ANEXO

INFRAESTRUCTURA DE FIRMA DIGITAL – REPÚBLICA ARGENTINA

LEY Nº 25.506

POLÍTICA ÚNICA DE CERTIFICACIÓN

AUTORIDAD CERTIFICANTE

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN

SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA

JEFATURA DE GABINETE DE MINISTROS

Versión 2.0

Diciembre 2014

ANEXO

ÍNDICE

ANEXO

ANEXO

1. – INTRODUCCIÓN.

1.1. - Descripción general.

El presente documento establece las políticas que se aplican a la relación entre un Certificador Licenciado en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley N° 25.506 y sus modificatorias) y los solicitantes, suscriptores y terceros usuarios de los certificados que éste emita. Un certificado vincula los datos de verificación de firma digital de una persona física o jurídica o con una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

La autoridad de aplicación de la Infraestructura de firma digital antes mencionada es la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, siendo la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, quien entiende en las funciones de ente licenciante.

1.2. - Nombre e Identificación del Documento.

Nombre: Política Única de Certificación de la Oficina Nacional de Tecnologías de Información.

Versión: 2.0

Fecha de aplicación:

Sitio de publicación: http://pki.jgm.gob.ar/cps/cps.pdf

OID: 2.16.32.1.1.3

Lugar: Ciudad Autónoma de Buenos Aires, República Argentina

ANEXO

1.3. – Participantes.

Integran la infraestructura del Certificador las siguientes entidades:

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.

Oficina Nacional de Tecnologías de Información

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

Correo electrónico: aconti@jefatura.gob.ar

Teléfonos: (54 11) 5985-8663

(54 11) 4343-9001 Int. 533

1.3.2. - Autoridad de Registro.

El Certificador posee una estructura de Autoridades de Registro, en adelante 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 organismos públicos que han sido habilitados para operar como AR del Certificador, incluyendo su domicilio, datos de contacto y si operan bajo modalidad de Puesto Móvil, se encuentran disponibles en su sitio web https://pki.jgm.gob.ar/app

ANEXO

1.3.3. - Suscriptores de certificados.

Podrán ser suscriptores de los certificados emitidos por la Autoridad Certificante de la ONTI, en adelante AC-ONTI:

- Las personas físicas que desempeñen funciones en entes públicos estatales.
- Las personas físicas o jurídicas que realicen trámites con el Estado, cuando existe una aplicación que requiera una firma digital, siempre que se cumplan las siguientes condiciones:
    a) Deberá existir una AR autorizada por el Certificador en el organismo responsable de la aplicación, quien debe informar de la misma al Certificador.
    b) Los solicitantes de certificados deberán efectuar el trámite de solicitud exclusivamente ante la AR autorizada.
- Los organismos y las empresas públicas.

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

Asimismo, la AC ONTI emite certificados para proveedores de servicios en relación a la firma digital, según lo dispuesto en el artículo 10° de la Decisión Administrativa N° 927 del 30 de noviembre de 2014.

1.3.4. - Terceros Usuarios.

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación, toda persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo al Anexo I del Decreto N° 2628 del 19 de diciembre de 2002.

ANEXO

1.4. - Uso de los certificados.

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

1.5. - Administración de la Política.

1.5.1. - Responsable del documento.

Será responsable de la presente Política Única el máximo responsable del Certificador licenciado, con los siguientes datos:

Correo electrónico: aconti@jefatura.gob.ar

Teléfonos:

(54 11) 5985-8663

(54 11) 4343-9001 Int. 533

1.5.2. – Contacto.

La presente Política Única es administrada por el máximo responsable del Certificador Licenciado:

Correo electrónico: aconti@jefatura.gob.ar

Teléfono: (54 11) 5985-8663

(54 11) 4343-9001 Int. 533

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

ANEXO

La Política Única de Certificación y el Formulario de Adhesión del Anexo I han sido presentados y autorizados por el ente licenciante de acuerdo a lo dispuesto por la Decisión Administrativa N° 927/ 2014 por …….. .

1.6. - Definiciones y Acrónimos.

1.6.1. – Definiciones.

- Autoridad de Aplicación: la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.
- Autoridad de Registro: es la entidad que tiene a su cargo las funciones de:
  - Recepción de las solicitudes de emisión de certificados.
  - Validación de la identidad y autenticación de los datos de los titulares de certificados.
  - Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
  - Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
  - Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
  - Identificación y autenticación de los solicitantes de revocación de certificados.
  - Archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el Certificador Licenciado.

ANEXO

- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

  Dichas funciones son delegadas por el Certificador Licenciado. Puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del ente licenciante.

- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un Certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).
- Certificador Licenciado: Se entiende por Certificador Licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. (artículo 17 de la Ley N° 25.506).
- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. (Anexo al Decreto N° 2628/02).
- Ente licenciante: la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS es Ente Licenciante.
- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada

ANEXO

digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL). (Anexo al Decreto N° 2628/02).

- Manual de Procedimientos: Conjunto de prácticas utilizadas por el Certificador Licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS). (Anexo al Decreto N° 2628/02).
- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el Certificador Licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02).
- Plan de Continuidad de las operaciones: Conjunto de procedimientos a seguir por el Certificador Licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del Certificador Licenciado. (Anexo al Decreto N° 2628/02).
- Política de Privacidad: conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.
- Servicio OCSP (Protocolo en línea del estado de un certificado – "Online Certificate Status Protocol"): servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el Certificador que brinda el servicio.

ANEXO

- Suscriptor o Titular de certificado digital: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- Tercero Usuario: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. (artículo 3° del Decreto N° 724 del 8 de junio de 2006).

1.6.2. – Acrónimos.

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

CUIT - Clave Única de Identificación Tributaria.

IEC - International Electrotechnical Commission.

IETF - Internet Engineering Task Force.

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

OID - Identificador de Objeto ("Object Identifier").

ONTI - Oficina Nacional de Tecnologías de Información.

RFC - Request for Comments.

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

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

ANEXO

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 no 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;

ANEXO

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 Única 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.

2.1. – Repositorios.

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

2.2. - Publicación de información del Certificador.

El Certificador garantizará el acceso a la información actualizada y vigente publicada en su repositorio de los siguientes elementos:

ANEXO

a) Formulario de Adhesión del Anexo I.

b) Política Única de Certificación.

c) Acuerdo Tipo con suscriptores.

d) Términos y condiciones Tipo con terceros usuarios ("*relying parties*").

e) Política de Privacidad.

f) Manual de Procedimientos (parte pública).

g) Información relevante de los informes de su última auditoría.

h) Repositorio de certificados revocados.

i) Certificados del Certificador Licenciado y acceso al de la Autoridad Certificante Raíz.

Adicionalmente a lo indicado, el Certificador mantiene en el mismo repositorio en línea de acceso público:

a) Su certificado OCSP.

b) Las Políticas de Certificación anteriores.

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

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

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 Única de Certificación.

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

ANEXO

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, la Política Única 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:

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 la Autoridad de Aplicación.

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

2.3. - Frecuencia de publicación.

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

2.4. - Controles de acceso a la información.

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

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

ANEXO

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

3. - IDENTIFICACIÓN Y AUTENTICACIÓN.

En esta sección se describen los procedimientos empleados para autenticar la identidad de los solicitantes de certificados digitales y utilizados por las Autoridades Certificantes o sus AR como prerrequisito para su emisión. También se describen los pasos para la autenticación de los solicitantes de renovación y revocación de certificados.

3.1.- Asignación de nombres de suscriptores.

3.1.1. - Tipos de Nombres.

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

3.1.2. - Necesidad de Nombres Distintivos.

Para los certificados de **los proveedores de servicios de firma digital o de aplicación**:

- "*commonName"* (OID 2.5.4.3: Nombre común): DEBE corresponder al nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.

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

ANEXO

- "*organizationName*" (OID 2.5.4.10: Nombre de la organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.

- "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

El valor para el campo [código de identificación] es:

- "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de **Personas Físicas**:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponderse con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.
- "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: "[tipo de documento]" "[nro. de documento]"

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

ANEXO

- En caso de ciudadanos argentinos o residentes: "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral.
- En caso de extranjeros:
    - "PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.
    - "EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.

- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de **Personas Jurídicas Públicas o Privadas**:

- "commonName" (OID 2.5.4.3: Nombre común): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada o con el nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).

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

- "organizationName" (OID 2.5.4.10: Nombre de la organización): para certificados de aplicaciones, DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada.

- "serialNumber" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y

ANEXO

respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

Los valores posibles para el campo [código de identificación] son:

a) "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

b) "ID" [país]: Número de identificación tributario para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

"countryName" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de 2 caracteres.

Para los certificados de **sitio seguro**:

- "commonName" (OID 2.5.4.3: Nombre común): DEBE contener la denominación del sitio web de Internet que se busca proteger.

- "organizationalUnitName" (OID 2.5.4.11: Nombre de la Suborganización): DEBE contener a las unidades operativas de las que depende el sitio web, de corresponder, pudiendo utilizarse varias instancias de este atributo de ser necesario.

- "organizationName" (OID 2.5.4.10: Nombre de la Organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del sitio web.

- "serialNumber" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

ANEXO

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

- "countryName" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

3.1.3. - Anonimato o uso de seudónimos.

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

3.1.4. - Reglas para la interpretación de nombres.

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

3.1.5. - Unicidad de nombres.

El nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias se basa en la utilización del número de identificación laboral o tributaria, tanto en el caso de personas físicas como jurídicas.

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

ANEXO

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados, excepto en el caso de personas jurídicas o aplicaciones, en los que se aceptará en base a la documentación presentada.

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

3.2. - Registro inicial.

Se describen los procedimientos a utilizar para autenticar, como paso previo a la emisión de UN (1) certificado, la identidad y demás atributos del solicitante que se presente ante el Certificador o ante la Autoridad de Registro operativamente vinculada. Se establecen los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

El Certificador DEBE cumplir con lo establecido en:

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

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

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

ANEXO

El Certificador comprueba que el solicitante se encuentra en posesión de la clave privada mediante la verificación de la solicitud del certificado digital en formato PKCS#10, el que no incluye dicha clave. Las claves siempre son generadas por el solicitante. En ningún caso el Certificador licenciado ni sus AR podrán tomar conocimiento o acceder bajo ninguna circunstancia a las claves de los solicitantes o titulares de los certificados, conforme el inciso b) del artículo 21 de la Ley N° 25.506.

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

Los procedimientos de autenticación de la identidad de los suscriptores de los certificados de personas jurídicas públicas o privadas comprenden los siguientes aspectos:

a) El requerimiento debe efectuarse únicamente por intermedio del responsable autorizado a actuar en nombre del suscriptor para el caso de certificados de personas jurídicas o de quien se encuentre a cargo del servicio, aplicación o sitio web.

b) El Certificador o la AR, en su caso, verificará la identidad del responsable antes mencionado y su autorización para gestionar el certificado correspondiente.

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

d) La identidad de la Persona Jurídica titular del certificado o responsable del servicio, aplicación o sitio web deberá ser verificada mediante documentación que acredite su condición de tal.

La documentación a presentar para la autenticación es la siguiente:

Para persona jurídicas privadas:

ANEXO

-Constancia de inscripción en el Registro Societario correspondiente a la jurisdicción, y poder que acredita el carácter de representante legal o apoderado de la persona autorizada a iniciar el trámite.

Ambos documentos deben estar autenticados ante escribano.

Opcionalmente, se podrá presentar constancia de escribano público de la existencia y validez de los mencionados documentos.

Para personas jurídicas públicas:

-Nota de la máxima autoridad del organismo solicitante acreditando la autorización para gestionar el certificado, acompañada de copia fiel de la norma de creación del organismo.

Además, cuando corresponda se requiere la presentación de nota que incluya nombre de la aplicación, servicio o unidad operativa responsable.

El Certificador DEBE cumplir con las siguientes exigencias reglamentarias impuestas por:

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

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

c) El artículo 34, inciso m) del Decreto Nº 2628/02 relativo a la protección de datos personales.

Debe conservarse la documentación que respalda el proceso de identificación de la persona responsable de la custodia de las claves criptográficas.

ANEXO

El responsable autorizado o a cargo del servicio, aplicación o sitio web debe firmar UN (1) acuerdo que contenga la confirmación de que la información incluida en el certificado es correcta.

3.2.3. - Autenticación de la identidad de Personas Físicas.

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

Se exige la presencia física del solicitante o suscriptor del certificado ante el Certificador o la Autoridad de Registro con la que se encuentre operativamente vinculado. La verificación se efectúa mediante la presentación de los siguientes documentos:

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

En todos los casos, se conservará UNA (1) copia digitalizada de la documentación de respaldo del proceso de autenticación por parte del Certificador o de la AR operativamente vinculada.

Se consideran obligatorias las exigencias reglamentarias impuestas por:

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

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

ANEXO

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

d) El artículo 34, inciso m) del Decreto Nº 2628/02 relativo a la protección de datos personales.

Adicionalmente, el Certificador debe celebrar UN (1) acuerdo con el solicitante o suscriptor, conforme el Anexo V de la presente Decisión Administrativa, del que surge su conformidad respecto a la veracidad de la información incluida en el certificado.

La Autoridad de Registro deberá verificar que el dispositivo criptográfico utilizado por el solicitante, si fuera el caso, cumple con las especificaciones técnicas establecidas por el ente licenciante.

3.2.4. - Información no verificada del suscriptor.

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

3.2.5. - Validación de autoridad.

Según lo dispuesto en el punto 3.2.2., el Certificador o la AR con la que se encuentre operativamente vinculado, verifica la autorización de la Persona Física que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente.

ANEXO

3.2.6. - Criterios para la interoperabilidad.

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

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

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

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

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

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

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

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

Si la solicitud del nuevo certificado se realiza antes de la expiración del certificado, no habiendo sido este revocado, no se exigirá la presencia física, debiendo el solicitante remitir la constancia firmada digitalmente del inicio del trámite de renovación.

En los certificados de personas jurídicas o de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, cumpliendo los pasos requeridos en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

ANEXO

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

En el caso de certificados digitales de personas físicas o jurídicas, la renovación en este apartado aplica a la emisión de UN (1) nuevo certificado sin que haya un cambio en la clave pública o en ningún otro dato del suscriptor. La renovación se podrá realizar solo UNA (1) vez y siempre que el certificado se encuentre vigente.

A los fines de la obtención del certificado, no se exigirá la presencia física del suscriptor, debiendo éste remitir la constancia firmada digitalmente del inicio del trámite de renovación.

En los certificados de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, según lo indicado en el apartado anterior.

3.4. - Requerimiento de revocación.

El suscriptor cuando se trate de los certificados de persona física o la persona física a cargo de la custodia de la clave privada para el resto de los casos, podrá revocar el certificado digital utilizando cualquiera de los siguientes métodos:

- A través de la aplicación de la AC ONTI: https://pki.jgm.gob.ar/app/ que se encuentra disponible VEINTICUATRO (24) horas, si tiene acceso a su clave privada o utilizando el código de revocación que le fuera informado al momento de la emisión de su certificado.
- Presentándose ante la AR correspondiente con documento que permita acreditar su identidad en caso de no poder utilizar alguno de los anteriores.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1. - Solicitud de certificado.

ANEXO

4.1.1. - Solicitantes de certificados.

Se describen las condiciones que deben cumplir los solicitantes de certificados.

4.1.2. - Solicitud de certificado.

Las solicitudes sólo podrán ser iniciadas por el solicitante, en el caso de certificados de personas físicas, por el representante legal o apoderado con poder suficiente a dichos efectos, o por el Responsable del Servicio, aplicación o sitio web, autorizado a tal fin, en el caso de personas jurídicas.

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2. - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas y 3.2.3. - Autenticación de la identidad de Personas Físicas, así como la constancia de C.U.I.T. o C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores de certificados.

Cuando se trate de solicitudes de certificados de personas físicas, el solicitante debe probar su carácter de suscriptor para esta Política Única de Certificación de acuerdo a lo indicado en el apartado 1.3.3. En el caso de solicitudes de certificados de proveedores de servicios de firma digital, aplicaciones, personas jurídicas o sitio seguro, el carácter de suscriptor debe ser probado por el representante legal o apoderado, el responsable del servicio, aplicación o sitio web, autorizado a tal fin.

Los pasos para realizar la solicitud son los siguientes:

a) Ingresar al sitio web del Certificador https://pki.jgm.gob.ar/app/ seleccionando el enlace a la aplicación de solicitud de emisión de certificados.
b) Completar la solicitud de certificado con los datos requeridos de acuerdo al tipo de certificado, seleccionando la AR que le corresponde.

ANEXO

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

d) Enviar su solicitud a la AC ONTI e imprimirla.

e) Presentarse ante la AR correspondiente para realizar la identificación personal y la verificación de la documentación requerida en cada caso.

Cabe agregar que 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.

4.2. - Procesamiento de la solicitud del certificado.

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

Adicionalmente a la documentación enunciada en el apartado 3.2.3, se deberá adjuntar:

- Nota de solicitud de certificado, firmada por el solicitante.
- Para acreditar el desempeño de funciones en entes públicos estatales, alternativamente se podrá presentar cualquiera de los siguientes documentos:

  -Copia fiel del Acto Administrativo de su designación.

ANEXO

-Constancia emitida por la Oficina de Recursos Humanos, Personal o equivalente de su organismo o entidad, que certifique la prestación de sus servicios.

-Constancia de certificación de servicios firmada por un superior jerárquico del organismo en que se desempeña el solicitante.

En caso de tratarse de persona físicas que requieran su certificado para efectuar trámites con el Estado, deberá cumplir con las condiciones adicionales establecidas por la AR asociada a ese trámite.

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

- Verifica la existencia de la solicitud en la aplicación del Certificador.
- Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida.
- Verifica la titularidad de la solicitud mediante el control de la nota de solicitud del certificado.
- Requiere al solicitante o su representante autorizado la firma de la nota de solicitud en su presencia.
- Resguarda toda la documentación respaldatoria del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

4.3. - Emisión del certificado.

4.3.1. - Proceso de emisión del certificado.

Cumplidos los recaudos del proceso de validación de identidad y otros datos del solicitante, de acuerdo con esta Política Única de Certificación y una vez aprobada la solicitud de

certificado por la AR, la AC ONTI emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor.

4.3.2. - Notificación de emisión.

La notificación de la emisión del certificado se efectúa a través de un correo electrónico remitido por la aplicación del Certificador a la cuenta de correo declarada por el solicitante o representante autorizado al momento de iniciar el trámite. En dicho correo se indica el enlace al que debe acceder para descargar el certificado emitido.

4.4. - 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 por los medios indicados en el apartado anterior.

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

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

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

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;
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.

ANEXO

De acuerdo a lo establecido en la Decisión Administrativa N° 927/2014:

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

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

Los Terceros Usuarios deben:

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

b) Verificar la validez del certificado digital.

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

Se aplica el punto 3.3.2.- Generación de UN (1) certificado con el mismo par de claves.

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

En el caso de certificados digitales de Personas Físicas, la renovación del certificado posterior a su revocación o luego de su expiración requiere por parte del suscriptor el cumplimiento de los procedimientos previstos en el punto 3.2.3. - Autenticación de la identidad de Personas Físicas.

ANEXO

Si la solicitud de UN (1) nuevo certificado se realiza antes de la expiración del anterior, no habiendo sido este revocado, no se exigirá la presencia física, debiendo el solicitante remitir la constancia firmada digitalmente del inicio del trámite de renovación.

Para los certificados de aplicaciones, incluyendo los de servidores, los responsables deben tramitar UN (1) nuevo certificado en todos los casos, cumpliendo los pasos requeridos en el apartado 3.2.2. Autenticación de la Identidad de las Personas Jurídicas Públicas o Privadas.

4.8. - Modificación del certificado.

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

4.9. - Suspensión y Revocación de Certificados.

Los certificados serán revocados de manera oportuna y sobre la base de UNA (1) solicitud de revocación de certificado validada.

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

4.9.1. - Causas de revocación.

El Certificador procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

ANEXO

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados de Personas Jurídicas o Aplicación.
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por Resolución de la Autoridad de Aplicación.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
- Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
- Por revocación de su propio certificado digital.

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

ANEXO

4.9.2. - 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 responsable autorizado que efectuara el requerimiento, en el caso de certificados de persona jurídica o aplicación.

c) El responsable autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación.

d) El responsable autorizado por la Persona Jurídica responsable del sitio web, en el caso de certificados de sitio seguro.

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

f) El Certificador o la AR operativamente vinculada.

g) El ente licenciante.

h) La autoridad judicial competente.

i) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación.

El Certificador garantiza que:

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

b) Las solicitudes de revocación, así como toda acción efectuada por el Certificador o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.

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

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

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

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.gob.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.gob.ar/app/ que se encuentra disponible VEINTICUATRO (24) horas, utilizando el código de revocación que le fue entregado al momento de la emisión del certificado.
- 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 pertenecientes a entes públicos estatales, la revocación podrá ser solicitada por un responsable autorizado del organismo en el que se desempeñe el titular del certificado, por nota dirigida al Responsable de la AR.

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

4.9.4. - Plazo para la solicitud de revocación.

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

ANEXO

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

El Certificador dispone de un servicio de recepción de solicitudes de revocación que se encuentra disponible en forma permanente, SIETE POR VEINTICUATRO (7x24) horas a través de la aplicación web de la AC ONTI.

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

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

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

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

Los Terceros Usuarios están obligados a confirmar la autenticidad y validez de las listas de certificados revocados mediante la verificación de la firma digital del Certificador y de su período de validez.

El Certificador cumple con lo establecido en el artículo 34, inciso g) del Decreto Nº 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes Anexos.

ANEXO

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

El Certificador genera y publica una Lista de Certificados Revocados asociada a esta Política Única de Certificación con una frecuencia diaria, disponible en:

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

y en:

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

con listas complementarias (delta CRL) en modo horario.

4.9.8.- Vigencia de la lista de certificados revocados.

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

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

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

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

ANEXO

4.9.10. - 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.gob.ar/ocsp

4.9.11. - 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 Única de Certificación.

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

En caso de compromiso de su clave privada, el titular del certificado correspondiente se encuentra obligado a comunicar inmediatamente dicha circunstancia al Certificador mediante alguno de los mecanismos previstos en el apartado 4.9.3. - Procedimientos para la solicitud de revocación.

4.9.13. - Causas de suspensión.

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

4.9.14. - Autorizados a solicitar la suspensión.

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

ANEXO

4.9.15. - Procedimientos para la solicitud de suspensión.

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

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

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

4.10. – Estado del certificado.

4.10.1. – Características técnicas.

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

- Lista de certificados revocados (CRL).
- Servicio OCSP.

Respecto a la CRL, se emite cada VEINTICUATRO (24) horas y delta CRLs en modo horario.

Con respecto a OCSP, permite verificar si el certificado se encuentra vigente o ha sido revocado.

4.10.2. – Disponibilidad del servicio.

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

4.10.3. – Aspectos operativos.

No existen otros aspectos a mencionar.

ANEXO

4.11. – Desvinculación del suscriptor.

Una vez expirado el certificado o si este fuera revocado, de no tramitar un nuevo certificado, su titular se considera desvinculado de los servicios del Certificador.

De igual forma se producirá la desvinculación, ante el cese de las operaciones del certificador.

4.12. – Recuperación y custodia de claves privadas.

En virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 25.506, el Certificador licenciado se obliga a no realizar bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados digitales. Asimismo, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley antes mencionada, el suscriptor de un certificado emitido en el marco de esta Política Única de Certificación se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación.

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

Se describen a continuación los procedimientos referidos a los controles de seguridad física, de gestión y operativos implementados por el Certificador. La descripción detallada se encuentra en el Plan de Seguridad.

5.1. - Controles de seguridad física.

Se cuenta con controles de seguridad relativos a:

a) Construcción y ubicación de instalaciones.

b) Niveles de acceso físico.

c) Comunicaciones, energía y ambientación.

d) Exposición al agua.

e) Prevención y protección contra incendios.

f) Medios de almacenamiento.

g) Disposición de material de descarte.

h) Instalaciones de seguridad externas.

5.2. - Controles de Gestión.

Se cuenta con controles de seguridad relativos a:

a) Definición de roles afectados al proceso de certificación.

b) Número de personas requeridas por función.

c) Identificación y autenticación para cada rol.

d) Separación de funciones

5.3. - Controles de seguridad del personal.

Se cuenta con controles de seguridad relativos a:

ANEXO

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

b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.

d) Frecuencia de procesos de actualización técnica.

e) Frecuencia de rotación de cargos.

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

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

5.4. - Procedimientos de Auditoría de Seguridad.

Se mantienen políticas de registro de eventos, cuyos procedimientos detallados serán desarrollados en el Manual de Procedimientos.

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

a) Tipo de eventos registrados: se cumple con lo establecido en el Anexo II Sección 3.

b) Frecuencia de procesamiento de registros.

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

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

e) Procedimientos de resguardo de los registros.

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

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

h) Evaluación de vulnerabilidades.

5.5. - Conservación de registros de eventos.

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

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

Se respeta lo establecido en el Anexo II Sección 3 respecto del registro de eventos.

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

a) Tipo de registro archivado: se cumple con lo establecido en el Anexo II Sección 3.

b) Período de guarda de los registros.

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

d) Procedimientos de resguardo de los registros.

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

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

g) Procedimientos para obtener y verificar la información archivada.

5.6. - Cambio de claves criptográficas.

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

En todos los casos el cambio de claves criptográficas 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.

5.7. - Plan de Continuidad de las Operaciones.

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

Se han desarrollado procedimientos referidos a:

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

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

c) Recuperación ante compromiso o sospecha de compromiso de la clave privada del Certificador.

ANEXO

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

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

5.8. - Plan de Cese de Actividades.

Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del certificador o de una o varias de sus autoridades certificantes o de registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación al ente licenciante, suscriptores, terceros usuarios, otros Certificadores y otros usuarios vinculados.

b) Revocación del certificado del Certificador y de los certificados emitidos.

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

El responsable de la custodia de archivos y documentación cumple con idénticas exigencias de seguridad que las previstas para el Certificador o su autoridad certificante o de registro que cesó.

Se contempla lo establecido por el artículo 44 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el artículo 33 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las

obligaciones establecidas en la presente decisión administrativa y sus correspondientes Anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA.

Se describen las medidas de seguridad implementadas por el Certificador para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además se incluyen los controles técnicos que se implementarán sobre las funciones operativas del Certificador, AR, repositorios, suscriptores, etcétera.

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

6.1.1. - Generación del par de claves criptográficas.

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

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

Las claves criptográficas de los suscriptores son generadas por software (nivel de seguridad normal) o por hardware (nivel de seguridad alto) y almacenada por ellos. En este último caso los dispositivos criptográficos utilizados deben ser FIPS 140-2 Nivel 2.

Las claves criptográficas utilizadas por los proveedores de otros servicios relacionados con la firma digital son generadas y almacenadas utilizando dispositivos criptográficos FIPS 140-2 Nivel 2 como mínimo.

ANEXO

6.1.2. - Entrega de la clave privada.

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

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

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

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, el de la AC Raíz de la REPÚBLICA ARGENTINA y aquellos emitidos a proveedores de otros servicios de firma digital se encuentran a disposición de los suscriptores y terceros usuarios en un repositorio en línea de acceso público a través de Internet en https://pki.jgm.gob.ar/app/

6.1.5. - Tamaño de claves.

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

Los suscriptores, incluyendo las AR y los proveedores de otros servicios de firma digital generan sus claves mediante el algoritmo RSA con un tamaño de clave 2048 bits, excepto el caso de las Autoridades de Sello de Tiempo que utilizarán una clave de 4096 bits.

6.1.6. - Generación de parámetros de claves asimétricas.

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

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

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

ANEXO

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

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

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

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

c) En caso de existir copias de resguardo de la clave privada, controles de seguridad establecidos sobre ellas.

d) Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico.

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

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

g) Procedimiento de destrucción de la clave privada.

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

6.2.1. – Controles y estándares para dispositivos criptográficos.

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

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

6.2.3. - Recuperación de clave privada.

Ante una situación que requiera recuperar su clave privada, y siempre que 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 con el mismo nivel de seguridad que aquel en el que se realicen las operaciones críticas de la AC ONTI.

No se implementan mecanismos de resguardo y recuperación de las claves privadas de 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 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, disponibilidad y confidencialidad, conservándola

en un lugar seguro, al igual que sus elementos de activación, de acuerdo a lo dispuesto por la Decisión Administrativa Nº 927/14 en cuanto a los niveles de resguardo de claves.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

El par de claves criptográficas del Certificador se genera y almacena en dispositivos criptográficos conforme a lo establecido en la presente Política, 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. - Almacenamiento de claves privadas en dispositivos criptográficos.

El almacenamiento de las claves criptográficas del Certificador se realiza en el mismo dispositivo de generación que brinda un alto nivel de seguridad de acuerdo a la certificación FIPS 140-2 nivel 3 y nivel 4 de seguridad física de acuerdo a lo establecido en el Anexo II de la Decisión Administrativa JGM N° 927/2014.

Las claves criptográficas de las AR y de los suscriptores de certificados de nivel de seguridad Alto son almacenadas en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se generan, con los mismos niveles de seguridad.

6.2.8. - Método de activación de claves privadas.

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

6.2.9. - Método de desactivación de claves privadas.

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

6.2.10. - Método de destrucción de claves privadas.

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

6.2.11. – Requisitos de los dispositivos criptográficos.

La AC ONTI utiliza un dispositivo criptográfico con la certificación FIPS 140-2 Nivel 3 para la generación y almacenamiento de sus claves.

En el caso de las AR se utilizan dispositivos criptográficos FIPS 140-2 Nivel 2.

Los suscriptores que opten por un nivel de seguridad Alto utilizan dispositivos criptográficos FIPS 140-2 Nivel 2.

Los proveedores de otros servicios relacionados con la firma digital, utilizan dispositivos FIPS 140-2 Nivel 2 como mínimo.

6.3. - Otros aspectos de administración de claves.

6.3.1. - Archivo permanente de la clave pública.

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

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

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

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

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

6.4. - Datos de activación.

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

ANEXO

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

6.4.1. - Generación e instalación de datos de activación.

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

Ni el Certificador ni las AR implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores o AR 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 las AR, de los proveedores de otros servicios relacionados con la firma digital y demás suscriptores de certificados emitidos por la AC ONTI, la elección de contraseñas fuertes para la protección de sus claves privadas y para el acceso a los dispositivos criptográficos que utilicen, si fuera aplicable.

ANEXO

6.5. - Controles de seguridad informática.

6.5.1. - Requisitos Técnicos específicos.

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

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

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

6.5.2. - Requisitos 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+.

El dispositivo criptográfico utilizado por el Certificador está certificado por el NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por las AR y por los suscriptores con nivel de seguridad Alto están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2.

Los dispositivos criptográficos utilizados por los proveedores de otros servicios en relación a la firma digital están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2 como mínimo.

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

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

6.6.1. - Controles de desarrollo de sistemas.

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

- Separación de ambientes de desarrollo, prueba y producción.
- Control de versiones para los componentes desarrollados.
- Pruebas con casos de uso.

ANEXO

6.6.2. – Controles de gestión de seguridad

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

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

No aplicable.

6.7. - Controles de seguridad de red.

Los controles de seguridad de la red interna y externa de la AC ONTI se encuentran a cargo del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS.

6.8. – Certificación de fecha y hora.

La AC ONTI no presta el servicio de emisión de sello de tiempo.

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

7.1. - Perfil del certificado.

Todos los certificados son emitidos conforme con lo establecido en la especificación ITU X.509 versión 3, y cumplen con las indicaciones establecidas en la sección **"**2 - Perfil de

ANEXO

certificados digitales" del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados.

Perfil del certificado de 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	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	sha1RSA (1.2.840.113549.1.1.5)
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

ANEXO

	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 2 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=APELLIDO Nombre
	serialNumber - 2.5.4.5	SERIALNUMBER=<CUIT/CUIL> <Número>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	public key algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 1 decipherOnly = 1

ANEXO

Identificador de clave del suscriptor	subjectkeyIdentifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	ExtendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	SubjectAltName 2.5.29.17	Dirección de correo electrónico (campo optativo)
Información de Acceso de la AC	authorityInfo Access 1.3.6.1.5.5.7.1.1	URL=http://pki.jgm.gob.ar/ocsp

ANEXO

Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.1 (claves generadas por software)

Perfil del certificado de persona jurídica.

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgoritm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName	S=Ciudad Autónoma de Buenos Aires

ANEXO

	- 2.5.4.8	
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 3 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación de la Persona jurídica pública
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1

ANEXO

		keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 1 decipherOnly = 1
Identificador de clave del suscriptor	subjectkeyIdentifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	ExtendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)

ANEXO

Nombres Alternativos del Suscriptor	SubjectAltName 2.5.29.17	CN=APELLIDO Nombre de la persona física a cargo de la custodia de la clave privada. SN= <CUIT/CUIL> <Número> OID=2.5.4.12 T=<Relación que vincula a la persona física con la persona jurídica>
Información de Acceso de la AC	authorityInfoAccess 1.3.6.1.5.5.7.1.1	URL=http://pki.jgm.gob.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.3 (claves generadas por disp. 140-2 nivel 3) OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.1 (claves generadas por software)

Perfil del certificado de aplicaciones.

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

ANEXO

Algoritmo de Firma	signatureAlgoritm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 3 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación de la Aplicación
	organizationName 2.5.4.10	O=nombre dela Persona Jurídica Pública responsable de la aplicación
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con la aplicación
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica

ANEXO

		Pública responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 1 decipherOnly = 1
Identificador de clave del suscriptor	subjectkeyIdentifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor

ANEXO

Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Respuesta OCSP (1.3.6.1.5.5.7.3.9)
Información de Acceso de la AC	authority InfoAccess 1.3.6.1.5.5.7.1.1	URL=http://pki.jgm.gob.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.3 (claves generadas por disp. 140-2 nivel 3) OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.1 (claves generadas por software)

Perfil del certificado de sitio seguro.

ANEXO

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	serialNumber 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	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital SSL
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 1 año> yyyy/mm/dd hh:mm:ss huso-horario

ANEXO

Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del sitio web de Internet
	organizationName 2.5.4.10	O=nombre dela Persona Jurídica Pública responsable del sitio web de Internet
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa de la que depende el sitio web aplicación
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 0 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0

ANEXO

Identificador de clave del suscriptor	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pkissl.jgm.gob.ar/crl/FDssl.crl DirecciónURL=http://pkisslcont.jgm.gob.ar/crl/FDssl.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Autenticación del servidor (1.3.6.1.5.5.7.3.1)

ANEXO

Información de Acceso de la AC	authority InformationAccess 1.3.6.1.5.5.7.1.1	URL=http://pkissl.jgm.gob.ar/ocsp
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.1 (claves generadas por software)

Perfil del certificado de proveedores de servicios de firma digital.

Para Autoridad de Competencia.

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	serialNumber 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	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572

ANEXO

	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiración a establecer por AC ONTI> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del servicio de emisión de sello de competencia
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública o Privada responsable del servicio
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública o Privada>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits

ANEXO

	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 1 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectKey Identifier	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de sellos de competencia Revocados	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección

ANEXO

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

ANEXO

Para Autoridad de Sello de tiempo.

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión	Version	V3 2 (correspondiente a versión 3)
Número de serie	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC ONTI a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgoritm	sha1RSA 1.2.840.113549.1.1.5
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30680604572
	organizationName - 2.5.4.10	O=Jefatura de Gabinete de Ministros
	organizationalUnitName - 2.5.4.11	OU=Oficina Nacional de Tecnologías de Información
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiración a establecer por AC

ANEXO

		ONTI> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del servicio de emisión de sello de tiempo
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública o Privada responsable del servicio
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública o Privada>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null

ANEXO

Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de sellos de tiempo Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://pki.jgm.gob.ar/crl/FD.crl Dirección URL=http://pkicont.jgm.gob.ar/crl/FD.crl
Política de Certificación	certificatePolicies 2.5.29.32	[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://pki.jgm.gob.ar/cps/cps.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.

ANEXO

Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC ONTI)
Uso Extendido de Clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Certificación digital de fecha y hora (1.3.6.1.5.5.7.3.8)
Declaración del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

7.2. - Perfil de la lista de certificados revocados.

Las listas de certificados revocados correspondientes a la presente Política Única de Certificación son emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 y cumplen con las indicaciones establecidas en la sección **"**3 - Perfil de CRLs" del Anexo IV – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

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	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma

ANEXO

(Issuer)	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	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 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (es una cadena de 20 bytes que identifica unívocamente la clave pública de la AC ONTI que firmó el certificado.) Id. de clave=70 ba 03 71 7a d8 10 e4 ee 52 b5 7f 32 8f 9f 6c 2e f7 84 0d
Número de CRL	CRL Number	Número de la CRL

ANEXO

Puntos de Distribución del emisor	issuingDistributionPoints 2.5.29.28	[1]Punto de distribución CRL URL=http://pki.jgm.gob.ar/crl/FD.crl [2]Punto de distribución CRL URL=http://pkicont.jgm.gob.ar/crl/FD.crl Solo Contiene certificados de usuario = no Solo Contiene certificados de la entidad emisora = no Lista de revocación de Certificados Indirecta = no
Certificados Revocados (Revoked certificates)	InvalidityDate	<fecha y hora UTC>
	Serial Number	Número de Serie del Certificado Revocado
	ReasonCode	Motivo de la Revocación
Algoritmo de Identificación Huella Digital		SHA1 1.3.14.3.2.26
Versión de CA		V0.0
Siguiente Publicación de lista de revocación		<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

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

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Se implementa conforme a lo indicado en la especificación RFC 6960 y cumple con las indicaciones establecidas en la sección “4 - Perfil

de la consulta en línea del estado del certificado" del Anexo IV – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

En base a lo dispuesto por las normas vigentes, la ONTI, en su calidad de Certificador Licenciado se encuentra sujeta a las auditorías que llevan a cabo las siguientes entidades pertenecientes al Sector Público:

- Ente Licenciante de la Infraestructura Nacional de Firma Digital de la REPÚBLICA ARGENTINA.
- Sindicatura General de la Nación (SIGEN).
- Auditoría General de la Nación (AGN).
- Unidad de Auditoría Interna (UAI) de Jefatura de Gabinete de Ministros.

Las mencionadas entidades realizan las auditorías en base a sus programas los que son comunicados e informados oportunamente.

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

Los informes resultantes de las auditorías son elevados a las autoridades de la ONTI. Sus aspectos relevantes son publicados en forma permanente e ininterrumpida en su sitio web.

El Certificador cumple las exigencias reglamentarias impuestas por:

ANEXO

- Los artículos 33 y 34 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma Ley, relativo a la publicación de informes de auditoría.
- Los artículos 18 a 21 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría y el artículo 20, vinculado a conflicto de intereses.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1. – Aranceles.

El Certificador no percibe aranceles por ninguno de los servicios que pudiera brindar relacionados con esta Política Única 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.

9.2. - Responsabilidad Financiera.

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

9.3. – Confidencialidad.

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.

9.3.1. - Información confidencial.

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

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

ANEXO

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

9.3.2. - Información no confidencial

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

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

9.3.3. – Responsabilidades de los roles involucrados

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

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

No será necesario el consentimiento cuando:

- Los datos se hayan obtenido de fuentes de acceso público irrestricto;

- Los datos se limiten a nombre, Documento Nacional de Identidad, identificación tributaria o previsional u ocupación.
- Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular.

9.4. – Privacidad.

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

9.5 - Derechos de Propiedad Intelectual.

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

El derecho de autor de la presente Política Única de Certificación y de toda otra documentación generada por el Certificador en relación con la Infraestructura de Firma Digital, pertenece 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.

ANEXO

9.6. – Responsabilidades y garantías.

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

9.7. – Deslinde de responsabilidad.

Las limitaciones de responsabilidad del Certificador licenciado se rigen por lo establecido en el art. 39 de la Ley N° 25.506, en las disposiciones de la presente Política y en el Acuerdo con suscriptores.

9.8. – Limitaciones a la responsabilidad frente a terceros.

Las limitaciones de responsabilidad del Certificador Licenciado respecto a otras entidades participantes, se rigen por lo establecido en el art. 39 de la Ley N° 25.506, en las disposiciones de la presente Política y en los Términos y Condiciones con terceros usuarios.

9.9. – Compensaciones por daños y perjuicios.

No aplicable

9.10. – Condiciones de vigencia.

La presente Política Única de Certificación se encuentra vigente a partir de la fecha de su aprobación por parte del Ente Licenciante y hasta tanto sea reemplazada por una nueva

versión. Todo cambio en la Política, una vez aprobado por el ente licenciante, será debidamente comunicado al suscriptor.

9.11.- Avisos personales y comunicaciones con los participantes.

No aplicable.

9.12.- Gestión del ciclo de vida del documento.

No se agrega información.

9.12.1. - Procedimientos de cambio.

Toda modificación a la Política Única de Certificación es aprobada previamente por el ente licenciante conforme a lo establecido por la Ley N° 25.506, artículo 21, inciso q) y por la Decisión Administrativa JGM N° 927/2014 y sus anexos respectivos.

Toda Política Única de Certificación es sometida a aprobación del ente licenciante durante el proceso de licenciamiento.

Todo cambio en la Política Única de Certificación es comunicado al suscriptor.

La presente Política Única de Certificación será revisada y actualizada periódicamente por el Certificador y sus nuevas versiones se pondrán en vigencia, previa aprobación del ente licenciante.

ANEXO

9.12.2 – Mecanismo y plazo de publicación y notificación.

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

9.12.3. – Condiciones de modificación del OID.

No aplicable.

9.13. - Procedimientos de resolución de conflictos.

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

La presente Política Única 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 interponer ante el ente licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.

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

ANEXO

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

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

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

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

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

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

9.14. - Legislación aplicable.

La legislación que respalda la interpretación, aplicación y validez de esta Política Única de Certificación es la Ley Nº 25.506, el Decreto Nº 2628/02, y toda otra norma complementaria dictada por la autoridad competente.

ANEXO

9.15. – Conformidad con normas aplicables.

La legislación aplicable a la actividad del Certificador es la Ley Nº 25.506, el Decreto Nº 2628/02, toda otra norma complementaria dictada por la autoridad competente y otras normas que sean aplicables.

9.16. – Cláusulas adicionales

No se establecen cláusulas adicionales.

9.17. – Otras cuestiones generales

No aplicable.