República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Anexo de Resolución

Número: ACTO-2022-83444729-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Jueves 11 de Agosto de 2022

Referencia: POLÍTICA ÚNICA DE CERTIFICACIÓN de la AC ONTI

INFRAESTRUCTURA DE FIRMA DIGITAL – REPÚBLICA ARGENTINA

LEY Nº 25.506

POLÍTICA ÚNICA DE CERTIFICACIÓN

AUTORIDAD CERTIFICANTE

de la

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA

SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA

SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO

JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN

Versión 4.0

Agosto 2022

ÍNDICE

1. – INTRODUCCIÓN.

1.1. - Descripción general.

El presente documento establece las políticas que se aplican a la relación entre la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante AC ONTI) en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley N° 25.506 y su modificatoria Ley N° 27.446) 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, persona jurídica pública o de una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

La Autoridad de Aplicación de la Infraestructura de Firma Digital antes mencionada es la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN, siendo dicho organismo y la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA, quienes conforman y entienden en las funciones de Ente Licenciante.

1.2. - Nombre e Identificación del Documento.

Nombre: Política Única de Certificación de la Autoridad Certificante ONTI

Versión: 4.0

Fecha de aplicación: a partir de su publicación en el Boletín Oficial de la República Argentina.

OID: 2.16.32.1.1.3

Lugar o Sitio de Publicación: https://www.argentina.gob.ar/modernizacion/firmadigital/documentosaconti

1.3. – Participantes.

Integran la infraestructura de la AC ONTI las siguientes entidades:

1.3.1. – AC ONTI.

La AC ONTI, cuyas funciones son administradas por la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN y/o las que en el futuro las reemplacen, presta los servicios de certificación, de acuerdo con los términos de la presente Política Única de Certificación.

Domicilio: Av. Roque Sáenz Peña N° 788 - Piso 5° - (C1035AAA) Ciudad Autónoma de Buenos Aires, Argentina.

Teléfono: (011) 5985-8600 interno 6193

CUIT: 30-71511756-4

Correo electrónico: firmadigital@jefatura.gob.ar

1.3.2. - Autoridad de Registro.

La AC ONTI posee una estructura de Autoridades de Registro (en adelante ARs), delegando en ellas las funciones de:

1. Recepción de las solicitudes de emisión 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 cuya verificación delegue la AC ONTI.

3. Remisión de las solicitudes aprobadas a la AC ONTI.

4. Recepción y validación de las solicitudes de revocación de certificados y su direccionamiento a la AC ONTI.

5. Validación y autenticación de la identidad de los solicitantes de revocación de certificados.

6. Archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la AC ONTI.

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

8. Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos de la AC ONTI en la parte que resulte aplicable.

9. Captura de fotografía y datos biométricos de los suscriptores de certificados, determinados por la reglamentación.

La AC ONTI conformará sus Autoridades de Registro en:

a) Entidades o jurisdicciones pertenecientes al Sector Público Nacional, Provincial, Municipal, en cualquiera de sus tres Poderes, Organismos Multilaterales, el Banco Central de la República Argentina, y otras organizaciones públicas.

b) Entes Públicos no Estatales.

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

La AC ONTI se reserva el derecho de dar de baja aquellas Autoridades de Registro que en un plazo de TRES (3) meses no aprueben solicitudes de emisión de certificados digitales.

Las entidades que tengan interés en constituirse como Autoridades de Registro de la AC ONTI, deberán solicitarlo a la AC ONTI, a través de los procedimientos electrónicos que determine la SUBSECRETARÍA DE INNOVACIÓN 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).

La AC ONTI 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 evaluará el cumplimiento de los requisitos establecidos para las ARs, entre los que se cuenta la capacitación de sus Oficiales de Registro, de los Responsables de Soporte Técnico de Firma Digital y los Responsables de la Autoridad de Registro, así como la presentación de un seguro de caución cuando correspondiere.

Los Oficiales de Registro y los Responsables de Soporte Técnico de Firma Digital deberán aprobar la mencionada capacitación.

Cumplidos los requisitos indicados anteriormente, la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA elevará un informe y solicitará autorización a la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA.

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

Las ARs serán notificadas de dicha autorización en su cuenta de usuario TAD, en caso de corresponder, o en su cuenta de usuario GDE y serán publicadas en el Boletín Oficial de la República Argentina.

Las Autoridades de Registro de la AC ONTI 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 DIEZ (10) años a partir de su fecha de vencimiento o revocación, se realizará por los medios establecidos por la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA.

Las Autoridades de Registro de la AC ONTI pueden desempeñar sus funciones en una modalidad fija o móvil.

Las Autoridades de Registro de la AC ONTI están obligadas a operar cooperativamente.

Los titulares de certificados podrán solicitar la revocación de su certificado ante cualquiera

de las Autoridades de Registro de la AC ONTI.

Toda documentación relacionada con cualquier trámite que efectúe una Autoridad de Registro ante la AC ONTI (tal como solicitudes de altas y bajas de ARs, designaciones de personal que cumple roles propios de la AR, presentación de certificados de seguros de caución) 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).

La información vinculada a las ARs de la AC ONTI, incluyendo domicilio y datos de contacto, se encuentra disponible en el sitio web de la AC ONTI:

https://pki.jgm.gob.ar/app/Listado_de_Autoridades_de_Registro.aspx

1.3.3. - Suscriptores de certificados.

Podrán ser suscriptores de los certificados emitidos por la AC ONTI:

a) 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.

b) Las personas jurídicas públicas que actúen como Autoridad de Sello de Competencia.

c) Las personas jurídicas públicas que requieran un certificado de aplicaciones.

La AC ONTI 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.

Asimismo, la AC ONTI emite certificados para la prestación de otros servicios en relación a la Firma Digital, según lo dispuesto en el artículo 33 del Anexo I de la Resolución de la entonces SECRETARÍA DE INNOVACIÓN PÚBLICA (SIP) N° 946 del 24 de septiembre de 2021.

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, de acuerdo a la normativa aplicable a la Firma Digital.

1.4. - Uso de los certificados.

Las claves correspondientes a los certificados digitales que se emitan bajo la presente Política Única de Certificación podrán ser utilizadas 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. - Organización Administradora del Documento.

El organismo responsable de la presente Política Única de Certificación es la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN, con los siguientes datos de contacto:

Correo electrónico: firmadigital@jefatura.gob.ar

Teléfono: (011) 3984 9000 interno: 6303/6342

1.5.2. – Contacto.

El responsable del registro, mantenimiento e interpretación de la presente Política Única de Certificación es el máximo responsable de la AC ONTI, cuyos datos de contacto figuran en el apartado anterior

1.5.3. - Organismo encargado de aprobar la Política Única de Certificación.

Esta Política Única de Certificación ha sido aprobada por la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

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 Única de Certificación.

Autoridad de Aplicación: La SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN es la Autoridad de Aplicación de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA establecida por la Ley N° 25.506 y su modificatoria.

Autoridad de Sello de Tiempo: Entidad que acredita la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

Autoridad de Registro: Entidad que tiene a su cargo las funciones indicadas en el artículo 28 del Decreto Nº 182/2019.

Certificado Digital: Documento digital firmado digitalmente por un Certificador Licenciado, que vincula los datos de verificación de firma a su titular. (Cfr. artículo 13 de la Ley N° 25.506).

Certificador Licenciado: Toda persona de existencia ideal, 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. (Cfr. artículo 17 de la Ley N° 25.506).

Autoridad de Sello de Competencia: Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.

Ente Licenciante: La SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN y la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA constituyen el Ente Licenciante.

Lista de Certificados Revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por la AC ONTI, la cual ha sido firmada digitalmente y publicada por ella. En inglés: Certificate Revocation List (CRL).

Manual de Procedimientos: Conjunto de prácticas utilizadas por la AC ONTI en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS).

Plan de Cese de Actividades: Conjunto de actividades a desarrollar por la AC ONTI en caso de finalizar la prestación de sus servicios.

Plan de Contingencia: Conjunto de procedimientos a seguir por la AC ONTI ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos de la AC ONTI.

Política de Privacidad: Conjunto de declaraciones que la AC ONTI se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por ella 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 protocolo 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 la AC ONTI que brinda el servicio.

Suscriptor o Titular de certificado digital: Persona, jurisdicción o entidad 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 ONTI - Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN.

AR - Autoridad de Registro.

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

CUIL - Clave Única de Identificación Laboral.

CUIT - Clave Única de Identificación Tributaria.

DER - Reglas Codificadas Distinguidas (“Distinguished Encoded Rules”)

DNFDEIT - DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA.

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

GDE – Sistema de Gestión Documental Electrónica.

HSM – Módulo de Seguridad de Hardware (“Hardware Security Module”).JGM – JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

JGM – JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

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”).

ONTI - Oficina Nacional de Tecnologías de Información.

OR - Oficial de Registro.

PIN – Número de Identificación Personal (“Personal Identification Number”)

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

RFC – Petición de Comentarios (“Request for Comments”)

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

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

SIP – (ex) SECRETARÍA DE INNOVACIÓN PÚBLICA.

SITSP – SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO.

SSIA – SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA.

ST – Responsable de Soporte Técnico de Firma Digital.

TAD – Plataforma de Trámites a Distancia.

X.509 - Estándar ITU-T ("International Telecommunication Union") 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 la AC ONTI que emita un certificado digital y el titular de ese certificado se rige por el Acuerdo con Suscriptores, sin perjuicio de las previsiones de la citada ley, y demás legislación vigente. Esa relación conforme el artículo 37 de la mencionada ley quedará encuadrada dentro del ámbito de responsabilidad civil contractual.

Al emitir un certificado digital o al reconocerlo en los términos del artículo 16 de la Ley N° 25.506, la AC ONTI 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, todo ello de acuerdo con lo establecido en el artículo 38 de la Ley N° 25.506. Corresponderá a la AC ONTI demostrar que actuó con la debida diligencia.

El artículo 32 del Decreto N° 182/2019, reglamentario de la Ley N° 25.506, establece la responsabilidad de la AC ONTI respecto de sus Autoridades de Registro.

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

Las ARs pueden constituirse como única unidad o con varias unidades dependientes jerárquicamente entre sí.

Las Autoridades de Registro pertenecientes a Ente Públicos no Estatales que sean conformadas en la AC ONTI, previa autorización de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA, 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.

La AC ONTI no es responsable en los siguientes casos, según el artículo 39 de la Ley N° 25.506:

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 la AC ONTI pueda demostrar que ha tomado todas las medidas razonables;

Los alcances de la responsabilidad de la AC ONTI se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en esta Política Única de Certificación en relación a la emisión, renovación y revocación de certificados.

Asimismo, la responsabilidad de la AC ONTI se limita a los ámbitos de su incumbencia directa, en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, 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 ONTI 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.

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 Autoridad de Registro sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán acordes a lo establecidos por la Ley N° 25.506, su Decreto Reglamentario N° 182/2019, la Resolución ex SIP N° 946/2021 o la que en el futuro la reemplace y a esta Política Única de Certificación.

A efectos de la aprobación de un nuevo certificado, la Autoridad de Registro siempre exigirá la presencia física del suscriptor. Con relación a la renovación y revocación de los certificados debe estarse a lo establecido en los apartados 3.3.1, 3.3.2 y 3.4 de esta Política Única de Certificación.

Todos los trámites realizados por las Autoridades de Registro son firmados digitalmente por los Oficiales de Registro, asumiendo así su plena responsabilidad en el proceso.

2.1. – Repositorios.

El servicio de repositorio de información, la publicación de la Lista de Certificados Revocados y el servicio de OCSP son administrados en forma directa por la AC ONTI.

2.2. - Publicación de información del Certificador

La AC ONTI garantiza el acceso a la información actualizada y vigente publicada en su repositorio, en cumplimiento con lo dispuesto en el artículo 12 del Anexo I de la Resolución ex SIP N° 946/2021.

Adicionalmente, la AC ONTI mantiene en el mismo repositorio en línea de acceso público:

a) Su certificado OCSP.

b) Información respecto a la fecha de la última auditoría dispuesta por la Autoridad de Aplicación.

c) 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 ONTI https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/a cap

La AC ONTI está obligada 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 21 inc. 9), 10) y 14) del Decreto N° 182/2019 y sus modificatorios y en la presente Política Única de Certificación.

2.3. - Listado de Autoridades de Registro - Frecuencia de publicación.

Se garantiza la actualización inmediata del Listado de Autoridades de Registro cada vez que cualquiera de los datos de las mismos sea modificado.

2.4. - Controles de acceso a la información.

Se garantizan los controles de los accesos al certificado de la AC ONTI, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política Única de Certificación y de su Manual de Procedimientos.

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 y utilizados por la AC ONTI o sus ARs como prerrequisito para su emisión. También se

describen los pasos para la autenticación de los solicitantes de renovación y 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 Aplicaciones:

- “commonName” (OID 2.5.4.3: Nombre común): corresponde al nombre de la aplicación o servicio.

- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): contiene a las unidades operativas relacionadas con el servicio, en caso de existir, pudiendo utilizarse varias instancias de este atributo de ser necesario.

- “organizationName” (OID 2.5.4.10: Nombre de la organización): este campo está presente y coincide con el nombre de la persona responsable del servicio o aplicación.

- “serialNumber” (OID 2.5.4.5: Nro. de serie): este campo está presente y contiene el número de identificación de la persona responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”.

El valor para el campo [código de identificación] es: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas Públicas argentinas.

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

Para los certificados de Personas Humanas:

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

- “serialNumber” (OID 2.5.4.5: Nro. de serie): este campo está presente y 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.

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

Para los Certificados de Personas Jurídicas Públicas:

- “commonName” (OID 2.5.4.3: Nombre común): Coincide con la denominación de la Persona Jurídica Pública.

- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): Contiene las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública.

- “serialNumber” (OID 2.5.4.5: Nro. de serie): Está presente y contiene el número de identificación de la Persona Jurídica Pública, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”. El valor posible para el campo [código de identificación] es: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas Públicas argentinas.

- “countryName” (OID 2.5.4.6: Código de país): Este campo está presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los Certificados de Autoridad de Sello de Tiempo:

- “commonName” (OID 2.5.4.3: Nombre común): Indica el nombre del servicio.

- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): Contiene las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública.

- “serialNumber” (OID 2.5.4.5: Nro de serie): Este campo está presente y contiene el número de identificación de la Persona Jurídica Pública, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”. El valor posible para el campo [código de identificación] es:

“CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas Públicas argentinas.

- “countryName” (OID 2.5.4.6: Código de país): Este campo está presente, representando el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los Certificados de Autoridad de Sello de Competencia:

- “commonName” (OID 2.5.4.3: Nombre común): Indica el nombre de la Autoridad de Competencia.

- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): Contiene las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública.

- “serialNumber” (OID 2.5.4.5: Nro de serie): Está presente y contiene el número de identificación de la Persona Jurídica Pública, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”. El valor posible para el campo [código de identificación] es: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas Públicas argentinas.

- “countryName” (OID 2.5.4.6: Código de país): Está presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

3.1.3. - Anonimato o uso de seudónimos.

No se emitirán certificados anónimos o cuyo Nombre Distintivo contenga 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 a la documentación presentada por el suscriptor de acuerdo a lo establecido en los apartados 3.2.2 y 3.2.3.

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 de los certificados emitidos por la AC ONTI es único para cada suscriptor. No se emite 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 certificado con el mismo CUIL / CUIT, los certificados se diferenciarán 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, excepto en el caso de certificados de aplicaciones en los que se aceptará en base a la documentación presentada.

La AC ONTI se reserva el derecho de tomar todas las acciones 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 ONTI o ante la Autoridad de Registro operativamente vinculada. Se establecen los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

La AC ONTI cumple con lo establecido en:

a) El artículo 21, inciso a) de la Ley de Firma Digital Nº 25.506 y el artículo 21, inciso 7) del Decreto Nº 182/2019, 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.

La AC ONTI comprueba que el solicitante es el titular del par de claves mediante la verificación de la solicitud del certificado digital en formato PKCS#10, la cual no incluye la clave privada. Las claves siempre son generadas por el solicitante. En ningún caso la AC ONTI ni sus ARs podrán tomar conocimiento, exigir o acceder bajo ninguna circunstancia a la clave privada de los solicitantes o titulares de los certificados, conforme el artículo 21 inciso b) de la Ley N° 25.506 y el artículo 21 inciso 3 del Anexo al Decreto Reglamentario N° 182/2019 y complementario.

La AC ONTI 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 la clave pública no pueda ser cambiada durante la transferencia.

Los datos recibidos por la AC ONTI se encuentran vinculados a dicha clave pública.

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

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

Los procedimientos de autenticación de la identidad comprenden los siguientes aspectos:

a) El requerimiento debe efectuarse únicamente por intermedio del responsable autorizado a actuar en nombre de la persona jurídica pública o de quien se encuentre a cargo del servicio o aplicación.

b) La Autoridad de Registro verificará la identidad del responsable antes mencionado y su autorización para gestionar el certificado correspondiente.

c) El responsable mencionado deberá validar su identidad según lo dispuesto en el apartado 3.2.3.

d) La identidad de la Persona Jurídica Pública titular del certificado deberá ser verificada mediante documentación que acredite su condición de tal.

En todos los casos, la siguiente documentación se presentará en formato digital a través de la plataforma de Trámites a Distancia (TAD) del sistema de Gestión Documental Electrónica – GDE o a través de éste último de corresponder:

Para personas jurídicas públicas:

a) Acto administrativo de la designación de la máxima autoridad del organismo público.

b) Autorización de la máxima autoridad del organismo al responsable de gestionar el certificado digital.

c) Designación del responsable autorizado.

d) Estructura organizativa del organismo público solicitante.

Entes públicos no estatales:

a) Designación de la máxima autoridad del Ente Público no estatal.

b) Autorización de la máxima autoridad del Ente Público no Estatal al responsable de gestionar el certificado digital.

c) Nota de designación del responsable autorizado.

d) Ley de creación del Ente Público no Estatal.

Se conserva la documentación que respalda el proceso de identificación de la persona responsable de la custodia de las claves criptográficas.

El suscriptor del certificado debe firmar el Acuerdo con Suscriptores del que surge la confirmación de que la información incluida en el certificado es correcta.

3.2.3. - Autenticación de la identidad de Personas Humanas.

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

Se exige la presencia física del solicitante o suscriptor del certificado ante la Autoridad de Registro. La verificación se efectúa mediante la presentación del Documento Nacional de Identidad Argentino.

Asimismo, la AR efectúa una captura y validación de la fotografía y/o de la huella dactilar del solicitante del certificado utilizando un dispositivo biométrico.

Se consideran obligatorias las exigencias reglamentarias impuestas por:

a) El artículo 21, inciso i) de la Ley Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21, inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.

c) El artículo 21, inciso 3) del Decreto Nº 182/2019 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

d) El artículo 34, inciso 14) del Decreto Nº 182/2019 relativo a la protección de datos personales.

Adicionalmente, la AC ONTI celebra con el solicitante o suscriptor un Acuerdo con Suscriptores, conforme el Anexo V de la Resolución ex SIP N° 946/2021, del que surge su conformidad respecto a la veracidad de la información incluida en el certificado.

Las Autoridades de Registro verifican que el dispositivo criptográfico utilizado por el solicitante cumpla con las especificaciones técnicas establecidas por la Autoridad de Aplicación, conforme lo establecido en el apartado 3, del Anexo II de la Resolución ex SIP N° 946/2021.

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.

Según lo dispuesto en el apartado 3.2.2., las Autoridades de Registro verifican la autorización de la persona humana que actúa en nombre de la Persona Jurídica Pública para gestionar el certificado correspondiente.

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).

En el caso de certificados digitales de personas humanas, jurídicas públicas o de aplicaciones, la renovación en este apartado aplica a la generación de UN (1) nuevo par de claves y su correspondiente certificado:

a) después de la revocación de UN (1) certificado.

b) después de la expiración de UN (1) certificado.

c) antes de la expiración de UN (1) certificado.

En los casos a) y b) se exigirá el cumplimiento de los procedimientos previstos en el apartado 3.2.3. - Autenticación de la identidad de Personas Humanas.

En el caso c) si la solicitud de la renovación se realiza antes de la expiración del certificado, no habiendo sido este revocado, no se exigirá la presencia física del suscriptor, debiendo el solicitante remitir la constancia del inicio del trámite de renovación firmada digitalmente con el certificado a renovar.

La renovación sin presencia física del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y las contraseñas necesarias para el acceso a su clave privada (PIN)

Sin perjuicio de ello en el caso de certificados de personas jurídicas públicas o aplicaciones, el solicitante deberá presentar nuevamente la documentación requerida en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas.

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

No aplicable.

3.4. - Requerimiento de revocación.

El suscriptor cuando se trate de los certificados de persona humana, podrá revocar el certificado digital utilizando cualquiera de los siguientes métodos:

a) A través de la aplicación de la AC ONTI, que se encuentra disponible VEINTICUATRO (24) horas, ingresando a https://pki.jgm.gob.ar/app/Signature/Revoke/certRevoke00Cert.aspx si tiene acceso a su clave privada

b) Utilizando el código de revocación que le fuera informado al momento de la emisión de su certificado, ingresando a https://pki.jgm.gob.ar/app/Signature/Revoke/certRevoke00Pin.aspx.

c) Presentándose ante una AR con documento que permita acreditar su identidad en caso de no poder utilizar alguno de los anteriores.

Asimismo, el requerimiento de revocación podrá ser solicitado por quienes se encuentren legitimados en el apartado “4.9.2. – Autorizados a solicitar la revocación” de la presente Política, siguiendo los lineamientos establecidos en el Manual de Procedimientos

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 de certificados podrán ser iniciadas:

a) En el caso de personas humanas únicamente por el solicitante.

b) En el caso de personas jurídicas públicas por el representante legal o apoderado con poder suficiente a dichos efectos.

c) En el caso de los certificados de aplicaciones por el responsable del área declarada en el campo OU (organizationalUnitName) del CSR (Certificate Signing Request) o superior jerárquico.

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2.- “Autenticación de la identidad de Personas Jurídicas Públicas” y 3.2.3.- “Autenticación de la identidad de Personas Humanas”.

Los pasos para realizar la solicitud son los siguientes:

a) Ingresar al sitio web de la AC ONTI https://pki.jgm.gob.ar/app seleccionando el enlace a la aplicación de solicitud de emisión de certificados.

b) Completar la solicitud de certificado con los datos requeridos de acuerdo al tipo de certificado, seleccionando una AR.

c) Declarar un correo electrónico de uso habitual y de acceso exclusivo de la persona solicitante, el que será considerado a los efectos de las notificaciones.

d) Aceptar el Acuerdo con Suscriptores en el que se hace referencia a la Política Única de Certificación que respalda la emisión del certificado.

e) Enviar la solicitud a la AC ONTI.

f) Presentarse ante la AR correspondiente para realizar la identificación personal y la verificación de la documentación y datos biométricos requeridos en cada caso.

4.2. - Procesamiento de la solicitud del certificado.

El procesamiento de la solicitud finaliza con su aceptación o rechazo por parte de la AR, la misma se encuentra firmada digitalmente por el Oficial de Registro interviniente asumiendo así su plena responsabilidad en dicho proceso.

En todos los casos, la AR efectúa los siguientes pasos:

a) Efectúa la captura y validación de la fotografía y/o de la huella dactilar del solicitante del certificado utilizando un dispositivo biométrico.

b) Valida la identidad del solicitante o su representante autorizado.

c) Verifica la existencia de la solicitud en la aplicación de la AC ONTI.

d) En caso de ser aprobada la solicitud por el Oficial de Registro la Autoridad Certificante procederá a la emisión del certificado. En caso contrario, de ser rechazada, no se emitirá el certificado correspondiente.

4.3. - Emisión del certificado.

4.3.1. - Proceso de emisión del certificado.

Cumplidos los recaudos del proceso de validación de identidad y otros datos del solicitante, de acuerdo con esta Política Única de Certificación y una vez aprobada la solicitud de certificado por la AR, la AC ONTI emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor.

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 ONTI a la cuenta de correo declarada por el solicitante o representante autorizado al momento de iniciar el trámite. En dicho correo se indica el enlace al que debe acceder para descargar el certificado emitido, y el código que podrá utilizar en caso de ser necesaria la revocación del certificado.

4.4.- Aceptación del certificado.

Un certificado emitido por AC ONTI 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.

El suscriptor debe cumplir las siguientes obligaciones:

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

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.

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

d) Informar sin demora a la AC ONTI el cambio de alguno de los datos contenidos en el certificado digital que

hubiera sido objeto de verificación.

Según lo establecido en la Resolución ex SIP N° 946/2021:

a) Resguardar y no divulgar aquellos factores de autenticación (contraseñas de usuario, PIN) que permitan utilizar la clave privada.

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

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

d) Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

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.

Se aplican los procedimientos previstos en el apartado 3.3.1.- “Renovación con generación de nuevo par de claves”.

4.8. - Modificación del certificado.

El suscriptor se encuentra obligado a notificar a la AC ONTI 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 en los plazos previstos en el apartado 4.9.4 de manera oportuna y sobre la base de una solicitud de revocación de certificado validada según los procedimientos establecidos en el apartado 4.9.3.

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

4.9.1. - Causas de revocación.

La AC ONTI procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

a) A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados personas jurídicas públicas o de certificados de aplicaciones.

b) Si determinara que el certificado digital 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 acto administrativo de la Autoridad de Aplicación debidamente fundado.

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.

l) Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506 y su modificatoria y sus normas complementarias.

4.9.2. - Autorizados a solicitar la revocación.

Se encuentran autorizados a solicitar la revocación de un certificado emitido por la AC ONTI:

a) En el caso de los certificados de personas humanas, el suscriptor del certificado.

b) En el caso de los certificados de persona Jurídica Pública o de aplicaciones, el responsable autorizado que efectuara el requerimiento.

c) En el caso de los certificados de persona jurídica pública o de aplicaciones, el responsable debidamente autorizado por la Persona Jurídica Pública que brinda el servicio o es titular del certificado o la aplicación.

d) El Certificador o la Autoridad de Registro.

e) El Ente Licenciante.

f) La Autoridad Judicial.

g) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación.

Un suscriptor podrá revocar su certificado digital emitido por la AC ONTI utilizando cualquiera de los siguientes métodos:

a) A través de la aplicación de la AC ONTI https://pki.jgm.gob.ar/app/Signature/Revoke/certRevoke00Cert.aspx que se encuentra disponible VEINTICUATRO (24) horas, si tiene acceso a su clave privada.

b) A través de la aplicación de la AC ONTI https://pki.jgm.gob.ar/app/Signature/Revoke/certRevoke00Pin.aspx que se encuentra disponible VEINTICUATRO (24) horas, utilizando el código de revocación que le fue entregado al momento de la emisión del certificado.

c) En caso de no poder utilizar alguno de los métodos anteriores, presentándose ante una de las ARs de AC ONTI, con documento de identidad que permita acreditar la misma, para realizar la identificación personal y proceder a la captura y validación de sus datos biométricos.

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

La AC ONTI 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 ONTI o la Autoridad de Registro en el proceso, están documentadas y conservadas en sus archivos.

c) Se documentan y archivan las causales de las revocaciones aprobadas.

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.

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 21, inciso 8 del Anexo al Decreto Nº 182/2019, a través de la aplicación web de la AC ONTI.

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

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

Por su parte, el cambio de la información del 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 ONTI pone 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 ONTI y de su período de validez.

La AC ONTI cumple con lo establecido en el artículo 21, inciso 9 del Anexo al Decreto Nº 182/2019 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la Resolución ex SIP N° 946/2021 y sus correspondientes Anexos.

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

La AC ONTI genera y publica una Lista de Certificados Revocados asociada a esta Política Única de Certificación cada VEINTICUATRO (24) horas, la misma se encuentra disponible en:

http://pki.jgm.gob.ar/crl/FD.crl

o "http://pki.jgm.gob.ar/crl/FD.crl" * MERGEFORMAT http://pki.jgm.gob.ar/crl/FD.crl

y en:

http://pkicont.jgm.gob.ar/crl/FD.crl

con listas complementarias (delta CRL) en modo horario.

4.9.8.- Vigencia de la lista de certificados revocados.

La lista de certificados revocados indica 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 ONTI 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.

Las CRL pueden ser descargadas del sitio web de la AC ONTI disponible en: http://pki.jgm.gob.ar/crl/FD.crl y

http://pkicont.jgm.gob.ar/crl/FD.crl

La delta CRL puede ser descargadas del sitio web de la AC ONTI disponible en:

http://pki.jgm.gob.ar/crl/FD+.crl y

http://pkicont.jgm.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 ONTI disponible en http://pki.jgm.gob.ar/ocsp y

http://pkicont.jgm.gob.ar/ocsp

La AC ONTI posee servicios de alta disponibilidad para la consulta del estado de verificación de los certificados; ante la eventualidad de no contar dicho servicio, posee sistemas de contingencia publicados en:

http://pkicont.jgm.gob.ar/crl/FD.crl y

http://pkicont.jgm.gob.ar/ocsp

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 ONTI 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 ONTI 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 ONTI: https://pki.jgm.gob.ar/app/CertificateAuthority/CertificatePublicKeyRequest.aspx. 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 ONTI.

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

En caso de compromiso de su clave privada, el titular del certificado correspondiente se encuentra obligado a comunicar inmediatamente dicha circunstancia a la AC ONTI 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 y modificatoria.

4.9.14. - Autorizados a solicitar la suspensión.

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

4.9.15. - Procedimientos para la solicitud de suspensión.

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

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

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

4.10. – Estado del certificado.

4.10.1. – Características técnicas.

Los servicios disponibles para la verificación del estado de los certificados emitidos por la AC ONTI 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 ONTI.

Cada Lista de Certificados Revocados complementaria (delta CRL) contendrá los números de serie de los certificados que fueron revocados durante el período comprendido entre la emisión de la última CRL y la emisión de dicha delta CRL; dicho período nunca superará las VEINTICUATRO (24) horas. Esta información se encontrará firmada digitalmente por la AC ONTI.

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 la AC ONTI.

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 ONTI.

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 ONTI, excepto en el caso en que tramitara un nuevo certificado.

De igual forma se producirá la desvinculación ante el cese de las operaciones de la AC ONTI.

4.12. – Recuperación y custodia de claves privadas.

En virtud de lo dispuesto en el artículo 21 inciso b) de la Ley N° 25.506 y en el artículo 21, inciso 3 del Anexo al Decreto N° 182/2019, la AC ONTI 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 artículo 25 inciso a) de la Ley N° 25.506, 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 ONTI. La descripción detallada se encuentra desarrollada 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.

Toda la información detallada sobre la seguridad física se encuentra definida en el Plan de Seguridad

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.

Toda la información detallada sobre los puntos antes mencionados se encuentra definida en el Plan de Seguridad y el documento Roles y 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.

Todo lo relativo a seguridad del personal se encuentra definido en el Plan de Seguridad

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 II Sección 3 de la Resolución ex SIP N° 946/2021.

b) Frecuencia de procesamiento de registros.

c) Período de guarda de los registros. Se cumple con lo establecido en el artículo 21 inciso i) 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.

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

h) Evaluación de vulnerabilidades.

Los procedimientos de auditoría de seguridad se encuentran definidos en el Plan de Seguridad.

5.5. - Conservación de registros de eventos.

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 II Sección 3 de la Resolución ex SIP N° 946/2021 respecto del registro de eventos.

Existen procedimientos de conservación y guarda de registros en los siguientes aspectos:

a) Tipo de registro archivado: se cumple con lo establecido en el Anexo II Sección 3 de la Resolución ex SIP N° 946/2021.

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.

g) Procedimientos para obtener y verificar la información archivada.

5.6. - Cambio de claves criptográficas.

El par de claves de AC ONTI 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 AC ONTI implica la emisión de un nuevo certificado por parte de la ACR-RA. Si la clave privada de AC ONTI 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 ONTI tomará los recaudos necesarios para efectuar con suficiente antelación la renovación de su licencia y la obtención del nuevo certificado, si correspondiese.

5.7. - Compromiso y recuperación ante desastres.

Los requerimientos relativos a la recuperación de los recursos de la AC ONTI en caso de falla o desastre se encuentran desarrollados en el Plan de Contingencia.

Los procedimientos implementados se refieren a los siguientes aspectos:

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 ONTI.

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

Los procedimientos cumplen con lo establecido por el artículo 20 del Anexo al Decreto Nº 182/2019, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8. - Plan de Cese de Actividades.

Los requisitos y procedimientos a ser adoptados en caso de finalización de servicios de la AC ONTI o de una o varias de sus Autoridades de Registro son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación al Ente Licenciante, Suscriptores, Terceros Usuarios, otros Certificadores Licenciados y usuarios vinculados.

b) Revocación del certificado de la AC ONTI y de los certificados emitidos.

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

La AC ONTI o las Autoridades de Registro que hubieran cesado cumplen con idénticas exigencias de seguridad para la custodia de archivos y documentación.

Con relación a las causales de caducidad de la licencia, se contempla lo establecido por el artículo 44 de la Ley Nº 25.506.

Asimismo, los procedimientos cumplen lo dispuesto por el artículo 20 del Anexo al Decreto Nº 182/2019, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la Resolución ex SIP N° 946/2021, y sus correspondientes Anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA.

Se describen las medidas de seguridad implementadas por la AC ONTI 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 ONTI y sus Autoridades de Registro, repositorios y suscriptores.

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

6.1.1. - Generación del par de claves criptográficas.

La AC ONTI, 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 o superior.

En el caso de las ARs, cada Oficial de Registro genera y almacena su par de claves utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2 o superior.

Para las claves criptográficas de los suscriptores de certificados de personas humanas los dispositivos criptográficos utilizados deben ser FIPS 140-2 Nivel 2 o superior.

Para las claves criptográficas utilizadas por las Autoridades de Sello de Competencia los dispositivos criptográficos utilizados deben ser FIPS 140-2 Nivel 3 o superior.

Los dispositivos criptográficos deben estar clasificados como ACTIVOS (ACTIVE por el NIST).

Excepcionalmente, en el caso de los suscriptores que no sean Oficiales de Registro, se admitirán dispositivos que se encuentren clasificados como HISTÓRICOS (HISTORICAL) por el NIST. Los suscriptores no deberán utilizar estos dispositivos transcurridos TRES (3) años desde su incorporación a dicha clasificación. Se recomienda que los suscriptores no realicen nuevas adquisiciones de dispositivos que se encuentren en tal condición.

La clave privada almacenada en un dispositivo criptográfico queda protegida a través de DOS (2) factores:

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

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. El PIN deberá contener como mínimo un largo de OCHO (8) caracteres requiriendo utilizar mayúsculas, minúsculas y números.

6.1.2. - Entrega de la clave privada.

En todos los casos, se 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 el artículo 21, inciso b) de la Ley Nº 25.506 y el artículo 21, inciso 3 del Anexo al Decreto Nº 182/2019.

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

Todo solicitante de un certificado emitido bajo esta Política Única de Certificación entrega su clave pública a la AC ONTI, a través de la aplicación correspondiente, durante el proceso de solicitud de su certificado.

La AC ONTI 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, de acuerdo a lo establecido en el apartado 3.2.1. del Manual de Procedimientos.

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 la AC ONTI 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 de la AC ONTI.

El certificado de la AC ONTI 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://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/a craiz

6.1.5. - Tamaño de claves.

La AC ONTI genera su par de claves criptográficas utilizando el algoritmo RSA de 4096 bits.

Los suscriptores, incluyendo las ARs y los proveedores de otros servicios de firma digital generan sus claves mediante el algoritmo RSA con un tamaño de clave de 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 apartado 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 utilizadas para firmar digitalmente, para funciones de autenticación y/o 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 de la AC ONTI, de los repositorios, de las ARs y de los suscriptores, abordándose 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 un dispositivo criptográfico.

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.

6.2.1. – Controles y estándares para dispositivos criptográficos.

Para la generación y el almacenamiento de las claves criptográficas, la AC ONTI, los suscriptores y los Oficiales de Registro utilizan los dispositivos referidos en los apartados 6.1.1. y 6.1.5.

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

Los controles empleados para la activación de la clave privada de la AC ONTI se basan en la presencia de M de N poseedores de claves de activación con M mayor a 2.

6.2.3. - Recuperación de clave privada.

Ante una situación que requiera recuperar su clave privada, y siempre que ésta no se encuentre comprometida, la AC ONTI 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 ONTI.

La AC ONTI no implementa mecanismos de resguardo y recuperación de las claves privadas de las ARs 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. Asimismo, las ARs no implementan mecanismos de resguardo y/o recuperación de las claves privadas de los suscriptores, de las contraseñas de acceso a estas, o de acceso a los dispositivos criptográficos.

6.2.4. - Copia de seguridad de clave privada.

La AC ONTI genera una copia de seguridad de su clave privada a través de un procedimiento que garantiza su integridad y confidencialidad.

6.2.5. - Archivo de clave privada.

La AC ONTI almacena las copias de resguardo 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 ex SIP N° 946/2021 en cuanto a los niveles de resguardo de claves.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

El par de claves criptográficas de la AC ONTI 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 soportadas en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

Las claves criptográficas de los suscriptores de certificados son generadas y almacenadas en un dispositivo criptográfico FIPS 140-2 nivel 2 o superior, no permitiendo su exportación.

6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos.

El almacenamiento de las claves criptográficas de la AC ONTI 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 II de la Resolución ex SIP N° 946/2021.

El par de claves criptográficas de los ORs y de los suscriptores de certificados es almacenado en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se genera, no permitiendo su exportación.

6.2.8. - Método de activación de claves privadas.

Para la activación de la clave privada de la AC ONTI 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 ONTI 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 ONTI 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 ONTI 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 Oficiales de Registro se utilizan dispositivos criptográficos FIPS 140-2 Nivel 2 o superior.

Los suscriptores utilizan dispositivos criptográficos FIPS 140-2 Nivel 2 o superior.

Las Autoridades de Sello de Competencia utilizan dispositivos criptográficos FIPS 140-2 Nivel 3 o superior.

Los proveedores de otros servicios relacionados con la firma digital, utilizan dispositivos FIPS 140-2 Nivel 3 o superior.

6.3. - Otros aspectos de administración de claves.

6.3.1. - Archivo permanente de la clave pública.

Los certificados emitidos a suscriptores, como así también el certificado de la AC ONTI, 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 la AC ONTI 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 suscriptores de certificados.

6.4.1. - Generación e instalación de datos de activación.

Los datos de activación del dispositivo criptográfico de la AC ONTI 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 la AC ONTI ni las ARs 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.

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

En relación a los suscriptores, la clave privada almacenada en un dispositivo criptográfico por hardware queda protegida a través de DOS (2) factores:

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

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. El PIN deberá contener como mínimo un largo de OCHO (8) caracteres requiriendo utilizar mayúsculas, minúsculas y números.

Los suscriptores no deben compartir sus dispositivos criptográficos ni definir administradores de contraseñas.

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

Es responsabilidad de las Autoridades de Registro, de los proveedores de otros servicios relacionados con la firma digital y demás suscriptores de certificados emitidos por la AC ONTI, 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.

La AC ONTI 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 de la AC ONTI 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.

Los puntos anteriormente detallados se encuentran definidos en el Plan de Seguridad.

6.5.2. - Requisitos de seguridad computacional.

Los dispositivos criptográficos utilizados por la AC ONTI, por los Oficiales de Registro, suscriptores y proveedores de otros servicios relacionados con la firma digital se encuentran certificados por el NIST (“National Institute of Standards and Technology”)

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.

La AC ONTI 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 ONTI se encuentran a cargo de la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

6.8. – Servicios de emisión de Sellos de Tiempo.

La AC ONTI presta el servicio de emisión de sello de tiempo para la certificación de fecha y hora, conforme lo establecido el artículo N° 33 del Anexo I de la Resolución ex SIP N° 946/2021.

Dicho servicio se implementa conforme a lo indicado en la especificación RFC 3161 “Internet X.509 PKI Time Stamp Protocol (TSP)” y a la especificación RFC 3628 “Policy Requirements for Time-Stamping Authorities (TSAs).

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 IV - Perfiles de los Certificados y de las Listas de Certificados Revocados de la Resolución ex SIP N° 946/2021.

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	(entero positivo asignado unívocamente por la AC ONTI 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=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=APELLIDO Nombre
	serialNumber - 2.5.4.5	SERIALNUMBER=
	countryName - 2.5.4.6	C=AR

Clave pública del suscriptor (Subject Public Key Info)	public key algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	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://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS

		Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	ExtendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	SubjectAltName 2.5.29.17	Dirección de correo electrónico (campo optativo)
Información de Acceso de la AC	authorityInfo Access 1.3.6.1.5.5.7.1.1	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pki.jgm.gob.ar/aia/cafdONTI.crt [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pkicont.jgm.gob.ar/aia/cafdONTI.crt [3]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)

		Nombre alternativo: Dirección URL=http://pki.jgm.gob.ar/ocsp [4]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pkicont.jgm.gob.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2 o superior)

Perfil del certificado de PERSONA JURÍDICA PÚBLICA

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	(entero positivo asignado unívocamente por la

		AC ONTI 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=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN= denominación de la Persona Jurídica Pública
	organizationName 2.5.4.10	O= DEBE coincidir con el nombre de la Persona Jurídica Pública

	organizationalUnitName 2.5.4.11	OU= PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario
	serialNumber - 2.5.4.5	SN=
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	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	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo:

Certificados Revocados		Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: https://www.argentina.gob.ar/sites/default/files/ac_onti_-_puc_v4.0_0.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley N° 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	SubjectAltName 2.5.29.17	Dirección de correo electrónico (campo optativo)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	Método = Emisor de autoridad de certificación URI = http://pki.jgm.gob.ar/aia/cafdONTI.crt Método = Emisor de autoridad de certificación URI = http://pkicont.jgm.gob.ar/aia/cafdONTI.crt Método = OCSP URI = http://pki.jgm.gob.ar/ocsp

		Método = OCSP URI = http://pkicont.jgm.gob.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

Perfil de certificados de proveedores de otros servicios en relación con la firma digital.

Perfil del certificado de APLICACIONES

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	(entero positivo asignado unívocamente por la AC ONTI 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=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	yyyy/mm/dd hh:mm:ss huso-horario
Nombre	commonName - 2.5.4.3	CN=Denominación de la Aplicación

distintivo del suscriptor (Subject DN)	organizationName 2.5.4.10	O=nombre de la Persona Jurídica Pública responsable de la aplicación
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con la aplicación
	serialNumber - 2.5.4.5	SN=
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	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://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: https://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley N° 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	Método = Emisor de autoridad de certificación URI = http://pki.jgm.gob.ar/aia/cafdONTI.crt Método = Emisor de autoridad de certificación URI =

		http://pkicont.jgm.gob.ar/aia/cafdONTI.crt Método = OCSP URI = http://pki.jgm.gob.ar/ocsp Método = OCSP URI = http://pkicont.jgm.gob.ar/ocsp

Perfil del certificado de Autoridad de SELLO DE TIEMPO.

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	(entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgoritm	sha256RSA (1.2.840.113549.1.1.11)
Nombre distintivo del	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital

emisor (Issuer)	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del servicio de emisión de sello de tiempo
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública responsable del servicio
	serialNumber - 2.5.4.5	SN=
	countryName - 2.5.4.6	C=AR

Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	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	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de sellos de tiempo Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación:

		Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley N° 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Impresión de fecha (1.3.6.1.5.5.7.3.8)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	Método = Emisor de autoridad de certificación URI = http://pki.jgm.gob.ar/aia/cafdONTI.crt Método = Emisor de autoridad de certificación URI = http://pkicont.jgm.gob.ar/aia/cafdONTI.crt Método = OCSP URI = http://pki.jgm.gob.ar/ocsp Método = OCSP URI = http://pkicont.jgm.gob.ar/ocsp

Perfil del certificado de AUTORIDAD DE SELLO DE COMPETENCIA

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	(entero positivo asignado unívocamente por la AC ONTI 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=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName -	S=Ciudad Autónoma de Buenos Aires

	2.5.4.8	
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN= nombre de la Autoridad de Competencia
	organizationName 2.5.4.10	O= DEBE coincidir con el nombre de la Persona Jurídica Pública
	organizationalUnitName 2.5.4.11	OU= PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario
	serialNumber - 2.5.4.5	SN=
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	
Restricciones	basicConstraint	Tipo de asunto = Entidad final

básicas	2.5.29.19	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://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: https://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley N° 25.506.
Identificador de la Clave	authorityKeyIdentifier 2.5.29.35	keyIdentifier = (Contiene un hash de 20 bytes del atributo

de la Autoridad Certificante		clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	Método = Emisor de autoridad de certificación URI = http://pki.jgm.gob.ar/aia/cafdONTI.crt Método = Emisor de autoridad de certificación URI = http://pkicont.jgm.gob.ar/aia/cafdONTI.crt Método = OCSP URI = http://pki.jgm.gob.ar/ocsp Método = OCSP URI = http://pkicont.jgm.gob.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

7.2. - Perfil de la LISTA DE CERTIFICADOS REVOCADOS.

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 IV “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución ex SIP N° 946/2021.

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=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros, Secretaría de la Gestión Pública, Subsecretaría de Tecnologías de Gestión
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Fecha efectiva	thisUpdate	yyyy/mm/dd hh:mm:ss huso-horario
Próxima	nextUpdate	

Actualización		yyyy/mm/dd hh:mm:ss huso-horario
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = (es una cadena de 20 bytes que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.) Id. de clave=70 ba 03 71 7a d8 10 e4 ee 52 b5 7f 32 8f 9f 6c 2e f7 84 0d
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://pki.jgm.gob.ar/crl/FD.crl [2]Punto de distribución CRL URL=http://pkicont.jgm.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	
	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 PÚBLICAción de lista de revocación		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 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP” y cumple con las indicaciones establecidas en la Sección 4 -"Perfil de la consulta en línea del estado del certificado” del Anexo IV “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución ex SIP N° 946/2021.

7.3.1. Consultas OCSP

Los siguientes datos se encuentran presentes en las consultas:

• Versión (versión).

• Requerimiento de servicio (service request).

• Identificador del certificado bajo consulta (target certificate identifier).

• Extensiones opcionales (optional extensions), las cuales podrían ser procesadas por quien responde.

Al recibir la consulta OCSP, se determina:

• Si el formato de la consulta es adecuado.

• Si quien responde se encuentra habilitado para responder la consulta.

• Si la consulta contiene la información que necesita quien responde.

Si alguna de estas condiciones no se cumpliera, da lugar a un mensaje de error. De lo contrario se devuelve una respuesta.

7.3.2. Respuestas OCSP

Todas las respuestas OCSP son firmadas digitalmente por la Autoridad certificante de la AC ONTI y contienen los siguientes datos:

• Versión de la sintaxis de respuesta.

• Identificador de quien responde.

• Fecha y hora en la que se genera la respuesta.

• Respuesta respecto al estado del certificado.

• Extensiones opcionales.

• Identificador (OID) único del algoritmo de firma.

• Firma de la respuesta.

La respuesta a una consulta OCSP consiste en:

• Identificador del certificado.

• Valor correspondiente al estado del certificado.

• Período de validez de la respuesta.

• Extensiones opcionales. Se especifican las siguientes respuestas posibles para el valor correspondiente al estado del certificado:

• Válido (good), indicando una respuesta positiva a la consulta. Este valor indica que no existe un certificado digital con el número de serie contenido en la consulta, que haya sido revocado durante su vigencia.

• Revocado (revoked), indicando que el certificado ha sido revocado.

• Desconocido (unknown), indicando que quien responde no reconoce el número de serie incluido en la consulta, debido comúnmente a la inclusión de un emisor desconocido.

8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

La Dirección Nacional de Firma Digital e Infraestructura Tecnológica, en su calidad de administradora de la AC ONTI, se encuentra sujeta a las auditorías dispuestas en el artículo 10 del Decreto N° 561/2016.

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 3 de la Ley N° 27.446 y otras normas reglamentarias.

Los informes resultantes de las auditorías son elevados a la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA. La información acerca de la fecha de la última auditoría de que hubiera sido objeto es publicada en su sitio web en forma permanente e ininterrumpida.

La AC ONTI 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) El artículo 6° del Anexo al Decreto Nº 182/2019 relativo al sistema de auditoría y el artículo 7° del mismo decreto relativo al informe de auditoría.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1. – Aranceles.

La AC ONTI no percibe aranceles por ninguno de los servicios de emisión, renovación y revocación de los certificados. Los certificados emitidos bajo la presente política son gratuitos.

9.2. - Responsabilidad Financiera.

La responsabilidad financiera de la AC ONTI surge de lo establecido por la Ley N° 25.506, su Decreto Reglamentario Nº 182/2019 y su modificatorio y en las disposiciones de la presente política.

Asimismo, en virtud de lo establecido en el Decreto N° precitado y su modificatorio, las Autoridades de Registro pertenecientes a Ente Públicos no Estatales dependientes de la AC ONTI, deberán constituir una garantía mediante un seguro de caución a fin de garantizar el cumplimiento de las obligaciones establecidas en la normativa vigente.

9.3. – Confidencialidad.

Toda la información vinculada a los certificados de firma digital se encuentra resguardada por la Ley de Protección de Datos Personales Nº 25.326, su reglamentación y normas complementarias y aclaratorias.

La información brindada por los solicitantes y suscriptores debe ser considerada confidencial y no ser divulgada a terceros sin el consentimiento previo de su titular, excepto que sea requerida por un juez en un proceso judicial o autoridad competente en un procedimiento administrativo.

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 por juez en un proceso judicial o autoridad competente en un procedimiento administrativo. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso la AC ONTI o la Autoridad de Registro durante el ciclo de vida del certificado.

La AC ONTI garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, es generada y custodiada conforme a lo que se especifica en la presente política.

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 la AC ONTI.

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

c) Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes a la AC ONTI.

9.3.2. - Información no confidencial.

La siguiente información recibida por la AC ONTI o por sus Autoridades de Registro no es considerada confidencial:

a) Contenido de los certificados y de las Listas de Certificados Revocados.

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

c) Políticas Únicas de Certificación y Manuales de Procedimientos.

d) Secciones públicas del Plan de Seguridad de la AC ONTI.

e) Política de privacidad de la AC ONTI.

f) Acuerdo con Suscriptores.

g) Términos y condiciones con terceros usuarios.

9.3.3. – Responsabilidades de los roles involucrados.

La información confidencial podrá ser revelada ante un requerimiento emanado por un juez en un proceso judicial o autoridad competente en un procedimiento administrativo.

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 expresa 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 la AC ONTI 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 Licenciado para la implementación de su AC, como así también toda la documentación relacionada, pertenece a la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

El derecho de autor de la presente Política Única de Certificación y de toda otra documentación generada por la AC ONTI en relación con la Infraestructura de Firma Digital, pertenece a la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN. Consecuentemente, dichos documentos no pueden ser reproducidos, copiados ni utilizados de ninguna manera, total o parcial, sin previo y formal consentimiento de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN, de acuerdo a la legislación vigente.

9.6. - Responsabilidades y garantías.

Las responsabilidades y garantías para la AC ONTI, sus Autoridades de Registro, los suscriptores, los terceros usuarios y otras entidades participantes, se originan en lo establecido por la Ley N° 25.506 y su Decreto Reglamentario Nº 182/2019 y modificatorio, la Resolución ex SIP N° 946/2021, sus modificatorias y en las disposiciones de la presente política.

9.7. – Deslinde de responsabilidad.

Las limitaciones de responsabilidad de la AC ONTI se rigen por lo establecido en el artículo 39 de la Ley N° 25.506, en las disposiciones de la presente política y en el Acuerdo con Suscriptores.

9.8. – Limitaciones a la responsabilidad frente a terceros.

Las limitaciones de responsabilidad de la AC ONTI 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 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 encuentra vigente a partir de la fecha de su aprobación por parte del Ente Licenciante y hasta tanto sea reemplazada por una nueva versión. Todo cambio en la Política, una vez aprobado por el Ente Licenciante, será debidamente comunicado 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 supervisada previamente por la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN conforme a lo establecido por el artículo 21, inciso q) de la Ley N° 25.506, el Decreto Nº 182/2019 y por la Resolución ex SIP N° 946/2021.

Toda Política Única de Certificación es sometida a aprobación de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN durante el proceso de licenciamiento.

Todo cambio en la Política Única de Certificación es comunicado al suscriptor a través de la publicación en el sitio web https://www.argentina.gob.ar/modernizacion/firmadigital/documentosaconti y en el Boletín Oficial de la República Argentina.

La presente Política Única de Certificación será revisada y actualizada periódicamente por la AC ONTI y sus

nuevas versiones se pondrán en vigencia, previa aprobación de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

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 https://www.argentina.gob.ar/modernizacion/firmadigital/documentosaconti

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° 19.549/72 (T.O. 2017) y su Decreto Reglamentario N° 1759/72 (T.O. 2017) y/o la Ley N° 19.983, según corresponda.

La presente Política Única de Certificación se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506 y su modificatoria, el Decreto Nº 182/2019 y modificatorios, la Resolución ex SIP N° 946/2021 y demás normativa complementaria dictada por la autoridad competente.

9.14. - Legislación aplicable.

La Ley N° 25.506 y su modificatoria, el Decreto Nº 182/2019 y modificatorios, la Resolución ex SIP N° 946/2021, las Resoluciones de la entonces SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA (SMA) Nros. 37-E/2016, 116-E/2017 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 establecen cláusulas adicionales.

9.17. – Otras cuestiones generales

No aplicable.

Historia de las revisiones:

VERSIÓN Y MODIFICACIÓN	FECHA DE EMISIÓN	DESCRIPCIÓN	MOTIVO DEL CAMBIO
Versión 1.6	22/09/2010	Política de Certificación	Licenciamiento AC ONTI
Versión 2.0	12/2014	Actualización Política Única de Certificación	Revisión
Versión 3.0	01/2019	Actualización Política Única de Certificación	Revisión
Versión 4.0.	08/2022	Actualización Política Única de Certificación	Revisión Adecuación a la Resolución ex SIP N° 946/2021

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
Date: 2022.08.11 09:55:51 -03:00

Luis Mariano PAPAGNI
Subsecretario
Subsecretaría de Innovación Administrativa
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2022.08.11 09:55:52 -03:00