Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO I

Infraestructura de Firma Digital – REPÚBLICA ARGENTINA

Ley Nº 25.506

MANUAL DE PROCEDIMIENTOS

POLÍTICA ÚNICA DE CERTIFICACIÓN de la AC ONTI

Versión 2.0

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN
SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN
SECRETARÍA DE GABINETE
JEFATURA DE GABINETE DE MINISTROS

ANEXO I

ANEXO I

ANEXO I

1. – INTRODUCCIÓN.

1.1. - Descripción general.

El presente Manual describe el conjunto de procedimientos utilizados por el Certificador cuyas funciones son ejercidas por la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante el Certificador) de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS en el cumplimiento de sus responsabilidades para la emisión y administración de los certificados digitales emitidos a favor de sus suscriptores, en el marco de la Ley N° 25.506 de Firma Digital, el Decreto N° 2628 del 19 de diciembre de 2002, la Decisión Administrativa N° 927 del 30 de noviembre de 2014 y demás normas reglamentarias. Este conjunto de procedimientos también regula el accionar del Certificador y sus Autoridades de Registro.

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

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

ANEXO I

1.2. - Nombre e Identificación del Documento.

Nombre: Manual de Procedimientos correspondiente a la Política Única de Certificación de la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN.

Versión: 2.0

Fecha de aplicación:

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

OID: 2.16.32.1.1.3

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

1.3. – Participantes.

Este Manual de Procedimientos es aplicable a:

a) El Certificador que emite certificados digitales para:
   - Personas Físicas.
   - Personas Jurídicas.
   - Servicio OCSP.

b) Las Autoridades de Registro (en adelante AR) que se constituyan en el ámbito de la Política Única de Certificación.

c) Los solicitantes y suscriptores de certificados digitales emitidos por el Certificador, en el ámbito de la mencionada Política.

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

ANEXO I

1.3.1. – Certificador.

La OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI) presta los servicios de certificación digital de acuerdo con los términos de la presente Política Única de Certificación.

1.3.2. - Autoridad de Registro.

El Certificador posee una estructura compuesta por ARs, las que serán responsables de efectuar las funciones de validación de identidad, de la titularidad de la clave pública asociada y de otros datos de los solicitantes y suscriptores de certificados digitales, de acuerdo al ámbito de aplicación establecido para cada una de ellas. Estas validaciones, de acuerdo con lo establecido en la Ley de Firma Digital N° 25.506 art. 21 inc. b), deberán ser llevadas a cabo por las AR sin tomar conocimiento o acceder bajo ninguna circunstancia a los datos de creación de firma del suscriptor (clave privada). Dicho ámbito de aplicación será determinado por:

a) Dominios de correo electrónico del ente público estatal en la cual se constituye la AR.
b) Alcance de la aplicación para la cual se constituye la AR.

Los organismos que se quieran conformar como Autoridades de Registro de la AC ONTI deberán solicitarlo por nota, informando si adicionalmente optarán por funcionar en puesto móvil, no pudiendo desarrollar su actividad exclusivamente en dicha modalidad.

Las AR serán autorizadas a funcionar como tales mediante notas firmadas por el máximo responsable del certificador licenciado.

ANEXO I

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

- RESPONSABLES DE LA AUTORIDAD DE REGISTRO:

- Son los nexos formales de comunicación entre el Responsable de la AC-ONTI y la Autoridad de Registro.
- Designan a quienes desempeñarán los roles dentro de la Autoridad de Registro (Oficiales de Registro y Soporte Técnico de Firma Digital).
- Controlan el cumplimiento de la Política Única de Certificación de la AC ONTI.
- Mantienen informado al Certificador sobre cualquier modificación en la conformación de la AR: designación o desvinculación de Oficiales de Registro, Soporte Técnico de Firma Digital, alta y baja de dominios asociados a la AR, domicilio físico donde se encuentre constituida la AR y sobre las aplicaciones que utilicen los certificados de la AC ONTI.

  Podrá designarse más de un Responsable de AR -se sugieren TRES (3)-, dependiendo de las características de la AR y de su cobertura.

- OFICIALES DE REGISTRO:

- Son los responsables de ejecutar la operatoria principal de la AR así como también de cumplir con las obligaciones, funciones y recaudos de seguridad que la AC-ONTI le delega.
- Aprueban solicitudes de certificados de firma digital a partir de la validación de la identidad del solicitante, de la titularidad de su clave pública y de los demás datos de la solicitud según las pautas establecidas por la Política Única de Certificación y por el presente Manual.

ANEXO I

- Rechazan solicitudes de certificados que no cumplen con los requisitos establecidos en la Política Única de Certificación y en el presente Manual.
- Revocan certificados siguiendo las pautas de la Política Única de Certificación y el presente Manual.

  Deben designarse al menos DOS (2) ORs. La cantidad dependerá del alcance o comunidad a la que atiende la AR.

➢ SOPORTE TÉCNICO DE FIRMA DIGITAL:

- Instruir acerca de las buenas prácticas de utilización de la tecnología de firma digital expresada en la Política Única de Certificación licenciada de la AC ONTI.
- Identificar y reconocer los dispositivos criptográficos que cumplan con la certificación de NIST FIPS 140-2 Nivel 2 o superior que requieren los solicitantes de certificados de nivel de seguridad alto.
- Difundir la tecnología de firma digital en su organismo a fin de que los agentes de esa jurisdicción tomen conocimiento de la posibilidad de acceso a la tecnología de firma digital a través de la AR constituida.
- Asistir a los solicitantes o suscriptores en el ámbito de su AR en la tramitación de los servicios provistos por el Certificador y en el manejo de la operatoria de la tecnología de firma digital de las distintas aplicaciones que requieran su uso.

Es responsabilidad del organismo público donde se constituye la AR asegurar la disponibilidad de todos los roles arriba mencionados como así también, asegurar su reemplazo en caso de producirse la desvinculación de alguno de ellos. Bajo ninguna circunstancia estas responsabilidades recaerán en el Certificador.

ANEXO I

Los organismos públicos que han sido autorizados para operar como AR del Certificador, incluyendo su domicilio, datos de contacto y si operan bajo modalidad de puesto móvil, se encuentran disponibles en el sitio web https://pki.jgm.gov.ar/app. Cada vez que sea autorizada una AR se actualizará en el sitio antes mencionado dentro de las CUARENTA Y OCHO (48) horas de dicha autorización. De igual forma y en el mismo plazo se procederá a su incorporación en la aplicación de la AC-ONTI.

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

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

- Realizar el proceso de aprobación de solicitudes en recintos donde no haya personal ajeno al proceso, cerciorándose de que no existan cámaras, dispositivos de captura de imágenes o aberturas que permitan la visualización externa del proceso de aprobación y generación de claves, ni otros datos de creación de firma digital.
- Utilizar equipamiento propio de la AR (PC o Notebook), que garantice la seguridad de la información, similares a las utilizadas en las instalaciones fijas (sistema operativo y antivirus actualizados y con soporte, así como otras configuraciones de seguridad aplicables).
- Realizar el resguardo digital de la documentación de respaldo, preferentemente en el momento en que se aprueba la solicitud, utilizando un dispositivo propio o de la instalación donde se realiza el proceso de aprobación; firmarla digitalmente y cargarla en la aplicación de la AC- ONTI.

ANEXO I

- Garantizar que la documentación de respaldo se encuentra bajo su control desde el momento en que la recibe hasta su resguardo en las instalaciones del organismo en la que funciona la AR.
- Los procedimientos de los ORs en las actividades relativas a la autenticación de la identidad de solicitantes y procesamiento de las solicitudes son idénticos a los realizados en las instalaciones fijas de la AR.

1.3.3. - Suscriptores de certificados.

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

- Las personas 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 certificados para ser usados en relación con el servicio *"Online Certificate Status Protocol"* (en adelante, OCSP) de consulta sobre el estado de un certificado.

1.3.4. - Terceros Usuarios.

Son Terceros Usuarios de los certificados emitidos bajo la Política Única de Certificación

asociada a este Manual de Procedimientos, toda persona 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° 2628/2002.

1.4. - Uso de los certificados.

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

1.5. - Administración del Manual de Procedimientos.

1.5.1. - Responsable del documento.

Será responsable del presente Manual de Procedimientos 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 interno 533

1.5.2. – Contacto.

El presente Manual de Procedimientos es administrado por el máximo responsable del Certificador Licenciado:

Correo electrónico: aconti@jefatura.gob.ar

Teléfono: (54 11) 5985-8663

(54 11) 4343-9001 Int. 533

ANEXO I

1.5.3. - Procedimiento de aprobación del Manual de Procedimientos.

El presente Manual de Procedimientos ha sido presentado y autorizado por el ente licenciante de acuerdo a lo dispuesto por la Decisión Administrativa N° 927/ 2014.

1.6. - Definiciones y Acrónimos.

1.6.1. – Definiciones.

- ACUERDO CON SUSCRIPTORES: Determina los derechos y obligaciones de la partes respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política de Única de Certificación.
- AUTORIDAD DE APLICACIÓN: La SECRETARÍA DE GABINETE 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, de la titularidad de la clave pública 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.
  - Identificación y autenticación de los solicitantes de revocación de certificados.

ANEXO I

- Archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el Certificador licenciado.
- 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 de fecha 19 de diciembre de 2002).

ANEXO I

- ENTE LICENCIANTE: La SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS es el 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 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.

- 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.

AR – Autoridad de Registro

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

CUIL - Clave Única de Identificación Laboral.

CUIT - Clave Única de Identificación Tributaria.

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

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

IEC – *"International Electrotechnical Commission".*

IETF – *"Internet Engineering Task Force".*

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

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

ANEXO I

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

ONTI - Oficina Nacional de Tecnologías de Información.

OR - Oficial de Registro.

PKCS #10 - Estándar de solicitud de certificación (*"Public-Key Cryptography Standards"*).

RFC – *"Request for Comments"*.

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

SHA-1 - Algoritmo de Hash Seguro (*"Secure Hash Algorithm"*).

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

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

2.1. – Repositorios.

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

- Su certificado digital.
- El certificado de la Autoridad Certificante Raíz.
- Repositorio de certificados digitales emitidos y su estado.
- Su certificado OCSP.
- La lista de certificados revocados (CRL).
- El listado de las Autoridades de Registro vinculadas al Certificador.
- Formulario de Adhesión del Anexo I.
- La Política Única de Certificación en sus versiones vigentes y anteriores.
- El Manual de Procedimientos en sus aspectos de carácter público, en sus versiones vigentes y anteriores.
- El Acuerdo con Suscriptores.

- Los Términos y Condiciones con Terceros Usuarios.
- La Política de Privacidad.
- Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.

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

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

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

2.2. - Publicación de información del Certificador.

El Certificador no establece restricciones de acceso a la Política Única de Certificación, al Acuerdo con Suscriptores, a los Términos y Condiciones con Terceros Usuarios, a este Manual de Procedimientos en sus aspectos de carácter público y a toda otra documentación técnica de carácter público que emita.

2.3. - Frecuencia de publicación.

Producida una actualización de los documentos relacionados con el Marco Legal u Operativo de la AC-ONTI, sus nuevas versiones se publicarán dentro de las VEINTICUATRO (24) horas luego de ser aprobados por la Autoridad de Aplicación, en el sitio web del Certificador https://pki.jgm.gov.ar/app.

Asimismo, se emitirá cada VEINTICUATRO (24) horas la CRL completa. Se emitirán deltas CRL con frecuencia horaria.

ANEXO I

2.4. - Controles de acceso a la información.

El Certificador no establece restricciones al acceso a la información que publica.

3. - IDENTIFICACIÓN Y AUTENTICACIÓN.

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

3.1.- Asignación de nombres de suscriptores.

3.1.1. - Tipos de Nombres.

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

3.1.2. - Necesidad de Nombres Distintivos.

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

3.1.3. - Anonimato o uso de seudónimos.

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

3.1.4. - Reglas para la interpretación de nombres.

Todos los nombres representados dentro de los certificados emitidos bajo la Política Única de Certificación vinculada a este Manual de Procedimientos coinciden con los correspondientes al documento de identidad del suscriptor para el caso de personas físicas,

o aquellos aportados por las personas jurídicas para su identificación, debidamente validados. Las discrepancias o conflictos que pudieran generarse cuando los datos de los suscriptores contengan caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

3.1.5. - Unicidad de nombres.

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

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

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados, excepto en el caso de personas jurídicas 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.

El Certificador emite certificados a los solicitantes que cumplan con los requisitos para ser suscriptor, efectuándose una validación de su identidad, para lo cual se requiere su

presencia física ante la AR. Asimismo, el solicitante debe probar su carácter de suscriptor para la correspondiente Política Única de Certificación.

I. En caso de tratarse de certificados cuyas claves son generadas por software (nivel de seguridad Normal) el solicitante efectuará el siguiente procedimiento:

a) Como paso previo el solicitante deberá obtener la documentación de respaldo necesaria de acuerdo al tipo de certificado que desea tramitar según corresponda a lo establecido en el apartado 3.2.2. o 3.2.3.

b) El solicitante ingresa al sitio web del Certificador https://pki.jgm.gov.ar/app y selecciona el trámite de solicitud de certificado que desea realizar.

c) Completa la solicitud de certificado con los datos requeridos de acuerdo a lo consignado en la documentación de respaldo y selecciona la AR que le corresponda de acuerdo al ámbito de aplicación establecido en el apartado 1.3.2.

d) Debe leer y aceptar el Acuerdo con Suscriptores en el que se hace referencia a la Política que respalda la emisión del certificado.

e) Genera el par de claves y envía su solicitud a la AC-ONTI de acuerdo con lo establecido en el apartado 3.2.1.

f) Imprime y firma la Nota de Solicitud en caso de coincidir el Código de Solicitud de la misma con el que aparece en la pantalla.

g) Recibe el correo electrónico enviado por la aplicación de la AC-ONTI y siguiendo las instrucciones allí detalladas, si corresponde, hace click en el link de verificación del correo electrónico.

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

ANEXO I

i) Se presenta personalmente ante la AR correspondiente con la documentación de respaldo consignada en los ítems a) y f) con el fin de realizar su identificación personal.

Al momento de presentación del solicitante, el Oficial de Registro efectúa los siguientes procedimientos:

a) Ingresa a la aplicación de la AC-ONTI disponible en el sitio web del Certificador y se autentica con su certificado como Oficial de Registro.
b) Verifica en la aplicación de la AC-ONTI la existencia de la solicitud de certificado del solicitante y verifica que este se encuentra dentro del ámbito de aplicación definido para esa AR según corresponda a lo establecido en el apartado 1.3.2.
c) Valida su identidad mediante la verificación de la documentación requerida.
d) Verifica la titularidad de la solicitud mediante el control del código hash de la Nota de Solicitud contra el que figura en la aplicación según se observa en el ítem b).
e) Verifica la coherencia de toda la documentación de respaldo presentada por el solicitante contra la registrada en la solicitud de certificado que se observa en el ítem b).
f) A continuación el solicitante contrafirma la Nota de Solicitud de su certificado ante el Oficial de Registro de la AR correspondiente, con lo cual acepta las condiciones de emisión y uso del certificado.
g) De haberse verificado el ítem e) y la coincidencia de ambas firmas hechas por el solicitante en la Nota de Solicitud, el Oficial de Registro procede a firmar la Nota de Solicitud en presencia del solicitante y luego firma digitalmente en el sistema la aprobación de la solicitud de certificado del solicitante.

ANEXO I

h) Resguarda toda la documentación vinculada al proceso de solicitud del certificado de acuerdo a lo establecido en los ítems 3.2.2 y 3.2.3.

II. En caso de tratarse de certificados cuyas claves son generadas en un dispositivo criptográfico (nivel de seguridad Alto), el solicitante efectuará los siguientes procedimientos:

a) Como paso previo el solicitante deberá obtener la documentación de respaldo necesaria de acuerdo al tipo de certificado que desea tramitar según corresponda a lo establecido en el apartado 3.2.2. o 3.2.3.

b) El solicitante ingresa al sitio web del Certificador https://pki.jgm.gov.ar/app y selecciona el trámite de solicitud de certificado que desea realizar.

c) Completa el formulario de envío de datos con los datos requeridos de acuerdo a lo consignado en la documentación de respaldo y selecciona la AR que le corresponda de acuerdo al ámbito de aplicación establecido en el apartado 1.3.2.

d) Imprime la Nota de Envío de Datos.

e) Recibe el correo electrónico enviado por la aplicación de la AC-ONTI y siguiendo las instrucciones allí detalladas, si corresponde, hace click en el link de verificación del correo electrónico.

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

g) Se presenta personalmente ante la AR correspondiente con la documentación de respaldo consignada en los ítems a) y d) y con el dispositivo criptográfico con el fin de continuar el trámite de solicitud.

ANEXO I

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

a) Ingresa a la aplicación de la AC-ONTI disponible en el sitio web del Certificador y se autentica con su certificado como Oficial de Registro.

b) Verifica en la aplicación de la AC-ONTI la existencia de la Nota de Envío de Datos del solicitante y verifica que esta se encuentra dentro del ámbito de aplicación definido para esa AR según corresponda a lo establecido en el apartado 1.3.2.

c) Valida su identidad mediante la verificación de la documentación requerida.

d) Verifica que el dispositivo criptográfico presentado por el solicitante cumple con los requisitos tecnológicos exigidos en la Política Única de Certificación (apartado 6.1.1). Esta verificación deberá ser efectuada por el Soporte Técnico de Firma Digital de la Autoridad de Registro. En caso de que el dispositivo no cumpla con los requisitos exigidos, no se continuará con el trámite de solicitud, rechazando la misma e informando al solicitante de tal situación.

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

a) Verifica que los datos que figuran en la Nota de Envío de Datos para los cuales va a realizar la solicitud son suyos y son correctos.

b) Debe leer y aceptar el Acuerdo con Suscriptores en el que se hace referencia a la Política que respalda la emisión del certificado.

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

d) Imprime y, en presencia del OR, firma la Nota de Solicitud en caso de coincidir el Código de Solicitud de la misma con el que aparece en la pantalla.

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

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

f) Verifica la titularidad de la solicitud mediante el control del código de la Nota de Solicitud contra el que figura en la aplicación según se observa en el ítem d). De coincidir el Oficial de Registro procede a firmar dicha nota en presencia del solicitante y luego firma digitalmente en el sistema la aprobación de la solicitud de certificado del solicitante

g) Resguarda toda la documentación vinculada al proceso de solicitud del certificado de acuerdo a lo establecido en los ítems 3.2.2 y 3.2.3.

En todos los casos, las AR están obligadas a guardar en la aplicación de la AC-ONTI una copia digitalizada firmada digitalmente por el OR de toda la documentación de respaldo de los trámites de solicitud dentro del plazo de DIEZ (10) días hábiles de aprobados.

Como alternativa, se admitirá que las Autoridades de Registro del Certificador desarrollen adicionalmente su actividad en puestos móviles, previa autorización del ente licenciante. En tal caso los procedimientos de registro inicial serán los mismos que los descriptos en el presente apartado.

ANEXO I

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

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

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

En el caso de solicitudes de certificados de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo criptográfico. Para certificados de nivel de seguridad Normal, el solicitante genera su par de claves y almacena la clave privada vía software en su propio equipo al momento de la solicitud.

El solicitante enviará a la AC-ONTI una solicitud de certificado, en formato PKCS#10 o SPKAC, para implementar la prueba de posesión de la clave privada, remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

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

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

ANEXO I

En el proceso de renovación, la comprobación de la posesión de la clave privada del suscriptor será realizada automáticamente por el Certificador a través de la aplicación de la AC-ONTI, dicha comprobación consistirá únicamente en la verificación de la firma digital de la solicitud de renovación recibida utilizando la clave pública del certificado del suscriptor el cual pretende renovar. De modo similar al caso de solicitud de certificado, si la firma digital de la solicitud de renovación se verifica significa que el suscriptor está en posesión de la clave privada correspondiente.

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.

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 deberá validar su identidad según lo dispuesto en el apartado 3.2.3.

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

<u>La documentación a presentar para la autenticación es la siguiente:</u>

ANEXO I

Para persona jurídicas privadas:

-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 público.

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.

La AR conservará toda la documentación de respaldo del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

En todos los casos, las AR están obligadas a guardar en la aplicación de la AC-ONTI una copia digitalizada firmada digitalmente por el OR de toda la documentación de respaldo de los trámites de solicitud dentro del plazo de DIEZ (10) días hábiles de aprobados.

El Certificador y la AR deberán cumplir con el artículo 21 incíso f) de le Ley N° 25.506 relativo a la recolección de datos personales.

ANEXO I

3.2.3. - Autenticación de la identidad de Personas Físicas.

Según lo establecido en la Política de Certificación asociada a este Manual de Procedimientos, el Certificador únicamente emite certificados para personas físicas que cumplan con los requisitos para ser suscriptor, efectuándose una validación de la identidad del solicitante. Asimismo, el solicitante debe probar la titularidad de los datos contenidos en su solicitud.

En todos los casos se exige la presencia física del solicitante o suscriptor del certificado ante la Autoridad de Registro con la que se encuentre operativamente vinculado; la verificación se efectuará mediante la presentación de la siguiente documentación:

a) De poseer nacionalidad o residencia argentina, se requiere Documento Nacional de Identidad (en original y fotocopia) y constancia de CUIL.
b) De tratarse de extranjeros sin residencia en el país, se requiere Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales (en original y fotocopia).
c) En todos los casos, Nota de solicitud de certificado, firmada por el solicitante.
d) De tratarse de personas físicas integrantes de entes públicos estatales, se deberá presentar adicionalmente una nota de certificación del cargo que ocupa ("Nota de certificación de servicios"). Esta podrá consistir en alguna de las siguientes opciones:
    - Copia autenticada del Acto Administrativo correspondiente a su designación.
    - Constancia emitida por la Oficina de Recursos Humanos, Personal o equivalente de su organismo o entidad, firmada por un funcionario responsable, en la que conste lugar y fecha de emisión, nombre y apellido, documento de identidad, cargo que ocupa en el mencionado organismo.

ANEXO I

- Constancia que incluya los datos indicados en el apartado anterior, firmada por el superior jerárquico o por la máxima autoridad del organismo en que se desempeña el solicitante.

e) En caso de tratarse de personas físicas no integrantes de entes públicos estatales que requieran su certificado para efectuar trámites con el Estado, la AR deberá exigir toda la documentación indicada en los ítems anteriores a excepción del ítem d). Será responsabilidad de cada AR determinar la documentación y los procedimientos de verificación adicionales que consideraran necesarios para validar el resto de los datos de los solicitantes.

La AR conservará toda la documentación de respaldo del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

En todos los casos, las AR están obligadas a guardar en la aplicación de la AC-ONTI una copia digitalizada firmada digitalmente por el OR de toda la documentación de respaldo de los trámites de solicitud dentro del plazo de DIEZ (10) días hábiles de aprobados.

El Certificador y la AR deberán cumplir con el artículo 21 inciso f) de le Ley N° 25.506 relativo a la recolección de datos personales.

3.2.4. - Información no verificada del suscriptor.

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

ANEXO I

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.

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).

El procedimiento descripto a continuación aplica únicamente al caso de certificados de personas físicas.

El proceso de renovación puede ser realizado solo si el certificado se encuentra vigente y debe ser iniciado únicamente por el suscriptor, quien deberá tener acceso a su clave privada vinculada al certificado a renovar. Solo se podrán efectuar un máximo de DOS (2) renovaciones para cada certificado emitido. Los datos contenidos en el certificado a renovar no deben haber variado, caso contrario se deberá proceder a su revocación y posterior solicitud de un nuevo certificado, según lo dispuesto en el apartado 4.1.1.

La solicitud de renovación puede ser efectuada por el suscriptor del certificado durante el período de vigencia del certificado dentro de los VEINTE (20) días anteriores a su vencimiento. Adicionalmente, el Certificador podrá implementar un servicio de alerta de certificados próximos a vencer. Este incluye el envío de un correo electrónico de alerta a la

cuenta de correo electrónico que figura en el certificado del suscriptor, siempre que este se encuentre en condiciones de renovar su certificado y que el mismo se encuentre dentro de los VEINTE (20) días anteriores próximos a su vencimiento; posteriormente se enviará un segundo mensaje de alerta por la misma vía cuando el certificado se encuentre dentro de los DIEZ (10) días anteriores próximos a su vencimiento y un tercer mensaje de alerta dentro de los CINCO (5) días.

Además, el servicio incluye la emisión de un aviso por correo electrónico si el certificado a vencer está relacionado con un rol en la aplicación de la AC; en tal caso el mensaje de alerta será enviado al Responsable de la AR correspondiente dentro de los CINCO (5) días anteriores al vencimiento.

Todo suscriptor de un certificado en los términos del presente documento debe iniciar el trámite de renovación ingresando al sitio web del Certificador disponible en https://pki.jgm.gov.ar/app y efectuar el siguiente procedimiento:

a) Selecciona el trámite de solicitud de renovación de certificado.

b) Autenticarse ante el Certificador utilizando la clave privada correspondiente al certificado que desea renovar.

c) La aplicación muestra los datos del certificado que el suscriptor desea renovar, el Acuerdo con Suscriptores y una declaración jurada con la leyenda "Declaro bajo juramento que todos los datos consignados en el certificado vigente no han cambiado y son actualmente válidos".

d) El suscriptor deberá indicar que acepta el Acuerdo con Suscriptores y que declara bajo juramento que sus datos no se han modificado tal como indica la leyenda anterior.

e) Si el suscriptor realizó menos de DOS (2) renovaciones con nuevo par de claves entonces la aplicación le permitirá al suscriptor indicar que desea renovar el certificado con

ANEXO I

un nuevo par de claves. Caso contrario esta opción no estará más disponible por lo que el suscriptor deberá tramitar un nuevo certificado, luego del vencimiento de su certificado actual.

f) Al seleccionar el usuario la opción anterior, la aplicación mostrará nuevamente en pantalla los datos del certificado a renovar, que aceptó el Acuerdo con Suscriptores, y que efectuó la declaración jurada de acuerdo al ítem c).

g) El suscriptor generará el nuevo par de claves y firmará, con la clave privada asociada al certificado a renovar, el requerimiento de renovación junto con todos los datos antes indicados. Durante la generación del nuevo par de claves el suscriptor deberá establecer los controles de acceso exclusivo a su nueva clave privada generada de manera de asegurarse que él es el único capaz de acceder a ella.

h) La aplicación de la AC-ONTI verificará la firma digital de la solicitud recibida y si todo es correcto entonces procederá automáticamente a la emisión del certificado renovado. Además enviará un correo electrónico de aviso de emisión del certificado renovado y un link para que el suscriptor pueda instalarlo.

El suscriptor deberá efectuar nuevamente el trámite de renovación en caso de haber recibido un correo electrónico informando del rechazo de la solicitud de renovación anterior o bien en caso de haber transcurrido un plazo de OCHO (8) horas de efectuada la solicitud sin haber recibido notificación respecto del trámite.

En los casos de certificados de personas jurídicas, no será posible efectuar la renovación automática. En este caso, el representante legal o autorizado de la persona jurídica deberá presentarse personalmente ante la AR con la documentación actualizada que acredite su condición de representante o autorizado. El OR verificará la mencionada documentación y de corresponder, procederá a aprobar la solicitud de renovación.

ANEXO I

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

En el caso de certificados digitales de personas físicas, 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 cuyos suscriptores no sean personas físicas se deberá tramitar UN (1) nuevo certificado, según lo indicado en el apartado anterior.

3.4. - Requerimiento de revocación.

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

En caso de que la solicitud no fuera efectuada por el suscriptor, la misma deberá ser remitida a la AR correspondiente por escrito, de acuerdo con lo establecido en el apartado 4.9.2, indicando las causas que motivaron la solicitud de revocación. Cumplido dicho

procedimiento, por medio de alguno de sus Oficiales de Registro, la Autoridad de Registro revocará el certificado.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1. - Solicitud de certificado.

4.1.1. - Solicitantes de certificados.

Los solicitantes que desempeñen sus funciones en entes públicos estatales deberán obtener la certificación de servicios, de acuerdo a lo indicado en el apartado 3.2.3, como paso previo a efectuar la solicitud del certificado en el sistema de la AC-ONTI.

En cualquiera de los casos los requerimientos técnicos con los que deberá contar el solicitante se encuentran publicados en sitio web del Certificador. En caso de necesitar asistencia respecto de este tema o de los trámites que provee el Certificador deberá requerirla únicamente al Soporte Técnico de Firma Digital de la AR a la cual realizará la solicitud.

4.1.2. - Solicitud de certificado

El proceso de solicitud debe ser iniciado solamente por el solicitante, en el caso de certificados de personas físicas, o bien por el representante legal o apoderado con poder suficiente a dichos efectos, en el caso de personas jurídicas privadas o la máxima autoridad, en el caso de personas jurídicas públicas.

Una vez iniciado el proceso de solicitud que se describe a continuación, es obligación del solicitante restringir todo acceso por parte de terceros a la estación de trabajo (equipo o dispositivo criptográfico) donde se encuentre realizando la solicitud, en caso de que tuviera que abandonar aquella temporalmente.

ANEXO I

4.1.2.1. - Solicitud de certificado con nivel de seguridad Normal.

Este apartado describe el proceso que debe ejecutar el solicitante o responsable autorizado para tramitar una solicitud de certificado de persona física o jurídica con nivel de seguridad normal, o sea que las claves serán generadas por software en el equipo del solicitante. Para ello deberá ejecutar el siguiente procedimiento:

1. Obtener la documentación de respaldo necesaria de acuerdo al tipo de certificado que desea tramitar según corresponda a lo establecido en el apartado 3.2.2. o 3.2.3. En el caso de tramitarse un certificado de persona jurídica de un ente público se debe tener en cuenta que el representante además deberá poseer el poder o autorización correspondiente.
2. Ingresar al sitio web del Certificador https://pki.jgm.gov.ar/app y seleccionar el trámite de solicitud de acuerdo al tipo de certificado que desea obtener: persona física o jurídica. Allí también se indicarán los requerimientos técnicos que debe poseer el equipo del solicitante.
3. *Seleccionar el nivel de seguridad:* el solicitante deberá seleccionar el nivel de seguridad del certificado que desea tramitar, para este caso deberá elegir la opción "Normal", de las siguientes opciones posibles:
    a. Alto: la generación de claves la realizará por medio de un dispositivo criptográfico de acuerdo con las características establecidas en el apartado 6.1.1. de la Política Única de Certificación.
    b. Normal: la generación de claves la realizará a través de su computadora.
4. *Ingreso de datos de Identidad del solicitante:*
    a. Caso de Certificado de Persona Física: deberá completar el formulario de solicitud de certificado con los datos que serán incluidos en el certificado. En

relación al número de CUIL / CUIT, deberá ingresar los datos requeridos por la aplicación a fin de efectuar su validación (Nombre y apellido, Sexo, Fecha de nacimiento, DNI). De no ser posible efectuar la validación mencionada, se le requerirá que ingrese nuevamente los datos solicitados y reitere la consulta. En caso de no estar disponible el servicio de validación, se le solicitará que ingrese manualmente el número de CUIT / CUIL. En este caso, la validación será efectuada por el Oficial de Registro al momento de procesar la solicitud del certificado, según se indica en el apartado 4.2.

b. Caso de Certificado de Persona Jurídica: en el caso de certificados de persona jurídica se deberá ingresar el número de CUIL / CUIT del representante autorizado que gestionará la solicitud.

5. *Ingreso de datos adicionales y de solicitud:*

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

i. Correo electrónico: en el caso de solicitantes pertenecientes a entes públicos deberá ingresar su cuenta de correo institucional. En otro caso el solicitante ingresará su cuenta de correo electrónico personal o corporativa.

ii. Datos de servicio: en el caso de solicitante pertenecientes a entes públicos, de acuerdo con la información que figura en la certificación de servicios deberá completar los siguientes campos:

1. Organización.
2. Área.
3. Provincia.

ANEXO I

4. Localidad.

b. Caso Certificado de Persona Jurídica: deberá completar los datos del formulario con la siguiente información:

i. Correo electrónico: en el caso de responsables autorizados pertenecientes a entes públicos deberá ingresar su cuenta de correo institucional. En otro caso el solicitante ingresará su cuenta de correo electrónico personal o corporativa.

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

iii. Denominación de la persona jurídica: nombre de la persona jurídica titular del certificado.

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

v. CUIT de la organización: CUIT de la persona jurídica titular del certificado.

vi. Provincia.

vii. Localidad.

6. Seleccionar Autoridad de Registro: de acuerdo al ámbito de aplicación establecido en el apartado 1.3.2, el sistema despliega automáticamente una o varias AR en función de los datos de la solicitud y a partir de la lista de AR autorizadas. En caso que se

mostraran varias AR, el solicitante deberá elegir la AR que le corresponde. De no efectuarse dicha elección, el sistema permite que el usuario indique si el certificado a tramitar será utilizado en alguna de las aplicaciones informáticas que figuran en la lista del Certificador. En tal caso, una vez elegida la aplicación, se le asignará automáticamente la AR correspondiente. En caso de que el solicitante no haya seleccionado alguna aplicación, se muestra la lista completa de AR en pantalla a fin de que el solicitante pueda efectuar la selección correspondiente; el usuario deberá seleccionar una AR a fin de poder continuar con el trámite de solicitud.

7. Confirmación de datos y aceptación del Acuerdo con Suscriptores: el solicitante debe aceptar el Acuerdo con Suscriptores en el cual se establecen los derechos y obligaciones que contrae el solicitante en su calidad de tal y como futuro suscriptor de un certificado.
8. Generación de claves: si los datos son correctos, se permitirá al solicitante efectuar la solicitud del certificado para lo cual procederá a generar su par de claves con el nivel de seguridad "Normal" de acuerdo a lo establecido en el apartado 3.2.1. El solicitante deberá establecer los controles de acceso exclusivo que aseguren que él es el único capaz de acceder a su clave privada.
9. Envío de Solicitud: el solicitante envía su solicitud a la AC-ONTI. La aplicación verifica que la solicitud sea válida y procede a generar un Código de Solicitud (Hash de la solicitud). En caso de haberse validado correctamente la aplicación muestra una pantalla que indica que el trámite se inició correctamente; la misma contiene los datos de la Nota de Solicitud que el solicitante debe imprimir a la vez que se le informa que recibirá un correo electrónico para continuar con el trámite.
10. Impresión de la Nota de Solicitud: debe imprimir la Nota de solicitud, la cual contiene:

ANEXO I

- Todos los datos de la solicitud.
- El Código de Solicitud (Hash de la solicitud).
- La declaración de haber leído y aceptado el Acuerdo con suscriptores y la Política Única de Certificación.
- La declaración de que los datos contenidos en la solicitud, que se incluirán en el certificado a emitir, son válidos.

11. Verificación de los datos de la Nota de Solicitud impresa: el solicitante debe verificar que el Código de la Nota de Solicitud impresa coincide exactamente con el que aparecerá en su pantalla, bajo ningún concepto el solicitante debe firmar la Nota de Solicitud sin hacer esta verificación. En caso accidental de cerrar la pantalla donde aparece el Código de Solicitud antes de realizar la mencionada verificación, se debe destruir la Nota de Solicitud impresa y comenzar el trámite nuevamente, se sugiere en este caso además ponerse en contacto con el Soporte Técnico de la AR. El solicitante debe además verificar que todos los datos impresos en la Nota de Solicitud son correctos y coinciden con los que aparecerán en su pantalla.
12. Firma de la Nota de Solicitud: Sólo en el caso que toda la información antes mencionada coincida el solicitante procederá a firmar sobre el campo "Firma y aclaración del solicitante" incluyendo la aclaración de su firma. En caso que ambos Códigos de Solicitud no coincidan el solicitante deberá detener el proceso de solicitud, destruir la Nota de Solicitud impresa y comenzar nuevamente todo el procedimiento de solicitud de certificado desde su inicio. Una vez que la Nota de Solicitud fue firmada, resulta crítico que esta sea resguardada por el solicitante en un lugar seguro, impidiendo el acceso a la misma por parte de terceros.
13. Recepción del correo electrónico de verificación: La aplicación envía un correo

electrónico al solicitante que contendrá un link para proseguir el trámite. El solicitante debe acceder al mencionado link para confirmar al Certificador que la dirección de correo electrónico ingresada es la correcta y que posee acceso a la cuenta de correo declarada.

14. Verificación de la cuenta de correo electrónico: al haber accedido al link de verificación accederá al sitio web del Certificador donde aparecerá un mensaje en pantalla informando al usuario:
    - Que su correo electrónico fue verificado.
    - Que debe presentarse personalmente ante un Oficial de Registro de la AR que seleccionó previamente; se sugiere que antes de hacerlo se ponga en contacto con el OR a fin de concertar el encuentro.
    - La documentación que debe presentar ante la AR.
    - El listado con el domicilio y demás datos de la AR, los datos de contacto del OR y del Soporte Técnico.
15. Instalación del certificado de la AC-Raíz y de la AC-ONTI: a continuación la aplicación le indicará las instrucciones para que el solicitante efectúe la instalación de los certificados mencionados. Una vez instalados, debe establecer el certificado de la AC-Raíz como certificado de confianza. También encontrará los datos de contacto del Soporte Técnico de la AR para el caso en que necesite asistencia técnica.
16. Presentación personal del solicitante ante la AR: previo contacto con el OR el solicitante deberá presentarse personalmente ante la AR correspondiente con la documentación de respaldo consignada en los apartados 3.2.2. o 3.2.3. según corresponda al trámite a realizar, y la Nota de Solicitud impresa y firmada de acuerdo

a lo establecido en el ítem número 12, con el fin de realizar su identificación personal. En el caso de tramitarse un certificado de persona jurídica de un ente público se debe tener en cuenta que el representante autorizado además deberá poseer el correspondiente poder o autorización.

4.1.2.2. - Solicitud de certificado con nivel de seguridad Alto.

Este apartado describe el proceso que debe ejecutar el solicitante o responsable autorizado para tramitar una solicitud de certificado de persona física o jurídica con nivel de seguridad alto, o sea que las claves serán generadas en un dispositivo criptográfico que deberá cumplir con los requerimientos establecidos en el apartado 6.1.1 de la Política Única de Certificación. Para este caso deberá ejecutar el siguiente procedimiento:

1. Obtener la documentación de respaldo necesaria de acuerdo al tipo de certificado que desea tramitar según corresponda a lo establecido en el apartado 3.2.2. o 3.2.3. En el caso de tramitarse un certificado de persona jurídica de un ente público se debe tener en cuenta que el representante además deberá poseer el poder o autorización correspondiente.
2. Ingresar al sitio web del Certificador https://pki.jgm.gov.ar/app y seleccionar el trámite de solicitud de acuerdo al tipo de certificado que desea obtener: persona física, jurídica, etc. Allí también se indicarán los requerimientos técnicos que debe poseer el equipo del solicitante.
3. *Seleccionar el nivel de seguridad:* el solicitante deberá seleccionar el nivel de seguridad del certificado que desea tramitar, para este caso deberá elegir la opción "Alto", de las siguientes opciones posibles:

ANEXO I

a. Alto: la generación de claves la realizará por medio de un dispositivo criptográfico de acuerdo con las características establecidas en el apartado 6.1.1. de la Política Única de Certificación.

b. Normal: la generación de claves la realizará a través de su computadora.

4. Ingreso de datos de Identidad del solicitante:

a. Caso de Certificado de Persona Física: deberá completar el formulario de solicitud de certificado con los datos que serán incluidos en el certificado. En relación al número de CUIL / CUIT, deberá ingresar los datos requeridos por la aplicación a fin de efectuar su validación (Nombre y apellido, Sexo, Fecha de nacimiento, DNI). De no ser posible efectuar la validación mencionada, se le requerirá que ingrese nuevamente los datos solicitados y reitere la consulta. En caso de no estar disponible el servicio de validación, se le solicitará que ingrese manualmente el número de CUIT / CUIL. En este caso, la validación será efectuada por el Oficial de Registro al momento de procesar la solicitud del certificado, según se indica en el apartado 4.2.

b. Caso de Certificado de Persona Jurídica: en el caso de certificados de persona jurídica se deberá ingresar el número de CUIL / CUIT del representante autorizado que gestionará la solicitud.

5. Ingreso de datos adicionales y de solicitud:

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

i. Correo electrónico: en el caso de solicitantes pertenecientes a entes públicos deberá ingresar su cuenta de correo institucional. En otro caso el solicitante ingresará su cuenta de correo electrónico personal

o corporativo.

ii. Datos de servicio: en el caso de solicitante pertenecientes a entes públicos, de acuerdo con la información que figura en la certificación de servicios deberá completar los siguientes campos:

1. Organización.
2. Área.
3. Provincia.
4. Localidad

b. Caso Certificado de Persona Jurídica: deberá completar los datos del formulario con la siguiente información:

i. Correo electrónico: en el caso de responsables autorizados pertenecientes a entes públicos deberá ingresar su cuenta de correo institucional. En otro caso el solicitante ingresará su cuenta de correo electrónico personal o corporativo.

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

iii. Denominación de la persona jurídica: nombre de la persona jurídica titular del certificado.

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

ANEXO I

v. CUIT de la organización: CUIT de la persona jurídica titular del certificado.

vi. Provincia.

vii. Localidad.

6. Seleccionar Autoridad de Registro: de acuerdo al ámbito de aplicación establecido en el apartado 1.3.2, el sistema desplegará automáticamente una o varias AR en función de los datos de la solicitud y a partir de la lista de ARs autorizadas. En caso que fueran mostradas varias AR, el solicitante deberá elegir la AR que le corresponde. De no efectuarse dicha elección, el sistema permite que el usuario indique si el certificado a tramitar será utilizado en alguna de las aplicaciones informáticas que figuran en la lista del Certificador. En tal caso, una vez elegida la aplicación, se le asignará automáticamente la AR correspondiente. En caso de que el solicitante no haya seleccionado alguna aplicación, se muestra la lista completa de AR en pantalla a fin de que el solicitante pueda efectuar la selección correspondiente; el usuario deberá seleccionar una AR a fin de poder continuar con el trámite de solicitud.
7. Confirmación y envío de Datos de Solicitud: a continuación la aplicación mostrará en pantalla todos los datos proporcionados por el solicitante que irán incluidos en el certificado a emitir, a la vez que tendrá la posibilidad de aceptar o cancelar el envío de sus datos de solicitud a la AC-ONTI. En caso de haber recibido correctamente los datos la aplicación mostrará una pantalla que indica que los datos se recibieron correctamente; el solicitante podrá imprimir esta nota, a la vez que se le informará que recibirá un correo electrónico.
8. Impresión de la Nota de Solicitud: el solicitante tendrá la posibilidad de imprimir esta

ANEXO I

nota que incluye todos los datos ingresados anteriormente; esto no es excluyente para la continuación del trámite.

9. Recepción del correo electrónico de verificación: la aplicación envía un correo electrónico al solicitante que contendrá un link para proseguir el trámite. El solicitante debe acceder al mencionado link para confirmar al Certificador que la dirección de correo electrónico ingresada es la correcta y que posee acceso a la cuenta de correo declarada.
10. Verificación de la cuenta de correo electrónico: al haber accedido al link de verificación accederá al sitio web del Certificador donde aparecerá un mensaje en pantalla informando al usuario:
    - Que su correo electrónico fue verificado.
    - Que debe llevar el dispositivo criptográfico.
    - Que debe presentarse personalmente ante un Oficial de Registro de la AR que seleccionó previamente; se sugiere que antes de hacerlo se ponga en contacto con el OR a fin de concertar el encuentro.
    - La documentación que debe presentar ante la AR.
    - El listado con la dirección y demás datos de la AR, los datos de contacto del OR y del Soporte Técnico.
11. Instalación del certificado de la AC-Raíz y de la AC-ONTI: a continuación la aplicación le indicará las instrucciones para que el solicitante efectúe la instalación de los certificados mencionados. Una vez instalados, debe establecer el certificado de la AC-Raíz como certificado de confianza. También encontrará los datos de contacto del Soporte Técnico de la AR para el caso en que necesite asistencia técnica.

ANEXO I

12. Presentación personal del solicitante ante la AR: previo contacto con el OR el solicitante deberá presentarse personalmente ante la AR correspondiente con la documentación de respaldo consignada en los apartados 3.2.2. o 3.2.3. según corresponda al trámite a realizar, la Nota de Envío de Datos impresa en caso de haberla impreso, además deberá llevar el dispositivo criptográfico utilizado. En el caso de tramitarse un certificado de persona jurídica de un ente público se debe tener en cuenta que el representante además deberá poseer el correspondiente poder o autorización.

4.2. - Procesamiento de la solicitud del certificado.

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

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

- Verifica que la solicitud se encuentra dentro del ámbito de aplicación de la AR de acuerdo a lo establecido en el apartado 1.3.2.
- Verifica que el solicitante, de acuerdo con las pautas establecidas en el presente Manual, cumpla con los requisitos que prueben su carácter de suscriptor para la correspondiente Política Única de Certificación.
- Verifica la existencia de la solicitud en la aplicación 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 del Código de la Nota de Solicitud de certificado contra el Código registrado en el sistema de la AC-ONTI.

- Requiere al solicitante o su representante autorizado la firma de la nota de solicitud en su presencia.
- Resguarda toda la documentación de respaldo del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

4.2.1. - Procesamiento de solicitudes de certificado con nivel de seguridad Normal.

Este apartado describe el proceso que debe ejecutar el OR para aceptar o rechazar una solicitud de certificado de persona física o jurídica con nivel de seguridad Normal.

A continuación se indican los pasos generales para el procesamiento de una solicitud de certificado, iniciando por la validación de la identidad de la persona que se presenta ante la AR, que en todos los casos será una persona física, para realizar el trámite para sí o como representante autorizado de una persona jurídica pública o privada. Los requisitos adicionales específicos cuando el suscriptor es una persona jurídica se detallan a continuación en los ítems 7.2 y 7.3.

1. Autenticación como OR: ingresa a la aplicación de la AC-ONTI disponible en el sitio web del Certificador y se autentica con su certificado como OR.
2. Verificación de la existencia de la solicitud de certificado del solicitante: para ello el OR ingresa a la aplicación de la AC-ONTI donde visualiza el listado de todas las solicitudes a evaluar que se encuentren bajo su visibilidad y verifica que la solicitud presentada se encuentre en el estado: "Solicitud pendiente de revisión por la AR"; debe seleccionar la solicitud a fin de poder visualizarla.

ANEXO I

3. Verificación del ámbito de aplicación: efectúa una primera verificación de los datos de la solicitud a fin de corroborar que el solicitante se encuentra dentro del ámbito de aplicación definido para esa AR según corresponda a lo establecido en el apartado 1.3.2.
4. Validación de identidad del solicitante:
   4.1. Validación del documento de identidad: Debe verificar que el documento de identidad presentado es válido, para ello deberá comprobar que:
      a. Corresponde a la persona que se presentó.
      b. La fotocopia del documento de identidad presentado coincide con el documento de identidad del cual se obtuvo copia.
      c. Hecha las validaciones anteriores, en presencia del OR el solicitante firma hológrafamente con aclaración de firma la fotocopia del documento de identidad presentado.
   4.2. Validación del CUIT/CUIL: Debe verificar el número de CUIT / CUIL, pudiendo presentarse los siguientes casos:
      a. El CUIT/CUIL fue validado automáticamente por la aplicación: el OR será informado a través de la interface de la aplicación de la AC-ONTI que este dato ya fue verificado. En este caso el OR seguirá con el procesamiento de la solicitud a partir del ítem 5)
      b. El CUIT/CUIL no fue validado por la aplicación: en caso de que la aplicación le indique que no se ha validado este dato, el OR podrá:
         I. Realizar la validación mediante la aplicación de la AC ONTI.
         II. Realizar la validación mediante el sitio web de ANSES utilizando como datos de entrada los que figuran en el documento de identidad presentado por el solicitante.

ANEXO I

III. Realizar la validación requiriendo al solicitante la constancia impresa de CUIT/CUIL correspondiente y verificando que el número corresponde al ingresado por el solicitante. Efectuada esta verificación, el OR y el solicitante firmarán la constancia obtenida en prueba de conformidad.

En cualquiera de los tres casos, el OR dejará indicado en la aplicación el método utilizado y seguirá con el procesamiento de la solicitud a partir del ítem 5.

En caso de que el solicitante no haya podido efectuar la validación o no haya presentado la constancia impresa de CUIT / CUIL, deberá interrumpirse el proceso de aprobación de la solicitud. El OR le indicará al solicitante que se presente en otro momento con la constancia correspondiente.

5. Verificación de la titularidad de la solicitud: el OR debe verificar que el solicitante es el titular de la clave pública asociada a la solicitud que pretende aprobar; validando que está en posesión de la clave privada correspondiente sin tener acceso o conocimiento de la misma. Para ello deberá:

   5.1. Identificar la solicitud a evaluar: identificará la solicitud a aprobar verificando que el código (hash) que figura en la Nota de Solicitud que presenta el solicitante coincide exactamente con el registrado en el sistema de la AC-ONTI.

   5.2. Corroborar los datos de la Nota de Solicitud: debe verificar que el resto de los datos que figuran en la Nota de Solicitud son correctos y se corresponden con los que posee registrado en su sistema la AC-ONTI.

   5.3. Corroborar la firma de la Nota de Solicitud: debe verificar que la Nota de Solicitud esté firmada hológrafamente por el solicitante en el campo rotulado "Firma y aclaración del solicitante". De no ser así, el Oficial de Registro deberá indicar en la Nota de Solicitud que la misma no es válida y procederá a efectuar el rechazo de la

solicitud en el sistema de la AC-ONTI. Se deberá verificar además que los campos de la Nota de Solicitud rotulados como: "Firma y aclaración del solicitante en presencia del Oficial de Registro" y "Firma y aclaración del Oficial de Registro en presencia del solicitante" no estén firmados por el solicitante al momento de la presentación de la Nota de Solicitud.

5.4. Contrafirma del solicitante de la Nota de Solicitud: Una vez validada toda la información de la Nota de Solicitud de acuerdo a los ítems anteriores, el solicitante firma hológrafamente con aclaración de firma el campo "Firma y aclaración del solicitante en presencia del Oficial de Registro".

6. Comprobación de la titularidad de la Nota de Solicitud: el Oficial de Registro debe verificar que ambas firmas hechas en la Nota de Solicitud coincidan y en ese caso firma hológrafamente con aclaración de firma el campo "Firma y aclaración del Oficial de Registro en presencia del solicitante". En caso de no coincidir las firmas del solicitante el OR deberá interrumpir el proceso de aprobación y deberá proceder al rechazo en la aplicación de la AC-ONTI de la solicitud que se pretendía aprobar.

7. Verificación de credenciales y notas de autorización:

7.1. Personas Físicas: en caso de que el solicitante pertenezca a un ente público deberá presentar la Certificación de Servicios o el Acto Administrativo correspondiente.

a. Certificación de Servicios: de presentarse una Certificación de Servicios se deberá verificar:

- Titularidad de la Certificación: Que la persona que se presenta es aquella cuyos datos figuran en la certificación de servicios presentada. A tal fin debe cotejar que todos los datos del documento de identidad coinciden con los que figuran en la mencionada certificación.

ANEXO I

- Validez de la Certificación: Que está firmada por una autoridad competente.
- Vigencia de la Certificación: Que la fecha de emisión de la Nota de Certificación de Servicios fue hecha dentro de los VEINTE (20) días hábiles de efectuada la solicitud del certificado.

b. Acto Administrativo: de presentarse un acto administrativo se deberá verificar:

- Que el mismo se encuentra autenticado por una autoridad competente.
- Que dicho acto corresponde a la designación de un cargo público en favor del solicitante.

Cumplido los ítems antes detallados, el OR podrá aprobar la solicitud del certificado de la persona física que fue validada.

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

a) Validación de la Nota de la máxima autoridad: requerirá al responsable autorizado la mencionada nota y verificará que la misma esté firmada y sellada por la autoridad competente antes mencionada.

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

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

ANEXO I

d) Validación de la copia fiel de la norma de creación del organismo: requerirá al responsable autorizado la copia fiel de la norma de creación del organismo. Además verificará que el nombre del organismo que allí figura coincide con el campo Organización de la solicitud registrada en el sistema de la AC-ONTI.

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

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

a. Validación de la Constancia de inscripción del Registro Societario: requerirá al responsable autorizado la mencionada constancia y verificará que está firmada y sellada por autoridad competente del registro societario correspondiente a la jurisdicción. Además deberá verificar que dicha constancia se encuentra autenticada ante escribano.

b. Validación del poder del responsable autorizado: requerirá al responsable autorizado el poder que acredita el carácter de representante legal o apoderado. Allí verificará que el mismo esté expedido por autoridad competente y que se encuentre debidamente autenticado ante escribano.

c. Validación del responsable autorizado: verificará que los datos de identidad que figuran en el poder coinciden con los datos de identidad del responsable autorizado que figuran en la Nota de Solicitud.

d. Verificación de la identidad del titular: verificará que el nombre de la persona jurídica que figura en la Constancia de inscripción del Registro Societario de la jurisdicción coincide con el campo "Denominación de la Persona Jurídica" que

figura en la solicitud registrada en el sistema de la AC-ONTI y con el que figura en el poder en favor del responsable autorizado.

e. Opcionalmente si en lugar del poder y la Constancia de Inscripción en el Registro Societario, el responsable autorizado presenta una constancia de escribano público de la existencia de tales documentos, el OR deberá ejecutar sobre este documento el mismo procedimiento de validación detallado en este apartado.

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

8. Finalización del trámite de solicitud:

Efectuados los mencionados controles, el Oficial de Registro podrá:

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

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

- Por no haberse presentado toda la documentación requerida.
- Por inconsistencias en la documentación presentada o entre esta y la solicitud registrada en el sistema de la AC-ONTI.
- Si la nota de solicitud no fue firmada por el solicitante al momento de la solicitud del certificado.

ANEXO I

- Si el solicitante no estableció los controles de acceso que aseguren que él es el único capaz de acceder a su clave privada.
- Debido a cualquier otro motivo que impida la validación de los datos del certificado o la ejecución de este procedimiento.
- Por pedido expreso del solicitante.

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

Se deberá resguardar toda la documentación de respaldo del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

Es requerimiento obligatorio para las AR guardar en la aplicación de la AC-ONTI una copia digitalizada firmada digitalmente por el OR de toda la documentación de respaldo del trámite de solicitud dentro del plazo de DIEZ (10) días hábiles de aprobada la misma.

4.2.2. - Procesamiento de solicitudes de certificado con nivel de seguridad Alto.

Este apartado describe el proceso que debe ejecutar el OR para aceptar o rechazar una solicitud de certificado de persona física o jurídica con nivel de seguridad Alto.

A continuación se indican los pasos generales para el procesamiento de una solicitud de certificado, iniciando por la validación de la identidad de la persona que se presenta ante la AR, que en todos los casos será una persona física, para realizar el trámite para sí o como representante autorizado de una persona jurídica pública o privada. Los requisitos

adicionales específicos cuando el suscriptor es una persona jurídica se detallan a continuación en los ítems 13.2 y 13.3.

La AR deberá previamente validar que el dispositivo criptográfico que utilizó el solicitante para realizar la solicitud cumple con los requerimientos establecidos en el apartado 6.1.1 de la Política Única de Certificación. Además también deberá cumplir con los requerimientos de configuración del dispositivo criptográfico que establezca el Certificador en su sitio web.

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

1. Autenticación como OR: ingresa a la aplicación de la AC-ONTI disponible en el sitio web del Certificador y se autentica con su certificado como OR.
2. Verifica la existencia de la solicitud de envío de datos del solicitante: para ello el OR ingresa a la aplicación de la AC-ONTI donde visualiza el listado de todas las solicitudes de envío de datos que se encuentren bajo su visibilidad, una vez identificada la solicitud debe seleccionarla a fin de poder visualizarla.
3. Verificación del ámbito de aplicación: efectúa una primera verificación de los datos de la solicitud a fin de corroborar que el solicitante se encuentra dentro del ámbito de aplicación definido para esa AR según corresponda a lo establecido en el apartado 1.3.2.
4. Validación de identidad del solicitante:
   4.1. Validación del documento de identidad: Debe verificar que el documento de identidad presentado es válido, para ello deberá comprobar que:
      a) Corresponde a la persona que se presentó.
      b) La fotocopia del documento de identidad presentado coincide con el documento de identidad del cual se obtuvo copia.

ANEXO I

c) Hechas las validaciones anteriores, en presencia del OR el solicitante firma hológrafamente con aclaración de firma la fotocopia del documento de identidad presentado.

5. Verificación de certificaciones: en caso de que el solicitante pertenezca a un ente público deberá presentar la Certificación de Servicios o el Acto Administrativo correspondiente.

5.1. Certificación de Servicios: de presentarse una Certificación de Servicios se deberá verificar:

a) Titularidad de la Certificación: Que la persona que se presenta es aquella cuyos datos figuran en la certificación de servicios presentada. A tal fin debe cotejar que todos los datos del documento de identidad coinciden con los que figuran en la mencionada certificación.

b) Validez de la Certificación: Que está firmada por una autoridad competente.

c) Vigencia de la Certificación: Que la fecha de emisión de la Nota de Certificación de Servicios fue hecha dentro de los VEINTE (20) días hábiles de efectuada la solicitud del certificado.

5.2. Acto Administrativo: de presentarse un acto administrativo se deberá verificar:

a) Que el mismo se encuentra autenticado por una autoridad competente.

b) Que dicho acto corresponde a la designación de un cargo público en favor del solicitante.

6. Aceptación de solicitud de envío de datos: al visualizar la solicitud el OR podrá continuar con el trámite de solicitud o rechazarla en caso de corresponder. En caso de rechazarla el solicitante deberá iniciar nuevamente el trámite de Envío de Datos; se debe tener presente que deberá volver a validar su cuenta de correo electrónico por lo que deberá

tener acceso a ella. En caso de que el OR continúe con el trámite de solicitud accederá a la pantalla de generación de la solicitud de certificado.

Para continuar con el trámite de solicitud, el OR deberá insertar en una computadora habilitada a tal fin el dispositivo criptográfico del solicitante, que fuera previamente validado por la AR. El procedimiento descripto a continuación deberá ser ejecutado por el solicitante o responsable autorizado desde la computadora habilitada por el OR:

7. Confirmación de datos y aceptación del Acuerdo con Suscriptores: desde la pantalla de generación de solicitud, el solicitante debe aceptar el Acuerdo con Suscriptores en el cual se establecen los derechos y obligaciones que contrae el solicitante en su calidad de tal y como futuro suscriptor de un certificado.
8. Generación de claves: desde la pantalla de generación de solicitud, el solicitante efectuará la solicitud del certificado para lo cual procederá a generar su par de claves con el nivel de seguridad "Alto" de acuerdo a lo establecido en el apartado 3.2.1. El solicitante deberá establecer los controles de acceso exclusivo que aseguren que él es el único capaz de acceder a su clave privada.
9. Envío de Solicitud de certificado: el solicitante envía su solicitud a la AC-ONTI. La aplicación verifica que la solicitud sea válida y procede a generar un Código de Solicitud (Hash). En caso de haberse validado correctamente la aplicación muestra una pantalla que indica que el trámite se inició correctamente; la misma contiene los datos de la Nota de Solicitud que el solicitante debe imprimir.
10. Impresión de la Nota de Solicitud: Debe imprimir la Nota de solicitud, la cual contiene:
    - Todos los datos de la solicitud.
    - El Código de Solicitud (Hash de la solicitud)

ANEXO I

- La declaración de haber leído y aceptado el Acuerdo con suscriptores y la Política Única de Certificación.
- La declaración de que los datos contenidos en la solicitud, que se incluirán en el certificado a emitir, son válidos.

11. Firma de la Nota de Solicitud: Sólo en el caso que toda la información antes mencionada coincida el solicitante procederá a firmar sobre el campo "Firma y aclaración del solicitante" incluyendo la aclaración de su firma. En caso que ambos Códigos de Solicitud no coincidan el solicitante deberá detener el proceso de solicitud, destruir la Nota de Solicitud impresa y comenzar nuevamente todo el procedimiento de solicitud de certificado desde su inicio, se debe tener presente que deberá volver a validar su cuenta de correo electrónico por lo que deberá tener acceso a ella..

Una vez firmada la Nota de Solicitud concluye el procedimiento de generación de la solicitud de certificado por parte del solicitante.

El procedimiento descripto a continuación deberá ser ejecutado por el OR desde su sesión desde la interface del sistema:

12. Validación de identidad del solicitante:

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

a) El CUIT/CUIL fue validado automáticamente por la aplicación: el OR será informado a través de la interface de la aplicación de la AC-ONTI que este dato ya fue verificado. En este caso el OR seguirá con el procesamiento de la solicitud a partir del ítem 13).

ANEXO I

b) El CUIT/CUIL no fue validado por la aplicación: en caso de que la aplicación le indique que no se ha validado este dato, el OR podrá:

I. Realizar la validación mediante la aplicación de la AC ONTI.

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

III. Realizar la validación requiriendo al solicitante la constancia impresa de CUIT/CUIL correspondiente y verificando que el número corresponde al ingresado por el solicitante. Efectuada esta verificación, el OR y el solicitante firmarán la constancia obtenida en prueba de conformidad.

En cualquiera de los tres casos, el OR dejará indicado en la aplicación el método utilizado y seguirá con el procesamiento de la solicitud a partir del ítem 13.

En caso de que el solicitante no haya podido efectuar la validación o no haya presentado la constancia impresa de CUIT / CUIL, deberá interrumpirse el proceso de aprobación de la solicitud. El OR le indicará al solicitante que se presente en otro momento con la constancia correspondiente.

13. Verificación de la titularidad de la solicitud: el OR debe verificar que el solicitante es el titular de la clave pública asociada a la solicitud que pretende aprobar; validando que está en posesión de la clave privada correspondiente sin tener acceso o conocimiento de la misma. Para ello deberá:

a) Identificar la solicitud a evaluar: identificará la solicitud a aprobar verificando que el código (hash) que figura en la Nota de Solicitud que presenta el solicitante coincide exactamente con el registrado en el sistema de la AC-ONTI.

ANEXO I

b) Corroborar los datos de la Nota de Solicitud: debe verificar que el resto de los datos que figuran en la Nota de Solicitud son correctos y se corresponden con los que posee registrado en su sistema la AC-ONTI.

c) Corroborar la firma de la Nota de Solicitud: debe verificar que la Nota de Solicitud esté firmada hológrafamente por el solicitante en el campo rotulado "Firma y aclaración del solicitante". De no ser así, el Oficial de Registro deberá indicar en la Nota de Solicitud que la misma no es válida y procederá a efectuar el rechazo de la solicitud en el sistema de la AC-ONTI.

13.1. Personas físicas: cumplido el procedimiento antes detallado, el OR podrá aprobar la solicitud del certificado de la persona física que fue validada.

13.2. Personas jurídicas públicas: el OR deberá ejecutar adicionalmente el procedimiento que se detalla a continuación para la validación de la correspondiente personas jurídica:

a) Validación de la Nota de la máxima autoridad: requerirá al responsable autorizado la mencionada nota y verificará que la misma esté firmada y sellada por la autoridad competente antes mencionada.

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

c) Verificación de la identidad del titular: verificará que el nombre del Organismo que figura en la Nota de la máxima autoridad del organismo coincide con el

ANEXO I

campo "Denominación de la Persona Jurídica" de la solicitud registrada en el sistema de la AC-ONTI.

d) Validación de la copia fiel de la norma de creación del organismo: requerirá al responsable autorizado la copia fiel de la norma de creación del organismo. Además verificará que el nombre del organismo que allí figura coincide con el campo Organización de la solicitud registrada en el sistema de la AC-ONTI.

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

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

a) Validación de la Constancia de inscripción del Registro Societario: requerirá al responsable autorizado la mencionada constancia y verificará que esté firmada y sellada por autoridad competente del registro societario correspondiente a la jurisdicción. Además deberá verificar que dicha constancia se encuentra autenticada ante escribano.

b) Validación del poder del responsable autorizado: requerirá al responsable autorizado el poder que acredita el carácter de representante legal o apoderado. Allí verificará que el mismo esté expedido por autoridad competente y que se encuentre debidamente autenticado ante escribano.

c) Validación del responsable autorizado: verificará que los datos de identidad que figuran en el poder coinciden con los datos de identidad del responsable autorizado que figuran en la Nota de Solicitud.

ANEXO I

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

e) Opcionalmente si en lugar del poder y la Constancia de Inscripción en el Registro Societario, el responsable autorizado presenta una constancia de escribano público de la existencia de tales documentos, el OR deberá ejecutar sobre este documento el mismo procedimiento de validación de validación detallado en este apartado.

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

14. Finalización de trámite de solicitud:

Efectuados los mencionados controles, el Oficial de Registro podrá:

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

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

- Por no haberse presentado toda la documentación requerida.
- Por inconsistencias en la documentación presentada o entre esta y la solicitud registrada en el sistema de la AC-ONTI.

- Si la nota de solicitud no fue firmada por el solicitante al momento de la solicitud del certificado.
- Si se solicitó un certificado con un dispositivo criptográfico no homologado.
- Si el solicitante no estableció los controles de acceso que aseguren que él es el único capaz de acceder a su clave privada.
- Debido a cualquier otro motivo que impida la validación de los datos del certificado o la ejecución de este procedimiento.
- Por pedido expreso del solicitante.

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

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

Es requerimiento obligatorio para las AR guardar en la aplicación de la AC-ONTI una copia digitalizada firmada digitalmente por el OR de toda la documentación de respaldo del trámite de solicitud dentro del plazo de DIEZ (10) días hábiles de aprobada la misma.

4.3. - Emisión del certificado.

4.3.1. - Proceso de emisión del certificado.

Cumplidos los recaudos del proceso de validación de identidad, titularidad de la clave pública y de otros datos de los solicitantes de acuerdo con lo establecido en este documento y la Política Única de Certificación y una vez aprobada la solicitud de certificado por la AR, el

ANEXO I

Certificador procederá a emitir el certificado digital firmándolo digitalmente; posteriormente el mismo será puesto a disposición del suscriptor.

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

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

Los certificados emitidos por el Certificador tienen los siguientes períodos de validez a partir de su fecha y hora de emisión:

- Certificados de personas físicas: DOS (2) años.
- Certificados de personas jurídicas Públicas o Privadas: TRES (3) años.

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 electrónico declarada por el solicitante o representante autorizado al momento en que se envió la solicitud de certificado.

La AC-ONTI enviará un correo electrónico al suscriptor notificándole de la emisión del certificado el cual contendrá un link desde el cual podrá acceder al sitio web del Certificador para realizar:

- La instalación del certificado, en el caso de certificados con nivel de seguridad Normal.
- La descarga del certificado como un archivo, en el caso de certificados con nivel de seguridad Alto.

ANEXO I

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

4.4. - Aceptación del certificado.

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

Cumplidos estos pasos, el Certificador procederá a publicar el certificado emitido en su sitio web.

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

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

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

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;
c) Solicitar la revocación de su certificado al Certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) Informar sin demora al Certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

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

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

ANEXO I

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

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

Los Terceros Usuarios deben:

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

b) Verificar la validez del certificado digital.

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

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.

Se aplica el punto 3.3.1.- Renovación con generación de nuevo par de claves (Rutina de Re Key).

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

ANEXO I

4.9. - Suspensión y Revocación de Certificados.

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

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

4.9.1. - Causas de revocación.

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

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados de Personas Jurídicas.
- 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.

ANEXO I

- 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.

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.
c) El responsable autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado.
d) Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización.
e) El Certificador o la AR operativamente vinculada.
f) El ente licenciante.
g) La autoridad judicial competente.
h) La Autoridad de Aplicación.

ANEXO I

4.9.3. - Procedimientos para la solicitud de revocación.

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

a) El suscriptor ingresa a la aplicación disponible en https://pki.jgm.gov.ar/app y selecciona la opción "Revocar". A continuación elige una de las siguientes opciones:
    I. Se autentica con su certificado digital.
    II. Ingresa con el pin de revocación que le fue suministrado al momento de descarga de su certificado y su número de documento de identidad.
b) El suscriptor completa el campo Motivo (obligatorio) y el Detalle (optativo).
c) Al presionar el botón "Revocar", la aplicación solicita la reconfirmación de la revocación.
d) Confirma la solicitud de revocación de su certificado.
e) La aplicación solicita al sistema la revocación del certificado.
f) El Certificador revoca el certificado y actualiza el estado del certificado a "Certificado revocado".
g) La aplicación avisa a través de un correo electrónico al suscriptor que su certificado ha sido revocado.

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

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

ANEXO I

a) En caso de que el suscriptor se presente ante la AR para solicitar la revocación, con el fin de verificar su identidad, el OR le requerirá su documento de identidad. En otro caso requerirá una nota formal de la autoridad competente que solicita la revocación.
b) Ingresa a la aplicación y selecciona el certificado que desea revocar de la lista de certificados vigentes.
c) De corresponder verifica que el documento de identidad presentado por el suscriptor coincida en número con el CUIT/CUIL que figura en el certificado.
d) Verifica los datos de la solicitud y certificado seleccionado.
e) Completa el campo Motivo (obligatorio, entre las opciones que se muestran) y Detalle (optativo).
f) Al presionar el botón Revocar, la aplicación requiere una reconfirmación de la revocación.
g) Confirma la revocación del certificado.
h) La aplicación solicita al sistema la revocación del certificado.
i) Actualiza el estado del certificado a "Certificado revocado".
j) La aplicación avisa a través de un correo electrónico al suscriptor que su certificado ha sido revocado.
k) Imprime la nota de revocación, que debe ser firmada por el suscriptor, a fin de archivarla con la documentación de respaldo de la emisión de certificados. En caso de que la solicitud de la revocación no sea efectuada por el suscriptor, deberá archivarse además la documentación de respaldo que avala dicha solicitud.

ANEXO I

4.9.4. - Plazo para la solicitud de revocación.

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

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

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

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

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

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

Los terceros usuarios, al momento de verificar una firma digital, están obligados a comprobar el estado de validez de los certificados mediante el control de la lista de certificados revocados o, en su defecto, mediante el servicio en línea de consultas sobre revocación descripto en el apartado 4.9.9. que el Certificador pondrá a disposición.

Los terceros usuarios están obligados a confirmar la validez de la lista de certificados revocados mediante la verificación de la firma digital del Certificador y de su período de validez.

ANEXO I

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

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

4.9.8.- Vigencia de la lista de certificados revocados.

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

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

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

- Mediante el acceso a la lista de certificados revocados disponible en el sitio http://pki.jgm.gov.ar/crl/FD.crl
- Mediante el servicio en línea de consulta sobre revocación (OCSP) disponible en el sitio web http://pki.jgm.gov.ar/ocsp

La CRL se encuentra disponible SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento. El Certificador garantiza el acceso permanente, eficiente y gratuito del público en general al servicio.

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

ANEXO I

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

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

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

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

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

Ante la falta de disponibilidad del servicio OCSP, se prevé un sitio alternativo que podrá ser accedido para su consulta, con idénticas prestaciones que el servicio principal.

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

ANEXO I

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

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

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

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

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

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

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

a) Por compromiso o sospecha de compromiso de la clave privada.
b) Por pérdida de la clave privada.
c) Porque ya no sea posible su utilización.
d) Ante el conocimiento de que esta ya no sea segura para operar.
e) Por cualquier otra circunstancia que el suscriptor considere que pueda resultar perjudicial a la seguridad de su clave privada.

ANEXO I

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

4.9.13. - Causas de suspensión.

No aplicable.

4.9.14. - Autorizados a solicitar la suspensión.

No aplicable.

4.9.15. - Procedimientos para la solicitud de suspensión.

No aplicable.

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

No aplicable.

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.

- Servicio de consulta a través de página web.

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.

En relación al servicio de consulta web, se podrá acceder a la información de certificados emitidos (vigentes o revocados).

4.10.2. – Disponibilidad del servicio.

Los servicios descriptos se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento, a partir de su sitio web https://pki.jgm.gov.ar/app

4.10.3. – Aspectos operativos.

No existen otros aspectos a mencionar.

4.11. – Desvinculación del suscriptor.

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

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

ANEXO I

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 la Política Única de Certificación asociada a este Manual de Procedimientos 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.

Desde este apartado en adelante se considera información confidencial.