INFRAESTRUCTURA DE FIRMA DIGITAL – REPÚBLICA ARGENTINA

LEY Nº 25.506

MANUAL DE PROCEDIMIENTOS

POLÍTICA ÚNICA DE CERTIFICACIÓN de la AC ONTI

DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA

SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA

SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA

SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN

JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN

Versión 3.0

Enero 2019

ÍNDICE

1. – INTRODUCCIÓN.

1.1. - Descripción general.

El presente Manual describe el conjunto de procedimientos utilizados por la AC ONTI administrada por la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA dependiente de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN, en cumplimiento de sus responsabilidades para la emisión 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 modificatoria Ley N° 27.446, su Decreto Reglamentario Decreto N° 2628 del 19 de diciembre de 2002, la Resolución N° 399-E/2016 del entonces MINISTERIO DE MODERNIZACIÓN, la Resolución Nº 37-E/2016 de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del ex MINISTERIO DE MODERNIZACIÓN y demás normas reglamentarias. Este conjunto de normas y procedimientos regula el accionar de AC ONTI y de sus Autoridades de Registro.

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

a) Política Única de Certificación.
b) Plan de Seguridad (incluyendo política y procedimientos de seguridad).
c) Plan de Continuidad de Operaciones.
d) Plan de Cese de Actividades.
e) Acuerdo con Suscriptores.
f) Términos y Condiciones con Terceros Usuarios.
g) Política de Privacidad.
h) Plataforma Tecnológica.

i) Requerimientos para la Conformación de las Autoridades de Registro.

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 a cargo de la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

.

Versión: 3.0

Fecha de aplicación: Enero 2019

Sitio de publicación: http://pki.jgm.gov.ar/docs/Manual_de_Procedimientosv3.0.pdf

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) AC ONTI que emite certificados digitales para:
   i) Personas Humanas.
   ii) Servicio OCSP.
b) Las Autoridades de Registro (en adelante AR) que se constituyan en el ámbito de la Política Única de Certificación.
c) Los solicitantes y suscriptores de certificados digitales emitidos por AC ONTI, en el ámbito de la mencionada Política.

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

1.3.1. – AC ONTI.

La Autoridad Certificante de la Oficina Nacional de Tecnologías de Información (en adelante, AC ONTI), administrada por la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN 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, responsables de efectuar las funciones de validación de identidad, de la titularidad de la clave pública asociada y de otros datos de los solicitantes y suscriptores de certificados digitales.

Las entidades públicas y privadas que tengan interés en constituirse como Autoridades de Registro de la AC ONTI, deberán solicitarlo por intermedio de su máxima autoridad, a la AC ONTI, a través de los procedimientos electrónicos que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, en el sistema de Gestión Documental Electrónica – GDE o en la Plataforma de Trámites a Distancia (TAD), según el caso, informando la modalidad (fija o móvil).

Con dicha solicitud, la AR deberá proporcionar determinada información y acompañar documentación con carácter de Declaración Jurada, en los términos de los Artículos 109 y

110 del Reglamento de Procedimientos Administrativos Decreto 1759/72 T.O. 2017 aprobado por el Decreto N° 894/2017.

La AC 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 y de los RESPONSABLES DE SOPORTE TÉCNICO, así como la presentación de un seguro de caución cuando correspondiere, entre otros. Cumplidos los requisitos mencionados, la AC ONTI elevará un informe y solicitará autorización a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

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

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

Las AR 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.

El plazo de guarda de la documentación respaldatoria de la emisión o revocación de los certificados digitales es de DIEZ (10) años a partir de la fecha de vencimiento o revocación. Su conservación se realizará por los medios establecidos por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

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

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

Toda la información vinculada a las AR conformadas en la AC ONTI, se encuentra disponible en el sitio web de la AC ONTI: https://pki.jgm.gov.ar

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, etc.) debe ser presentada por los interesados únicamente a través de la plataforma de Trámites a Distancia (TAD), o del sistema de Gestión Documental Electrónica – GDE en caso de corresponder. A tal fin, la Autoridad de Registro debe constituir una cuenta de usuario en la Plataforma de Trámites a Distancia (TAD) como requisito previo a su autorización para operar en tal carácter, en el caso de no disponer de un usuario en el sistema de Gestión Documental Electrónica - GDE.

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

a) RESPONSABLES DE LA AUTORIDAD DE REGISTRO:

Son los nexos formales de comunicación entre el Responsable de la AC-ONTI y la Autoridad de Registro, con las siguientes funciones:

i. Designan a quienes desempeñarán los roles dentro de la Autoridad de Registro (Oficiales de Registro y Responsables de Soporte Técnico de Firma Digital).

ii. Controlan el cumplimiento de la Política Única de Certificación de la AC ONTI.

iii. Mantienen informado mediante Comunicación Oficial en la Plataforma de Trámites a Distancia (TAD) o del sistema de Gestión Documental Electrónica – GDE a la AC ONTI sobre cualquier modificación en la conformación de la AR: designación o

desvinculación 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, dependiendo de las características de la AR.

b) 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, en particular:

i. Aprobar 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.
ii. Rechazar solicitudes de certificados que no cumplen con los requisitos establecidos en la Política Única de Certificación y en el presente Manual.
iii. Revocar certificados siguiendo las pautas de la Política Única de Certificación y el presente Manual.
iv. Informar a los suscriptores de sus derechos, obligaciones y condiciones técnicas necesarias.
v. Cumplir las funciones establecidas en el Plan de Cese de Actividades en el caso de cese de operaciones de la AC ONTI.

Deben designarse al menos DOS (2) ORs.

Los Oficiales de Registro de las AR deben ser personas que tengan una relación de empleo con la AR. En caso de no existir una relación de empleo, deberán solicitar autorización a la AC ONTI, acreditando su idoneidad. Los OFICIALES DE REGISTRO deben acreditar la aprobación del curso de capacitación brindado por la AC ONTI.

c) RESPONSABLE DE SOPORTE TÉCNICO DE FIRMA DIGITAL:

Ejercen las siguientes funciones:

i. Instruir acerca de las buenas prácticas de utilización de la tecnología de firma digital expresada en la Política Única de Certificación de la AC ONTI.

ii. Identificar y reconocer los dispositivos criptográficos que cumplan con la certificación de NIST FIPS 140-2 Nivel 2 o superior que requieren los solicitantes de certificados.

iii. Cumplir las funciones de Mesa de Ayuda de la AR.

iv. Asistir 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.

Es responsabilidad de la organización donde se constituye la AR asegurar la disponibilidad de todos los roles mencionados anteriormente, 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, e informar a la AC ONTI para su autorización por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA. Bajo ninguna circunstancia estas responsabilidades recaerán en la AC ONTI. Los Oficiales de Registro y Responsables de Soporte Técnico designados en reemplazo de los autorizados,

deberán cumplir idénticas condiciones y aprobar las actividades de capacitación como requisito para ser autorizada su designación.

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

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

El suscriptor declara que la información contenida en el certificado digital es fidedigna, en los términos de los Artículos 109 y 110 del Reglamento de Procedimientos Administrativos Decreto 1759/72 T.O. 2017 aprobado por el Decreto N° 894/2017.

Toda la información vinculada a las AR conformadas en la AC ONTI, se encuentra disponible en su sitio web: https://pki.jgm.gov.ar/

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

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

a) 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.

b) 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).

c) 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 las personas humanas, que requieran un certificado digital para firmar digitalmente cualquier documento o transacción, pudiendo ser utilizados para cualquier uso o aplicación, como así también para autenticación o cifrado.

La AC 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 de aplicación y presta el servicio de sello de tiempo, según lo dispuesto en el artículo 9° de la Resolución MM N° 399-E/2016° del 5 de octubre de 2016.

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 al Anexo I del Decreto N° 2628/2002 del 19 de diciembre de 2002 y modificatorios.

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. - Responsable del documento.

Será responsable del presente Manual de Procedimientos la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN, con los siguientes datos:
Correo electrónico: consultapki@modernizacion.gob.ar

1.5.2. – Contacto.

El presente Manual de Procedimientos es administrado por el máximo responsable de la AC ONTI, cuyos datos de contacto figuran en el apartado anterior.

1.5.3. - Procedimiento de aprobación del Manual de Procedimientos.

El presente Manual de Procedimientos ha sido presentado ante la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN durante el proceso de licenciamiento y con ocasión de su modificación, y ha sido aprobado por el correspondiente acto administrativo.

1.6. - Definiciones y Acrónimos.

1.6.1. – Definiciones.

ACUERDO CON SUSCRIPTORES: Establece los derechos y obligaciones de las partes 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 GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN es la Autoridad de Aplicación de la Infraestructura de Firma Digital establecida por la Ley N° 25.506 y modificatorias.

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

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).

CERTIFICACIÓN DIGITAL DE FECHA Y HORA: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. (Anexo al Decreto N° 2628 de fecha 19 de diciembre de 2002).

ENTE LICENCIANTE: La SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA constituyen el Ente Licenciante.

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

MANUAL DE PROCEDIMIENTOS: Conjunto de prácticas utilizadas por el AC ONTI licenciado en la emisión y administración de los certificados. En inglés: *"Certification Practice Statement"* (CPS). (Anexo al Decreto N° 2628/02)

PLAN DE CESE DE ACTIVIDADES: Conjunto de actividades a desarrollar por el AC ONTI licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02)

PLAN DE CONTINUIDAD DE LAS OPERACIONES: Conjunto de procedimientos a seguir por el AC ONTI licenciado 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 del AC ONTI licenciado. (Anexo al Decreto N° 2628/02).

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

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

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

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

1.6.2. – Acrónimos.

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

AC ONTI - Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN dependiente de la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA.

AR – Autoridad de Registro

CRL - Lista de Certificados Revocados (*"Certificate Revocation List"*).

CUIL - Clave Única de Identificación Laboral.

CUIT - Clave Única de Identificación Tributaria.

DNTEID - DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA

DNSAFD - DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACION Y FIRMA DIGITAL.

FIPS - Estándares Federales de Procesamiento de la Información (*"Federal Information Processing Standard"*).

GDE – Sistema de Gestión Documental Electrónica

HSM – Módulo de Seguridad de Hardware (*"Hardware Security Module"*).

IEC – *"International Electrotechnical Commission".*

IETF – *"Internet Engineering Task Force".*

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 – Contraseña que protege la clave privada del suscriptor, deberá contener como mínimo un largo de 8 caracteres requiriendo utilizar mayúsculas, minúsculas y números.**PKCS #10** - Estándar de solicitud de certificación (*"Public-Key Cryptography Standards"*).

RFC – *"Request for Comments"*.

RSA - Sistema Criptográfico de Clave Pública (*"Rivest, Shamir y Adleman"*).

SHA-256 - Algoritmo de Hash Seguro (*"Secure Hash Algorithm"*).

SGM JGM – SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

SMA – SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

TAD – Plataforma de Trámites a Distancia del sistema de Gestión Documental Electrónica – GDE.

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

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

Conforme a lo dispuesto por la Ley N° 25.506, la relación entre AC ONTI que emite un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la citada ley y demás legislación vigente. 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 los 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 36 del Decreto N° 2628/02 y sus modificatorios, establece la responsabilidad de AC ONTI respecto de las Autoridades de Registro.

En ese sentido prescribe que una AR puede constituirse como única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo delegar su operatoria en otras Autoridades de Registro, siempre que medie la aprobación de la AC ONTI y de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

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 AR, sin perjuicio del derecho de la AC ONTI de reclamar a la AR las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

Las Autoridades de Registro pertenecientes al sector privado que serán conformadas en la AC ONTI, previa autorización de la SECRETARÍA DE MODERNIZACIÓN 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:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados digitales y que no estén expresamente previstos en la Ley N° 25.506;
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el AC ONTI pueda demostrar que ha tomado todas las medidas razonables.

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

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

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

La AC ONTI no asume responsabilidad:

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

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

c) en aquellos casos de eventuales inexactitudes en los datos contenidos en el certificado que resulten de información facilitada por el suscriptor del certificado y que hubieran sido

objeto de verificación de acuerdo con los procedimientos establecidos en la Política Única de Certificación y en el Manual de Procedimientos

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

2.1. – Repositorios.

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

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

a) Su certificado digital.

b) El certificado de la Autoridad Certificante Raíz.

c) Repositorio de certificados digitales emitidos y su estado.

d) Su certificado OCSP.

e) La lista de certificados revocados (CRL).

f) El listado de las Autoridades de Registro vinculadas al AC ONTI.

g) La Política Única de Certificación en sus versiones vigentes y anteriores.

h) El Manual de Procedimientos en sus aspectos de carácter público, en sus versiones vigentes y anteriores.

i) El Acuerdo con Suscriptores.

j) Los Términos y Condiciones con Terceros Usuarios.

k) La Política de Privacidad.

l) Información relevante 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://pki.jgm.gov.ar/app 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 la AC ONTI.

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

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

a) Su certificado OCSP.
b) Las Políticas de Certificación anteriores.
c) Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.
d) Las versiones anteriores de certificados de la ACR-RA.

La AC ONTI se encuentra obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en el artículo 21, inc. k) de la Ley N° 25.506, el artículo 34 inc. g), h) y m) del Decreto N° 2628/02 y sus modificatorios, y en la 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://pki.jgm.gov.ar/app

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 en sus aspectos de carácter público y a toda otra documentación técnica de carácter público que emita.

2.3. - Frecuencia de publicación.

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

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

2.4. - Controles de acceso a la información.

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

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

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

3. - IDENTIFICACIÓN Y AUTENTICACIÓN.

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

3.1.- Asignación de nombres de suscriptores.

3.1.1. - Tipos de Nombres.

El nombre a utilizar es el que surge de la documentación presentada por el solicitante, de acuerdo al apartado 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 UN (1) 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 al documento de identidad del suscriptor. Las discrepancias o conflictos que pudieran generarse cuando los datos de los 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 es único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias se basa en la utilización del número de CUIL / CUIT. Si se suscribiera más de UN (1) certificado con el mismo CUIL / CUIT, los certificados se 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 aplicación 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 ONTI 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.

I. El solicitante del certificado efectuará los siguientes procedimientos:

a) Como paso previo deberá obtener el dispositivo criptográfico y la documentación necesaria de acuerdo al tipo de certificado que desea tramitar según corresponda a lo establecido en el apartado 3.2.2. o 3.2.3. La misma será remitida a través de la Plataforma de Trámites a Distancia (TAD) o del sistema de Gestión Documental Electrónica – GDE en caso de corresponder.

b) El solicitante ingresa al sitio web de la AC ONTI https://pki.jgm.gov.ar/app 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 y siguiendo las instrucciones allí detalladas, si corresponde, hace click 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 o suscriptor, el Oficial de Registro efectúa el siguiente procedimiento:

a) Ingresa a la aplicación de la AC-ONTI 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 toma de la foto y huella dactilar 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) Debe leer y aceptar el Acuerdo con Suscriptores en el que se hace referencia a la Política 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 remitida 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.

Como alternativa, se admitirá que las Autoridades de Registro de la AC ONTI desarrollen adicionalmente su actividad en puestos móviles, previa autorización de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA. 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 certificados de personas humanas 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

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 o la AR 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 o Privadas.

Este apartado resulta aplicable únicamente para los casos de emisión de certificados de aplicaciones, a fin de autenticar la identidad de la persona jurídica titular de la aplicación.

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 titular de la aplicación.

b) La AC ONTI o la AR, en su caso, 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 titular de la aplicación deberá ser verificada mediante los procedimientos que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, mediante clave fiscal AFIP, los administradores de relaciones y

apoderamientos contemplados en la plataforma de Trámites a Distancia (TAD) del sistema de Gestión Documental Electrónica – GDE.

En todos los casos, la personería y calidad de representante y/o apoderado se acreditará en la plataforma de Trámites a Distancia (TAD) mediante la clave fiscal AFIP, el administrador de relaciones y apoderamiento.

Para personas jurídicas:

a) La acreditación del carácter de representante legal o apoderado de la persona autorizada a iniciar el trámite se realizará de acuerdo con los procedimientos para el administrador de relaciones y para apoderamiento en la Plataforma de Trámites a Distancia (TAD) que determine la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

Para entidades públicas:

1. Nota del órgano con competencia dentro del organismo para gestionar el certificado.
2. La nota debe incluir el nombre de la aplicación, servicio o unidad operativa responsable.

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

El responsable autorizado o a cargo de la aplicación debe firmar un acuerdo que contenga la confirmación de que la información incluida en el certificado es correcta.

Todos los documentos anteriormente detallados, tanto para entidades públicas o privadas, serán presentados por los interesados 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, de acuerdo a lo que establezca la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

La AC ONTI y la AR cumplen con lo dispuesto en el artículo 21 incíso f) de le Ley N° 25.506 relativo a la recolección de datos personales.

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 únicamente emite certificados para personas humanas que cumplan con los requisitos para ser suscriptor, efectuándose una validación de la identidad del solicitante. En todos los casos se exige la presencia física del solicitante o suscriptor del certificado ante la Autoridad de Registro; la verificación se efectuará mediante la presentación de la siguiente documentación, la que deberá ser remitida a través de la Plataforma de Trámites a Distancia (TAD) o del sistema de Gestión Documental Electrónica – GDE en caso de corresponder:

a) De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.
b) De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.
c) Adicionalmente, la AR efectuará una captura fotográfica del rostro y de la huella dactilar del solicitante del certificado utilizando un dispositivo biométrico homologado.

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

La Autoridad de Registro deberá verificar que el dispositivo criptográfico utilizado por el solicitante, cumple con las especificaciones técnicas establecidas por la SECRETARÍA DE

MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN.

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 34, inciso i) del Decreto Nº 2628/02 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

d) El artículo 34, inciso m) del Decreto Nº 2628/02 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 punto 3.2.2., la AC ONTI o la AR verifican la autorización de la Persona Humana que actúa en nombre de la Persona Jurídica 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).

No aplicable

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

No aplicable

3.4. - Requerimiento de revocación.

Un suscriptor 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 cualquier AR vinculada a la AC ONTI ante la cual solicitará la revocación del certificado 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.

La persona humana a cargo de la custodia de la clave privada de certificados de aplicación, podrá solicitar su revocación enviando una nota por TAD.

En caso de que la solicitud no fuera efectuada por el suscriptor, deberá ser remitida a cualquier AR vinculada con la AC ONTI, 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. En caso de necesitar asistencia respecto de este tema o de los trámites que provee la AC ONTI deberá requerirla únicamente al Responsable de Soporte Técnico de Firma Digital de la AR a la cual realizará la solicitud. 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 solamente por el solicitante, en el caso de certificados de personas humanas, o bien por el representante legal o apoderado con poder suficiente a dichos efectos, en el caso de certificados de aplicación.

A continuación se describe el proceso que debe ejecutar el solicitante o responsable autorizado para tramitar una solicitud de certificado de persona humana o de aplicación con nivel de seguridad alto, o sea que las claves serán 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. Obtener la documentación de respaldo necesaria de acuerdo al tipo de certificado que desea tramitar según corresponda a lo establecido en el apartado 3.2.2. o 3.2.3.
2. Ingresar al sitio web de la AC ONTI https://pki.jgm.gov.ar/app y seleccionar el trámite de solicitud de acuerdo al tipo de certificado que desea obtener. Allí también se indicarán los requerimientos técnicos que debe poseer el equipo del solicitante.
3. Ingreso de datos de Identidad del solicitante:
    a. Caso de Certificado de Persona Humana: 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.

b. Caso de Certificado de Aplicación: se deberá ingresar el número de CUIL / CUIT del representante autorizado que gestionará la solicitud.

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 Aplicación: deberá completar los datos del formulario con la siguiente información:

i. Correo electrónico:

ii. Posición o función: este dato significa la relación que vincula a la persona humana que realiza la solicitud con la aplicación, esto es el cargo que posee la persona humana en el área de la organización o empresa donde se desempeña según lo establecido en la autorización que lo acredita como tal.

iii. Denominación de la persona jurídica: nombre de la persona jurídica

titular de la aplicación.

iv. Unidad operativa relacionada con el suscriptor: nombre que designa la unidad operativa relacionada con la persona jurídica titular de la aplicación.

v. CUIT de la organización: CUIT de la persona jurídica titular de la aplicación.

vi. Provincia.

vii. Localidad.

5. Seleccionar 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 AC-ONTI. 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 de esta 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:

a) Que su correo electrónico fue verificado.
b) Que debe llevar el dispositivo criptográfico.
c) Que debe presentarse personalmente ante un Oficial de Registro de la AR que seleccionó previamente; se sugiere que antes de hacerlo se ponga en contacto con el OR a fin de concertar el encuentro.
d) La documentación que debe remitir a la AR.
e) El listado con la dirección y demás datos de la AR, los datos de contacto del OR y del Soporte Técnico.

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-Raíz 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://argentina.gob.ar, 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 completó 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:

a) 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.
b) Verifica la existencia de la solicitud en la aplicación de la AC ONTI.
c) Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida.
d) Verifica la titularidad de la solicitud siguiendo el procedimiento de validación establecido en el presente Manual.
e) 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 emisión de certificado de persona humana o de aplicación. Se indican 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, para realizar el trámite para sí o como representante autorizado de una aplicación.

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 solicitud 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. Verifica 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, una vez identificada la solicitud debe seleccionarla a fin de poder visualizarla.
3. Validación de 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, para ello el OR deberá validar 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. Es requisito ineludible para la prosecución del trámite que la persona que va a realizar el trámite descripto a continuación sea el titular.
4. Aceptación de 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 o responsable autorizado 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 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 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 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 de acuerdo al tipo de certificado (persona humana o de aplicación) el OR deberá realizar el siguiente procedimiento:
   9.1. 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.

9.2. Certificados de aplicación: el OR deberá ejecutar adicionalmente el procedimiento que se detalla a continuación para la validación de la correspondiente persona jurídica titular de la aplicación:

a) Validación de la Nota de la máxima autoridad: verificará que la misma esté firmada por la autoridad competente antes mencionada.

b) Validación del responsable autorizado: verificará que los datos de identidad que figuran en la nota de la máxima autoridad del organismo coinciden con los datos de identidad del responsable autorizado.

c) Verificación de la identidad del titular: verificará que el nombre del Organismo que figura en la nota de la máxima autoridad del organismo coincide con el campo “Denominación de la Persona Jurídica” de la solicitud registrada en el sistema de la AC-ONTI.

d) Verificación del nombre del organismo con el campo Organización de la solicitud registrada en el sistema de la AC-ONTI.

Cumplido el procedimiento anterior el OR podrá proceder a la aprobación de la solicitud de certificado de aplicación de la persona jurídica pública que fue objeto de validación.

9.3. Personas jurídicas privadas: el OR deberá ejecutar adicionalmente el procedimiento que se detalla a continuación para la validación de la correspondiente persona jurídica:

a) Acreditación de la persona jurídica: mediante la clave fiscal de AFIP, el administrador de relaciones y el sistema de apoderamientos de la platafor,a de Trámites a Distancia (TAD).

b) Validación de la representación del responsable autorizado: ídem anterior.

c) Validación del responsable autorizado: verificará que los datos de identidad que figuran en el poder coinciden con los datos de identidad del responsable autorizado que figuran en el sistema de la AC-ONTI.

d) Verificación de la identidad del titular: verificará que el nombre de la persona jurídica que figura en la Constancia de inscripción del Registro Societario de la jurisdicción coincide con el campo “Denominación de la Persona Jurídica” que figura en la solicitud registrada en el sistema de la AC-ONTI y con el que figura en el poder en favor del responsable autorizado.

Cumplido el procedimiento anterior el OR podrá aprobar la solicitud de certificado de aplicación de la persona jurídica privada que fue objeto de validación.

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:

i. Por no haberse presentado toda la documentación requerida.

ii. Por inconsistencias en la documentación presentada o entre esta y la solicitud registrada en el sistema de la AC-ONTI.

iii. Debido a cualquier otro motivo que impida la validación de los datos del certificado o la ejecución de este procedimiento.

iv. Por pedido expreso del solicitante.

v. Por haber transcurrido 20 (VEINTE) días desde el momento de inicio del trámite de solicitud sin haber sido completado.

vi. Por inconsistencia de los datos biométricos con los datos de identidad.

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.
12. El Oficial de Registro deberá ingresar al sistema de registro biométrico de AC ONTI a fin de realizar el registro de la foto y huella dactilar del solicitante y demás datos de la solicitud.

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

Resguarda toda la documentación de respaldo del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, 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:

a) Certificados de personas humanas: DOS (2) años.

b) Certificados de aplicación de personas jurídicas Públicas o Privadas: TRES (3) 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 notificándole 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 a la 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 N° 399–E/2016 del ex MINISTERIO DE MODERNIZACIÓN, el suscriptor debe:

a) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.
b) Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la Política Única de Certificación.
c) Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores 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.

No aplicable

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 mediante la solicitud de revocación de certificado validada por la AR.

4.9.1. - Causas de revocación.

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

a) A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados de aplicación.
b) Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
c) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
d) Por Resolución Judicial.
e) Por Resolución de la Autoridad de Aplicación.

f) Por fallecimiento del titular.

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

h) Por declaración judicial de incapacidad del titular.

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

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

k) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.

l) Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02, la Resolución Nº 399-E/2016 del ex MINISTERIO DE MODERNIZACIÓN, la Resolución Nº 37-E de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del ex MINISTERIO DE MODERNIZACIÓN y demás normativa sobre firma digital.

m) Por revocación de su propio certificado digital.

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) El suscriptor del certificado.

b) El responsable autorizado por la Persona Jurídica titular de la aplicación o es titular del certificado.

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

d) La AC ONTI o cualquiera 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://pki.jgm.gov.ar/app 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 alguna de las AR vinculadas con la AC ONTI.

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 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) días por VEINTICUATRO (24) horas a través de la aplicación web de la AC ONTI.

El plazo máximo entre la revocación y la publicación del estado del certificado, indicando la revocación, es de VEINTICUATRO (24) horas.

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 disposición.

Los Terceros Usuarios están obligados a confirmar la validez de la lista 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 34, inciso g) del Decreto Nº 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la Resolución MM N° 399-E/2016 y sus correspondientes Anexos.

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

La AC 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:

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

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

La CRL se encuentra disponible SIETE (7) días por VEINTICUATRO (24) horas, sujeta 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 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.gov.ar/crl/FD+.crl y

http://pkicont.jgm.gov.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 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 delta CRL asociadas hasta las DOS (2) últimas posteriores al momento de recepcionado el documento firmado cuyo certificado se desea validar.

Las características operacionales de ambos servicios se encuentran disponibles en el sitio web: https://pki.jgm.gov.ar/app

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.gov.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.gov.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.gov.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" (revoked) 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 su clave privada 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 procederá de acuerdo 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 punto 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:

a) Lista de certificados revocados (CRL).

b) Servicio OCSP.

c) Servicio de búsqueda y consulta de certificados emitidos.

Cada lista de certificados revocados (CRL) emitida contendrá información sobre los números de serie de todos los certificados revocados 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 permite 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 está 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://pki.jgm.gov.ar/app

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.

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, 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 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 MM N° 399-E/2016.

b) Frecuencia de procesamiento de registros.

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

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

e) Procedimientos de resguardo de los registros.

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

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

h) Evaluación de vulnerabilidades.

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 I Sección 3 de la Resolución MM N° 399-E/2016 respecto del registro de eventos.

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

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

b) Período de guarda de los registros.

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

d) Procedimientos de resguardo de los registros.

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

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

g) Procedimientos para obtener y verificar la información archivada.

5.6. - Cambio de claves criptográficas.

El par de claves de la AC 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 AC-Raíz. 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. - Plan de respuesta a incidentes y recuperación ante desastres

Se describen los requerimientos relativos a la recuperación de los recursos de la AC ONTI en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Continuidad de las Operaciones (Plan de Contingencia) y en el Plan de Seguridad.

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 33 del Decreto Nº 2628/02 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8. - Plan de Cese de Actividades.

Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios de la AC ONTI o de una o varias de sus Autoridades Certificantes o de Registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, 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, se cumple con idénticas exigencias de seguridad que las previstas para la AC ONTI o su Autoridad de Registro que cesó.

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

6. - CONTROLES DE SEGURIDAD TÉCNICA.

Se describen las medidas de seguridad implementadas por la AC 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, AR, repositorios, suscriptores, etc.

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.

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

Los suscriptores de certificados de personas humanas deben generar y almacenar su par de claves utilizando un dispositivo criptográfico con certificación “Overall” FIPS 140 Versión 2 Nivel 2 o superior.

Las claves criptográficas utilizadas por los proveedores de otros servicios relacionados con la firma digital serán generadas y almacenadas por módulos criptográficos de software o utilizando dispositivos criptográficos FIPS 140-2 Nivel 2 o superior (hardware).

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

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 la Ley Nº 25.506, artículo 21, inciso b) y el Decreto Nº 2628/02, artículo 34, inciso i).

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

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

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

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

Todo solicitante de un certificado emitido bajo la Política Única de Certificación entrega su clave pública a la AC-ONTI durante el proceso de solicitud de su certificado. La AC-ONTI

por su parte utiliza técnicas de “prueba de posesión” para determinar que el solicitante se encuentra en posesión de la clave privada asociada a dicha clave pública.

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

El procedimiento descripto asegura que:

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

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

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

6.1.4. - Disponibilidad de la clave pública de la AC ONTI.

El certificado de la AC ONTI y el de la ACRaíz-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://pki.jgm.gov.ar/app

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 AR 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 punto 6.1.5.

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

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

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

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

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

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

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

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

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

f) Procedimiento de destrucción de la clave privada.

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

6.2.1. – Controles y estándares para dispositivos criptográficos.

Para la generación y el almacenamiento de las claves criptográficas, 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.

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

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

6.2.3. - Recuperación de clave privada.

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

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

6.2.4. - Copia de seguridad de clave privada.

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

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

6.2.5. - Archivo de clave privada.

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 MM N° 399-E/2016 en cuanto a los niveles de resguardo de claves.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

El par de claves criptográficas de la AC ONTI se genera y almacena en dispositivos criptográficos conforme a lo establecido en la Política Única de Certificación, salvo en el caso de las copias de resguardo que también están soportados en dispositivos criptográficos (HSM) homologados FIPS 140-2 nivel 3.

El par de claves criptográficas de las AR y de los suscriptores de certificados de personas humanas deberá ser generada y almacenada en un dispositivo criptográfico con certificación “Overall” FIPS 140 Versión 2 nivel 2 o superior, no permitiendo su exportación.

6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos.

El almacenamiento de las claves criptográficas 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 I de la Resolución MM N° 399-E/2016.

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

6.2.8. - Método de activación de claves privadas.

Para la activación de la clave privada de la AC-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 OR y suscriptores se utilizan dispositivos criptográficos con certificación “Overall” FIPS 140 Versión 2 Nivel 2 o superior.

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

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

6.3. - Otros aspectos de administración de claves.

6.3.1. - Archivo permanente de la clave pública.

Los certificados emitidos a los suscriptores, como así también el certificado de la AC-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 el 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 AR implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores o a sus dispositivos criptográficos.

6.4.2. - Protección de los datos de activación.

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.

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:

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

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

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

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

e) Archivo de datos históricos y de auditoría de la AC ONTI y usuarios.

f) Registro de eventos de seguridad.

g) Prueba de seguridad relativa a servicios de certificación.

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

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

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

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

6.5.2. - Requisitos de seguridad computacional.

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

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

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

Los dispositivos criptográficos utilizados por los proveedores de otros servicios en relación a la firma digital están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2 como mínimo para el caso de dispositivos criptográficos de hardware, o FIPS 140-2 Nivel 1 para el caso de módulos criptográficos de software.

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

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

6.6.1. - Controles de desarrollo de sistemas.

La AC ONTI cumple con procedimientos específicos para el diseño, desarrollo y prueba de los sistemas entre los que se encuentran:

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

b) Control de versiones para los componentes desarrollados.

c) Pruebas con casos de uso.

6.6.2. – Controles de gestión de seguridad

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

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

No aplicable.

6.7. - Controles de seguridad de red.

Los controles de seguridad de la red interna y externa de la AC ONTI se encuentran a cargo de la DIRECCIÓN NACIONAL DE INFRAESTRUCTURA TECNOLÓGICA Y CIBERSEGURIDAD dependiente de la SUBSECRETARÍA PAÍS DIGITAL de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN 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 9°, inc. b) de la Resolución MM Nº 399-E/16.Dicho servicio se implementa conforme a lo indicado en los estándares ETSI TS 102 023 *"Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities",* ETSI TS 101 861 *"Time stamping profile"* 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 III - Perfiles de los Certificados y de las Listas de Certificados Revocados de la Resolución MM N° 399–E/2016.

Perfil del certificado de PERSONA HUMANA.

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgoritm	sha256RSA (1.2.840.113549.1.1.11)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 2 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=APELLIDO Nombre
	serialNumber - 2.5.4.5	SERIALNUMBER=<CUIT/CUIL> <Número>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	public key algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null

Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectkeyIdentifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gov.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	ExtendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	SubjectAltName 2.5.29.17	Dirección de correo electrónico (campo optativo)
Información de Acceso de la AC	authorityInfo Access 1.3.6.1.5.5.7.1.1	[1]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://pki.jgm.gov.ar/aia/cafdONTI.crt [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)

		Nombre alternativo: Dirección URL=http://pkicont.jgm.gov.ar/aia/cafdONTI.crt [3]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pki.jgm.gov.ar/ocsp [4]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://pkicont.jgm.gov.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2 o superior)

Perfil del certificado de APLICACIÓN

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgoritm	sha256RSA (1.2.840.113549.1.1.11)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información

	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 3 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación de la Aplicación
	organizationName 2.5.4.10	O=nombre dela Persona Jurídica Pública responsable de la aplicación
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con la aplicación
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectkeyIdentifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl

Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gov.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Respuesta OCSP (1.3.6.1.5.5.7.3.9)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	Método = Emisor de autoridad de certificación URI = http://pki.jgm.gov.ar/aia/cafdONTI.crt Método = Emisor de autoridad de certificación URI = http://pkicont.jgm.gov.ar/aia/cafdONTI.crt Método = OCSP URI = http://pki.jgm.gov.ar/ocsp Método = OCSP URI = http://pkicont.jgm.gov.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.3 (claves generadas por disp. 140-2 nivel 3) OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.1 (claves generadas por software)

Perfil del certificado de proveedores de servicios de firma digital.

Para Autoridad de Sello de tiempo.

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)

Algoritmo de Firma	signatureAlgoritm	sha256RSA (1.2.840.113549.1.1.11)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiración a establecer por AC ONTI> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del servicio de emisión de sello de tiempo
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública o Privada responsable del servicio
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública o Privada>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.113549.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor

Puntos de Distribución de la Lista de sellos de tiempo Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gov.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gov.ar/cps/cps.pdf User notice = certificado emitido por un AC ONTI Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Certificación digital de fecha y hora (1.3.6.1.5.5.7.3.8)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	Método = Emisor de autoridad de certificación URI = http://pki.jgm.gov.ar/aia/cafdONTI.crt Método = Emisor de autoridad de certificación URI = http://pkicont.jgm.gov.ar/aia/cafdONTI.crt Método = OCSP URI = http://pki.jgm.gov.ar/ocsp Método = OCSP URI = http://pkicont.jgm.gov.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

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 III “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución MM N° 399–E/2016.

Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	1 (correspondiente a versión 2)
Algoritmo de Firma	signatureAlgorithm 1.2.840.113549.1.1.11	sha256RSA
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3 serialNumber - 2.5.4.5 organizationName - 2.5.4.10 organizationalUnitName - 2.5.4.11 stateOrProvinceName - 2.5.4.8 countryName - 2.5.4.6	CN=Autoridad Certificante de Firma Digital SERIALNUMBER=CUIT 30680604572 O=Jefatura de Gabinete de Ministros, Secretaría de la Gestión Pública, Subsecretaría de Tecnologías de Gestión OU=Oficina Nacional de Tecnologías de Información S=Ciudad Autónoma de Buenos Aires C=AR
Fecha efectiva	thisUpdate	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario
Próxima Actualización	nextUpdate	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 bytes que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.) Id. de clave=70 ba 03 71 7a d8 10 e4 ee 52 b5 7f 32 8f 9f 6c 2e f7 84 0d
Número de CRL	CRL Number	Número de la CRL
Puntos de Distribución del emisor	issuingDistributionPoints 2.5.29.28	[1]Punto de distribución CRL URL=http://pki.jgm.gob.ar/crl/FD.crl [2]Punto de distribución CRL URL=http://pkicont.jgm.gob.ar/crl/FD.crl Solo Contiene certificados de usuario = no Solo Contiene certificados de la entidad emisora = no Lista de revocación de Certificados Indirecta = no

Certificados Revocados (Revoked certificates)	InvalidityDate	<fecha y hora UTC>
	Serial Number	Número de Serie del Certificado Revocado
	ReasonCode	Motivo de la Revocación
Algoritmo de Identificación Huella Digital		SHA1 1.3.14.3.2.26
Versión de CA		V0.0
Siguiente Publicación de lista de revocación		<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

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

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

8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

De acuerdo a lo dispuesto en el artículo 34 de la Ley N° 25.506, modificada por su similar Nº 27.446, la DNTEID, 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 aprobados por la Autoridad de Aplicación y son comunicados e informados oportunamente.

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

Los informes resultantes de las auditorías son elevados a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA. Sus aspectos relevantes son publicados en forma permanente e ininterrumpida en su sitio web.

La AC ONTI cumple las exigencias reglamentarias impuestas por:

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

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

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1. – Aranceles.

La AC ONTI no percibe aranceles por ninguno de los servicios que pudieran brindar relacionados con la Política Única de Certificación. Los certificados emitidos bajo la Política Única de Certificación son gratuitos.

9.2. - Responsabilidad Financiera.

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

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

Las Autoridades de Registro y sus Oficiales de Registro son responsables de la validación de la identidad de los suscriptores. Los criterios de valoración que seguirá la AR sobre la

documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán los normalmente aceptados en Derecho.

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

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

9.3. – Confidencialidad.

Toda información referida a solicitantes o suscriptores de certificados que sea recibida por 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 judicialmente. 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 AR durante el ciclo de vida del certificado.

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

9.3.1. - Información confidencial.

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso 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, será generada y custodiada conforme a lo que se especifique

en la Política Única de Certificación. Asimismo, se considera confidencial cualquier información:

a) Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por la AC ONTI.
b) Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
c) Relacionada con los Planes de Continuidad de Operaciones, controles, procedimientos de seguridad y registros de auditoría pertenecientes al 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 AR no es considerada confidencial:

a) Contenido de los certificados y de las listas de certificados revocados.
b) Información sobre personas humanas que se encuentre disponible en certificados o en directorios de acceso público.
c) Políticas de Certificación y Manual de Procedimientos (en sus aspectos no confidenciales).
d) Secciones públicas de la Política de Seguridad de la AC ONTI.
e) Política de privacidad de la AC ONTI.

9.3.3. – Responsabilidades de los roles involucrados

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

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

No será necesario el consentimiento cuando:

a) Los datos se hayan obtenido de fuentes de acceso público irrestricto;
b) Los datos se limiten a nombre, Documento Nacional de Identidad, identificación tributaria o previsional u ocupación.
c) Aquellos para los que 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 ONTI para la implementación de su AC, como así también toda la documentación relacionada, pertenece a la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN..

El derecho de autor de la Política Única de Certificación y de toda otra documentación generada por la AC ONTI en relación con la Infraestructura de Firma Digital, pertenece a la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN 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 SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN 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 2628/02, la Resolución MM Nº 399-E/2016 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 presente Política y en el Acuerdo con suscriptores.

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

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

9.8. – 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 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 los normalmente aceptados en Derecho. La Autoridad de Registro siempre exigirá la presencia física del suscriptor.

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

9.9. – 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 la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA y hasta tanto sea reemplazado por una nueva versión. Toda modificación en el Manual de Procedimientos, una vez aprobado 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 SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA conforme a lo establecido por la Ley N° 25.506, artículo 21, inciso q) y por la Resolución MM N° 399-E/2016 y sus Anexos respectivos.

El Manual de Procedimientos es sometido a aprobación de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA durante el proceso de licenciamiento.

Toda modificación en el Manual de Procedimientos será comunicada al suscriptor.

El Manual de Procedimientos será revisado y actualizado periódicamente por la AC ONTI y sus nuevas versiones se pondrán en vigencia, previa aprobación de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA.

9.12.2 – Mecanismo y plazo de publicación y notificación.

Una copia de la versión vigente del Manual de Procedimientos se encuentra disponible en forma pública y accesible a través de Internet en el sitio web http://pki.jgm.gov.ar/docs/Manual_de_Procedimientos_ACONTIv3.0.pdf

9.12.3. – Condiciones de modificación del OID.

No aplicable.

9.13. - Procedimientos de resolución de conflictos.

Cualquier controversia y/o conflicto resultante de la aplicación 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° 894/2017.

El Manual de Procedimientos se encuentra en un todo subordinado a las prescripciones de la Ley N° 25.506, el Decreto Nº 2628/02 y modificatorios, la Resolución MM Nº 399-E/2016, la Resolución SMA Nº 37-E/2016 y demás normativa complementaria dictada por la autoridad competente.

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

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por la AC ONTI, sólo será procedente previa acreditación de haberse efectuado reclamo ante este último con resultado negativo. Acreditada dicha circunstancia, el ente licenciante

procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

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

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

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

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

En ningún caso el Manual de Procedimientos de la AC ONTI prevalecerá sobre lo dispuesto por la normativa legal vigente de firma digital.

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

9.14. - Legislación aplicable.

La Ley N° 25.506 y modificatorias, el Decreto Nº 2628/02 y modificatorios, la Resolución MM Nº 399-E/16 y sus modificatorias, las Resoluciones SMA Nros. 37-E/2016, 116-E/2017, 63-E/2018 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	Adecuación DA N° 927/2014
Versión 3.0	01/2019	Actualización	Actualización documentación AC ONTI

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

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2019-01737737-APN-DNTEID#JGM

CIUDAD DE BUENOS AIRES
Miércoles 9 de Enero de 2019

Referencia: Manual de Procedimientos AC ONTI v3.0

El documento fue importado por el sistema GEDO con un total de 89 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.01.09 21:25:48 -03'00'

Alejandra Battaglia
Directora Nacional
Dirección Nacional de Tramitación e Identificación a Distancia
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.01.09 21:25:49 -03'00'