MANUAL DE PROCEDIMIENTOS de CERTIFICACIÓN

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

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

Versión 1.0
Septiembre, 2010

Índice

1. INTRODUCCIÓN

1.1. Resumen

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 la Gestión Pública de la Jefatura de Gabinete de Ministros en el cumplimiento de sus responsabilidades de administración de certificados digitales emitidos a favor de sus suscriptores, en el marco de la Ley N° 25.506 de firma digital, su Decreto Reglamentario N° 2628/02 y la Decisión Administrativa JGM Nº 6/07 y demás normas reglamentarias.

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

a) Política de Certificación
b) Plan de Seguridad (integrado por la Política de Seguridad y el Manual de Procedimientos de Seguridad)
c) Plan de Contingencias
d) Plan de Cese de Actividades
e) Acuerdo con Suscriptores
f) Términos y Condiciones con Terceros Usuarios
g) Política de Privacidad
h) Plataforma tecnológica

1.2. Identificación

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

1.3. Participantes y aplicabilidad

Este Manual de Procedimientos es aplicable a:

a) El Certificador que emite certificados digitales para personas físicas.
b) Las Autoridades de Registro (en adelante AR) que se constituyan en el ámbito de la Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado
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.

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 Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado y del presente Manual de Procedimientos de Certificación.

1.3.2. Autoridad de Registro

El Certificador posee una estructura de Autoridades de Registro constituidas en los entes públicos, las que serán responsables de efectuar las funciones de validación de identidad y de otros datos de los solicitantes y suscriptores de certificados digitales, de acuerdo al ámbito de aplicación establecido para cada una de ellas. Dicho ámbito de aplicación será determinado por:

a) Dominio de correo electrónico del ente público en la cual se constituye la AR.

b) Alcance de la aplicación para la cual se constituye la AR.

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

Los organismos que han sido habilitados para operar como AR del Certificador se encuentran disponibles en su 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.

1.3.3. Procedimiento de designación de Autoridades de Registro pertenecientes a la Administración Pública Nacional.

La ONTI en su calidad de Certificador posee una estructura de Autoridades de Registro que efectúan las funciones de validación de identidad y de otros datos de los solicitantes y suscriptores de certificados, registrando las presentaciones y trámites que les sean formulados por éstos.
Cuando las Autoridades de Registro del Certificador pertenezcan a entidades y Jurisdicciones de la Administración Pública Nacional el procedimiento a seguir a los fines del nombramiento de sus Oficiales de Registro será el anunciado a continuación:

Marco Normativo:
Conforme surge de los términos del artículo 39 del decreto reglamentario N° 2628/02 las áreas de Recursos Humanos correspondientes a las entidades y jurisdicciones pertenecientes a la Administración pública Nacional cumplirán las funciones de Autoridad de Registro del Certificador, respecto a los agentes y funcionarios de su jurisdicción. En caso de designación de otra unidad en las funciones de Autoridad de Registro, la máxima autoridad del Organismo que así lo requiera deberá informarlo al certificador.

1. El Responsable de la Autoridad de Registro comunicará al Certificador que el área de Recursos Humanos del Organismo al que pertenece, desempeñará las funciones de Autoridad de Registro.
2. El Organismo perteneciente a la Administración Pública Nacional que decidiere que otra unidad adicional al área de Recursos Humanos desempeñe la función de Autoridad de Registro, comunicará al Certificador mediante nota suscripta por su máxima autoridad, la unidad del Organismo que va a desempeñarse como Autoridad de Registro del Certificador licenciado.
    - El certificador procederá a aprobar o bien a denegar la propuesta, haciéndole saber al Organismo respecto de las obligaciones y responsabilidades que asume al respecto, conforme así lo determina el artículo 36 del Decreto Reglamentario N° 2628/02.
3. La máxima autoridad del organismo así también deberá designar por lo menos un Instructor de Firma Digital y un Responsable de Soporte de Firma Digital.

Para ambas situaciones enunciadas:

1) El Responsable de la AR procederá a comunicar la designación del agente que ejercerá el rol de Oficial de Registro en la o las respectivas autoridades de Registro constituidas. La persona o personas involucradas para ocupar dicho rol y función dentro de la operatoria de la Autoridad de Registro deberán haber aprobado previamente el curso y capacitación impartida al efecto por el Certificador.
2) El Oficial de Registro deberá solicitar un certificado de nivel de seguridad alto debiendo contar al momento de dicha solicitud con un dispositivo criptográfico provisto por el Organismo en el cual desempeña su función el que quedará bajo su absoluto y exclusivo control.
3) Finalmente el certificado del Oficial de Registro de nivel de seguridad alto solicitado, será dado de alta por el responsable de la aplicación de la AC ONTI, procediéndose a relacionarlo con la AR donde llevará a cabo su función, previa constatación del documento o disposición que apruebe su designación.

1.3.4. Procedimiento de designación de Autoridades de Registro pertenecientes al Sector Público.

Marco Normativo:
Conforme surge del artículo 35 del Decreto Reglamentario Nº 2628/02, los Certificadores licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador licenciado, cumpliendo las normas y

procedimientos establecidos por la presente reglamentación. Las funciones detentadas por la Autoridad de Registro se encuentran detalladas en los incisos que enumera el artículo referido.

Procedimiento:

1) La máxima autoridad del Organismo o entidad perteneciente al Sector Público comunicará al Certificador la unidad del Organismo que va a desempeñarse como Autoridad de Registro del Certificador licenciado.

2) El certificador procederá a aprobar o bien a denegar dicha propuesta, haciéndole saber al Organismo respecto de las obligaciones y responsabilidades que asume al respecto conforme surgen del artículo 36 del Decreto Reglamentario N° 2628/02.

3) En caso de aprobación, la Máxima autoridad de la Autoridades de Registro o RESPONSABLE de dicha Autoridad de Registro aprobada por el Certificador procederá a comunicar la designación de los agentes que ejercerán el o los roles de OFICIAL DE REGISTRO en la o las respectivas autoridades de Registro constituidas. La persona involucrada para ocupar dicho rol y función dentro de la operatoria de la Autoridad de Registro deberá haber aprobado previamente el curso y capacitación impartida al efecto por el Certificador.

4) El Oficial de Registro deberá solicitar un certificado de nivel de seguridad alto debiendo contar al momento de dicha solicitud con un dispositivo criptográfico provisto por el Organismo en el cual desempeña su función el que quedará bajo su absoluto y exclusivo control.

5) El certificado del Oficial de Registro de nivel de seguridad alto solicitado, será dado de alta por el responsable de la aplicación de la AC ONTI, procediéndose a relacionarlo con la AR donde llevará a cabo su función, previa constatación del documento o disposición que apruebe su designación.

6) La máxima autoridad del organismo deberá así también designar por lo menos un Instructor de Firma Digital y un Responsable de Soporte de Firma Digital.

1.3.5. Plan de transición aplicable a Oficiales de Registro.

Atento la necesidad de habilitar y relacionar los certificados de los Oficiales de Registro a la nueva solución desarrollada en el marco del proceso de licenciamiento de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI), se establece a continuación el siguiente PLAN DE TRANSICION.

Se reconocerán como Oficial de Registro “ACTIVOS” a todos aquellos que se encuentren en ejercicio de dicho rol y función dentro de la operatoria de una Autoridad de Registro en funcionamiento y detenten una designación vigente dentro del marco o estructura de la AC ONTI no licenciada.

El Oficial de Registro activo pasará a formar parte de la estructura de la Autoridad Certificante licenciada, siempre que su designación se encuentre confirmada como tal dentro de la Autoridad de Registro a la cual se encuentra vinculado, mediante nota dirigida al Certificador, la cual deberá encontrarse suscripta por el Responsable de la Autoridad de Registro correspondiente o bien aprobada por el Certificador en los casos que así correspondan.

A los fines de ejercer sus funciones dentro de la operatoria de la Autoridad Certificante de la ONTI licenciada, el referido Oficial de registro deberá tener aprobada la capacitación requerida para el ejercicio de dicho rol, capacitación que será la impartida por la ONTI, mediante el dictado de un curso diseñado al efecto, el que será oportunamente evaluado.

El Oficial de Registro procederá a solicitar a la nueva aplicación de la Autoridad Certificante de la ONTI un certificado de nivel de seguridad alto, debiendo contar al momento de dicha solicitud con un dispositivo criptográfico provisto por el Organismo al que pertenezca, el que quedará bajo su absoluto y exclusivo control.

La nueva aplicación de la AC licenciada de la ONTI emitirá a favor del Oficial de Registro un certificado de nivel de seguridad alto. Dicho certificado será dado de alta por el responsable de la nueva aplicación de la AC ONTI, procediéndose a relacionarlo con la AR donde llevará a cabo su función, previa constatación del documento o disposición que apruebe su designación.

El Certificador procederá a enviar a los Oficiales de Registro activos un ejemplar de la nueva Política de Certificación de la Autoridad Certificante de la ONTI titulada: “Política de Certificación y del Manual de Procedimientos de Certificación para personas físicas de Entes Públicos, Estatales o no Estatales y Personas Físicas que realicen trámites con el estado”. El Oficial de Registro deberá suscribir y aceptar dicha nota de envío de la documentación, lo que implicará que se impone de los términos y condiciones de dicha política así como de las obligaciones y responsabilidad que asume en el ejercicio de su función dentro del marco de la nueva estructura de firma digital de la ONTI.

Asimismo, se les comunicará a los Oficiales de registro que las Autoridades de Registro que funcionen dentro de la estructura del Certificador licenciado, serán susceptibles de ser auditadas por el Certificador conforme así lo determina el artículo 32 de la Decisión Administrativa Nº 6/07 y 13 del Decreto Reglamentario Nº 2628/02.

1.3.6. Suscriptores de certificados

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

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

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

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

Podrán también ser suscriptores de la AC ONTI las personas físicas que realicen trámites para los que el Estado requiera una firma digital, siempre que la AR encargada del proceso de registración haya sido previamente autorizada por el Certificador para realizar este tipo de emisión.

1.3.7. Aplicabilidad

Los certificados digitales emitidos en el marco de la Política vinculada a este Manual de Procedimientos, podrán ser utilizados para firmar cualquier transacción electrónica asociada a la función correspondiente a cada suscriptor. Para el caso de las personas físicas no pertenecientes a Entes Públicos, solo podrán utilizar los certificados digitales para realizar trámites con el Estado.

Se contempla también la emisión de certificados para la verificación en línea del estado de los certificados (OCSP), los que serán emitidos únicamente a favor de la AC ONTI.

Para los certificados digitales emitidos a favor de personas físicas, se definen dos niveles de seguridad:

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

b) Normal: correspondiente a los certificados solicitados y almacenados vía contenedor de certificados.

1.4. Contactos

El presente Manual de Procedimientos es administrado por:

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

Por consultas o sugerencias, dirigirse a:

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

2. ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACIÓN

2.1. Obligaciones

2.1.1. Obligaciones del certificador

Las obligaciones del certificador se encuentran establecidas en el apartado 2.1.1. de la Política de Certificación.

2.1.2. Obligaciones de la Autoridad de Registro

Las obligaciones de las AR se encuentran establecidas en el apartado 2.1.2. de la Política de Certificación.

Adicionalmente los entes públicos que constituyan una AR asumen las siguientes obligaciones:

- Instruir a sus suscriptores 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 por medio de la designación de un Instructor de Firma Digital quien será el responsable encargado de ejercer esa tarea.

- Instruir a sus usuarios acerca de las buenas prácticas de utilización de la tecnología de firma digital por medio del mencionado Instructor de Firma Digital.
- Asistir a solicitantes o suscriptores 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 por medio de la designación de un Responsable de Soporte de Firma Digital quien será el encargado de ejercer esa tarea.

Los roles de Instructor de Firma Digital y de Responsable de Soporte de Firma Digital podrán recaer en una o varias personas y sus funciones serán asignadas por autoridad competente del organismo. Eventualmente ambos roles podrán ser asignados a una misma persona si la autoridad competente así lo decidiese. Una vez que los roles antes citados fueron designados el responsable de la AR deberá informar de tal situación mediante una nota enviada al Certificador.

Es responsabilidad del ente público donde se constituye la AR asegurar la disponibilidad de ambos roles, como así también, asegurar su reemplazo, en caso de producirse la baja de alguno de ellos. Bajo ninguna circunstancia estas responsabilidades recaerán en el Certificador.

2.1.3. Obligaciones del suscriptor del certificado

El suscriptor de un certificado digital asume las obligaciones establecidas en el apartado 2.1.3 de la Política de Certificación.

2.1.4. Obligaciones de terceros usuarios

Los terceros usuarios de un certificado digital asumen las obligaciones establecidas en el apartado 2.1.4 de la Política de Certificación.

2.1.5. Obligaciones del servicio de repositorio

El Certificador brinda el servicio de repositorio según lo establecido en el apartado 2.1.5 de la Política de Certificación.

2.2. Responsabilidades

El Certificador asume la responsabilidad ante terceros con el alcance establecido en el apartado 2.2 de la Política de Certificación.

2.3. Responsabilidad Financiera

2.3.1. Responsabilidad Financiera del certificador

Las responsabilidades financieras se originan en lo establecido por la Ley 25.506 y su Decreto Reglamentario Nº 2628/02 y en las disposiciones de la Política de Certificación vinculada a este Manual de Procedimientos.

2.4. Interpretación y Legalidad

2.4.1. Legislación aplicable

La interpretación, obligatoriedad, diseño y validez de este Manual de Procedimientos se encuentra sometido a lo establecido por la Ley Nº 25.506, su Decreto Reglamentario Nº 2628/02, la Decisión Administrativa N° 6/07 y demás normas complementarias dictadas por la Autoridad de Aplicación.

2.4.2. Forma de interpretación y aplicación

La interpretación y/o aplicación de las disposiciones del presente Manual de Procedimientos y de cualquiera de sus documentos asociados, será resuelta según las normas mencionadas en el apartado 2.4.1 y los procedimientos indicados en el apartado 2.4.3.

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

2.4.3. Procedimientos de resolución de conflictos

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

El presente Manual de Procedimientos se encuentra en un todo subordinado a las prescripciones de la Ley N° 25.506 y su reglamentación.
Los titulares de certificados y los terceros usuarios podrán interponer ante el Ente Licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por el Certificador, sólo será procedente previa acreditación de haberse efectuado reclamo ante este último con resultado negativo. Acreditada dicha circunstancia, el Ente Licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.
A los efectos del reclamo antes citado, se procederá de la siguiente manera:

- Una vez recibido el reclamo en las oficinas del Certificador, este citará al reclamante a una audiencia y labrará un acta que deje expresa constancia de los hechos que motivan el reclamo y de todas y cada uno de los antecedentes que le sirvan de causa.
- Una vez que el Certificador emita opinión, se notificará al reclamente y se le otorgará un plazo de CINCO (5) días hábiles administrativos para ofrecer y producir la prueba de su descargo.
- La ONTI resolverá en un plazo de DIEZ (10) días lo que estime corresponder, dictanto el Acto Administrativo correspondiente, conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable.

2.5. Aranceles

El Certificador no percibe aranceles por ninguno de sus servicios relacionados con la Política de Certificación vinculada a este Manual de Procedimientos de Certificación.

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

2.6.1. Publicación de información del Certificador

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

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

La información antedicha se encuentra disponible 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.

2.6.2. 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.

2.6.3. Controles de acceso a la información

El Certificador no establece restricciones al acceso a la Política 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.

El Certificador garantiza el acceso a su certificado de clave pública y su estado de validez, a la Lista de Certificados Revocados y sus correspondientes deltas, a la Política de Certificación y a este Manual de Procedimientos, en sus versiones anteriores y actualizadas excepto en sus aspectos confidenciales.

2.6.4. Repositorios

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

El repositorio se encuentra disponible para uso público durante las VEINTICUATRO (24) horas diarias los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento.

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

2.7. Auditorias

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

La información relevante de los informes de las auditorías es publicada en el sitio web del Certificador https://pki.jgm.gov.ar/app

Se realiza una auditoría previa al licenciamiento del Certificador a fin de verificar el cumplimiento de los requisitos correspondientes al licenciamiento. Con posterioridad, el Certificador será sujeto a auditorías ordinarias para controlar la continuidad del cumplimiento de las normas vigentes y a auditorías extraordinarias de oficio, según lo disponga la Autoridad de Aplicación.

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

El Certificador realizará auditorías a sus AR en base a un cronograma anual. Podrá asimismo realizar revisiones ad-hoc cuando las circunstancias lo ameriten. La realización de auditorías periódicas será notificada con al menos CINCO (5) días de anticipación y tendrá como resultado un informe que comprenderá tanto las observaciones encontradas, como un dictamen respecto a la confiabilidad y calidad de la operatoria de la AR y el cumplimiento de las especificaciones de este Manual de Procedimientos y demás documentación aplicable.

El Certificador se reserva el derecho de suspender temporalmente o revocar la autorización para actuar como AR Delegada, en caso de detectar incumplimientos graves en la operatoria de la AR.

2.8. Confidencialidad

En todos los casos detallados a continuación en este ítem se aplica la Ley Nº 25.506 en relación a la información provista por los solicitantes y/o suscriptores de certificados.

2.8.1. Información confidencial

Resulta de aplicación lo establecido en el apartado 2.8.1 de la Política de Certificación.

2.8.2. Información no confidencial

Resulta de aplicación lo establecido en el apartado 2.8.2 de la Política de Certificación.

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

Resulta de aplicación lo establecido en el apartado 2.8.3 de la Política de Certificación.

2.8.4. Divulgación de información a autoridades judiciales

Resulta de aplicación lo establecido en el apartado 2.8.4 de la Política de Certificación.

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

Resulta de aplicación lo establecido en el apartado 2.8.5 de la Política de Certificación.

2.8.6. Divulgación de información por solicitud del suscriptor

Resulta de aplicación lo establecido en el apartado 2.8.6 de la Política de Certificación.

2.8.7. Otras circunstancias de divulgación de información

Resulta de aplicación lo establecido en el apartado 2.8.7 de la Política de Certificación.

2.9. Derechos de Propiedad Intelectual

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

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Registro inicial

El Certificador emite certificados a las personas físicas que cumplan con los requisitos para ser suscriptor, efectuándose una validación personal de la identidad del solicitante, para lo cual se requiere su presencia física ante la AR. Asimismo, el solicitante debe probar su carácter de suscriptor para la correspondiente Política de Certificación. La única excepción a la emisión de certificados para persona físicas es el caso del Certificado OCSP, mencionado en el apartado 1.3.4.

A fin de efectuar la validación mencionada, se deben cumplir los siguientes procedimientos:

a) El solicitante ingresa al sitio web del Certificador https://pki.jgm.gov.ar/app
b) Completa la solicitud de certificado con sus datos personales.
c) Acepta el Acuerdo con Suscriptores en el que se hace referencia a la Política que respalda la emisión del certificado.
d) Envía su solicitud a la AC ONTI e imprime la Nota de Solicitud.
e) Verifica que el Código de Solicitud de la Nota de Solicitud coincida con el que aparece en la pantalla y en ese caso firma la Nota de Solicitud.
f) Se presenta ante la AR correspondiente con la documentación requerida con el fin de realizar su identificación personal.

El Oficial de Registro efectúa los siguientes procedimientos con el fin de realizar la identificación del solicitante y corroborar la titularidad de la solicitud de certificado:

a) Verifica la existencia en el sistema de la solicitud
b) Al momento de presentación del solicitante o suscriptor en sus oficinas, valida su identidad mediante la verificación de la documentación requerida
c) Verifica la titularidad de la solicitud mediante el control de la nota correspondiente
d) Requiere al solicitante la firma de la nota de solicitud en su presencia

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

Cumplido el proceso de autenticación de su identidad, 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.

El Certificador se obliga a cumplir con las disposiciones de la Política 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.

3.1.1. Tipos de Nombres

Los Tipos de Nombres admitidos para los suscriptores de certificados son los correspondientes a los documentos de identificación requeridos.

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 de Certificación.

3.1.3. Reglas para la interpretación de nombres

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

3.1.4. Unicidad de nombres

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

3.1.5. Procedimiento de resolución de disputas sobre nombres

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

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

No se aplica por tratarse de un Manual de Procedimientos vinculado a una Política de Certificación de personas físicas.

3.1.7. Métodos para comprobar la posesión de la clave privada

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

En el caso de solicitudes de certificados de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo 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 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 AC ONTI comprobará que la solicitud recibida es válida verificando la firma digital de la misma con la clave pública recibida.; De este modo si la firma digital es válida significa que la persona que realizó

la solicitud está en posesión de la clave privada asociada y que la información transmitida no ha sido alterada.

De acuerdo con el artículo 21 inciso b) de la Ley Nº 25.506 y el artículo 34 inciso i) del Decreto Nº 2628/2002 el certificador está obligado a abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada de los solicitantes y titulares de los certificados por él emitidos.

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

No es aplicable, ya que la presente Política de Certificación vinculada al presente Manual de Procedimientos no contempla la emisión de certificados digitales a personas jurídicas.

3.1.9. Autenticación de la identidad de personas físicas

El solicitante del certificado se presenta personalmente ante el Oficial de Registro de la Autoridad de Registro asignada con la siguiente documentación a fin de realizar la verificación de su identidad:

a) Documento Nacional de Identidad, Libreta Cívica o Libreta de Enrolamiento (original y fotocopia) para ciudadanos argentinos o residentes o Pasaporte o Cédula MERCOSUR (original y fotocopia) para extranjeros.
b) 1. Para el caso de personas físicas de entes públicos estatales, Nota de certificación de servicios. Esta consiste en:

    a. Constancia emitida por la Oficina de Recursos Humanos, Personal o equivalente de su organismo o entidad, firmada por un funcionario responsable, según modelo de publicado en

http://pki.jgm.gov.ar/docs/Nota_de_certificacion_de_servicios_RRHH.pdf , en la que conste lugar y fecha de emisión, nombre y apellido, documento de identidad, organismo, unidad y cargo que ocupa en el mencionado organismo o entidad, fecha de inicio y de caducidad del cargo (en caso de no tener fecha de caducidad esto debe ser indicado en la misma nota) y los datos correspondientes al funcionario a quien reporta (apellido, nombre, cargo o puesto y documento de identidad).

b. Adicionalmente, deberá acompañarse una nota del funcionario de reporte del solicitante o suscriptor, según modelo publicado en http://pki.jgm.gov.ar/docs/Nota_de_certificacion_Funciones.pdf . indicando el cargo o puesto que éste ocupa: esta nota debe contener además el nombre y apellido y, documento de identidad tanto del solicitante como del funcionario de reporte.

c. Opcionalmente, podrá ser acompañada por una copia autenticada del Acto Administrativo correspondiente a su designación.

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

c) Nota de solicitud de certificado, firmada y aclarada por el solicitante sobre el campo rotulado "Firma y aclaración del solicitante", el resto de los campos de la Nota de Solicitud no deben ser firmados.

El Oficial de Registro ingresa a la aplicación 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 Autoridad de Registro". A continuación verificará que el solicitante es el titular de la solicitud, para ello debe verificar que toda la información que figura en la Nota de solicitud coincida con toda la documentación presentada (original y fotocopia) y con la que figura en el sistema de recepción de solicitudes.

Con el fin de ejecutar el procedimiento de autenticación antes mencionado el Oficial de Registro correspondiente, en presencia del solicitante, deberá verificar:

a) Que el documento de identidad presentado es válido, para ello deberá verificar que:
   1. Corresponde a la persona que se presentó.
   2. El nombre, apellido, tipo, número y versión del documento (original, duplicado, etc.) coinciden con los declarados por el solicitante tal como figura en la Nota de solicitud.
   3. La fotocopia del documento de identidad presentado coincide con el documento de identidad del cual se obtuvo copia.
   4. Hecha las validaciones anteriores, en presencia del Oficial de Registro el solicitante

firma hológrafamente con aclaración de firma la fotocopia del documento de identidad presentado.

b) Que la Nota de Certificación de Servicios presentada es válida, para ello deberá verificar que:
   1. Dicha persona es aquella cuyos datos figuran en la certificación de servicios presentada. A tal fin debe cotejar todos los datos del documento de identidad mencionados en el ítem a.2. con los que figuran en la mencionada certificación.
   2. Que el cargo o puesto coincide con el que figura en la Nota de Solicitud.
   3. Que la jurisdicción y unidad a la cual el cargo o puesto está asociado coincide con las que figuran en la Nota de Solicitud.
   4. Que está firmada por una autoridad competente
   5. Que la fecha de emisión de la Nota de Certificación de Servicios fue hecha dentro de los VEINTE (20) días de efectuada la solicitud del certificado.
   6. Que la fecha de solicitud del certificado y de presentación del solicitante ante la AR se encuentra dentro del período de validez del cargo o puesto, según la fecha de inicio y de caducidad que figura en la nota.

c) Que la Nota del funcionario de reporte del solicitante es válida, verificando que se encuentre firmada por el funcionario informado en la Nota de Certificación de Servicios debiendo hacer sobre esta nota las mismas verificaciones que las realizadas en los puntos anteriores respecto de la Nota de Solicitud.

d) Que el código de solicitud (hash) que figura en la Nota de Solicitud se corresponde con el que posee registrado en su sistema la AC ONTI.

e) Que el resto de los datos que figuran en la Nota de Solicitud se corresponden con los que posee registrado en su sistema la AC ONTI.

f) Que la Nota de Solicitud esté firmada hológrafamente por el solicitante en el campo rotulado "Firma del y aclaración del solicitante". Verifica 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.

Una vez validada toda la información de la Nota de Solicitud, el solicitante firma hológrafamente con aclaración de firma el campo “Firma y aclaración del solicitante en presencia del Oficial de Registro”.
El Oficial de Registro verifica 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”.
La AR conserva toda la documentación respaldatoria del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

El solicitante al contrafirmar la Nota de Solicitud en presencia del Oficial de Registro declara expresamente:

- Ser el titular de la solicitud identificada por el Código de Solicitud (hash) provisto por la AC ONTI al momento de la recepción de la solicitud.
- Que los datos contenidos en la solicitud, que se incluirán en el certificado a emitir, son válidos.
- Que realizó el procedimiento de solicitud siguiendo los pasos indicados en el apartado 4.1.1.
- Que aceptó el Acuerdo con suscriptores, incluyendo la aceptación de la Política de Certificación.

El solicitante recibe vía correo electrónico una notificación en la que se le indica que su certificado ha sido emitido, incluyendo las instrucciones para su instalación.

Efectuados los mencionados controles, el Oficial de Registro podrá:

a) Aprobar la solicitud, en tal caso la misma cambia a 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:

    1. Por no haberse presentado toda la documentación requerida o si la misma no puede ser validada.
    2. Por pedido expreso del solicitante.

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

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

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

3.3. Generación de nuevo certificado (posterior a revocación)

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

3.4. Requerimiento de revocación

En caso que el titular del certificado se encuentre en posesión de su clave privada podrá solicitar la revocación ingresando al sitio web del certificador en: https://pki.jgm.gov.ar/app
De no cumplirse el supuesto anterior, podrá efectuar la solicitud de revocación ingresando al sitio web del certificador a https://pki.jgm.gov.ar/app y suministrando el código de revocación provisto al momento de la emisión del certificado y su documento de identidad.
En los dos casos antes mencionados el servicio se encuentra disponible las VEINTICUATRO (24) horas. del día (sujeto a un razonable calendario de mantenimiento) y la revocación se efectuará en forma automática.

En el caso que el suscriptor no pudiera utilizar alguno de los métodos antes mencionados, únicamente podrá solicitar la revocación de su certificado presentándose personalmente ante la Autoridad de Registro correspondiente acreditando su identidad con su documento de identidad. Cumplido dicho procedimiento, el Oficial de Registro revocará el certificado.

En caso de que la solicitud no fuera efectuada por el suscriptor, la misma deberá ser remitida por un funcionario autorizado o autoridad de acuerdo con lo establecido en el apartado 4.4.2 por nota escrita dirigida a la AR correspondiente en la que debe indicar 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. y guardará la documentación respaldatoria del proceso efectuado por el término de DIEZ (10) años.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de certificado

4.1.1. Solicitud de nuevo certificado

El proceso de solicitud debe ser iniciado solamente por el interesado. La solicitud del certificado se encuentra sujeta a revisión y aprobación por parte del Certificador.

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 esta realizando la solicitud, en caso de que tuviera que abandonar aquella temporalmente.

Iniciación del proceso:

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

a) Completar el formulario de solicitud de certificado.
b) El sistema asigna 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 fueran asignadas varias AR, el usuario deberá elegir la AR que le corresponde. De no efectuarse dicha asignación, el sistema permite que el usuario indique si el certificado a tramitar es para ser utilizado en alguna de las aplicaciones transversales 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 usuario 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.

c) Cumplidos los pasos anteriores, el solicitante completa el formulario de solicitud con los datos que serán incluidos en el certificado a emitir de acuerdo con lo establecido en el apartado 3.1.2.

d) El solicitante acepta el acuerdo con suscriptores incluyendo la Política de Certificación..

e) Si los datos son correctos, se permitirá al solicitante efectuar la solicitud de certificado para lo cual el solicitante realizará los siguientes pasos:

1. En caso que decida realizar la solicitud con nivel de seguridad "Alto" deberá insertar el dispositivo criptográfico.
2. Procede a generar su par de claves con el nivel de seguridad elegido por este ("Alto" o "Normal"). En ambos casos deberá establecer los controles de acceso que aseguren que él es el único capaz de acceder a su clave privada.
3. Envía la solicitud a la AC ONTI en formato PKCS#10.
4. La aplicación verifica que la solicitud sea válida y procede a generar un identificador de trámite y un código de solicitud (hash).
5. 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.
6. Como paso siguiente el solicitante debe imprimir la Nota de solicitud, la cual contiene:
   - Todos los datos de la solicitud.
   - El código de solicitud (hash)
   - La declaración de la titularidad de la solicitud identificada por el Código de Solicitud provisto por la AC ONTI
   - La declaración de haber leído y aceptado el Acuerdo con suscriptores y la Política de Certificación.
   - La declaración de que los datos contenidos en la solicitud, que se incluirán en el certificado a emitir, son válidos..
7. El solicitante debe verificar que el Código de Solicitud 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 debe destruir la Nota de Solicitud impresa y comenzar el trámite nuevamente. 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.

8. 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.
9. 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.

f) La aplicación envía un correo electrónico al solicitante que contendrá un link de acceso a la aplicación. El solicitante debe acceder al mismo para confirmar al Certificador que la dirección de correo electrónico ingresada es la correcta y que posee acceso a la cuenta de correo declarada. El correo electrónico contiene además un identificador de trámite, que el usuario podrá utilizar para consultar el estado del mismo.
g) A continuación aparecerá un mensaje en pantalla informando al usuario:
    - que su correo electrónico fue verificado,
    - que el trámite cambió de estado,
    - detalle de la documentación que debe presentar ante la AR.

Para continuar el proceso el solicitante deberá presentarse ante la AR asignada con toda la documentación indicada en el apartado 3.1.9 a fin de efectuar la verificación de sus datos.

4.1.2. Solicitud de renovación

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. Solo se podrán efectuar un máximo de dos 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.

Adicionalmente, el Certificador podrá implementar un servicio de alerta de certificados próximos a vencer. Este incluye el envío de de un correo electrónico de alerta a la cuenta de correo electrónico que figura en el certificado del suscriptor, cuando el certificado se encuentre dentro de los QUINCE (15) 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 CINCO (5) días anteriores próximos a su vencimiento.
Además, el servicio incluye la emisión de un aviso por correo electrónico en forma de resumen por cada una de las AR involucradas en la emisión de los certificados que vencen en los próximos QUINCE (15) y CINCO (5) días. Si el certificado a vencer está relacionado al rol de un Oficial de Registro, el correo electrónico es enviado además a la AR central.

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) Acceder a la aplicación de renovación de certificados.
b) Autenticarse ante el Certificador utilizando la clave privada y el certificado que desea renovar para firmar el requerimiento de renovación. La aplicación mostrará los datos contenidos en dicho certificado.
c) Confirmar la renovación por medio del envío de la solicitud de renovación a la AC ONTI, firmada digitalmente.

Una vez remitida la solicitud, la aplicación realizará el siguiente procedimiento:

a) Genera un identificador de trámite y lo informa al suscriptor por pantalla.
b) Envía un correo electrónico al suscriptor para alertar que el trámite se encuentra iniciado correctamente.
c) Muestra una pantalla que indica si el trámite se inició correctamente.

En cualquier circunstancia el suscriptor establecerá los controles de acceso a la clave privada que aseguren que él es el único capaz de acceder a ella.

El procedimiento de aprobación deberá ser realizado por la misma AR que fuera asignada al solicitante, cuando efectuara la solicitud inicial del certificado a renovar. En los casos de suscriptores de entes públicos estatales, a fin de obtener la aprobación de la renovación, no será requerida la presencia física del suscriptor ante la AR, debiendo remitir a la AR la Nota de Certificación de

Servicios emitida por la Oficina de Recursos Humanos o equivalente junto con la nota del funcionario de reporte del suscriptor, ambas notas con idénticas características a las establecidas en el apartado 3.1.9.

Para el resto de los casos, la posibilidad de renovación de certificado como así también el procedimiento podrá ser definido en cada acuerdo a firmar con el Certificador; en cualquier caso se mantendrán las condiciones establecidas por la Política de Certificación para el proceso de renovación.

La única excepción será el caso de un suscriptor que se desempeñe en un ente público estatal que no hubiera constituido una AR al momento en que aquel efectuara la solicitud inicial del certificado, por lo que se le hubiera asignado otra AR para la aprobación de la misma. En caso que la AR se hubiera constituido posteriormente y esta estuviera en funcionamiento al momento de solicitar la renovación, el suscriptor podrá gestionarla ante la nueva AR constituida en el ente público donde se desempeña, pudiendo la nueva AR solicitar su presentación ante ella, con toda la documentación requerida para la emisión de un nuevo certificado mencionada en el apartado 3.1.9.

En los casos en que intervenga la misma AR para la aprobación de la renovación, el Oficial de Registro, deberá verificar:

a) La recepción de la solicitud de renovación en la aplicación de la AC ONTI y a través de ella accederá al certificado a renovar.
b) Que la Nota de Certificación de Servicios presentada es válida; para ello deberá verificar que:
    1. Dicha persona es aquella cuyos datos figuran en la certificación de servicios presentada. A tal fin debe cotejar el nombre, apellido, tipo, número y versión (si corresponde) del documento de identidad con los que figuran en la mencionada certificación.
    2. Que el cargo o puesto coincide con el que figura en la Nota de Certificación de Servicios.
    3. Que la jurisdicción y unidad a la cual el cargo o puesto está asociado coincide con las que figuran en la Nota de Certificación de Servicios.
    4. Que está firmada por una autoridad competente.
    5. Que la fecha de emisión de la certificación de servicios fue hecha dentro de los VEINTE (20) días de efectuada la solicitud de renovación del certificado.
    6. Que la fecha de solicitud del certificado se encuentra dentro del período de validez del cargo o puesto, según la fecha de inicio y de caducidad que figura en la nota.
    7. Que la Nota del funcionario de reporte del solicitante es válida, verificando que se encuentre firmada por el funcionario informado en la Nota de Certificación de Servicios debiendo hacer sobre esta nota las mismas verificaciones que las realizadas en los

puntos anteriores respecto de la Nota de Solicitud.

Efectuados los mencionados controles, el Oficial de Registro podrá:

a) Aprobar la solicitud de renovación; en tal caso la misma cambia a 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:
    1. Por no haberse presentado toda la documentación requerida para la renovación o si la misma no puede ser validada.
    2. Por pedido expreso del solicitante.

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

4.2. Emisión del certificado

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

La AC ONTI enviará un correo electrónico al suscriptor desde el cual podrá acceder al sitio web del Certificador para realizar su descarga e instalación; en el mismo correo electrónico se le enviará su código de revocación.

El solicitante deberá almacenar la clave privada, el certificado emitido y el código de revocación. Los certificados emitidos por el Certificador tienen un período de validez de DOS (2) años a partir de su fecha y hora de emisión.

4.3. Aceptación del certificado

Cumplidas las condiciones establecidas en el apartado 4.3 de la Política de Certificación, un certificado se considera aceptado por su titular una vez, que ha sido emitido por la AC ONTI y remitido 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.

4.4. Suspensión y Revocación de Certificados

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

4.4.1. Causas de revocación

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

a) A solicitud del titular del certificado
b) Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación
c) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros
d) Por condiciones especiales definidas en la Política de Certificación
e) Por Resolución Judicial o Acto Administrativo de Autoridad competente
f) Por fallecimiento del titular.
g) Por declaración judicial de ausencia con presunción de fallecimiento del titular
h) Por declaración judicial de incapacidad del titular
i) Si se determina que la información contenida en el certificado digital ha dejado de ser válida
j) Cuando la clave privada asociada al certificado digital, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
k) Cuando cese el vínculo del suscriptor con el ente o sea modificada su situación de revista o cargo.

l) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
m) Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, del Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
n) Por revocación del certificado digital del Certificador
o) Cuando así lo establezcan las condiciones indicadas en el Acuerdo aplicable a la AR, de existir

En caso que el Certificador determinara que un certificado ha dejado de cumplir con lo dispuesto en la Política de Certificación y/o con las normas legales y reglamentarias de la Infraestructura de Firma Digital de la República Argentina, revocará el mismo en un plazo no superior a las VEINTICUATRO (24) horas de haber efectuado dicha comprobación.

4.4.2. Autorizados a solicitar la revocación

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

a) El suscriptor del certificado
b) El Responsable de la Autoridad de Registro.
c) La autoridad competente del ente público de quien depende el suscriptor.
d) El responsable del Certificador o de la Autoridad de Registro correspondiente a ese suscriptor.
e) La Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina
f) La Autoridad Judicial competente
g) En el caso de certificados emitidos a favor de personas físicas no pertenecientes a entes públicos estatales, el Certificador procederá a su revocación a solicitud de su titular o en los supuestos previstos en el acuerdo correspondiente.

4.4.3. Procedimientos para la solicitud de revocación

4.4.3.1. Revocación de Certificados de Firma Digital por el suscriptor

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:
    1 Se autentica con su certificado digital.
    2 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) 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 el método antes mencionado deberá presentarse personalmente con su documento de identidad ante la AR que aprobó su certificado.

4.4.3.2. Revocación de Certificados Digital por la Autoridad de Registro

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

a) En caso de que el suscriptor se presente ante la AR para solicitar la revocación, con el fin de verificar su identidad, el OR le requerirá su documento de identidad. En otro caso requerirá el documento de identidad de la autoridad competente que solicita la revocación a fin de efectuar la verificación de su identidad.
b) Ingresa a la aplicación y selecciona el certificado que desea revocar de la lista de certificados vigentes.
c) De corresponder verifica que el documento de identidad presentado por el suscriptor coincida en número con el que figura en el certificado y que la versión del documento (original, duplicado, etc.) sea la misma o posterior a la 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 presenta 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 o la autoridad competente que solicita la revocación, a fin de archivarla con la documentación respaldatoria 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 legal respaldatoria que avala dicha solicitud.

4.4.4. 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 4.4.1 y se hayan cumplido los procedimientos previstos en el apartado 4.4.3.

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.

4.4.5. Causas de suspensión

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

4.4.6. Autorizados a solicitar la suspensión

No aplicable

4.4.7. Procedimientos para la solicitud de suspensión

No aplicable

4.4.8. Límites del periodo de suspensión de un certificado

No aplicable

4.4.9. Frecuencia de emisión de listas de certificados revocados

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

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

Los terceros usuarios, 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 4.4.11. 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.

4.4.11. 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 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 ".crl". Las delta CRL se identificarán con el mismo nombre de la CRL asociada, con el agregado del signo "+" y un número, indicando la secuencia.

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

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 https://pki.jgm.gov.ar/app

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.

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

Se aplica lo establecido en el apartado 4.4.12 de la Política de Certificación.
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 https://pki.jgm.gov.ar/app
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.

4.4.13. Otras formas disponibles para la divulgación de la revocación

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

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

No aplicable

4.4.15. Requisitos específicos para casos de compromiso de claves

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 4.4.3. 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 está 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.

El Certificador operará en consecuencia a lo establecido en la Política 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 procede a actualizar la CRL y la delta CRL correspondiente y a su publicación de acuerdo a lo establecido en el punto 4.4.4.

4.5. Procedimientos de Auditoría de Seguridad

El Certificador mantiene registros de auditoría de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros y conservándolos por al menos DIEZ (10) años.
Asimismo, atendiendo a lo expresado en el punto 2.7 Auditoría, se mantendrán registros no informatizados de toda aquella información generada en formato de papel.

Estos registros se encuentran disponibles tanto para la auditoria interna del organismo del que depende la ONTI, como de la Autoridad de Aplicación y de otros organismos o entidades que tengan competencias al respecto.

Los principales procedimientos implementados a fin de respaldar la realización de las auditorías sobre la AC-ONTI son los siguientes:

a) Registro de logs de auditoría
   Procesamiento: semanal
   Archivo: semanal
   Período de conservación: DIEZ (10) años
   Métodos de protección contra borrado o modificación: implementados a través de mecanismos de hash.
   Resguardo: se conservan dos copias en lugar físico seguro
b) Notificación de eventos significativos: todo el personal del Certificador es responsable cumplir un procedimiento de notificación de eventos que puedan comprometer la seguridad de los sistemas.
c) Informes de vulnerabilidad

Los Registros de logs de auditoría son generados por el Responsable de Auditoria según rol definido en el manual de Roles y Funciones. Se conservan bajo llave bajo la custodia del Responsable de Seguridad Informática. Este posee en su poder un juego de llaves, junto al Administrador de la Aplicación. Una tercer copia de la misma se encuentra en poder del Responsable del Certificador. Los archivos de logs de auditoría solo pueden ser visualizados por el Responsable de Auditoria.

Tanto los logs de auditoria como lo informes de vulnerabilidades y las constancias de notificación de eventos de seguridad se mantienen a disposición de los organismos autorizados a efectuar auditorías sobre el Certificador indicados en el apartado 2.7. El procedimiento para su generación y mantenimiento se encuentra especificado en el Manual de Procedimientos de Seguridad.

4.6. Archivo de registros de eventos

El Certificador mantiene un sistema de registro de eventos sobre cada una de las siguientes actividades. Para cada evento se registrará:

- Fecha y hora de ocurrencia
- Número de serie o secuencia
- Tipo de evento

- Fuente del registro
- Identificación de la entidad que efectuó el registro

:

Administración del ciclo de vida de las claves criptográficas	a) Generación y almacenamiento de las claves criptográficas del Certificador b) Resguardo de las claves criptográficas del Certificador c) Recuperación de las claves critpográficas del Certificador d) Utilización de las claves criptográficas del Certificador e) Archivo de las claves criptográficas del Certificador f) Retiro del servicio de datos relacionado con las claves criptográficas g) Destrucción de las claves criptográficas h) Identificación de la entidad que autoriza una operación de administración de claves critpográficas i) Identificación de la entidad que administra los datos relativos a las claves criptográficas j) Compromiso de la clave privada
Administración del ciclo de vida de los certificados	a) Recepción de solicitudes de certificados b) Transferencia de claves públicas para a emisión del certificados c) Cambios en los datos de la solicitud del certificado d) Generación de certificados

	e) Distribución de la clave pública del certificado f) Solicitud de revocación del certificado g) Generación y emisión de CRL h) Acciones tomadas en relación con la expiración de un certificado
Administración del ciclo de vida de los dispositivos criptográficos	a) Recepción del dispositivo b) Ingreso o retiro del dispositivo del lugar de almacenamiento c) Instalación del dispositivo d) Uso del dispositivo e) Desinstalación del dispositivo f) Envío de un dispositivo para servicio técnico o reparación g) Retiro, baja o borrado de información del dispositivo
Información relacionada con la solicitud de certificados	a) Tipos de documentos de identificación presentados por el solicitante. b) Otra información de identificación, en caso de ser aplicable c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación d) Identificación de la entidad que recibe y acepta la solicitud e) Método utilizado para validar los documentos de identificación f) Identificación de la Autoridad de Registro, de ser posible
Eventos de seguridad	a) Archivos sensibles de seguridad o registros leídos o escritos incluyendo el registro diario de eventos b) Borrado de datos sensibles de seguridad c) Cambios en los perfiles de seguridad d) Registros de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos e) Caídas del sistema, fallas en el hardware y

	software u otras anomalías f) Acciones desarrolladas por los operadores y administradores del sistemas y responsables de seguridad g) Cambios en la relación entre el Certificador, la AC ONTI y las AR y el personal relacionado con el proceso de certificación h) Decisiones de no utilizar procesos o procedimientos de cifrado y/o autenticación i) Accesos al sistema de la AC ONTI o a cualquiera de sus componentes

Los registros de eventos citados anteriormente no se almacenan en texto plano. Respecto a los relojes de los servidores involucrados en los servicios de certificación están sincronizados con un desvío menor a un segundo para permitir un correcto registro de eventos y utilizan Hora Universal Coordinada (UTC). Se encuentran configurados según el horario oficial de la Ciudad Autónoma de Buenos Aires. Toda la información respecto a horarios se expresa en formato yyyy/mm/dd hh:mm:ss huso-horario.

Todos los archivos que contienen registros de eventos se conservan en un espacio físico acondicionado dentro del ámbito de la ONTI por un plazo mínimo de DIEZ (10) años. Aquellos con antigüedad mayor a un año pueden trasladarse a un archivo secundario en un lugar físico protegido, manteniendo las mismas medidas de seguridad.

4.7. Cambio de clave

El cambio de claves del Certificador antes del vencimiento de su período de validez implica la emisión de un nuevo certificado siguiendo los siguientes procedimientos:

El par de claves del Certificador ha sido generado con motivo del licenciamiento de la Política de Certificación para Personas Físicas de Entes Públicos, Estatales o no Estatales, y Personas Físicas que realicen trámites con el Estado y tendrán una vigencia de DIEZ (10) años. Por su parte la licencia tiene una vigencia de CINCO (5) años.

En todos los casos este cambio de clave implica la emisión de un nuevo certificado por parte de la AC Raíz de la República Argentina (ACR RA). Si la clave privada del Certificador estuviese comprometida, la Autoridad de Aplicación revocará su certificado y esa clave ya no podrá ser usada para firmar digitalmente.

El Certificador iniciará ante la Autoridad de Aplicación el proceso de renovación de su licencia con una antelación no menor a DOS (2) años de su vencimiento y procederá a la generación de un nuevo par de claves. Una vez concedida la renovación de la licencia, la nueva clave pública será distribuida en un certificado firmado por la ACR RA. El certificado digital renovado será publicado en el Repositorio del Certificador, manteniéndose los mismos servicios y accesos prestados.

4.8. Plan de Contingencia y recuperación ante desastres

El Certificador ha implementado un plan de contingencia que garantiza el mantenimiento de sus servicios mínimos (procesos de revocación, de emisión de la CRL y de consulta de CRL actualizadas y servicio de OSCP) ante hechos que comprometan la continuidad de sus operaciones. Los procesos y procedimientos para el plan de contingencia y recuperación de desastres se encuentran definidos en el documento Plan de Contingencia.

Declarada la contingencia, se integrará un Comité de Contingencia, que tendrá la responsabilidad de dirigir las operaciones de recuperación y restauración del procesamiento, de acuerdo a lo establecido en el Plan de Contingencia.

El Certificador declarará la emergencia ante los siguientes eventos, en la medida que impidan el desarrollo de sus operaciones:

- Revocación de su certificado
- Compromiso o sospecha de compromiso de su clave privada
- Destrucción o falla masiva del hardware o software para la administración del ciclo de vida de los certificados
- Destrucción o falla masiva de las fuentes de energía
- Siniestro que afecte a la estructura del edificio
- Fallas en los sistemas de comunicaciones

- Fallas en los suministros, como por ejemplo, aire acondicionado o líneas de energía eléctrica estabilizada, por períodos extensos
- Otros eventos de similar impacto en la operatoria del Certificador

Ante la emergencia, el Responsable de Contingencia es el encargado de administrar el cumplimiento del Plan.
Se prevé la realización de pruebas y simulaciones del Plan con una periodicidad de UN (1) año o cuando los cambios realizados en los aplicativos al Hardware, Software de Base y/o Software Aplicativo lo ameriten. Las pruebas del plan tienen por finalidad brindar los elementos necesarios para minimizar el tiempo de recuperación ante interrupciones no planificadas y contar con información real respecto a los procesos de recuperación de datos.

4.9. Plan de Cese de Actividades

La estrategia prevista para el caso de cese de actividades, así como los procedimientos a seguir desde la declaración de cese hasta la inhabilitación lógica y física de sus instalaciones se encuentran establecidas en un documento específico denominado Plan de Cese de Actividades.

El Certificador cesará en su calidad de licenciado de acuerdo con lo estipulado en el artículo 22 de la Ley N° 25.506 por:

a) Decisión unilateral comunicada a la Autoridad de Aplicación

b) Cancelación de su licencia dispuesta por la Autoridad de Aplicación, según Art. 44 de la Ley 25.506.

c) Disolución del organismo o de la unidad organizativa que detenta las funciones de Certificador, en cuyo caso las funciones propias de este último serán asignadas a otro organismo

Declarado el cese, toda información del Certificador, cualquiera sea el soporte utilizado, será resguardada en el Archivo constituido a tal efecto, por un plazo de DIEZ (10) años, incluyendo toda la documentación en poder de las AR.

5. CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

La descripción detallada de los procedimientos referidos a los controles de seguridad física, funcional y de personal se desarrolla en un documento específico denominado Manual de Procedimientos de Seguridad.

5.1. Controles de seguridad física

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

Los servidores utilizados en el proceso de administración del ciclo de vida de los certificados se encuentran aislados en un recinto exclusivo, dentro de un área de máxima seguridad de la ONTI.

Se desarrollan controles de seguridad física que protegen las instalaciones y que comprenden:

- Monitoreo ambiental de temperatura, humedad, ruido, flujo de aire, polvo, polución, etc.
- Prevención contra agentes naturales como agua, vapor, calor, fuego, gases, polvo, etc.
- Estructura sólida de bóveda
- Prevención contra explosiones y derrumbes
- Prevención temprana contra incendios
- Sistemas de extinción de fuego
- Sistemas de refrigeración y control de humedad
- Sistemas de alimentación eléctrica redundante
- Sistema de suministro de energía ininterrumpida
- Sistema de generación de energía alternativa
- Sistemas de conectividad redundantes
- Control de acceso con identificación biométrica
- Cámara para monitoreo completo de acceso y áreas críticas.

El acceso al recinto de firma digital está limitado al personal expresamente autorizado por el Responsable del Certificador y se encuentra limitado aquellos asignados a tareas de mantenimiento y administración.

El almacenamiento de los datos de activación de la clave privada de la AC ONTI se realiza en el recinto de firma digital, cumpliendo con los niveles de seguridad establecidos en la normativa vigente. Las copias de respaldo de sistemas y datos de la AC se almacenan debidamente rotuladas en un cofre de seguridad y bajo los niveles de seguridad y autorización, dentro del Mencionado recinto.

De igual forma se mantienen copias de respaldo de sistemas y datos en una sede alternativa, con similares niveles de seguridad.

Los controles de Seguridad Fìsica de las AR se encuentran contempladas en el documento "Procedimiento Control Acceso a Instalaciones Exclusivas", el cual establece que la instalación de la AR debe contar con un mínimo de DOS (2) niveles de seguridad. El primer nivel se establece a través de un control que llevará el registro de ingresos y egresos del edificio y el nivel 2, es un registro de ingresos al ambiente de operaciones de la AR.

5.2. Controles Funcionales

El personal de la AC ONTI que desempeñe cada uno de los roles definidos realizará los controles funcionales, según las responsabilidades que le fueran asignadas, de acuerdo a lo establecido en la Política de Certificación, en el presente Manual y en el documento "Roles y Funciones".
La asignación de roles es efectuada por Disposición del Responsable del Certificador, contemplando los siguientes criterios:

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

Los controles a realizar alcanzarán entre otros, las siguientes áreas:

a) Definición y asignación de roles confiables
b) Separación de funciones
c) Número de personas requeridas por función (titular y sustituto)
d) Identificación y autenticación para cada rol
e) Conocimiento del desarrollo de las tareas asignadas en cada rol

El personal designado en las funciones mencionadas es considerado confiable y sometido a los procesos de investigación establecidos en el apartado siguiente. Las designaciones son notificadas por escrito a cada uno de los interesados, quienes dejan constancia escrita de su aceptación

5.3. Controles de Seguridad del Personal

El Certificador sigue una política de administración de personal que provee razonable seguridad acerca de la confiabilidad y competencia del personal para el adecuado cumplimiento de sus funciones. Estas acciones de control se coordinarán con la Unidad de Recursos Humanos de la Jefatura de Gabinete de Ministros.

Se establecen procedimientos de control sobre los siguientes aspectos:

a) Antecedentes laborales, calificaciones, experiencia e idoneidad del personal de acuerdo a las funciones que desempeña en la operatoria del Certificador: todo el personal involucrado es sometido a adecuados procesos de investigación que permitan demostrar su confiabilidad y competencia para las funciones a cumplir. A tal fin se evaluan los antecedentes laborales, calificaciones profesionales, experiencia e idoneidad para las funciones a desempeñar. En caso de las AR delegadas en otros entes públicos, los responsables de cada AR deberán efectuar las evaluaciones mencionadas.. Esta investigación es obligatoria como paso previo al inicio de la relación laboral.

b) Entrenamiento y capacitación inicial: se realiza un proceso de capacitación inicial a todo el personal incorporado. Este comprende cursos de entrenamiento relacionados a la operatoria específica de cada rol incluyendo los siguientes contenidos:

- Política de Certificación
- Política y procedimientos de Seguridad
- Procedimientos operativos específicos relacionados con los distintos roles
- Planes de contingencia

c) Frecuencia de procesos de actualización técnica: se realizan procesos de actualización técnica para todo el personal incorporado como mínimo una vez al año, o bien cuando los cambios en la tecnología, en las normas legales aplicables o en las políticas y procedimientos implementados lo hagan necesario.

d) Sanciones a aplicar por acciones no autorizadas: se aplicarán las sanciones administrativas establecidas en el régimen jurídico de la función pública.

e) Requisitos para contratación de personal: se realizan las evaluaciones indicadas en el apartado a) y los entrenamientos mencionados en el apartado b)

Documentación y materiales provistos al personal: todo el personal del Certificador tiene acceso a toda la documentación técnica pública que sea emitida y aprobada, y a toda documentación de carácter confidencial cuyo conocimiento fuera necesario para el cumplimiento de sus roles específicos. Asimismo, se le hace entrega de todo material adicional que fuera necesario para el cumplimiento de sus funciones (por ejemplo, dispositivos criptográficos, llaves, tarjetas de acceso, etc.) como paso previo al inicio de su relación laboral. El personal mencionado firma un acuse de recibo por el material entregado y un compromiso de confidencialidad en los casos necesarios.

5.3.1. Procedimiento de entrega y recepción de elementos sensibles

La entrega de dispositivos y demás credenciales de acceso a cualquier sistema, dato o recurso de la AC ONTI o de sus AR se realizará a partir de una autorización expresa del Responsable del Certificador, donde conste:

- Lugar y Fecha
- Datos personales del receptor (apellido y nombre, cargo o rol dentro de la AC ONTI, DNI, dirección de correo electrónico, dirección postal y número telefónico)
- Datos del elemento sensible (tipo, marca, número de serie, etc.)
- Motivo de la entrega

- Período por el cual se hace la entrega
- Firma del responsable del Certificador
- Constancia de la recepción indicando fecha, firma y aclaración.

Una copia de esta constancia quedará en poder del Certificador y una segunda, en poder del receptor.

En las oficinas de la AC ONTI se llevará un registro actualizado de todos los dispositivos entregados y devueltos.

En caso de robo o extravío, el responsable al que se le ha asignado el elemento sensible deberá notificar inmediatamente y por escrito de tal circunstancia al Responsable del Certificador, a fin de que se adopten las medidas necesarias para evitar cualquier compromiso de los recursos de la AC ONTI. A partir de dicha notificación se procederá al reintegro del dispositivo debiendo cumplirse el procedimiento antes señalado.

En caso de pérdida de un dispositivo criptográfico, el responsable de tal elemento podrá ser sujeto del cargo de reposición, según lo determine el Responsable del Certificador.

Una vez recibido el dispositivo y si fuera el caso, el responsable deberá presentarse ante el Área de Soporte Técnico para su inicialización.

6. CONTROLES DE SEGURIDAD TÉCNICA

El Certificador define en el Manual de Procedimientos de Seguridad:

a) Las medidas de seguridad a fin de proteger sus claves criptográficas pública y privada y todos los demás datos críticos necesarios para operar con módulos criptográficos (números pin, passwords, claves manuales compartidas o no por el personal, etc.).
b) Otros controles de seguridad que garantizan las funciones de generación de claves, identificación de usuarios, emisión y renovación de certificados, auditoría y archivos.

6.1. Generación e instalación del par de claves criptográficas

6.1.1. Generación del par de claves criptográficas

6.1.1.1. Generación del par de claves del Certificador

El Certificador genera el par de claves criptográficas en un ambiente seguro por personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3.

El Certificador genera sus claves mediante el algoritmo RSA con un tamaño de 4096 bits.

6.1.1.2. Generación del par de claves de la Autoridad de Registro

La clave privada de la AR es generada y almacenada por su responsable, utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2.

La Autoridad de Registro genera sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

El procedimiento para general el par de claves de la primera AR se encuentra descripto en el documento " Implementación Aplicativo de Gestión PKI"

6.1.1.3. Generación del par de claves del suscriptor:

Las claves privadas de los suscriptores son generadas y almacenadas por ellos, sobre dispositivos criptográficos homologados FIPS 140-2 Nivel 2 en el caso de certificados de nivel de seguridad alto.

Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

El par de claves del suscriptor de un certificado es generado de manera tal que su clave privada se encuentre bajo su exclusivo y permanente conocimiento y control, absteniéndose el Certificador de acceder o tomar conocimiento por cualquier otro medio de su clave privada. El suscriptor es considerado titular del par de claves, como tal, está obligado a:

- Generar su par de claves en un sistema confiable.

- Establecer los controles de acceso que aseguren que él es el único capaz de acceder a su clave privada.
- Generar su par de claves de manera segura siguiendo el procedimiento establecido por este manual tal como se describe en el apartado 4.1.
- No revelar su clave privada a terceros bajo ninguna circunstancia.

6.1.2. Entrega de la clave privada al suscriptor

Las características del procedimiento de generación de la clave privada del suscriptor garantizan que esta es generada por el mismo y en ningún momento es accedida o trasmitida por cualquier otro medio al Certificador.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública del solicitante es entregada al Certificador durante el proceso de solicitud de certificado utilizando técnicas de “prueba de posesión” de la clave privada asociada tal como se describe en el apartado 3.1.7.

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

La clave pública del solicitante es generada y transferida al Certificador durante el proceso de solicitud de certificado de manera tal que asegure que:

a) No puede ser cambiada durante la transferencia.
b) El remitente posee la clave privada que corresponde a la clave pública transferida.

La solicitud de un certificado se emite en formato PKCS#10, o bien en el formato que lo reemplace en el futuro.

6.1.4. Disponibilidad de la clave pública del Certificador

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

El proceso de verificación de la validez de los certificados de los suscriptores se realiza automáticamente a través del siguiente procedimiento:

1. A través de la verificación de la cadena de confianza del certificado del suscriptor, proceso que se ejecuta de la siguiente manera:

    a. Contra el certificado de la AC ONTI, es decir aquella que emitió el certificado del suscriptor
    b. Contra el certificado de la ACR RA, la cual emitió el certificado de la AC ONTI

2. Realizando la verificación de la vigencia y el estado de los certificados, mediante la consulta a las CRL emitidas por las AC ONTI y la ACR RA.

6.1.5. Tamaño de claves

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

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

El algoritmo de firma en ambos casos es SHA-1 con RSA.

6.1.6. Generación de parámetros de claves asimétricas

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

6.1.7. Verificación de calidad de los parámetros

La verificación de calidad de los parámetros es realizada por la aplicación de la AC ONTI. Esta verificación abarca al menos la correcta longitud de claves y los distintos parámetros de los certificados.

6.1.8. Generación de claves por hardware o software

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

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

b) Para la generación de las claves criptográficas utilizadas para la firma de información de estado de certificados: dispositivos que cumplen FIPS 140-2 nivel 3

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

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

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

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

Las claves contenidas en los certificados de usuarios emitidos por AC ONTI tienen como propósito su utilización para firmar digitalmente.
Los valores a utilizar en los certificados son “Firma Digital y No Repudio”.

6.2. Protección de la clave privada

El Certificador establece los siguientes procedimientos de control sobre su clave privada:

a) Se establecen responsables de su control.
b) Se establece un procedimiento de custodia de la clave privada.
c) Se establece un procedimiento de activación de la clave privada.
d) Se establece un procedimiento de destrucción de la clave privada.

Idénticos procedimientos de control se establecen sobre la clave privada de las AR.

En el ANEXO "Procedimiento Retiro de Bienes y su Resguardo" se establecen los procedimientos de resguardo de Clave Privada.

6.2.1. Estándares para módulos criptográficos

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

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

b) Para la generación de las claves criptográficas de las Autoridades de Registro se utilizarán dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 2

c) Para certificados de suscriptores de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en dispositivos criptográficos especiales que cumplen con las características definidas en FIPS 140-2 para el nivel 2

6.2.2. Control "M de N" de clave privada

Las claves privadas de la AC ONTI son activadas exclusivamente en el recinto donde opera o en el sitio de contingencia, dentro del nivel de seguridad asignado a las operaciones críticas del Certificador.

En el ANEXO “Procedimiento de Inicialización del HSM” se establecen los procedimientos de activación de la clave privada del Certificador

El procedimiento de utilización de las claves privadas del Certificador se efectúa de manera segura, de manera tal que siempre es necesaria la presencia de DOS (2) personas distintas para su activación de un universo de CINCO (5) personas posibles.

6.2.3. Recuperación de clave privada

Ante una situación que requiera recuperar la clave privada de la AC ONTI el Certificador cuenta con procedimientos y elementos para su recuperación.

Esta recuperación sólo es realizada por personal autorizado, sobre dispositivos criptográficos seguros y exclusivamente en los niveles de seguridad donde se encuentran las instalaciones críticas de la AC ONTI.

En el ANEXO “Procedimiento Retiro de Bienes y su Resguardo” se establecen los procedimientos de recuperación de la clave privada del Certificador

No se implementan mecanismos de resguardo y recuperación de la clave privada para las Autoridades de Registro y Suscriptores.

6.2.4. Copia de seguridad de clave privada

El Certificador genera una copia de seguridad de la clave privada garantizando su integridad y confidencialidad a través del procedimiento establecido en el ANEXO “Procedimiento Retiro de Bienes y su Resguardo”

En el se establecen los procedimientos de copia de seguridad de la clave privada del Certificador.

6.2.5. Archivo de clave privada

La clave privada de la AC-ONTI es archivada garantizando su integridad y confidencialidad.

En el ANEXO "Procedimiento Retiro de Bienes y su Resguardo" se establecen los procedimientos de archivo de la clave privada del Certificador

6.2.6. Inserción de claves privadas en módulos criptográficos

El par de claves criptográficas de la AC ONTI se genera y almacena en dispositivos criptográficos siguiendo el siguiente procedimiento:

a) Las copias de resguardo también están soportados en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

b) El par de claves criptográficas del personal de las AR y de los suscriptores de certificados de nivel de seguridad Alto se almacena en el mismo dispositivo criptográfico con las características definidas en FIPS 140-2 para el nivel 2 donde se genera y no permite su exportación.

6.2.7. Método de activación de claves privadas

La clave privada de la AC-ONTI se activa previa autenticación de los responsables de su control a través de un procedimiento seguro.

En el ANEXO "Procedimiento de Inicialización del HSM" se establecen los procedimientos de activación de la clave privada del Certificador

6.2.8. Método de desactivación de claves privadas

La clave privada de la AC-ONTI se desactiva previa autenticación de los responsables de su control a través de un procedimiento seguro.

En el ANEXO se establecen los procedimientos de desactivación de la clave privada del Certificador

6.2.9. Método de destrucción de claves privadas

En caso de cese de actividades del Certificador o de compromiso de la clave privada de la AC ONTI, los dispositivos criptográficos serán reformateados e inicializados nuevamente por personal autorizado.

En el ANEXO se establecen los procedimientos de destrucción de la clave privada del Certificador

6.3. Otros aspectos de administración de claves

6.3.1. Archivo permanente de clave pública

Todos los certificados emitidos por la AC ONTI, incluyendo su propio certificado, se encuentran disponibles en un repositorio almacenados en dispositivos ópticos y/o magnéticos, disponibles en el siguiente sitio web https://pki.jgm.gov.ar/app .
Los certificados se almacenan en formato estándar bajo codificación internacional DER, en una estructura que contiene los datos de identificación del Certificador o de los suscriptores, según sea el caso, y la clave pública correspondiente, todo lo cual se encuentra firmado digitalmente de manera de garantizar la integridad de su contenido.

En el ANEXO “Implementación de Backup” establece el Hardware, el Software y los procedimientos que actúan en el back up de la clave pública del Certificador

6.3.2. Período de uso de clave pública y privada

La clave privada asociada con el certificado digital de la AC ONTI, tiene una validez de DIEZ (10) años, y de no mediar una revocación anticipada, se lo utilizará para firmar certificados de suscriptores.

Las claves privadas de los suscriptores, asociadas a los certificados emitidos por la AC ONTI se utilizarán únicamente durante su período de validez, que será de DOS (2) años. El período de uso de la clave privada y su certificado asociado puede ser extendido por medio de la renovación del certificado de acuerdo con lo establecido en el apartado 4.1.2.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación del dispositivo criptográfico de la AC ONTI tienen un control "M de N" en base a DOS (2) funcionarios testigos que deben estar presentes de un total de CINCO (5) funcionarios posibles.

Los suscriptores están obligados a establecer los mecanismos que aseguren la exclusividad de acceso a su clave privada de acuerdo con los niveles de seguridad establecidos en el apartado 1.3.4.

6.4.2. Protección de los datos de activación

Los suscriptores son responsables de la custodia de sus dispositivos criptográficos y de la confidencialidad de la contraseña de protección de su clave privada y de acceso al dispositivo criptográfico, si fuera el caso. La AC ONTI no establece mecanismos de respaldo de dichas contraseñas.

6.4.3. Otros aspectos referidos a los datos de activación

Los suscriptores son responsables de seleccionar contraseñas fuertes para la activación de sus claves privadas.

A tal efecto, se formulan las siguientes sugerencias:

- Utilizar al menos 8 caracteres, que incluyan letras mayúsculas, minúsculas y números
- No elegir contraseñas fácilmente deducibles como por ejemplo, nombres de familiares, direcciones, números telefónicos, etc.
- En caso de que se utilice un dispositivo criptográfico con doble autenticación, la contraseña de accesos no debe coincidir con la de activación de la clave privada.

6.5. Controles de seguridad informática

6.5.1. Requisitos Técnicos específicos

El Certificador establece los siguientes controles de seguridad referidos a su equipamiento:

a) Control de acceso a los servicios y roles afectados al proceso de certificación
   Controles de seguridad físicos y lógicos para proteger el acceso a las instalaciones del Certificador y el acceso lógico a los sistemas involucrados en su gestión.
b) Separación de funciones para los roles de certificación
   Ninguno de los intervinientes posee más de un rol o función
c) Identificación y autenticación de los roles de certificación
   Se utiliza una autenticación robusta (2 factores como mínimo) para todos los roles afectados al proceso de certificación
d) Utilización de criptografía para las sesiones de comunicación y bases de datos
   Las comunicaciones entre los componentes críticos de la AC ONTI se realizan en forma cifrada.
e) Archivo de datos históricos y de auditoria del Certificador y usuarios
   Se almacenan y archivan los datos históricos y de auditoría del certificador y de los trámites de los suscriptores según lo establecido en el apartado 4.6
f) Auditoría de eventos de seguridad
   Todos los eventos de seguridad ocurridos durante el proceso de certificación se registran en archivos de logs.
g) Auto-testing de seguridad relativa a servicios de certificación

De forma periódica se realizan pruebas de seguridad de los servicios involucrados en la certificación

h) Caminos confiables para identificación de roles de certificación
i) Mecanismos de recuperación para claves y sistema de certificación.

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

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

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

6.5.2. Calificaciones de seguridad computacional

Todo el equipamiento afectado a las tareas sensibles de la AC ONTI se encuentra ubicado en la sala de acceso exclusivo, bajo los niveles de acceso requeridos por la normativa.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

El Certificador posee separación de ambientes de desarrollo, prueba y producción.

6.6.2. Controles de administración de seguridad

Se establecen los siguientes controles respecto a la integridad del sistema de archivos del Certificador que permiten controlar la alteración y verificar si es un cambio válido.

6.6.3. Calificaciones de seguridad del ciclo de vida

Se aplica lo establecido en la Política de Certificación.

6.7. Controles de seguridad de red

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

6.8. Controles de ingeniería de módulos criptográficos

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

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

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

7. PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

7.1. Perfil del certificado

Resulta de aplicación lo establecido en el apartado 7.1. de la Política de Certificación.

7.2. Perfil de la lista de certificados revocados

Resulta de aplicación lo establecido en el apartado 7.2. de la Política de Certificación.

8. ADMINISTRACIÓN DE ESPECIFICACIONES

8.1. Procedimientos de cambio de especificaciones

El Certificador cuenta con procedimientos de administración de cambios para efectuar modificaciones a su Política de Certificación, a su Manual de Procedimientos y a los demás documentos exigidos por la DA 6/2007. Toda modificación será sometida a la aprobación del Ente Licenciante.

8.2. Procedimientos de publicación y notificación

El Certificador, una vez notificada de la aprobación de las modificaciones a los documentos indicados en el apartado 8.1 por parte de la Autoridad de Aplicación, y siempre que se trate de documentos de carácter público, publicará en su sitio web las modificaciones aprobadas, indicando, en cada caso, el texto reemplazado. Asimismo, se publicará el texto de las nuevas versiones de los mencionados documentos.

Los suscriptores que posean certificados vigentes a la fecha de aplicación del cambio serán notificados por correo electrónico en las direcciones declaradas en los correspondientes certificados.

Los documentos vigentes de carácter público y sus versiones anteriores se encuentran disponibles en su sitio web https://pki.jgm.gov.ar/app

8.3. Procedimientos de aprobación

Toda documentación emitida por el certificador exigida por la DA 6/2007, así como cualquier modificación a efectuar a la misma o cualquier cambio en los datos relativos a su licencia, serán sometidos a aprobación por parte del Ente Licenciante.

Historia de las revisiones:

Versión y Modificación	Fecha de emisión	Descripción	Motivo del Cambio
Versión 3.6	23/09/2010		

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