfdr.crt
Declaración del certificado calificado	QCStatement 1.3.6.1.5.5.7.1.3	PKIX QCSyntax-v2 Semantics Identifier (OID): 2.16.32.1.10.3

7.2. - Perfil de la LISTA DE CERTIFICADOS REVOCADOS (CRL).

Las listas de certificados revocados correspondientes a la presente Política Única de Certificación son emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 y cumplen con las indicaciones establecidas en la sección “3 - Perfil de CRLs” del Anexo III “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución MM N° 399–E/2016.

Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	1 (correspondiente a versión 2)
Algoritmo de Firma	signatureAlgorithm 1.2.840.113549.1.1.11	sha256RSA
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=AC MODERNIZACIÓN-PFDR
	organizationName - 2.5.4.10	O=MINISTERIO DE MODERNIZACIÓN
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30715117564
	countryName - 2.5.4.6	C=AR
Fecha efectiva	thisUpdate	(fecha y hora UTC) yyyy/mm/dd hh:mm:ss huso-horario
Próxima Actualización	nextUpdate	(fecha y hora UTC) yyyy/mm/dd hh:mm:ss huso-horario
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = (Identificador de la clave de la AC) (es una cadena de 20 bytes que identifica unívocamente la clave pública de la AC que firmó el certificado.)

Número de CRL	CRL Number	Número de la CRL
Puntos de Distribución del emisor	issuingDistributionPoints 2.5.29.28	[1]Punto de distribución CRL URL=http://firmar.gob.ar/crl/FD.crl Solo Contiene certificados de usuario = no Solo Contiene certificados de la entidad emisora = no Lista de revocación de Certificados Indirecta = no
Certificados Revocados (Revoked certificates)	InvalidityDate	(fecha y hora UTC)
	Serial Number	Número de Serie del Certificado Revocado
	ReasonCode	Motivo de la Revocación
Algoritmo de Identificación Huella Digital		SHA1 1.3.14.3.2.26
Versión de CA		V0.0
Siguiente Publicación de lista de revocación		(fecha y hora UTC) yyyy/mm/dd hh:mm:ss huso-horario

7.3. - Perfil de la consulta en línea del estado del certificado

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Se implementa conforme a lo indicado en la especificación RFC 5019 y cumple con las indicaciones establecidas en la sección “4 - Perfil de la consulta en línea del estado del certificado” del Anexo III “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución MM N° 399–E/2016.

8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

La DNTEID, en su calidad de administrador de la AC MODERNIZACIÓN-PFDR, se encuentra sujeta a las auditorías dispuestas en el artículo 10 del Decreto N° 561/16 de fecha 6 de abril de 2016.

Las auditorías se realizan en base a los programas de trabajo que son generados por la Autoridad de Aplicación, los que son comunicados e informados oportunamente.

Los aspectos a evaluar se encuentran establecidos en el artículo 27 de la Ley N° 25.506 y otras normas reglamentarias.

Los informes resultantes de las auditorías son elevados a la SECRETARÍA DE MODERNIZACIÓN

ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN. Sus aspectos relevantes son publicados en forma permanente e ininterrumpida en su sitio web.

El Certificador cumple las exigencias reglamentarias impuestas por:

a) El artículo 33 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma Ley, relativo a la publicación de informes de auditoría.

b) Los artículos 19 y 21 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1. – Aranceles.

El Certificador no percibe aranceles por ninguno de los servicios que pudiera brindar relacionados con la presente Política Única de Certificación. Los certificados emitidos bajo esta Política Única de Certificación son gratuitos.

9.2. - Responsabilidad Financiera.

La responsabilidad financiera surge de la Ley N° 25.506, su Decreto Reglamentario Nº 2628/02 y modificatorios, y de las disposiciones de la presente Política Única de Certificación.

Asimismo, en virtud de lo establecido en el Decreto Nº 1063/16 (modificatorio del Decreto Nº 2628/02), las Autoridades de Registro del sector privado dependientes de Certificadores Licenciados de organismos públicos, deberán constituir una garantía mediante un seguro de caución a fin de garantizar el cumplimiento de las obligaciones establecidas en la normativa vigente.

Las Autoridades de Registro y sus Oficiales de Registro son responsables de la validación de la identidad de los suscriptores. Los criterios de valoración que seguirá la AR sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán los normalmente aceptados en Derecho.

La Autoridad de Registro siempre exigirá la presencia física del suscriptor.

Todos los trámites realizados por las ARs son firmados digitalmente por los oficiales de registro y operadores que los realizan, asumiendo así su plena responsabilidad en el proceso.

9.3. – Confidencialidad.

Toda información referida a solicitantes o suscriptores de certificados que sea recibida por el Certificador o por sus Autoridades de Registro, será tratada en forma confidencial y no puede hacerse pública sin el consentimiento previo de los titulares de los datos, salvo que sea requerida judicialmente. La exigencia se extiende a toda otra información referida a los solicitantes y los suscriptores de certificados a la que tenga acceso el Certificador o sus AR durante el ciclo de vida del certificado.

Lo indicado no es aplicable cuando se trate de información que se transcriba en el certificado o sea obtenida de fuentes públicas.

9.3.1. - Información confidencial.

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no es divulgada a terceros sin su consentimiento previo y

expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso el Certificador o la Autoridad de Registro durante el ciclo de vida del certificado.

El Certificador garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifique en la presente Política Única de Certificación. Asimismo, se considera confidencial cualquier información:

a) Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por el Certificador.

b) Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.

c) Relacionada con los Planes de Continuidad de Operaciones, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.

En todos los casos resulta de aplicación la Ley N° 25.326 de protección de datos personales, su reglamentación y normas complementarias.

9.3.2. - Información no confidencial

La siguiente información recibida por el Certificador o por sus AR no es considerada confidencial:

a) Contenido de los certificados y de las listas de certificados revocados.

b) Información sobre personas humanas que se encuentre disponible en certificados o en directorios de acceso público.

c) Políticas de Certificación y Manual de Procedimientos (en sus aspectos no confidenciales).

d) Secciones públicas de la Política de Seguridad del Certificador.

e) Política de privacidad del Certificador.

9.3.3. – Responsabilidades de los roles involucrados

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente y/o de autoridad administrativa, en el marco de un proceso judicial y/o de un proceso administrativo, respectivamente.

Toda divulgación de información referida a los datos de identificación del suscriptor o a cualquier otra información generada o recibida durante el ciclo de vida del certificado sólo podrá efectuarse previa autorización escrita del suscriptor del certificado.

No será necesario el consentimiento cuando:

a) Los datos se hayan obtenido de fuentes de acceso público irrestricto;

b) Los datos se limiten a nombre, Documento Nacional de Identidad, identificación tributaria o previsional u ocupación.

c) Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular.

9.4. – Privacidad.

Todos los aspectos vinculados a la privacidad de los datos personales se encuentran sujetos a la normativa vigente en materia de Protección de los Datos Personales (Ley Nº 25.326 y normas reglamentarias, complementarias y aclaratorias). Las consideraciones particulares se incluyen en la Política de Privacidad.

9.5 - Derechos de Propiedad Intelectual.

El derecho de autor de los sistemas y aplicaciones informáticas desarrollados por el Certificador para la implementación de su AC, como así también toda la documentación relacionada, pertenece al MINISTERIO DE MODERNIZACIÓN.

El derecho de autor de la presente Política Única de Certificación y de toda otra documentación generada por el Certificador en relación con la Infraestructura de Firma Digital, pertenece al MINISTERIO DE MODERNIZACIÓN. Consecuentemente, dichos documentos no pueden ser reproducidos, copiados ni utilizados de ninguna manera, total o parcial, sin previo y formal consentimiento del MINISTERIO DE MODERNIZACIÓN, de acuerdo a la legislación vigente.

9.6. – Responsabilidades y garantías.

Las responsabilidades y garantías para el Certificador, sus AR, los suscriptores, los terceros usuarios y otras entidades participantes, se originan en lo establecido por la Ley N° 25.506, su Decreto Reglamentario Nº 2628/02, la Resolución MM Nº 399-E/2016 y en las disposiciones de la presente Política Única de Certificación.

9.7. – Deslinde de responsabilidad.

Las limitaciones de responsabilidad del Certificador se rigen por lo establecido en el artículo 39 de la Ley N° 25.506, en las disposiciones de la presente Política Única de Certificación, en el Acuerdo con Suscriptores y en el Acuerdo de Utilización de la Plataforma de Firma Digital Remota.

9.8. – Limitaciones a la responsabilidad frente a terceros.

Las limitaciones de responsabilidad del Certificador respecto a otras entidades participantes, se rigen por lo establecido en el artículo 39 de la Ley N° 25.506, en las disposiciones de la presente Política Única de Certificación y en los Términos y Condiciones con Terceros Usuarios.

9.9. – Compensaciones por daños y perjuicios.

No aplicable.

9.10. – Condiciones de vigencia.

La presente Política Única de Certificación se encontrará vigente a partir de la fecha de su aprobación por parte del ente licenciante y hasta tanto sea reemplazada por una nueva versión. Toda modificación en la Política Única de Certificación, una vez aprobada por el ente licenciante, será debidamente comunicada al suscriptor.

9.11.- Avisos personales y comunicaciones con los participantes.

No aplicable.

9.12.- Gestión del ciclo de vida del documento.

No se agrega información.

9.12.1. - Procedimientos de cambio.

Toda modificación a la Política Única de Certificación es aprobada previamente por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN conforme a lo establecido por la Ley N° 25.506, artículo 21, inciso q) y por la Resolución MM N° 399-E/2016 y sus Anexos respectivos.

La Política Única de Certificación es sometida a aprobación de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN durante el proceso de licenciamiento.

Toda modificación en la Política Única de Certificación será comunicada al suscriptor.

La presente Política Única de Certificación será revisada y actualizada periódicamente por el Certificador y sus nuevas versiones se pondrán en vigencia, previa aprobación de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN.

9.12.2 – Mecanismo y plazo de publicación y notificación.

Una copia de la versión vigente de la presente Política Única de Certificación se encuentra disponible en forma pública y accesible a través de Internet en el sitio web http://firmar.gob.ar/cps/cps.pdf

9.12.3. – Condiciones de modificación del OID.

No aplicable.

9.13. - Procedimientos de resolución de conflictos.

Cualquier controversia y/o conflicto resultante de la aplicación de esta Política Única de Certificación, deberá ser resuelto en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N° 1759/72 T.O. 2017.

La presente Política Única de Certificación se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506, el Decreto Nº 2628/02 y modificatorios, la Resolución MM Nº 399-E/2016, la Resolución SMA Nº 37-E/2016 y demás normativa complementaria dictada por la autoridad competente.

Los titulares de certificados y los terceros usuarios podrán interponer ante el ente licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por el Certificador, sólo será procedente previa acreditación de haberse efectuado reclamo ante este último con resultado negativo. Acreditada dicha circunstancia, el ente licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

A los efectos del reclamo antes citado, se procederá de la siguiente manera:

a) Una vez recibido el reclamo en las oficinas del Certificador, este citará al reclamante a una audiencia y labrará un acta que deje expresa constancia de los hechos que motivan el reclamo y de todos y cada uno de los antecedentes que le sirvan de causa.

b) Una vez que el Certificador emita opinión, se notificará al reclamante y se le otorgará un plazo de CINCO (5) días hábiles administrativos para ofrecer y producir la prueba de su descargo.

c) La SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA resolverá en un plazo de DIEZ (10) días lo que estime corresponder, dictando el Acto Administrativo correspondiente, conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable.

En ningún caso la Política Única de Certificación del Certificador prevalecerá sobre lo dispuesto por la normativa legal vigente de firma digital.

El suscriptor o los terceros usuarios podrán accionar ante el ente licenciante, previo agotamiento del procedimiento ante el Certificador Licenciado correspondiente, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

9.14. - Legislación aplicable.

La Ley N° 25.506, el Decreto Nº 2628/02 y modificatorios, la Resolución MM Nº 399-E/16, la Resolución SMA Nº 37-E/2016 y demás normativa complementaria dictada por la autoridad competente, constituyen el marco normativo aplicable en materia de Firma Digital en la REPÚBLICA ARGENTINA.

9.15. – Conformidad con normas aplicables.

Se aplicará la normativa indicada en el apartado 9.14.

9.16. – Cláusulas adicionales.

No se incluyen cláusulas adicionales.

9.17. – Otras cuestiones generales.

No aplicable.

Historia de las revisiones:

VERSIÓN Y MODIFICACIÓN	FECHA DE EMISIÓN	DESCRIPCIÓN	MOTIVO DEL CAMBIO
Versión 1.0	XX/XX/2018	Política Única de Certificación	Licenciamiento AC MODERNIZACIÓN-PFDR
Versión 2.0	21/08/2018	Política Única de Certificación	Revisión

Nota: Cada nueva versión y/o modificación suplanta a las anteriores, resultando sólo vigente la última, la que está representada por el presente documento.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.08.27 11:05:53 -03'00'

Alejandra Battaglia
Directora Nacional
Dirección Nacional de Tramitación e Identificación a Distancia
Ministerio de Modernización

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.08.27 11:05:56 -03'00'