POLÍTICA DE CERTIFICACIÓN

para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado

Jefatura de Gabinete de Ministros
Secretaría de la Gestión Pública
Subsecretaría de Tecnologías de Gestión
Oficina Nacional de Tecnologías de Información

Versión 1.6
Septiembre, 2010

Índice

1. INTRODUCCIÓN

1.1. Descripción general

El presente documento define los términos que rigen la relación entre la Oficina Nacional de Tecnologías de Información (en adelante el Certificador) de la Subsecretaría de Tecnologías de Gestión de la Secretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros, las Autoridades de Registro (AR), los suscriptores y los terceros usuarios, en su condición de receptores de documentos firmados bajo la presente Política, en el marco del la Ley N° 25.506 de Firma Digital, su Decreto Reglamentario N° 2628/02 y la Decisión Administrativa Nº 6/07 y demás normas reglamentarias.

1.2. Identificación

Nombre: Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado
Versión: 1.0
Fecha de aplicación: 21 de Octubre de 2010
Sitio de publicación: http://pki.jgm.gov.ar/cps/cps.pdf
OID: 2.16.32.1.1.3
Lugar: Buenos Aires, Argentina

1.3. Participantes y aplicabilidad

Esta Política es aplicable a:

a) El Certificador, que emite certificados digitales para personas físicas
b) Las AR, que se constituyan en el ámbito de la presente Política
c) Los solicitantes y suscriptores de certificados digitales emitidos por el Certificador, en el ámbito de la presente Política
d) Los terceros usuarios, que verifican firmas digitales basadas en certificados digitales emitidos por el Certificador, en el ámbito de la presente Política.

1.3.1. Certificador

La Oficina Nacional de Tecnologías de Información (en adelante, la ONTI) en su calidad de Certificador, presta los servicios de certificación, de acuerdo con los términos de la presente Política.

1.3.2. Autoridad de Registro

El Certificador posee una estructura de AR que efectúan las funciones de validación de identidad y de otros datos de los solicitantes y suscriptores de certificados, registrando las presentaciones y trámites que les sean formulados por éstos.

Los entes públicos que han sido habilitados para operar como AR del Certificador se encuentran disponibles en su sitio web https://pki.jgm.gov.ar/app

Las AR serán autorizadas a funcionar como tales mediante notas firmadas por el del Director Nacional de la ONTI.

1.3.3. Suscriptores de certificados

Podrán ser suscriptores de los certificados emitidos por la Autoridad Certificante de la ONTI:

a) Las personas físicas que desempeñen funciones en entes públicos estatales o integren entes públicos no estatales.

b) Las personas físicas que realicen trámites con el Estado, cuando se requiera una firma digital.

En los casos de entes no pertenecientes a la Administración Pública Nacional, el Certificador podrá exigir previamente la suscripción de un acuerdo específico.

Además la AC ONTI será suscriptora de un certificado para ser usado en relación con el servicio On Line Certificate Status Protocol (en adelante, OCSP) de consulta sobre el estado de un certificado.

1.3.4. Aplicabilidad

Para el caso de personas físicas que desempeñen funciones en un ente público estatal, los certificados digitales emitidos en el marco de la presente Política podrán ser utilizados para firmar cualquier transacción electrónica asociada a la función correspondiente a cada suscriptor. En cualquier otro caso, solo se podrán utilizar para la realización de trámites ante el Estado.

La presente Política contempla también la emisión de certificados para responder a los requerimientos de verificación en línea del estado de los certificados (OCSP). Estos certificados, serán emitidos únicamente a favor de la AC ONTI.

La presente Política contempla y define dos niveles de seguridad para los certificados emitidos a favor de sus suscriptores (excluidos certificados OCSP):

a) Nivel de seguridad Alto: para los certificados solicitados mediante el uso de dispositivos criptográficos (ej: tokens, smart cards).

b) Nivel de seguridad Normal: correspondiente a los certificados solicitados y almacenados vía software.

1.4. Contactos

La presente Política de Certificación es administrada por:

Oficina Nacional de Tecnologías de Información
Domicilio: Roque Sáenz Peña 511 - 5° piso (C1035AAA) Ciudad Autónoma de Buenos Aires Argentina

Por consultas o sugerencias, dirigirse a:

Oficina Nacional de Tecnologías de Información
Domicilio: Roque Sáenz Peña 511 - 5° piso (C1035AAA) Ciudad Autónoma de Buenos Aires Argentina
Por correo electrónico: contactopki@sgp.gov.ar
Teléfono: (54 11) 4343-9001 Int. 519 / 521
Fax: (54 11) 4345-7458

2. ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACIÓN

2.1. Obligaciones

2.1.1. Obligaciones del certificador

De acuerdo a lo establecido en la Ley Nº 25.506, en su artículo 21:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
b) 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 por él emitidos;
c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
g) Mantener la confidencialidad de toda información que no figure en el certificado digital;
h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;
j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;
k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;
l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;
m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;
q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
u) Constituir domicilio legal en la República Argentina;
v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

De acuerdo a lo establecido en el Decreto Nº 2628/02, en sus artículos 26, 32, 33 y 34:

Artículo 26:

a) Deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley N° 25.506, en el Decreto Nº 2628/02 y en las normas complementarias.
b) Someterse a auditorías anuales.

Artículo 32:

Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.

d) Expedir certificados que cumplan con:

1) Lo previsto en los artículos 13 y 14 de la Ley N° 25.506.
2) Los estándares tecnológicos aprobados por la Jefatura de Gabinete de Ministros.

e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.

f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.

g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.

h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.

i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.

j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.

k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.

l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Artículo 33:

Servicios de Terceros. En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Artículo 34:

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos. El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

r) El Certificador deberá cumplir además con toda otra obligación emanada de las prescripciones de la Decisión Administrativa Nº 6/07 y sus anexos complementarios y con aquellas establecidas en la presente Política de Certificación.

2.1.2. Obligaciones de la Autoridad de Registro

De acuerdo a lo establecido en el Decreto Nº 2628/02, en su artículo 35:
Una Autoridad de Registro es una entidad responsable de las siguientes funciones:

a) Recibir las solicitudes de emisión de certificados.

b) Validar la identidad y autenticación de los datos de los titulares de certificados.

c) Validar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador.

d) Remitir las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) Recibir y validar las solicitudes de revocación de certificados y su direccionamiento a la AC ONTI.

f) Identificar y autenticar los solicitantes de revocación de certificados.

g) Archivar y conservar toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) Cumplir las normas y recaudos establecidos para la protección de datos personales.

i) Cumplir las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador con el que se encuentre vinculada, en la parte que resulte aplicable.

De acuerdo a lo establecido en la Decisión Administrativa Nº 6/7, y con referencia a los Oficiales de Registro que desempeñen funciones en la AR:
Proteger su par de claves, de manera que su clave privada se encuentre en todo momento bajo su exclusivo conocimiento y control y con todas las medidas de seguridad establecidas por el certificador.

Adicionalmente para el caso de las AR que aprueben solicitudes de personas físicas que realicen trámites con el Estado y de aquellas que se constituyan en organismos o entidades no pertenecientes a la esfera nacional, deberán cumplir con lo dispuesto en el Acuerdo respectivo.

2.1.3. Obligaciones de los suscriptores del certificado

De acuerdo a lo establecido en la Ley Nº 25.506, en su artículo 25:

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

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

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

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

De acuerdo a lo establecido en la Decisión Administrativa Nº 06/07:

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

- Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la presente Política de Certificación,

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

2.1.4. Obligaciones de los terceros usuarios

De acuerdo a lo establecido en el punto 2.1.4 del Anexo II de la Decisión Administrativa N° 6/07:

a) Conocer los alcances de la Política de Certificación conforme a los Términos y condiciones con terceros usuarios;

b) Rechazar la utilización del certificado para aquellos fines distintos a los previstos en esta Política de Certificación;

c) Verificar la validez del certificado digital.

2.1.5. Obligaciones del servicio de repositorio

El Certificador está obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en el artículo 21 de la Ley N° 25.506, el Decreto N° 2628/02, y en la presente Política de Certificación.

- Obligaciones establecidas en el artículo 21 inciso k) de la Ley N° 25.506:

a) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, la política de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la Autoridad de Aplicación.

- Obligaciones establecidas en el artículo 34 incisos g), h) y m) del Decreto N° 2628/02:

a) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
b) Mantener actualizados los repositorios de certificados revocados por el período establecido por la Autoridad de Aplicación.
c) Cumplir con las normas y recaudos establecidos para la protección de datos personales.

- Obligaciones adicionales y aclaraciones establecidas en la DA N° 6/07:

a) Disponer y dedicar los recursos establecidos para la seguridad de los datos almacenados, desde el punto de vista técnico y legal.

2.2. Responsabilidades

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

Al emitir un certificado digital o al reconocerlo en los términos del artículo 16 de la Ley 25.506, el Certificador 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 al Certificador demostrar que actuó con la debida diligencia.

El artículo 36 del Decreto N° 2628/02, Reglamentario de la Ley N° 25.506, establece la responsabilidad del Certificador respecto de las AR.

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 AR, siempre que medie la aprobación del Certificador.

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

El Certificador tampoco es responsable en los siguientes casos, según el artículo 39 de la Ley antes mencionada:

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

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

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

Los alcances de la responsabilidad del Certificador se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en esta Política de Certificación en relación a la emisión, renovación y revocación de certificados. Los alcances de la responsabilidad del Certificador se limitan a los ámbitos de su incumbencia directa, en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.

El Certificador 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.

2.3. Responsabilidad Financiera

2.3.1. Responsabilidad Financiera del Certificador

Las responsabilidades financieras se originan en lo establecido por la Ley 25.506 y su Decreto Reglamentario Nº 2628/02 y en las disposiciones de la presente Política.

2.4. Interpretación y aplicación de las normas

2.4.1. Legislación aplicable

La interpretación, obligatoriedad, diseño y validez de esta Política de Certificación se encuentran sometidos a lo establecido por la Ley Nº 25.506, su Decreto Reglamentario Nº 2628/02 y la Decisión Administrativa N° 06/07 y demás normas complementarias dictadas por la Autoridad de Aplicación.

2.4.2. Forma de interpretación y aplicación

La interpretación y/o aplicación de las disposiciones de la presente Política de Certificación y de cualquiera de sus documentos asociados, será resuelta según las normas mencionadas en el punto 2.4.1 y los procedimientos indicados en el punto 2.4.3.

Si se presentaren conflictos de interpretación de una o más disposiciones de esta Política de Certificación, el suscriptor o tercero usuario deberá agotar la vía administrativa con este Certificador, luego de cumplida esa instancia podrá accionar ante la Autoridad de Aplicación.

2.4.3. Procedimientos de resolución de conflictos

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

La presente Política de Certificación se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506 y su reglamentación.

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

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

2.5. Aranceles

El Certificador no percibe aranceles por ninguno de los servicios que pudiera brindar relacionados con esta Política de Certificación. Los certificados emitidos bajo la presente Política son gratuitos y no se cobra ningún tipo de arancel o tasa por su solicitud, emisión, renovación, revocación o utilización.

2.6. Publicación y Repositorios de certificados y listas de certificados revocados (CRLs)

2.6.1. Publicación de información del certificador

El Certificador mantiene un repositorio en línea de acceso público que contiene:

a) Su certificado digital
b) Su certificado OCSP
c) La lista de certificados revocados (CRL)
d) La Política de Certificación en sus versiones vigente y anteriores
e) El Manual de Procedimientos en sus aspectos de carácter público, en sus versiones vigente y anteriores
f) El modelo del Acuerdo con Suscriptores
g) Los Términos y Condiciones con Terceros Usuarios
h) La Política de Privacidad
i) Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.

La información antedicha se encuentra disponible durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana en el sitio web del Certificador https://pki.jgm.gov.ar/app

2.6.2. Frecuencia de publicación

Producida una actualización de los documentos relacionados con el marco legal u operativo de la AC ONTI, estos documentos actualizados se publicarán dentro de las VEINTICUATRO (24) horas luego de ser aprobados por la Autoridad de Aplicación.

Asimismo, se emitirá cada VEINTICUATRO (24) horas la Lista de Certificados Revocados (CRL completa). Se emitirán CRL complementarias (delta CRL) con frecuencia horaria.

2.6.3. Controles de acceso a la información

El Certificador garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

2.6.4. Repositorios de certificados y listas de revocación

El servicio de repositorio de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por el Certificador.

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.

2.7. Auditorías

El Certificador se encuentra sujeto a las auditorías de acuerdo a lo establecido en la Ley N° 25.506, su Decreto Reglamentario Nº 2628/02 y la Decisión Administrativa Nº 06/07.

La información relevante de los informes de las auditorías es publicada en el sitio web del certificador https://pki.jgm.gov.ar/app/ Se realiza una auditoría previa al licenciamiento del Certificador a fin de verificar el cumplimiento de los requisitos correspondientes al licenciamiento. Con posterioridad, el Certificador será sujeto a auditorías ordinarias para controlar la continuidad del cumplimiento de las normas vigentes y a auditorías extraordinarias de oficio, según lo disponga la Autoridad de Aplicación.

En su carácter de organismo comprendido en el artículo 8 de la Ley N° 24.156, el Certificador podrá ser auditado por la Sindicatura General de la Nación - SIGEN y por la Auditoría General de la Nación – AGN, en forma periódica.

Adicionalmente, el Certificador realizará auditorías periódicas sobre sus Autoridades de Registro.

2.8. Confidencialidad

2.8.1. Información confidencial

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

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

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

- Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por el Certificador
- Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
- Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.

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

2.8.2. Información no confidencial

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

- La que se encuentra contenida en su propio certificado digital
- La que se incluya en la CRL
- Toda otra referida a personas físicas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público.

Es considerada no confidencial la información incluida en los documentos publicados en el repositorio del Certificador mencionados en el apartado 2.6.1 de la presente Política..

2.8.3. Publicación de información sobre la revocación o suspensión de un certificado

La información contenida en la CRL referida a la revocación de un certificado no es considerada confidencial.
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.
El estado de suspensión de un certificado no es aplicable en el marco de la Ley N° 25.506.

2.8.4. Divulgación de información a autoridades judiciales

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial.

2.8.5. Divulgación de información como parte de un proceso judicial o administrativo

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial o ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

2.8.6. Divulgación de información por solicitud del suscriptor

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

No será necesario el consentimiento cuando:

- Los datos se hayan obtenido de fuentes de acceso público irrestricto;
- Los datos se limiten a nombre, documento nacional de identidad, pasaporte, documento de identidad expedido por país miembro del MERCOSUR u ocupación.
- Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular

2.8.7. Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales el Certificador pueda divulgar la información.

2.9. Derechos de Propiedad Intelectual

El derecho de autor de los sistemas y aplicaciones informáticas desarrollados por el Certificador para la implementación de su AC, como así toda la documentación relacionada, pertenece a la ONTI.

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Registro inicial

El Certificador emite certificados a personas físicas, que cumplan con los requisitos para ser suscriptor, efectuándose una validación personal de la identidad del solicitante, para lo cual se requiere su presencia física ante el Oficial de Registro. Asimismo, el solicitante debe probar su carácter de suscriptor para esta Política de Certificación. La única excepción a la emisión de certificados para persona físicas es el caso del Certificado OCSP, mencionado precedentemente.

A fin de efectuar la validación de identidad indicada, el solicitante en forma personal, debe cumplir los siguientes pasos:

a) Ingresa al sitio web del Certificador https://pki.jgm.gov.ar/app/

b) Completa la solicitud de certificado con sus datos personales y selecciona el nivel de seguridad.

c) Acepta el Acuerdo con Suscriptores en el que se hace referencia a la Política que respalda la emisión del certificado.

d) Envía su solicitud a la AC ONTI e imprime la nota de solicitud.

e) Se presenta ante la AR correspondiente con la documentación requerida para realizar su identificación personal.

Cumplido el proceso de autenticación de su identidad, el solicitante firma la nota de solicitud de su certificado ante el Oficial de Registro de la AR correspondiente, con lo cual acepta las condiciones de emisión y uso del certificado.

3.1.1. Tipos de Nombres

Los Tipos de Nombres admitidos para los suscriptores de certificados son los que figuren en la documentación de identificación del solicitante.

3.1.2. Necesidad de Nombres Distintivos

Los atributos definidos a continuación son los mínimos incluidos en los certificados para identificar unívocamente a su titular, cualquiera sea su nivel de seguridad:

"commonName": corresponde con los nombres y apellidos que figuran en el documento de identidad del solicitante o suscriptor.

"*serialNumber":* contiene el tipo y número del documento del suscriptor. Se admitirán los siguientes documentos de identidad:

- Para solicitantes que sean ciudadanos argentinos o residentes: Documento Nacional de Identidad, Libreta de Enrolamiento o Libreta Cívica.
- Para solicitantes extranjeros, Cédula de MERCOSUR, según las disposiciones vigentes, o Pasaporte y código de país emisor.

"title": actividad, cargo o función del suscriptor dentro del ente público estatal. En el resto de los casos, actividad, pasividad, profesión u ocupación.

"emailAddress": deberá contener la dirección de correo electrónico institucional del suscriptor, para el caso de entes públicos estatales. En el resto de los casos, salvo que posean una cuenta institucional, podrá ser definido en cada acuerdo a firmar con el Certificador.

"organizationalUnitName": para el caso de las personas físicas de entes públicos estatales, contiene la información relativa al ente al que el suscriptor pertenece. Pueden existir varias ocurrencias de este atributo, representando la dependencia jerárquica del área del ente con la que se vincula el solicitante o suscriptor. En el resto de los casos, podrá ser definido en cada acuerdo a firmar con el Certificador.

"organizationName": para el caso de personas físicas de entes públicos estatales, identifica la jurisdicción del Sector Público en la que desempeña sus funciones. Deberá consignar si pertenece al Sector Público, Provincial o Municipal, individualizando el Poder al que corresponde (Ejecutivo,

Legislativo, Judicial o Ministerio Público) y la denominación de la Provincia o Municipio cuando sea aplicable. En el resto de los casos podrá ser definido en cada acuerdo a firmar con el Certificador.

"localityName": identifica la localidad donde se desempeña el solicitante o suscriptor, en el caso de personas físicas de entes públicos, o la localidad donde reside, para las personas físicas que realicen trámites con el Estado.. En el caso de personas que residan en el exterior, se consignará la expresión "Provincia 25".

"stateOrProvinceName": identifica la provincia donde se desempeña el solicitante o suscriptor, en el caso de personas físicas de entes públicos, o la provincia donde reside, para las personas físicas que realicen trámites con el Estado.. En el caso de personas que residan en el exterior, se consignará la expresión "Provincia 25".

"countryName": debe contener el valor "AR", por "Argentina" representando el país de emisión del certificador.

3.1.3. Reglas para la interpretación de nombres

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

3.1.4. Unicidad de nombres

El nombre distintivo es único para cada suscriptor y está integrado por los campos indicados en el punto 3.1.2.

3.1.5. Procedimiento de resolución de disputas sobre nombres

El Certificador se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos que pudieran generarse respecto al uso y titularidad de nombres por parte de los solicitantes o suscriptores.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

No se aplica por tratarse de una Política de Certificación para personas físicas.

3.1.7. 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 del Certificador.

En el caso de solicitudes de certificados de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo. Para certificados de nivel de seguridad Normal, el solicitante genera su par de claves y almacena la clave privada vía software en su propio equipo al momento de la solicitud. La aplicación de la AC ONTI validará el requerimiento del certificado (PKCS#10) con el fin de verificar la posesión del la clave privada por parte del solicitante.

3.1.8. Autenticación de la identidad de personas jurídicas públicas o privadas

No se aplica por tratarse de una Política de Certificación para personas físicas.

3.1.9. Autenticación de la identidad de personas físicas

Según lo establecido en la presente Política de Certificación, el Certificador únicamente emite certificados para personas físicas que cumplan con los requisitos para ser suscriptor, efectuándose una validación de la identidad del solicitante, para lo cual se requiere su presencia física ante la AR correspondiente. Asimismo, el solicitante debe probar la titularidad de los datos contenidos en su solicitud.

La verificación se efectuará mediante la presentación de la siguiente documentación:

a) Documento Nacional de Identidad, Libreta Cívica o Libreta de Enrolamiento (original y fotocopia) para ciudadanos argentinos o residentes o Pasaporte o Cédula MERCOSUR (original y fotocopia) para extranjeros.

b) Para el caso de personas físicas de entes públicos estatales, Nota de certificación del cargo que ocupa. Esta podrá consistir en:
   - Copia autenticada del Acto Administrativo correspondiente a su designación o
   - Constancia emitida por la Oficina de Recursos Humanos, Personal o equivalente de su organismo o entidad, firmada por un funcionario responsable, en la que conste lugar y fecha de emisión, nombre y apellido, documento de identidad, organismo, unidad y cargo que ocupa en el mencionado organismo o entidad y los datos correspondientes al funcionario a quien reporta (Apellido y Nombre y cargo). Adicionalmente, deberá aumentarse una nota del funcionario de reporte del solicitante o suscriptor, indicando el cargo que éste ocupa.

c) Para el resto de los casos, podrá ser definido en cada acuerdo a firmar con el Certificador

d) Nota de solicitud de certificado, firmada por el solicitante.

El Oficial de Registro efectúa los siguientes pasos:

- Verifica la existencia en el sistema de la solicitud, si correspondiese
- Al momento de presentación del solicitante o suscriptor en sus oficinas, valida su identidad mediante la verificación de la documentación requerida
- Verifica la titularidad de la solicitud mediante el control de la nota correspondiente, si fuera aplicable
- De corresponder, requiere al solicitante la firma de la nota de solicitud en su presencia
- Resguarda toda la documentación respaldatoria 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.

El Certificador podrá autorizar un procedimiento en aquellos casos que exista un impedimento justificado que imposibilite la presentación física del solicitante o suscriptor ante la AR correspondiente, siempre que se garantice la identificación de su identidad.

3.2. Generación de nuevo par de claves (Re Key)

En caso de que por alguna causa resultase necesario cambiar el par de claves de un certificado vigente, el suscriptor deberá solicitar la revocación de su certificado e iniciar el proceso de solicitud de certificado. De haber expirado el certificado, no se permitirá la reutilización del mismo par de claves.

3.3. Generación de nuevo par de claves después de una revocación - Sin compromiso de claves

En caso de que por alguna causa resultase necesario cambiar el par de claves de un certificado vigente, el suscriptor deberá solicitar la revocación de su certificado e iniciar el proceso de solicitud de certificado. De haber expirado el certificado, no se permitirá la reutilización del mismo par de claves.

3.4. Requerimiento de revocación

Un suscriptor podrá revocar su certificado digital utilizando cualquiera de los siguientes métodos:

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

- A través de la aplicación de la AC ONTI https://pki.jgm.gov.ar/app/ que se encuentra disponible VEINTICUATRO (24) horas, utilizando el código de revocación que le fue entregado al momento de su solicitud.

- En caso de no poder utilizar alguno de los anteriores, presentándose ante la AR correspondiente, con documento de identidad que permita acreditar su identidad.

En caso de suscriptores en entes públicos estatales, la revocación podrá ser solicitada por un funcionario competente del organismo indicado en el certificado, por nota dirigida al Responsable de la AR.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de certificado

4.1.1. Solicitud de nuevo certificado

Todo solicitante o suscriptor que se postule para obtener un certificado debe completar una solicitud, en el sitio web https://pki.jgm.gov.ar/app/ del Certificador, que estará sujeta a revisión y aprobación por la AR correspondiente.

El proceso de solicitud puede ser iniciado solamente por el interesado, quien posteriormente debe acreditar fehacientemente su identidad.

Al ingresar en el sitio web del certificador, debe seleccionar el enlace a la aplicación de solicitud de emisión de certificados para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado y completar los datos solicitados. Para el caso de funcionarios, agentes o personas contratadas en el Sector Público, se aceptará únicamente como dirección de correo electrónico válida aquella que revista carácter institucional y se encuentre accesible por un cliente de correo electrónico.

Una vez ingresados sus datos y como paso previo a la generación del par de claves, seleccionará el nivel de seguridad del certificado requerido (alto o normal).

Adicionalmente, el solicitante deberá leer y aceptar el Acuerdo con Suscriptores para continuar el proceso.

4.1.2. Solicitud de renovación

El proceso de renovación puede ser realizado solo si el certificado se encuentra vigente y debe ser iniciado solamente por el suscriptor, quien deberá tener acceso a su clave privada vinculada al

certificado. Los datos contenidos en el certificado a renovar no deben haber variado. Caso contrario, deberá proceder a su revocación y posterior solicitud de un nuevo certificado, según lo dispuesto en el punto 4.1.1.

El suscriptor deberá ingresar al sitio web del Certificador https://pki.jgm.gov.ar/app/ y seleccionar la opción de renovación de certificados y seguir los pasos indicados.

La aprobación de la renovación está sujeta a la presentación de la documentación pertinente ante la AR que le corresponda.

4.2. Emisión del certificado

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

4.3. Aceptación del certificado

Un certificado emitido por el Certificador se considera aceptado por su titular una vez que éste haya sido puesto a su disposición.

4.4. Suspensión y Revocación de Certificados

El estado de suspensión de certificados no es admitido en el marco de la Ley N° 25.506.

4.4.1. Causas de revocación

El Certificador revocará los certificados digitales que hubiera emitido en los siguientes casos:

- A solicitud del titular del certificado
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros
- Por Resolución Judicial o Acto Administrativo de Autoridad competente

- Por fallecimiento del titular
- Por declaración judicial de ausencia con presunción de fallecimiento del titular
- Por declaración judicial de incapacidad del titular
- Si se determina que la información contenida en el certificado ha dejado de ser válida
- Cuando la clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Cuando cese el vínculo entre el suscriptor y el ente o sea modificada su situación de revista o cargo
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
- Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
- Por revocación del certificado digital del Certificador
- Cuando así lo establezcan las condiciones indicadas en el Acuerdo aplicable a la AR, de existir

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

4.4.2. Autorizados a solicitar la revocación

Se encuentran autorizados a solicitar la revocación de un certificado emitido por el Certificador:

a) El suscriptor del certificado.

b) El máximo responsable del área de Recursos Humanos del ente público estatal en que se desempeñe el suscriptor del certificado.

c) La Autoridad competente del ente público de quien depende el suscriptor.

d) El Responsable del Certificador o de la AR correspondiente a ese suscriptor.

e) La Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina.

f) La Autoridad Judicial competente.

g) En el caso de certificados emitidos a favor de personas físicas no pertenecientes a entes públicos estatales, el Certificador procederá a la su revocación a solicitud de su titular o en los supuestos previstos en el acuerdo correspondiente.

4.4.3. Procedimientos para la solicitud de revocación

Para solicitar la revocación de su certificado, el suscriptor seguirá lo indicado en el apartado 3.4 Requerimiento de Revocación.

La AR conservará como documentación probatoria toda solicitud de revocación y el material probatorio vinculado.

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

4.4.4. Plazo para la solicitud de revocación

Las solicitudes de revocación se procesan en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.4.1.

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

El plazo máximo entre la de revocación y su publicación es de VEINTICUATRO (24) horas.

4.4.5. Causas de suspensión

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

4.4.6. Autorizados a solicitar la suspensión

No aplicable

4.4.7. Procedimientos para la solicitud de suspensión

No aplicable

4.4.8. Límites del periodo de suspensión de un certificado

No aplicable

4.4.9. Frecuencia de emisión de listas de certificados revocados

El Certificador genera y publica una Lista de Certificados Revocados con una frecuencia diaria con listas complementarias (delta CRL) en modo horario.

4.4.10. Requisitos para la verificación de la lista de certificados revocados

Los terceros usuarios están obligados a verificar el estado de validez de los certificados mediante el control de la lista de certificados revocados o en su defecto, mediante el servicio de consultas en línea sobre el estado de los certificados (OCSP), que el Certificador pondrá a su disposición.
Los terceros usuarios están obligados a confirmar la validez de la CRL mediante la verificación de la firma digital del Certificador y de su período de validez.

El Certificador garantiza el acceso permanente y gratuito del público en general a la CRL, disponible en su sitio web http://pki.jgm.gov.ar/crl/FD.crl

4.4.11. Disponibilidad en línea del servicio de revocación y verificación del estado del certificado

El Certificador posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento.

Ambos servicios se encuentran disponibles a partir de su sitio web https://pki.jgm.gov.ar/app

4.4.12. Requisitos para la verificación en línea del estado de revocación

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y representa una alternativa a la consulta a la CRL, la que también estará disponible. El servicio OCSP se provee por medio del sitio web http://pki.jgm.gov.ar/ocsp

4.4.13. Otras formas disponibles para la divulgación de la revocación

El Certificador no utiliza otros medios para la divulgación del estado de revocación de los certificados que los contemplados en la presente Política de Certificación.

4.4.14. Requisitos para la verificación de otras formas de divulgación de revocación

No aplicable

4.4.15. Requisitos específicos para casos de compromiso de claves

En caso de compromiso de la clave privada del suscriptor del certificado, éste es responsable de efectuar su revocación o bien de comunicar de inmediato tal situación al Responsable de la AR por

algunas de las vías indicadas en el apartado 3.4 y el Certificador operará en consecuencia a lo establecido en la presente Política.

4.5. Procedimientos de Auditoría de Seguridad

El Certificador mantiene registros de auditoría de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros, que se conservarán por un plazo mínimo de DIEZ (10) años.

Asimismo, atendiendo a lo expresado en el punto 2.7 Auditoría, se mantendrán registros no informatizados de toda aquella información generada en formato de papel.

Estos registros se encuentran disponibles tanto para la auditoría interna como para la Autoridad de Aplicación y otros organismos o entidades que tengan competencias para acceder a esa información.

4.6. Archivo de registro de eventos

El Certificador mantiene un sistema de registro de archivos de transacciones que permite mantener en un entorno seguro toda la información considerada relevante y requerida, contemplando las siguientes actividades:

a) Administración del ciclo de vida de las claves criptográficas
b) Administración del ciclo de vida de los certificados
c) Información relacionada con la solicitud del certificado
d) Eventos de seguridad

Los archivos de registros se mantienen por un período de DIEZ (10) años a partir de su generación.

4.7. Cambio de claves criptográficas

El par de claves del Certificador ha sido generado con motivo del licenciamiento de la presente Política de Certificación y tendrá 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 del certificador implica la emisión de un nuevo certificado por parte de la AC Raíz de la República Argentina. Si la clave privada del Certificador 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.

El Certificador tomará los recaudos necesarios para efectuar con suficiente antelación la renovación de su licencia y la obtención del certificado, si correspondiese.

4.8. Plan de contingencia y recuperación ante desastres

El Certificador ha implementado un Plan de contingencia ante hechos que comprometan la continuidad de sus operaciones, que garantiza el mantenimiento de sus servicios esenciales, los que incluirán como mínimo la recepción de solicitudes de revocación, y la consulta de CRL actualizadas y el servicio OSCP.

Dicho Plan de Contingencia describe los procedimientos que se implementan para minimizar las interrupciones de las actividades y para salvaguardar los procesos críticos, de las consecuencias de fallas significativas o masivas. El Plan involucra a la totalidad de los recursos físicos, software, personal e información, con el objeto de garantizar la adecuada y continua prestación de servicios.

Los procesos y procedimientos se encuentran definidos en dicho Plan, sobre el que se contemplan mecanismos de prueba y simulación con un periodicidad de SEIS (6) meses o cuando los cambios realizados sobre el hardware o software de base o aplicativo así lo ameriten.

4.9. Plan de Cese de Actividades

El Certificador cesará en su calidad de Licenciado de acuerdo con lo estipulado en el artículo 22 de la Ley N° 25506 por:

a) Decisión unilateral comunicada a la Autoridad de Aplicación

b) Disolución o reestructuración del organismo que ejerce las funciones de Certificador

c) Cancelación de su licencia dispuesta por la Autoridad de Aplicación, dados los supuestos previstos en el artículo 44 de la Ley 25.506

El Certificador dispone de un Plan de Cese de Actividades donde se contemplan las estrategias y procedimientos a seguir desde la declaración de cese hasta la inhabilitación lógica y física de sus instalaciones.

Declarado el cese, toda información del Certificador, cualquiera sea el soporte utilizado, será resguardada en el Archivo constituido a tal efecto,, por un plazo de DIEZ (10) años, incluyendo toda la documentación en poder de las AR. Si el cese se debiera a la disolución o reestructuración del organismo, los registros serán transferidos al organismo al que se le asignen las funciones correspondientes.

5. CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

La descripción detallada de los procedimientos referidos a los controles de seguridad física, funcional y del personal se desarrolla en el Plan de Seguridad del Certificador.

5.1. Controles de seguridad física

El Certificador implementa controles apropiados que restringen el acceso a los equipos, programas y datos utilizados para proveer el servicio de certificación, solamente a personas debidamente autorizadas.

Se implementan procedimientos de control sobre los siguientes aspectos:

a) Construcción y localización de instalaciones
b) Acceso físico

c) Energía y aire acondicionado
d) Exposición al agua
e) Prevención y protección contra incendios
f) Medios de almacenamiento
g) Disposición de material de descarte
h) Instalaciones de seguridad externas

5.2. Controles Funcionales

Las funciones del Certificador son llevadas a cabo por personal calificado y son realizadas de acuerdo a roles asignados a tal efecto, descriptos en el Documento “Roles y Funciones” del Certificador.

La autoridad competente del organismo o quien éste designe, asignará dichos roles, respetando los siguientes criterios:

a) Cada uno de los roles tiene un titular asignado y por lo menos, un sustituto
b) Se asegurará una adecuada separación de funciones, a fin de evitar incompatibilidades en la asignación de los roles mencionados

En el caso de las AR, el Certificador efectuará los controles funcionales pertinentes, verificando el cumplimiento de las responsabilidades y procedimientos según lo dispuesto en la presente Política de Certificación y demás documentación del Certificador.
Las personas que ejercen cada uno de los roles mencionados dispondrán de adecuadas credenciales de identificación y autenticación, cuando fuera aplicable, de acuerdo a las tareas que desempeñen.

5.3. Controles de Seguridad del Personal

El Certificador sigue una política de administración de personal que provee razonable seguridad acerca de la confiabilidad y competencia del personal para el adecuado cumplimiento de sus funciones.

Se establecen procedimientos de control sobre los siguientes aspectos:

a) Antecedentes penales, laborales, de competencia e idoneidad conforme los requisitos establecidos para la contratación o designación en los regímenes aplicables.

b) Instancias de capacitación vinculadas a los roles y tareas que se desempeñan, con la frecuencia de actualización técnica requerida en cada caso.
c) Sanciones a aplicar de acuerdo a los regímenes de contratación o designación aplicables, según corresponda
d) Credenciales, elementos de identificación personal y demás documentación provista al personal que desempeñe funciones en el Certificador.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación de claves

6.1.1. Generación del par de claves criptográficas

El Certificador, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política, generará el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits.

En el caso de las AR, cada Oficial de Registro generará y almacenará su par de claves utilizando un dispositivo criptográfico homologado FIPS 140-2 Nivel 2 y utilizando el algoritmo RSA con un tamaño mínimo de 1024 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos, de acuerdo con los niveles de seguridad establecidos en el punto 1.3.1. En el caso que se utilicen dispositivos criptográficos, estos deberán ser homologados FIPS 140-2 Nivel 2. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

El par de claves del suscriptor de un certificado emitido en los términos de esta Política de Certificación debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

6.1.2. Entrega de la clave privada al suscriptor

El Certificador se abstendrá de generar, exigir o por cualquier medio tomar conocimiento o acceder a la clave privada de los suscriptores, de acuerdo a lo dispuesto por la Ley 25.506 artículo 21 inc. b) y el Decreto Nº 2628/02 artículo 34 inc. i).

6.1.3. Entrega de la clave pública al emisor del certificado

El solicitante entregará su clave pública a la AC ONTI, a través de la aplicación correspondiente, durante el proceso de solicitud de su certificado. La AC ONTI por su parte utilizará técnicas de "prueba de posesión" para determinar que el solicitantes se encuentra en posesión de la clave privada asociada a dicha clave pública.

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

El procedimiento descripto asegura que:

- La clave pública no pueda ser cambiada durante la transferencia.
- Los datos recibidos por el Certificador se encuentran vinculados a dicha clave pública
- El remitente posee la clave privada que corresponde a la clave pública transferida.

6.1.4. Disponibilidad de la clave pública del Certificador

El certificado del Certificador y su cadena de certificación se encuentran a disposición de los suscriptores y terceros usuarios en un repositorio en línea de acceso público a través de Internet, accesible a partir de https://pki.jgm.gov.ar/app/

6.1.5. Tamaño de claves

La longitud de las claves criptográficas del certificado del Certificador es de 4096 bits.

La longitud de las claves criptográficas de los certificados de suscriptores emitidos por el Certificador es de 1024 bits como mínimo.

El algoritmo de firma utilizado es SHA-1 con RSA.

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. Verificación de calidad de los parámetros

La verificación de calidad de los parámetros será realizada por la aplicación del Certificador. Esta verificación abarca la correcta longitud de la clave y la utilización de los algoritmos especificados en esta sección.

6.1.8. Generación de claves por hardware o software

Para la generación de claves criptográficas, el Certificador utiliza dispositivos de las siguientes características:

- Para la generación de las claves criptográficas del Certificador: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 3.

- Para la generación de las claves criptográficas utilizadas para la firma de información de estado de certificados: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 3.

- Para la generación de las claves criptográficas utilizadas por las AR para la aprobación de solicitudes, de renovaciones o revocaciones: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 2.

- Para certificados de suscriptores de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo criptográfico especial que cumple con las características definidas en FIPS 140-2 para el nivel 2.

- Para certificados de nivel de seguridad Normal, el solicitante genera su par de claves y almacena la clave privada vía software al momento de la solicitud.

6.1.9. Propósitos de utilización de claves (campo "Key Usage" en certificados X.509 v.3)

Las claves contenidas en los certificados emitidos por la AC ONTI tienen como propósito su utilización para firmar digitalmente, por lo que los valores a utilizar en la extensión "*KeyUsage"* de los certificados son Firma Digital ("*digitalSignature*") y No Repudio ("*nonRepudiation*").

6.2. Protección de la clave privada

6.2.1. Estándares para dispositivos criptográficos

Para la generación y el almacenamiento de las claves criptográficas, el Certificador, las AR y los suscriptores que opten por un nivel Alto para sus certificados, utilizan los dispositivos referidos en el apartado 6.1.1.

6.2.2. Control "M de N" de clave privada

El procedimiento de utilización de las claves privadas del Certificador se efectúa en forma segura, de manera tal que siempre es necesaria la presencia de una cantidad determinada de personas distintas para su activación de un universo mayor posible.

6.2.3. Recuperación de clave privada

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

No se implementan mecanismos de resguardo y recuperación de las claves privadas de las AR 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 la clave privada

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

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

6.2.5. Archivo de clave privada

El Certificador almacena las copias de reguardo de su clave privada a través de un procedimiento que garantiza su integridad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación, de acuerdo a lo dispuesto por la Decisión Administrativa Nº 06/07 en cuanto a los niveles de reguardo de claves.

6.2.6. Incorporación de claves privadas en dispositivos criptográficos

El par de claves criptográficas del Certificador se genera y almacena en dispositivos criptográficos conforme a lo establecido en la presente Política, salvo en el caso de las copias de resguardo que también están soportados en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

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

6.2.7. 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, quienes validan las operaciones críticas, autorizando su ejecución por medio de llaves especiales que obran en su poder.

6.2.8. Método de desactivación de claves privadas

La desactivación de las claves privadas se lleva adelante mediante el proceso de desactivación de partición; cuando se requiere utilizar temporalmente un equipamiento de respaldo o se realicen tareas de mantenimiento.

6.2.9. Método de destrucción de claves privadas

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

6.3. Otros aspectos de administración de claves

6.3.1. Archivo Permanente de clave pública

Los certificados emitidos a suscriptores y a los Oficiales de Registro como así también el de la AC ONTI 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

La clave privada asociada con el certificado digital del Certificador, tiene una validez de DIEZ (10) años.

Los certificados digitales de las AR y de los suscriptores tendrán una validez de DOS (2) años.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

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

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

6.4.2. Protección de los datos de activación

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

6.4.3. Otros aspectos referidos a los datos de activación

Es responsabilidad de los Oficiales de Registro y de los suscriptores de certificados emitidos por la AC ONTI, elegir contraseñas fuertes para la protección de sus claves privadas y para el acceso a los dispositivos criptográficos que utilicen, si fuera aplicable.

6.5. Controles de seguridad Informática

6.5.1. Requisitos Técnicos específicos

El Certificador establece los controles de seguridad referidos a su equipamiento que cumple con los requisitos técnicos definidos por la normativa vigente.

Los controles implementados se refieren a los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación
b) El Certificador implementa controles de seguridad físicos y lógicos para proteger por una lado el acceso a las instalaciones de la AC ONTI y por otro, el acceso lógico a los sistemas involucrados en la gestión del Certificador
c) Separación de funciones para los roles de certificación
d) Existe una adecuada separación de funciones, no asignándose funciones o roles incompatibles a los intervinientes.
e) Identificación y autenticación de los roles afectados al proceso de certificación
f) Se gestionará una autenticación robusta (2 factores como mínimo) para todos los roles afectados al proceso de certificación.
g) Utilización de criptografía para las sesiones de comunicación y bases de datos
h) Las comunicaciones entre los componentes críticos de la AC ONTI se realizan en forma cifrada.
i) Archivo de datos históricos y de auditoría del Certificador y usuarios
j) Se almacenarán y archivarán los datos históricos y de auditoría del Certificador como así también los correspondientes a los trámites de los suscriptores.
k) Registro de eventos de seguridad
l) Todas las operaciones y actividades de la AC ONTI ocurridas durante el proceso de certificación generan información de control y registros de eventos que permiten verificar el correcto funcionamiento y la seguridad de los sistemas.
m) Prueba de seguridad relativa a servicios de certificación
n) Se realizarán pruebas periódicas de seguridad de los servicios involucrados en los procesos de certificación.
o) Mecanismos confiables para identificación de roles afectados al proceso de certificación
p) Los sistemas y servicios que gestionan las tareas de certificación, poseen mecanismos confiables para identificación de roles.
q) Mecanismos de recuperación para claves y sistema de certificación

r) En el documento Plan de Contingencia se describen los mecanismos de recuperación de los sistemas para garantizar la continuidad de operaciones.

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

La descripción de los controles de seguridad establecidos sobre los servidores del Certificador se incluye en el Plan de Seguridad.

6.5.2. Calificaciones de seguridad computacional

El certificador cumple con las siguientes calificaciones de seguridad sobre los productos en los que se basa la implementación:

- Windows 2008 R2 Server Enterprise: en proceso de evaluación para certificar EAL4+
- Windows 2008 Server Enterprise x86: certificado EAL4+
- Forefront TMG 2010 Enterprise x64: en proceso de evaluación para certificar EAL4+
- SQL 2008 Enterprise x64 SP1: certificado EAL4+
- Forefront Client Security:-Sin certificar
- System Center Data Protection Manager 2010:- Sin certificar

6.6. Controles Técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

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

a) Separación de ambientes de desarrollo, prueba y producción
b) Control de versiones para los componentes desarrollados

6.6.2. Controles de administración de seguridad

Existen controles respecto a la integridad del sistema de archivos de la AC ONTI que permiten controlar si hubo alteraciones no autorizadas.

6.6.3. Calificaciones de seguridad del ciclo de vida

No aplicable

6.7. Controles de seguridad de red

Los servicios que provee el Certificador que se encuentran conectados a una red de comunicación pública, son protegidos por la tecnología apropiada que garantiza su seguridad.

6.8. Controles de ingeniería de módulos criptográficos

El dispositivo criptográfico utilizado por el certificador está certificado por el NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por las AR están certificados por NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

Los dispositivos criptográficos utilizados por suscriptores de nivel de seguridad Alto están certificados por NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

7. Perfiles de Certificados y de Listas de Certificados Revocados

7.1. Perfil del certificado

Los certificados emitidos por el Certificador respaldados por esta Política de Certificación cumplen con los requerimientos de la DA 6/2007 y lo establecido en la especificación ITU X509 versión 3 (ISO/IEC 9594-8), adoptada como Estándar Técnico de la Infraestructura de Firma Digital de la República Argentina.

El Certificador adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

- RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” [RFC3739].
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC5280].

7.1.1. Perfil del certificado de la persona física

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión (Version)		V3 2 (correspondiente a versión 3)
Número de serie (SerialNumber)	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)	1.2.840.113549.1.1.5	sha1RSA
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
(notBefore/notAfter)	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
	email	E=<dirección de correo del suscriptor>
	serialNumber - 2.5.4.5	SERIALNUMBER=<Tipo> <Número de documento> <Versión=1 char>
	title - 2.5.4.12	T=<Nombre del cargo> o <lo indicado en el convenio correspondiente> (posición o función del suscriptor dentro de la organización, debe corresponder con los atributos O/OU y con la certificación de cargo presentada)
	organizationName - 2.5.4.10	O=<Nombre de la organización> o <lo indicado en el convenio correspondiente>
	organizationalUnitName - 2.5.4.11	OU=<Nombre de la unidad donde desarrolla su función> o <lo indicado en el convenio correspondiente>
	localityName - 2.5.4.7	L=<Nombre de localidad>
	stateOrProvinceName - 2.5.4.8	S = <Nombre de la provincia>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor	public key algorithm 1.2.840.11.35.49.1.1.1	RSA
	Public key length	**1024 bits**

	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas (Basic Constraints)	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave (Key Usage)	keyUsage 2.5.29.15	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del asunto (Subject Key Identifier)	(Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	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
Bases del certificado		[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://pki.jgm.gov.ar/cps/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: http://pkicont.jgm.gov.ar/cps/cps.pdf Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la República Argentina, Autoridad Certificante Raíz
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.)
Uso Extendido de Clave (Extended Key Usage)	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 (Subject Alternative Name)	SubjectAltName 2.5.29.17	Name = <Dirección de correo electrónico> (dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822)

Acceso Información Emisor (Authority Information Access)		[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 Nombre alternativo: Dirección URL=http://PKI.jgm.gov.ar/ocsp Dirección URL=http://PKIcont.jgm.gov.ar/ocsp
Algoritmo de Identificación		SHA1
Huella Digital		<Huella digital del certificado>
Información de la plantilla de certificado		Plantilla=1.3.6.1.4.1.311.21.8.15857867.913644.13845672.12138563.12347226.69.3351984.12088013 Número de versión mayor=100 Número de versión menor=2
Directivas de aplicación		[1]Directiva de certificado de la aplicación: Identificador de directiva=Autenticación del cliente [2]Directiva de certificado de la aplicación: Identificador de directiva=Correo seguro

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión (Version)		V3 2 (correspondiente a versión 3)
Número de serie (SerialNumber)	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)	1.2.840.113549.1.1.5	sha1RSA
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
(notBefore/notAfter)	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
	email	E=<dirección de correo del suscriptor>
	serialNumber - 2.5.4.5	SERIALNUMBER=<Tipo> <Número de documento> <Versión=1 char>
	title - 2.5.4.12	T=<Nombre del cargo> o <lo indicado en el convenio correspondiente> (posición o función del suscriptor dentro de la organización, debe corresponder con los atributos O/OU y con la certificación de cargo presentada)
	organizationName - 2.5.4.10	O=<Nombre de la organización> o <lo indicado en el convenio correspondiente>
	organizationalUnitName - 2.5.4.11	OU=<Nombre de la unidad donde desarrolla su función> o <lo indicado en el convenio correspondiente>
	localityName - 2.5.4.7	L=<Nombre de localidad>
	stateOrProvinceName - 2.5.4.8	S = <Nombre de la provincia>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor	public key algorithm 1.2.840.11.35.49.1.1.1	RSA
	Public key length	**2048 bits**
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas (Basic Constraints)	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave (Key Usage)	keyUsage 2.5.29.15	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0

Identificador de clave del asunto (Subject Key Identifier)	(Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	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
Bases del certificado		[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://pki.jgm.gov.ar/cps/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: http://pkicont.jgm.gov.ar/cps/cps.pdf Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la República Argentina, Autoridad Certificante Raíz
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.)
Uso Extendido de Clave (Extended Key Usage)	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 (Subject Alternative Name)	SubjectAltName 2.5.29.17	Name = <Dirección de correo electrónico> (dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822)
Acceso Información Emisor (Authority Information Access)		[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 Nombre alternativo: Dirección URL=http://PKI.jgm.gov.ar/ocsp Dirección URL=http://PKIcont.jgm.gov.ar/ocsp
Algoritmo de Identificación		SHA1
Huella Digital		<Huella digital del certificado>

Información de la plantilla de certificado		Plantilla=1.3.6.1.4.1.311.21.8.15857867.913644.13845672.12138563.12347226.69.3351984.12088013 Número de versión mayor=100 Número de versión menor=2
Directivas de aplicación		[1]Directiva de certificado de la aplicación: Identificador de directiva=Autenticación del cliente [2]Directiva de certificado de la aplicación: Identificador de directiva=Correo seguro

7.1.2. Perfil del certificado del servicio de consulta OCSP

En lo referente a OCSPs el certificador adhiere a las recomendaciones del documento:

Certificado x.509 v3 Atributos Extensiones	OIDs	Contenido
Versión (Version)		2 (correspondiente a versión 3)
Número de serie (SerialNumber)	Serial Number 2.5.4.5	<Número de serie del certificado>
Algoritmo de Firma (SignatureAlgorithm)	1.2.840.113549.1.1.5	sha1RSA
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
Validez (desde, hasta)	notBefore notAfter	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario <fecha y hora de emisión UTC+ 7 dias> yyyy/mm/dd hh:mm:ss huso-horario

Nombre distintivo del suscriptor (Subject)	commonName - 2.5.4.3	CN = PKIWEBSW001V.ACPKI.AR commonName = Servicio OCSP
Clave pública del suscriptor (Subject public key info)	public key algorithm 1.2.840.11.35.49.1.1.1	RSA
	Public key length	1024 bits
	Clave pública del suscriptor	<Clave pública del suscriptor> (PKCS#1)
Restricciones básicas (Basic Constraints)	basicConstraint 2.5.29.19	cA = False pathLengthConstraint = Null
Usos de clave (Key Usage)	keyUsage 2.5.29.15	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del asunto (Subject Key Identifier)		b6 a6 56 b4 6f 04 7f 88 60 8f f8 4c 48 31 45 d9 0c 70 d2 0c Contiene un Hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	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
Bases del certificado		[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://pki.jgm.gov.ar/cps/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: http://pkicont.jgm.gov.ar/cps/cps.pdf Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la Republica Argentina, Autoridad Certificante Raiz
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	Id. de clave=70 ba 03 71 7a d8 10 e4 ee 52 b5 7f 32 8f 9f 6c 2e f7 84 0d keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.)

Uso Extendido de Clave (Extended Key Usage)		Firma de OCSP (1.3.6.1.5.5.7.3.9) OCSP signing id-kp-OCSPSigning oid 1.3.6.1.5.5.7.3.9
Nombres Alternativos del Suscriptor (Subject Alternative Name)	SubjectAltName 2.5.29.17	Nombre DNS=PKIWEBSW001V.ACPKI.AR
Acceso Información Emisor (Authority Information Access)		caIssuers <http> <URL> [1]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://www.jgm.gov.ar/pki/cer/ONTIAC.cer caOCSP <http> <URL> [2]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://www.jgm.gov.ar/pki/ocsp/
Algoritmo de Identificación		SHA1
Huella Digital		<Huella digital de la CRL>
Información de la plantilla de certificado		Plantilla=1.3.6.1.4.1.311.21.8.15857867.913644.13845672.12138563.12347226.69.3520907.9008002 Número de versión mayor=100 Número de versión menor=1
Directivas de aplicación		[1]Directiva de certificado de la aplicación: Identificador de directiva=Firma de OCSP
Comprobacion de no revocacion de OCSP		05 00

7.1.3. Perfil del certificado de AC

Certificado x.509 v3 Atributos Extensiones	OIDs	Contenido
Versión (Version)		V3 2 (correspondiente a versión 3)
Número de serie (SerialNumber)	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la CA RAIZ a cada certificado de hasta 20 octetos)
Algoritmo de Firma (SignatureAlgoritm)	1.2.840.113549.1.1.5	sha1RSA 1.2.840.113549.1.1.5 SHA 1 with RSA Encryption
Nombre distintivo del emisor	commonName - 2.5.4.3	CN =AC Raíz
	serialNumber - 2.5.4.5	SERIALNUMBER=
	organizationName - 2.5.4.10	O = Infraestructura de Firma Digital
	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
(notBefore/notAfter)	notAfter	<fecha y hora de emisión UTC+ 10 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	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
		OU=Secretatria de Gestion Publica
		OU= Subsecretaria de Tecnologias de Gestion
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject public key info)	Public Key Algorithm	RSA
	Publick key leght	4096 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas (Basic Constraints)		Tipo de asunto=Entidad emisora de certificados (CA) Restricción de longitud de ruta=0 CA = TRUE PathRestriccionLength= 0

Usos de clave (Key Usage)		digitalSignature = 0 nonRepudiation = 0 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 1 cRLSign = 1 encipherOnly = 0 decipherOnly = 0
Identificador de clave del asunto (Subject Key Identifier)		Contiene un Hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRL Distribution Point)		DistributionPoint [1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://acraiz.cdp1.gov.ar/ca.crl [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://acraiz.cdp2.gov.ar/ca.crl
Bases del Certificado		[1]Directiva de certificados: Identificador de directiva=2.16.32.1.1.0 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://acraiz.gov.ar/cps.pdf [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso=Ley 25.506 - Infraestructura de Firma Digital de la Republica Argentina, Autoridad Certificante Raiz
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)		keyIdentifier = <Identificador de la clave de la AC>
Acceso Información Emisor (Authority Information Access)		[1]Acceso a información de Emisor Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=**http://acraiz.gov.ar/ca.crt**
Algoritmo de Identificación		SHA1
Huella Digital		<xx xx>

7.2. Perfil de la lista de certificados revocados

En lo referente a CRLs el certificador adhiere a las recomendaciones del documento:

- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC5280]

Atributos Extensiones	Nombre del campo y OID	Contenido
Versión (Version)		1 (correspondiente a versión 2)
Algoritmo de Firma (SignatureAlgorithm)	1.2.840.113549.1.1.5	SHA1RSA
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
Proxima Actualización	nextUpdate	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 byte 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)	OID - 2.5.29.20	Número de la CRL
Indicador Delta CRL	Delta CRL Indicator - 2.5.29.27	Delta CRL

Puntos de Distribución del emisor (IssuingDistributionPoints)	IssuingDistributionPoints - 2.5.29.28	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección Dirección URL=http://pki.jgm.gov.ar/crl/FD.crl [2]Punto de distribución CRL Nombre del punto de distribución: Nombre Completo: Dirección URL=http://pkicont.jgm.gov.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	Fecha de Invalidez	<fecha y hora UTC>
	Serial Number	Número de Serie del Certificado Revocado
	ReasonCode	Motivo de la Revocación
Algoritmo de Identificación Huella Digital		SHA1
Versión de CA		V0.0
Siguiente Publicación de lista de revocación		<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

8. ADMINISTRACIÒN DE ESPECIFICACIONES

8.1. Procedimientos de cambio de especificaciones

La presente Política será revisada y actualizada periódicamente por el Certificador y sus nuevas versiones se pondrán en vigencia, previa aprobación de la Autoridad de Aplicación.

8.2. Procedimientos de publicación y notificación

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

Una vez que la Autoridad de Aplicación notifique al Certificador la aprobación de las modificaciones a la Política de Certificación, éste procederá a su publicación en el sitio web antes mencionado.

8.3. Procedimientos de aprobación

La presente Política de Certificación, así como cualquier modificación a efectuar a la misma o cualquier cambio en los datos relativos a su licencia, serán sometidos a aprobación por parte de la Autoridad de Aplicación.

Historia de las revisiones:

Versión y Modificación	Fecha de emisión	Descripción	Motivo del Cambio
Versión 1.6	22/09/2010		

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