República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Anexo de Resolución

Número: ACTO-2022-84144485-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Viernes 12 de Agosto de 2022

Referencia: Manual de Procedimientos AC ONTI

INFRAESTRUCTURA DE FIRMA DIGITAL – REPÚBLICA ARGENTINA

LEY N° 25.506

MANUAL DE PROCEDIMIENTOS

AUTORIDAD CERTIFICANTE

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI)

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 Manual describe el conjunto de procedimientos utilizados por la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante AC ONTI) en el cumplimiento de sus responsabilidades para la emisión, renovación, revocación y administración de los certificados digitales emitidos a favor de sus suscriptores, en el marco de la Ley N° 25.506 de Firma Digital y su modificatoria Ley N° 27.446, su Decreto Reglamentario N° 182/2019 y modificatorios, la Resolución N° 946/2021 de la (ex) SECRETARÍA DE INNOVACIÓN PÚBLICA y demás normas reglamentarias. Este conjunto de normas y procedimientos regula el accionar de la AC ONTI y de sus Autoridades de Registro.

Este Manual de Procedimientos forma parte de la documentación técnica emitida por la AC ONTI junto con los siguientes documentos:

a) Política Única de Certificación.

b) Acuerdo con Suscriptores.

c) Términos y Condiciones con Terceros Usuarios.

d) Política de Privacidad.

e) Plan de Cese de Actividades.

f) Plan de Seguridad.

g) Plan de Contingencia.

h) Descripción de la Plataforma Tecnológica.

i) Descripción de sus servicios.

1.2. - Nombre e Identificación del Documento.

Nombre: Manual de Procedimientos correspondiente a la Política Única de Certificación de la Autoridad Certificante de la Oficina Nacional de Tecnologías de Información (AC ONTI) a cargo de 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 un futuro las reemplacen.

Versión: 4.0

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

Sitio de publicación: https://www.argentina.gob.ar/modernizacion/firmadigital/documentosaconti

OID: 2.16.32.1.1.3

Lugar de publicación: Ciudad Autónoma de Buenos Aires, República Argentina.

1.3. – Participantes.

Este Manual de Procedimientos es aplicable a:

a) La AC ONTI que emite certificados digitales para:

- 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.
- Personas Jurídicas Públicas que actúen como Autoridad de Sello de Competencia.
- Servicio OCSP de consulta sobre el estado de un certificado.
- Otros servicios en relación a la firma digital (art. 33 Anexo I Resolución ex SIP N° 946/2021).

b) Las Autoridades de Registro (en adelante ARs) que se constituyan en el ámbito de aplicación de la Política Única de Certificación de la AC ONTI.

c) Los solicitantes y suscriptores de certificados digitales emitidos por la AC ONTI, en el ámbito de aplicación de la mencionada política.

d) Los terceros usuarios que verifican firmas digitales basadas en certificados digitales emitidos por la AC ONTI, en el ámbito de aplicación de la mencionada política.

1.3.1. – Certificador

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, presta los servicios de certificación, de acuerdo con los términos de la Política Única de Certificación.

1.3.2. - Autoridad de Registro.

La AC ONTI posee una estructura compuesta por ARs, las que serán responsables de efectuar las funciones establecidas en el apartado 1.3.2 de la Política Única de Certificación de la AC ONTI versión 4.0.

Las entidades o jurisdicciones que tengan interés en constituirse como Autoridades de Registro de la AC ONTI,

deberán solicitarlo a ésta por intermedio de un funcionario de jerarquía no inferior a subsecretario o equivalente, dependiendo la estructura organizacional de que se trate, o por intermedio del presidente de la entidad en caso de Entes Públicos no estatales. La solicitud debe efectuarse a través de los procedimientos electrónicos que determine 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, 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 Autoridades de Registro, entre los que se cuenta la capacitación de sus Oficiales de Registro, de los Responsables de Soporte Técnico de Firma Digital y de los Responsables de la Autoridad de Registro, así como la presentación de un seguro de caución cuando correspondiere. El curso de capacitación deberá ser aprobado únicamente por los Oficiales de Registro y los Responsables de Soporte Técnico de Firma Digital. Cumplidos los requisitos mencionados, la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA elevará un informe y el proyecto de disposición autorizando la conformación de la Autoridad de Registro 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 disposición en su cuenta de usuario TAD, en caso de corresponder, o en su cuenta de usuario GDE, sin perjuicio de su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

Las ARs 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 la 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 instalación fija o en modalidad 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

Es responsabilidad de la organización donde se constituye la AR asegurar la disponibilidad de todos los roles, como así también de los servicios prestados por la AR a los usuarios de sus aplicaciones informáticas, garantizando la continuidad operativa. Asimismo, ante la desvinculación de integrantes designados en los roles indicados, se deberán designar los reemplazos correspondientes. Bajo ninguna circunstancia estas responsabilidades recaerán en la AC ONTI. Los Oficiales de Registro y Responsables de Soporte Técnico de Firma Digital designados, deberán cumplir idénticas condiciones y aprobar las mismas actividades de capacitación como requisito para ser autorizada su designación.

Las Autoridades de Registro de la AC ONTI cuentan con los siguientes roles y funciones:

RESPONSABLES DE LA AUTORIDAD DE REGISTRO:

- Son los nexos formales de comunicación entre el Responsable de la AC ONTI y la Autoridad de Registro.
- Designan a quienes desempeñarán los roles dentro de la Autoridad de Registro (Oficiales de Registro y Responsables de Soporte Técnico de Firma Digital).
- Controlan el cumplimiento de la Política Única de Certificación de la AC ONTI y del presente Manual de Procedimientos, en las partes que resulte aplicable.
- Mantienen informada a la AC ONTI, mediante comunicación oficial en la Plataforma de Trámites a Distancia (TAD) o en el sistema de Gestión Documental Electrónica (GDE), sobre cualquier modificación en la conformación de la AR, en los siguientes casos: designación o baja de Oficiales de Registro, Responsable de Soporte Técnico de Firma Digital, alta y baja de dominios asociados a la AR, domicilio físico donde se encuentre constituida la AR y sobre las aplicaciones que utilicen los certificados de la AC ONTI.

Se sugiere designar más de un Responsable de AR, en función de las características de la misma.

OFICIALES DE REGISTRO:

- Son los responsables de ejecutar la operatoria principal de la AR, así como también de cumplir con las obligaciones, funciones y recaudos de seguridad que la AC ONTI le delega.
- Aprueban solicitudes de certificados de firma digital a partir de la validación de la identidad del solicitante, de la titularidad de su clave pública y de los demás datos de la solicitud según las pautas establecidas por la Política Única de Certificación y por el presente Manual.
- Rechazan solicitudes de certificados que no cumplen con los requisitos establecidos por la Política Única de Certificación y por el presente Manual.
- Aprueban solicitudes de renovación de certificados de firma digital según las pautas establecidas por la Política Única de Certificación y por el presente Manual.
- Aprueban las solicitudes de revocación de certificados de firma digital, siguiendo las pautas de la Política Única de Certificación y del presente Manual.
- Informan a los suscriptores de sus derechos, obligaciones y condiciones técnicas necesarias.
- Cumplen las funciones establecidas en el Plan de Cese de Actividades en el caso de cese de operaciones de la

AC ONTI.

- Las Autoridades de Registro deben designar para su conformación al menos DOS (2) Oficiales de Registros.

RESPONSABLE DE SOPORTE TÉCNICO DE FIRMA DIGITAL:

- Instruyen acerca de las buenas prácticas de utilización de la tecnología de firma digital expresada en la Política Única de Certificación de la AC ONTI.
- Identifican y reconocen los dispositivos criptográficos que cumplan con la certificación de NIST FIPS 140-2 Nivel 2 o superior que requieren los solicitantes de certificados.
- Cumplen las funciones de Mesa de Ayuda de la AR.
- Asisten a los solicitantes o suscriptores en el ámbito de su AR en la tramitación de los servicios provistos por la AC ONTI y en el manejo de la operatoria de la tecnología de firma digital de las distintas aplicaciones que requieran su uso.

1.3.2.1. Consideraciones en las operaciones de la AR para funcionar en puesto móvil.

Cuando la AR requiera funcionar en puesto móvil, se deberán adoptar las siguientes medidas para la operación de sus ORs:

- Realizar el proceso de aprobación de solicitudes en recintos donde no haya personal ajeno al proceso, cerciorándose de que no existan cámaras, dispositivos de captura de imágenes o aberturas que permitan la visualización externa del proceso de aprobación y generación de claves, ni otros datos de creación de firma digital.
- Utilizar equipamiento propio de la AR (PC o Notebook), que garantice la seguridad de la información, similares a las utilizadas en las instalaciones fijas (sistema operativo y antivirus actualizados y con soporte, así como otras configuraciones de seguridad aplicables).
- Los procedimientos de los ORs en las actividades relativas a la autenticación de la identidad de solicitantes y procesamiento de las solicitudes son idénticos a los realizados en las instalaciones fijas de la AR.

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 certificados para ser usados en relación con el servicio *"Online 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 ex SIP N° 946/2021.

1.3.4. - Terceros Usuarios.

Son Terceros Usuarios de los certificados emitidos bajo la Política Única de Certificación asociada a este Manual de Procedimientos, 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 Política Única de Certificación asociada a este Manual de Procedimientos 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 del Manual de Procedimientos.

1.5.1. - Organización Administradora del Documento.

Será responsable del presente Manual de Procedimientos 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

1.5.2. – Contacto.

El responsable del registro, mantenimiento e interpretación del presente Manual de Procedimientos es el máximo responsable de la AC ONTI, cuyos datos de contacto figuran en el apartado anterior.

1.5.3. - Organismo encargado de aprobar el Manual de Procedimientos.

El presente Manual de Procedimientos ha sido aprobado 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 respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política de 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 modificatorias.

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

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

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.

Certificado digital: Documento digital firmado digitalmente por un certificador licenciado, que vincula los datos de verificación de firma a su titular (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. (artículo 17 de la Ley N° 25.506).

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

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

OCSP - Protocolo en línea del estado de un certificado (“*Online 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"*).

SITSP – SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO.

SIP – (EX) SECRETARÍA DE INNOVACIÓN PÚBLICA.

SSIA – SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA.

ST – Responsable de Soporte Técnico de Firma Digital.

TAD – Plataforma de Tramites 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 emite 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 del derecho de la AC ONTI de reclamar a la AR 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 Entes 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 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 la 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 que pudiera hacerse de los certificados, tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.

La AC 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 este Manual.

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 AR sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán acordes a lo establecido 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 la Política Única de Certificación, vinculada a este Manual.

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 la Política Única de Certificación vinculada a este Manual.

Todos los trámites realizados por las ARs 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 su servicio de OCSP son administrados en forma directa por la AC ONTI.

La AC ONTI mantiene un repositorio en línea de acceso público que contiene:

- Su certificado digital.
- El certificado de la Autoridad Certificante Raíz, en sus versiones vigentes y anteriores.
- Repositorio de certificados digitales emitidos y su estado.
- Su certificado OCSP.
- La Lista de Certificados Revocados (CRL).
- El listado de las Autoridades de Registro vinculadas a la AC ONTI.
- La Política Única de Certificación en sus versiones vigentes y anteriores.
- El Manual de Procedimientos, en sus versiones vigentes y anteriores.
- El Acuerdo con Suscriptores.
- Los Términos y Condiciones con Terceros Usuarios.
- La Política de Privacidad.
- Información referida a la fecha de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.

La información antedicha se encuentra disponible en el sitio web de la AC ONTI en https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/a cap durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento.

El procedimiento de emisión y publicación de la CRL y de las delta CRL se ejecuta en forma automática por la aplicación de la AC ONTI.

2.2. - Publicación de información del certificador.

La AC ONTI garantizará 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 Nº 946/2021.

La AC ONTI se encuentra 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 Política Única de Certificación.

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 no establece restricciones de acceso a la Política Única de Certificación, al Acuerdo con Suscriptores,

a los Términos y Condiciones con Terceros Usuarios, a este Manual de Procedimientos y a toda otra documentación técnica de carácter público que emita.

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

Se garantiza la actualización del Listado de Autoridades de Registro cada vez que cualquiera de los datos de las mismas 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 de Certificación y del 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 modificatorias 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 Autoridades de Registro 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 siguiente.

3.1.2. - Necesidad de Nombres Distintivos.

Los atributos mínimos incluidos en los certificados con el fin de identificar unívocamente a su titular se encuentran definidos en el apartado 3.1.2. de la Política Única de Certificación.

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 Política Única de Certificación vinculada a este Manual de Procedimientos 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 decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite el certificado debe demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2. - Registro inicial.

La AC ONTl emite certificados a los solicitantes que cumplan con los requisitos para ser suscriptor, efectuándose una validación de su identidad, para lo cual se requiere su presencia física ante la AR.

1. El solicitante del certificado de persona humana efectuará los siguientes procedimientos:

    a) Como paso previo deberá obtener el dispositivo criptográfico y la documentación necesaria para la tramitación.

b) El solicitante ingresa al sitio web de la AC ONTI https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/a cap y selecciona el trámite de solicitud de certificado que desea realizar.

c) Completa el formulario de envío de datos con los datos requeridos.

d) Recibe el correo electrónico enviado por la aplicación de la AC ONTI. A continuación, siguiendo las instrucciones allí detalladas, si corresponde, hace clic en el link de verificación del correo electrónico.

e) Instala el certificado de la AC-Raíz y el de la AC ONTI y establece el certificado de la AC-Raíz como certificado de confianza.

f) Se presenta personalmente ante la AR seleccionada previamente con el dispositivo criptográfico con el fin de continuar el trámite de solicitud.

Al momento de presentación del solicitante, el Oficial de Registro efectúa el siguiente procedimiento:

a) Ingresa a la aplicación de la AC ONTI https://pki.jgm.gov.ar/ar/Default.aspx disponible en el sitio web de la AC ONTI y se autentica con su certificado como Oficial de Registro.

b) Valida la identidad del solicitante mediante la verificación de la documentación remitida.

c) Efectúa la captura, validación y guarda de los datos biométricos del solicitante.

d) Verifica que el dispositivo criptográfico presentado por el solicitante cumple con los requisitos tecnológicos exigidos en la Política Única de Certificación (apartado 6.1.1).

Esta verificación deberá ser efectuada por alguno de los Responsables de Soporte Técnico de Firma Digital de la Autoridad de Registro. En caso de que el dispositivo no cumpla con los requisitos exigidos, no se continuará con el trámite de solicitud, rechazando la misma e informando al solicitante de tal situación.

El solicitante efectúa el siguiente procedimiento en la computadora habilitada por el OR, con el fin de realizar la solicitud de su certificado a partir de los datos que figuran en el sistema de la AC ONTI:

a) Verifica que los datos que figuran en el sistema de la AC ONTI para los cuales va a realizar la solicitud son suyos y son correctos.

b) Lee y acepta el Acuerdo con Suscriptores en el que se hace referencia a la Política Única de Certificación que respalda la emisión del certificado.

c) Inserta su dispositivo criptográfico en la computadora, genera su par de claves y envía su solicitud a la AC ONTI de acuerdo con lo establecido en el apartado 3.2.1.

Cumplidos los pasos anteriores, el Oficial de Registro continúa con el siguiente procedimiento:

a) Verifica la coherencia de toda la documentación de respaldo presentada por el solicitante contra la registrada en la solicitud de certificado que generó el solicitante en el ítem c).

b) De no haberse interrumpido el trámite desde el momento de la solicitud realizada por el solicitante hasta el momento de la aprobación por parte del Oficial de Registro, y habiendo este realizado las verificaciones del ítem anterior, el OR procederá a firmar digitalmente en el sistema la aprobación de la solicitud de certificado del solicitante.

Los procedimientos de registro inicial de los certificados de Personas Jurídicas Públicas y de Aplicaciones serán reglamentado 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.

Se admitirá que las Autoridades de Registro de la AC ONTI desarrollen su actividad en puestos móviles, previa autorización del Ente Licenciante. En tal caso los procedimientos de registro inicial serán los mismos que los descriptos en el presente apartado.

La AC ONTI se obliga a cumplir con las disposiciones de la Política Única de Certificación, con el Manual de Procedimientos vinculado a la misma, con las cláusulas del Acuerdo con Suscriptores y con la normativa aplicable a firma digital.

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

El solicitante o suscriptor generará su par de claves criptográficas usando su propio equipamiento durante el proceso de solicitud del certificado. Las claves son generadas y almacenadas por el solicitante, no quedando almacenada la clave privada en el sistema informático de la AC ONTI.

El solicitante de un certificado de persona humana debe realizar la generación de su par de claves y el almacenamiento de la clave privada generada en un dispositivo criptográfico. El solicitante enviará a la AC ONTI una solicitud de certificado, en formato PKCS#10, para permitir implementar la prueba de posesión de la clave privada, remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

La aplicación de la AC ONTI comprobará que la solicitud recibida es válida, de este modo se garantiza que la persona que realizó la solicitud está en posesión de la clave privada asociada y que la información transmitida no ha sido alterada.

Luego de verificar la validez de la firma digital de la solicitud, la aplicación procede a generar un Código de Solicitud el cual identifica unívocamente la solicitud recibida; este código será utilizado por la AC ONTI vinculada para comprobar que el solicitante está en posesión de la clave privada asociada con el mismo sin tomar conocimiento o acceso alguno a dicha clave privada.

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 AR 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:

<u>Para personas jurídicas públicas:</u>

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.

<u>Entes públicos no estatales:</u>

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.

Según lo establecido en la Política de Certificación asociada a este Manual de Procedimientos, la AC ONTI emite certificados para personas humanas que cumplan con los requisitos para ser suscriptor, efectuándose una validación de la identidad del solicitante. En los casos de la emisión de un nuevo certificado se exige la presencia física del solicitante ante la Autoridad de Registro, quien deberá presentar el Documento Nacional de Identidad argentino. El OR deberá verificar que la foto del DNI corresponde efectivamente al solicitante que se está presentando ante él.

La AR efectúa la captura, validación y guarda de la fotografía del rostro y de las huellas dactilares del solicitante del certificado utilizando un dispositivo biométrico.

La Autoridad de Registro verifica que el dispositivo criptográfico utilizado por el solicitante, cumple 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.

Adicionalmente, la AC ONTI celebra un Acuerdo con Suscriptores con el solicitante o suscriptor, 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.

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.

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. del presente Manual, las ARs 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 o jurídicas, 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 o de 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.

Un suscriptor de un certificado de persona humana podrá solicitar la revocación de su certificado digital ingresando al sitio web de la AC ONTI: https://pki.jgm.gov.ar/app y accediendo a la sección correspondiente a este trámite. Podrá realizarlo directamente cuando aún se encuentre en posesión de su clave privada o bien suministrando su documento de identidad y el código de revocación provisto al momento de la emisión del certificado. En ambos casos la revocación se efectuará en forma automática. Caso contrario, deberá presentarse personalmente ante una AR, acreditando su identidad con su documento de identidad. Cumplido dicho procedimiento, el Oficial de Registro

solicitará a la AC la revocación del certificado del suscriptor.

En el caso de certificados de Aplicaciones o Persona Jurídica Pública, la persona humana a cargo de la custodia de la clave privada podrá solicitar su revocación enviando una nota por sistema de Gestión Documental Electrónica – GDE o en la Plataforma de Trámites a Distancia (TAD), según el caso.

En caso de que la solicitud no fuera efectuada por el suscriptor, la misma deberá ser remitida a la AR, de acuerdo con lo establecido en el apartado 4.9.2, indicando las causas que motivaron la solicitud de revocación. Cumplido dicho procedimiento, por medio de alguno de sus Oficiales de Registro, la Autoridad de Registro solicitará a la AC la revocación del certificado.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1. - Solicitud de certificado.

4.1.1. - Solicitantes de certificados.

Los requerimientos técnicos con los que deberá contar el solicitante a fin de iniciar el proceso de solicitud se encuentran publicados en sitio web de la AC ONTI https://www.argentina.gob.ar/servicio/solicitar-certificado-de-firma-digital-por-hardw are-token. En caso de necesitar asistencia respecto de este tema o de los trámites que provee la AC ONTI, deberá requerirla al Responsable de Soporte Técnico de Firma Digital de la AR. Los datos de contacto de dichos responsables se encuentran en el Listado de Autoridades de Registro publicado en el sitio web de la AC ONTI.

4.1.2. - Solicitud de certificado

El proceso de solicitud debe ser iniciado:

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.

A continuación, se describe el proceso que debe ejecutar el solicitante para tramitar una solicitud de certificado. Las claves deberán ser generadas en un dispositivo criptográfico que deberá cumplir con los requerimientos establecidos en el apartado 6.1.1 de la Política Única de Certificación. A tal fin se deberá ejecutar el siguiente procedimiento:

1. Obtención de la documentación de respaldo según lo establecido en el apartado 3.2.3 del presente

Manual.

2. Ingreso al sitio web de la AC ONTI https://www.argentina.gob.ar/servicio/solicitar-certificado-de-firma-digital-por-hardw are-token y selección del trámite de solicitud. Allí también se indicarán los requerimientos técnicos que debe poseer el equipo del solicitante.

3. Ingreso de datos de Identidad del solicitante:

Deberá completar el formulario de solicitud de certificado con los datos que serán incluidos en el certificado. En relación al número de CUIL/CUIT, deberá ingresar los datos requeridos por la aplicación a fin de efectuar su validación de identidad: Nombre y apellido, sexo, fecha de nacimiento, DNI. Dicha validación será efectuada luego por el Oficial de Registro al momento de procesar la solicitud del certificado, según se indica en el apartado 4.2. del presente Manual.

4. Ingreso de datos adicionales y de solicitud:

a. Caso Certificado de persona humana: deberá completar los datos del formulario con la siguiente información:

i. Correo electrónico:

ii. Datos de localidad: deberá completar los siguientes campos:

1. Provincia.

2. Localidad

En caso de haber otros campos además de los indicados el solicitante deberá completarlos ingresando: NO APLICA.

b. Caso Certificado de Aplicaciones: deberá iniciar un trámite en la Plataforma de Trámites a Distancia (TAD) o el sistema de Gestión Documental Electrónica – GDE, según el caso, y completar los datos del formulario.

5. *Selección de la Autoridad de Registro*: de acuerdo al ámbito de aplicación establecido en el apartado 1.3.2, el sistema desplegará automáticamente la lista completa de Autoridades de Registro en pantalla a fin de que el solicitante pueda efectuar la selección correspondiente; el usuario deberá seleccionar una AR a fin de poder continuar con el trámite de solicitud.

6. *Confirmación y envío de Datos de Solicitud:* a continuación, la aplicación mostrará en pantalla todos los datos proporcionados por el solicitante que irán incluidos en el certificado a emitir, a la vez que tendrá la posibilidad de aceptar o cancelar el envío de sus datos de solicitud a la ACONTI. En caso de haber recibido correctamente los datos la aplicación mostrará una pantalla que indica que los datos se recibieron correctamente, a la vez que se le informará que recibirá un correo electrónico.

7. *Recepción del correo electrónico de verificación:* la aplicación envía un correo electrónico al solicitante que contendrá un link para proseguir el trámite. El solicitante debe acceder al mencionado link para confirmar a la AC ONTI que la dirección de correo electrónico ingresada es la correcta y que posee acceso a la cuenta de correo declarada. El solicitante deberá realizar esta validación como paso previo obligatorio a la presentación ante la AR que seleccionó anteriormente.

8. *Verificación de la cuenta de correo electrónico:* al haber accedido al link de verificación accederá al sitio web de la AC ONTI donde aparecerá un mensaje en pantalla informando al usuario:

- Que su correo electrónico fue verificado.
- Que debe llevar el dispositivo criptográfico.
- Que debe presentarse personalmente ante un Oficial de Registro de la AR que seleccionó previamente.
- La documentación que debe remitir a la AR.
- El listado con la dirección y demás datos de la AR, los datos de contacto del OR y del Responsable de Soporte Técnico de Firma Digital.

9. *Instalación de los certificados de la AC-Raíz de la República Argentina y de la AC ONTI:* a continuación, la aplicación le indicará las instrucciones para que el solicitante efectúe la instalación de los certificados mencionados. Una vez instalados, debe establecer el certificado de la AC-RA como certificado de confianza. También encontrará los datos de contacto del Responsable de Soporte Técnico de Firma Digital de la AR para el caso en que necesite asistencia técnica.

10. *Presentación personal del solicitante ante la AR:* el solicitante deberá solicitar un turno a través del sitio https://turnos.argentina.gob.ar/turnos/seleccionTurno/327, elegir la Autoridad de Registro y el horario en el que deberá presentarse personalmente ante la AR con el dispositivo criptográfico utilizado y su documento de identidad. El solicitante deberá elegir la misma AR que seleccionó en el punto 5 cuando completo el formulario con sus datos de solicitud.

4.2. - Procesamiento de la solicitud del certificado.

El procesamiento de la solicitud del certificado finaliza con su aceptación o rechazo por parte de la AR.

En todos los casos, el OR cumple los siguientes pasos:

- Verifica que el solicitante, de acuerdo con las pautas establecidas en el presente Manual, cumpla con los requisitos que prueben su carácter de suscriptor para la correspondiente Política Única de Certificación.
- Verifica la existencia de la solicitud en la aplicación de la AC ONTI.
- Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida.
- Verifica la titularidad de la solicitud siguiendo el procedimiento de validación establecido en el presente Manual.
- Realiza la captura fotográfica y de la huella dactilar del solicitante en el sistema establecido por la AC ONTI.

Se describe a continuación el proceso que debe ejecutar el OR para aceptar o rechazar una solicitud de certificado de persona humana, indicándose los pasos generales para el procesamiento de dicha solicitud de certificado; para ello el OR deberá realizar la validación de la identidad de la persona que se presenta ante la AR, que en todos los casos será una persona humana.

La AR deberá previamente validar que el dispositivo criptográfico que utilizó el solicitante para realizar la solicitud cumple con los requerimientos establecidos en el apartado 6.1.1 de la Política Única de Certificación. Además,

también deberá cumplir con los requerimientos de configuración del dispositivo criptográfico que establezca la AC ONTI en su sitio web.

A fin de visualizar la Nota de Envío de Datos efectuada por el solicitante el OR ejecutará el siguiente procedimiento:

1. *Autenticación como OR:* ingresa a la aplicación de la AC ONTI disponible en el sitio web de la AC ONTI y se autentica con su certificado como OR.

2. *Verificación de la existencia de la solicitud de envío de datos del solicitante:* para ello el OR ingresa a la aplicación de la AC ONTI donde visualiza el listado de todas las solicitudes de envío de datos que se encuentren bajo su visibilidad, una vez identificada la solicitud debe seleccionarla a fin de poder visualizarla.

3. *Validación de la identidad del solicitante:*

Validación del documento de identidad: Debe verificar que el documento de identidad presentado es válido, para ello deberá comprobar que corresponde a la persona que se presentó, validando que la foto del documento corresponda a la persona que se presentó y que el tipo y número del documento de identidad presentado coincide con el que figura en la solicitud registrada en el sistema de la AC ONTI. Así también, deberán capturar la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital utilizando el servicio de verificación de identidad provisto por el REGISTRO NACIONAL DE LAS PERSONAS o el que en el futuro lo reemplace.

4. *Aceptación de la solicitud de envío de datos:* al visualizar la solicitud el OR podrá continuar con el trámite de solicitud o rechazarla en caso de corresponder. En caso de rechazarla el solicitante deberá iniciar nuevamente el trámite de Envío de Datos; se debe tener presente que deberá volver a validar su cuenta de correo electrónico, por lo que deberá tener acceso a ella. En caso de que el OR continúe con el trámite de solicitud accederá a la pantalla de generación de la solicitud de certificado.

Para continuar con el trámite de solicitud, el OR deberá retirar su token e insertar en la computadora el dispositivo criptográfico del solicitante, que fuera previamente validado por la AR. El procedimiento descripto a continuación deberá ser ejecutado por el solicitante desde la computadora habilitada por el OR:

5. *Confirmación de datos y aceptación del Acuerdo con Suscriptores:* desde la pantalla de generación de solicitud, el solicitante debe aceptar el Acuerdo con Suscriptores en el cual se establecen los derechos y obligaciones que contrae el solicitante en su calidad de tal y como futuro suscriptor de un certificado.

6. *Generación del par de claves:* desde la pantalla de generación de solicitud, el solicitante efectuará la solicitud del certificado para lo cual procederá a generar su par de claves en su token de acuerdo a lo establecido en el apartado 3.2.1. El solicitante deberá establecer los controles de acceso exclusivo en su token de manera de que aseguren que él es el único capaz de acceder a su clave privada.

7. *Envío de la Solicitud de certificado:* el solicitante envía su solicitud a la AC ONTI. La aplicación verifica que la solicitud sea válida y procede a generar un Código de Solicitud (Hash). En caso de haberse validado correctamente la aplicación muestra una pantalla que indica que el trámite se inició correctamente.

Una vez realizado el procedimiento anterior concluye la generación de la solicitud de certificado por parte del solicitante. El OR deberá a continuación retirar el token del solicitante de la computadora e insertar su propio token a fin de poder continuar operando.

El procedimiento descripto a continuación deberá ser ejecutado por el OR:

8. *Validación de la identidad del solicitante:*

8.1. Validación del CUIT/CUIL: Debe verificar el número de CUIT / CUIL, pudiendo presentarse los siguientes casos:

I. Realizar la validación mediante el sitio web de ANSES utilizando como datos de entrada los que figuran en el documento de identidad presentado por el solicitante.

II. Realizar la validación consultando el número de CUIL del solicitante al dorso del Documento de Identidad presentado por el solicitante (sólo disponible en los nuevos DNI).

9. A continuación, para el caso de certificados de personas humanas, de no haberse interrumpido el trámite desde el momento de realizada la solicitud por el solicitante en el punto 8 hasta el momento actual de la aprobación, el OR podrá aprobar la solicitud del certificado de la persona humana que fue validada; caso contrario, se procederá a rechazar la solicitud.

10. Finalización de trámite de solicitud:

Efectuados los mencionados controles, el Oficial de Registro podrá:

a) Aprobar la solicitud, en tal caso cambia la misma al estado “Solicitud aprobada para su emisión”.

b) Rechazar la solicitud, cambiando su estado a “Solicitud rechazada por la Autoridad de Registro”. En tal caso se envía automáticamente un correo electrónico al solicitante informando el rechazo de la solicitud y los motivos que la ocasionaron, finalizando el trámite. La solicitud podrá ser rechazada por alguna de las siguientes causas:

- Por no haberse presentado toda la documentación requerida.
- Por inconsistencias en la documentación presentada o entre esta y la solicitud registrada en el sistema de la AC ONTI.
- Debido a cualquier otro motivo que impida la validación de los datos del certificado o la ejecución de este procedimiento.
- Por pedido expreso del solicitante.
- Por haber transcurrido VEINTE (20) días desde el momento de inicio del trámite de solicitud sin haber sido completado.
- Por inconsistencia de los datos biométricos con los datos de identidad.
- En caso de haberse interrumpido el proceso desde el punto 8 hasta el momento de la aprobación de dicha solicitud, o en caso de que el OR no haya estado presente en algún momento durante el lapso antes mencionado.

11. Una vez aprobada la solicitud por el OR y emitido el certificado por la AC ONTI, el OR deberá insertar en su computadora el dispositivo criptográfico del suscriptor a fin de realizar la instalación del certificado.

Transcurrido un plazo de VEINTE (20) días hábiles, las solicitudes pendientes de aprobación serán automáticamente rechazadas.

Toda la documentación de respaldo del proceso de validación de la identidad de los solicitantes y suscriptores de certificados se resguarda por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

4.3. - Emisión del certificado.

4.3.1. - Proceso de emisión del certificado.

Cumplidos los recaudos del proceso de validación de identidad, titularidad de la clave pública y de otros datos de los solicitantes de acuerdo con lo establecido en este documento y la Política Única de Certificación y una vez aprobada la solicitud de certificado por la AR, la AC ONTI procederá a emitir el certificado digital firmándolo digitalmente; posteriormente el mismo será puesto a disposición del suscriptor.

Al emitirse el certificado se genera un código de revocación, que podrá ser utilizado luego por el suscriptor en el circuito de revocación para realizar dicha operación en caso de que este no posea acceso a su clave privada.

El solicitante deberá almacenar la clave privada, el certificado emitido y conservar el código de revocación.

Los certificados emitidos por la AC ONTI tienen los siguientes períodos de validez a partir de su fecha y hora de emisión:

- Certificados de personas humanas: DOS (2) años.
- Certificados de aplicaciones: TRES (3) años.
- Certificados de personas jurídicas públicas: DOS (2) años.
- Certificados de Autoridad de Sello de Competencia: DOS (2) años.
- Certificados de Autoridad de Sello de Tiempo: DOS (2) años.

4.3.2. - Notificación de emisión.

La notificación de la emisión del certificado de personas humanas se efectúa a través de un correo electrónico remitido por la aplicación de la AC ONTI a la cuenta de correo electrónico declarada por el suscriptor o representante autorizado al momento de iniciar la solicitud de certificado.

La AC ONTI enviará un correo electrónico al suscriptor notificándolo de la emisión del certificado, el cual contendrá un link desde el cual podrá acceder al sitio web de la AC ONTI para realizar la descarga del certificado como un archivo en caso de ser necesario.

En el mismo correo electrónico se le enviará el código de revocación mencionado en el apartado 4.3.1.

4.4. - Aceptación del certificado.

Cumplidas las condiciones establecidas en el apartado 4.3 de la Política Única de Certificación, un certificado se considera aceptado por su titular una vez que ha sido emitido por la AC ONTI y dicha emisión notificada por correo electrónico a la cuenta declarada por dicho titular.

Cumplidos estos pasos, la AC ONTI procederá a publicar el certificado emitido en su sitio web.

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

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

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

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

b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable.

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

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

De acuerdo a lo establecido en la Resolución ex SIP N° 946/2021:

- Resguardar y no divulgar aquellos factores de autenticación (contraseñas de usuario, PIN) que permitan utilizar la clave privada.
- Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.
- Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la Política Única de Certificación.
- Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

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 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, debe proceder a la revocación de dicho certificado y de ser necesario, tramitar uno nuevo.

4.9. - Suspensión y Revocación de Certificados.

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

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

4.9.1. - Causas de revocación.

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

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados de aplicaciones.
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por acto administrativo de la Autoridad de Aplicación debidamente fundado.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
- 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.

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

4.9.2. - Autorizados a solicitar la revocación.

Se encuentran autorizados a solicitar la revocación de un certificado emitido por la AC 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) La AC ONTI o una de sus AR.

e) El Ente Licenciante.

f) La Autoridad Judicial competente.

g) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación.

El suscriptor puede solicitar la revocación de su certificado siguiendo el siguiente procedimiento:

a) El suscriptor ingresa a la aplicación disponible en https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/firmadigital/a cap y selecciona la opción “Revocar”. A continuación, elige una de las siguientes opciones:

I. Se autentica con su certificado digital.

II. Ingresa con el pin de revocación que le fue suministrado al momento de descarga de su certificado y su número de documento de identidad.

b) El suscriptor completa el campo Motivo (obligatorio) y el Detalle (optativo).

c) Al presionar el botón “Revocar”, la aplicación solicita la reconfirmación de la revocación.

d) Confirma la solicitud de revocación de su certificado.

e) La aplicación solicita al sistema la revocación del certificado.

f) La AC ONTI revoca el certificado y actualiza el estado del certificado a “Certificado revocado”.

g) La aplicación avisa a través de un correo electrónico al suscriptor que su certificado ha sido revocado.

Solo en caso de que el suscriptor no pueda revocar su certificado por los métodos antes mencionados deberá presentarse personalmente con su documento de identidad ante la AR.

Con el fin de efectuar la revocación de un certificado digital el Oficial de Registro de la AR realiza el siguiente procedimiento:

a) En caso de que el suscriptor se presente ante la AR para solicitar la revocación, con el fin de verificar su identidad, el OR le requerirá su documento de identidad.

b) Ingresa a la aplicación y selecciona el certificado que desea revocar de la lista de certificados vigentes.

c) De corresponder verifica que el documento de identidad presentado por el suscriptor coincida en número con el CUIT/CUIL que figura en el certificado.

d) Efectúa una captura de fotografía y/o de la huella dactilar del solicitante de la revocación utilizando un dispositivo biométrico

e) Verifica los datos de la solicitud y certificado seleccionado.

f) Completa el campo Motivo (obligatorio, entre las opciones que se muestran) y Detalle (optativo).

g) Al presionar el botón Revocar, la aplicación requiere una reconfirmación de la revocación.

h) Confirma la revocación del certificado.

i) La aplicación solicita al sistema la revocación del certificado.

j) Actualiza el estado del certificado a “Certificado revocado”.

k) La aplicación avisa a través de un correo electrónico al suscriptor que su certificado ha sido revocado.

4.9.4. - Plazo para la solicitud de revocación.

Las solicitudes de revocación se gestionan en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1 y se hayan cumplido los procedimientos previstos en el apartado 4.9.3.

La AC ONTI dispone de un servicio de recepción de solicitudes de revocación que se encuentra disponible en forma permanente SIETE (7) x VEINTICUATRO (24) horas a través de la aplicación web de la AC ONTI.

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

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

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

Los Terceros Usuarios, al momento de verificar una firma digital, están obligados a comprobar el estado de validez de los certificados mediante el control de la Lista de Certificados Revocados o, en su defecto, mediante el servicio en línea de consultas sobre el estado de los certificados (OCSP) descripto en el apartado 4.9.9. 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 con una frecuencia diaria con listas complementarias (delta CRL) en modo horario.

4.9.8.- Vigencia de la lista de certificados revocados.

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

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

La verificación del estado de validez de un certificado podrá efectuarse por alguno de los siguientes métodos:

Mediante el acceso a la lista de certificados revocados disponible en el sitio http://pki.jgm.gob.ar/crl/FD.crl

- Mediante el servicio en línea de consulta sobre el estado de los certificados (OCSP) disponible en el sitio web http://pki.jgm.gob.ar/ocsp

Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento. La AC ONTI garantiza el acceso permanente, eficiente y gratuito del público en general al servicio.

El usuario podrá descargar en forma manual o a través de sus aplicaciones los archivos correspondientes a la CRL completa y las delta CRL horarias. Ambas CRL tienen la extensión de archivo “.crl”. Las delta CRL se identificarán con el mismo nombre de la CRL asociada, con el agregado del signo “+” y un número, indicando la secuencia.

Las delta CRL son acumulativas o incrementales respecto a las anteriores delta CRL correspondientes a un período determinado (en este caso de 24 horas) y la CRL asociada. Las delta 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

Al momento de verificar una firma digital, con el fin de comprobar el estado de validez del certificado, los terceros usuarios deberán tener en cuenta que una vez que un certificado es revocado, esta circunstancia será reflejada en el servicio OCSP y en la próxima delta CRL a publicarse, en un plazo máximo de UNA (1) hora desde el momento de efectuada la revocación. Debido a esto y con el fin de efectuar la correcta verificación del estado de validez de un certificado, los terceros usuarios deberán poseer la CRL correspondiente a las últimas VEINTICUATRO (24) horas y todas las deltas CRL asociadas hasta las DOS (2) últimas posteriores al momento de recepcionado el documento firmado cuyo certificado se desea validar.

Ante la falta de disponibilidad del sitio principal de publicación de la CRL, se cuenta con una instalación alternativa que responderá en forma inmediata a cualquier requerimiento de acceso y descarga de dicha lista, con idénticas prestaciones que el sitio principal.

Se cuenta asimismo con un segundo punto de distribución de la CRL que responderá en caso de que no se encuentre disponible el punto de distribución principal. Este segundo punto de distribución se encuentra disponible en http://pkicont.jgm.gob.ar/crl/FD.crl

Ante la falta de disponibilidad del servicio OCSP, se prevé un sitio alternativo que podrá ser accedido para su consulta, con idénticas prestaciones que el servicio principal, disponible en http://pkicont.jgm.gob.ar/ocsp.

Los certificados digitales emitidos por la AC ONTI contienen la dirección de Internet de ambos puntos de distribución de la Lista de Certificados Revocados, como así también del servicio en línea de consulta sobre revocación de los certificados.

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

Para verificar en línea el estado de un certificado, la aplicación del usuario realizará una consulta sobre su estado a partir de la dirección de Internet http://pkicont.jgm.gob.ar/ocsp

El formato de la petición se realiza según la sintaxis ASN.1. El servicio “OCSP responder” de la AC ONTI devuelve los siguientes valores: “bueno" (*good*), "revocado" (r*evoked*) o "desconocido" (*unknown*), para cada uno de los certificados para los que se ha efectuado una consulta. Adicionalmente, como respuesta se puede devolver un código de error. Las respuestas se firman digitalmente con la clave privada correspondiente al certificado OCSP emitido bajo titularidad de la AC ONTI, excepto en el caso del código de error antes referido.

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

La AC ONTI no utiliza otros medios para la divulgación del estado de revocación de los certificados que los contemplados en su Política Única de Certificación y cuyos procedimientos se encuentran descriptos en el presente

Manual.

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

El suscriptor del certificado es responsable de efectuar su revocación o bien de comunicar de inmediato de tal situación a la AR por algunas de las vías indicadas en el apartado 4.9.3 cuando se den algunas de las siguientes causas:

a) Por compromiso o sospecha de compromiso de la clave privada.

b) Por pérdida de la clave privada.

c) Porque ya no sea posible su utilización.

d) Ante el conocimiento de que esta ya no sea segura para operar.

e) Por cualquier otra circunstancia que el suscriptor considere que pueda resultar perjudicial a la seguridad de su clave privada.

La AC ONTI operará en consecuencia a lo establecido en la Política Única de Certificación vinculada al presente Manual, procediendo a la revocación del certificado correspondiente y a notificar al suscriptor a través de un correo electrónico de dicha circunstancia. Asimismo, procederá a actualizar la CRL y la delta CRL correspondiente y a su publicación de acuerdo a lo establecido en el apartado 4.9.9.

4.9.13. - Causas de suspensión.

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

4.9.14. - Autorizados a solicitar la suspensión.

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

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.

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.

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:

- Lista de certificados revocados (CRL).
- Servicio OCSP.
- 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 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 que abarca desde la emisión de la última CRL hasta el momento de emisión de dicha delta CRL; dicho período nunca superará las VEINTICUATRO (24) horas. Esta información se encontrará firmada digitalmente por 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.

Los servicios descriptos se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento, a partir de su sitio web https://www.argentina.gob.ar/jefatura/innovacion-tecnologica/innovacion-administrativa /firma-digital/autoridad-certificante-de-la

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, de no poseer otro certificado, 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 inciso b) del artículo 21 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 inciso a) del artículo 25 de la ley antes mencionada, el suscriptor de un certificado emitido en el marco de la Política Única de Certificación asociada a este Manual de Procedimientos 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 de los mismos 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 I 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 inciso i) del artículo 21 de la Ley N° 25.506 respecto a los certificados emitidos.

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

e) Procedimientos de resguardo de los registros.

f) Sistemas de recolección y análisis de registros.

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 I 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 la 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 la AC ONTI implica la emisión de un nuevo certificado por parte de la ACR-RA. Si la clave privada de la 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 certificado, si correspondiese.

5.7. - Compromiso y recuperación ante desastres

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

Se han desarrollado procedimientos referidos a:

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

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

c) Recuperación ante compromiso o sospecha de compromiso de la clave privada de la AC 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 otros 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.

En relación a la custodia de archivos y documentación, la AC ONTI o la Autoridad de Registro que hubiera cesado. cumplen con idénticas exigencias de seguridad.

Se contempla lo establecido por el artículo 44 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el artículo 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 ARs, 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 la Política Única de Certificación vinculada a este Manual 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.

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.

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 utilizados para firmar digitalmente, para funciones de autenticación y para cifrado.

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

La protección de la clave privada es considerada desde la perspectiva de la AC ONTI, de los repositorios, de las ARs y de los suscriptores. Para cada una de estas entidades se abordan los siguientes temas:

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

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

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

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

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

f) Procedimiento de destrucción de la clave privada.

g) Requisitos aplicables al dispositivo criptográfico utilizado para el almacenamiento de las claves privadas.

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, en cada caso, los medios y los dispositivos referidos en el apartado 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 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 los OR y de los suscriptores. Estos deberán proceder a la revocación del certificado y a tramitar una nueva solicitud de emisión de certificado, si así correspondiere. 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.

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

6.2.5. - Archivo de clave privada.

La AC ONTI almacena la copia de reguardo de su clave privada a través de un procedimiento que garantiza su integridad, disponibilidad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación, de acuerdo a lo dispuesto por la Resolución 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 (HSM) conforme a lo establecido en la Política Única de Certificación vinculada a este Manual. En el caso de las copias de resguardo, también están soportados en dispositivos criptográficos (HSM) homologados FIPS 140-2 Nivel 3.

El par de claves criptográficas de las ARs y de los suscriptores de certificados es almacenado en el mismo dispositivo criptográfico con certificación FIPS 140-2 Nivel 2 o superior donde se genera, 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.

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

6.2.8. - Método de activación de claves privadas.

Para la activación de la clave privada de la AC 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 con certificación 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 los 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 usuarios 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, instruirá 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 AR, 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:

- Control de acceso a los servicios y roles afectados al proceso de certificación.
- Separación de funciones entre los roles afectados al proceso de certificación.
- Identificación y autenticación de los roles afectados al proceso de certificación.
- Utilización de criptografía para las sesiones de comunicación y bases de datos.
- Archivo de datos históricos y de auditoría de la AC ONTI y usuarios.
- Registro de eventos de seguridad.
- Prueba de seguridad relativa a servicios de certificación.
- Mecanismos confiables para identificación de roles afectados al proceso de certificación.
- 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:

- Separación de ambientes de desarrollo, prueba y producción.
- Control de versiones para los componentes desarrollados.
- 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 SUBSECRETARIA DE INNOVACION ADMINISTRATIVA de la SECRETARÍA DE INNOVACIÓN TECNOLÓGICA DEL SECTOR PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

6.8. – Certificación de fecha y hora.

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.

En relación a los perfiles de los certificados, resulta de aplicación lo establecido en el apartado 7.1. de la Política Única de Certificación.

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.

En relación al perfil de la lista de certificados revocados, resulta de aplicación lo establecido en el apartado 7.2. de la Política Única de Certificación.

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.

De acuerdo a lo dispuesto en el artículo 10 del Decreto N° 561/2016, la DNFDEIT, en su calidad de administrador de la AC ONTI, se encuentra sujeta a las auditorías que lleva a cabo la SINDICATURA GENERAL DE LA NACIÓN (SIGEN).

La mencionada entidad realiza las auditorías en base a sus programas que son generados por la Autoridad de Aplicación y 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 es publicada en forma permanente e ininterrumpida en su sitio web.

La AC ONTI cumple las exigencias reglamentarias impuestas por:

- 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.
- 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 la Ley N° 25.506, su Decreto Reglamentario Nº 182/2019 y modificatorios, y de las disposiciones de la Política Única de Certificación vinculada a este Manual.

Asimismo, en virtud de lo establecido en el Decreto Nº 182/2019, 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.

Toda información referida a solicitantes o suscriptores de certificados que sea recibida por la AC ONTI o por sus Autoridades de Registro, será tratada en forma confidencial y no puede hacerse pública sin el consentimiento previo de los titulares de los datos, salvo que sea requerida por un juez en un proceso judicial o autoridad competente en un procedimiento administrativo. La exigencia se extiende a toda otra información referida a los solicitantes y los suscriptores de certificados a la que tenga acceso la AC ONTI o sus ARs durante el ciclo de vida del certificado.

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

9.3.1. - Información confidencial.

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente o por autoridad administrativa competente en el marco de 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 especifique en la Política Única de Certificación vinculada a este Manual. Asimismo, se considera confidencial cualquier información:

- 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.
- Almacenada en cualquier soporte, incluyendo aquella que se transmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
- Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes a la AC ONTI.

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

9.3.2. - Información no confidencial

La siguiente información recibida por la AC ONTI o por sus ARs no es considerada confidencial:

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

b) Información sobre personas humanas o jurídicas públicas que se encuentre disponible en certificados o

en directorios de acceso público.

c) Políticas de Certificación y Manual 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 de juez competente mediante resolución fundada en causa judicial o ante requerimiento de autoridad administrativa competente, en el marco de 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 escrita del suscriptor del certificado.

No será necesario el consentimiento cuando:

- Los datos se hayan obtenido de fuentes de acceso público irrestricto;
- Los datos se limiten a nombre, Documento Nacional de Identidad, identificación tributaria o previsional u ocupación.
- 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 la AC 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 del presente Manual de Procedimientos 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 AR, los suscriptores, los terceros usuarios y otras entidades participantes, se originan en lo establecido por la Ley N° 25.506, su Decreto Reglamentario Nº 182/2019, la Resolución ex SIP N° 946/2021 y en las disposiciones de la Política Única de Certificación.

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 Política Única de Certificación vinculada a este Manual 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 Política Única de Certificación vinculada a este Manual y en los Términos y Condiciones con Terceros Usuarios.

Los criterios de valoración que seguirá la AR sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán 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 la Política Única de Certificación vinculada a este Manual.

9.9. – Compensaciones por daños y perjuicios.

No aplicable.

9.10. – Condiciones de vigencia.

El presente Manual de Procedimientos se encontrará vigente a partir de la fecha de su aprobación por parte del Ente Licenciante y hasta tanto sea reemplazado por una nueva versión. Toda modificación en el Manual de Procedimientos, una vez aprobada por el Ente Licenciante, será debidamente comunicada al suscriptor.

9.11.- Avisos personales y comunicaciones con los participantes.

No aplicable.

9.12.- Gestión del ciclo de vida del documento.

No se agrega información.

9.12.1. - Procedimientos de cambio.

Toda modificación al Manual de Procedimientos es aprobada 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, 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 y la que en el futuro la remplace.

El Manual de Procedimientos es sometido 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.

Toda modificación en el Manual de Procedimientos será comunicada 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.

El presente Manual de Procedimientos será revisado y actualizado 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 del presente Manual de Procedimientos 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 del Manual de Procedimientos, deberá ser resuelto en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N| 1759/72 T.O. 2017 y/o la Ley N° 19.983, según corresponda.

El presente Manual de Procedimientos se encuentra en un todo subordinado 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 modificatorias, el Decreto Nº 182/2019 y modificatorios, la Resolución ex SIP N° 946/2021, las Resoluciones ex 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 incluyen cláusulas adicionales.

9.17. – Otras cuestiones generales

No aplicable.

Historia de las revisiones:

VERSIÓN Y MODIFICACIÓN	FECHA DE EMISIÓN	DESCRIPCIÓN	MOTIVO DEL CAMBIO
Versión 2.0	08/2015	Actualización Manual de	Adecuación DA N°

		Procedimientos	927/2014
Versión 3.0	12/2018	Actualización Manual de Procedimientos	Actualización documentación AC ONTI
Versión 4.0.	08/2022	Actualización Manual de Procedimientos	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: 2022.08.12 12:50:49 -03:00

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