Jefatura de Gabinete de Ministros

Subsecretaría de la Gestión Pública

ANEXO

Política de certificación de la Autoridad Certificante Raíz de la República Argentina

1- INTRODUCCION

1.1.- Descripción general

En el ámbito de la Subsecretaría de la Gestión Pública, funciona la Infraestructura de Firma Digital de la República Argentina (en adelante IFDRA) cuya Autoridad Certificante Raíz (en adelante ACR RA) emite certificados digitales a los certificadores que obtengan licencia para sus políticas de certificación, una vez verificado el cumplimiento de los requisitos establecidos por la ley de firma digital y las normas complementarias.

La relación del ente licenciante con los certificadores de firma digital, que soliciten licencia para sus políticas de certificación, se rigen por la Ley Nº 25.506, su Decreto Reglamentario Nº 2628/02 y los Decretos Nº 1028/03, 409/05, 724/06, la Decisión Administrativa Nº 06/2007 y sus normas complementarias.

Esta política de certificación indica la aplicabilidad de los certificados emitidos por la ACR RA de acuerdo con lo establecido por el ente licenciante de la IFDRA.

Esta política de certificación se complementa con los siguientes documentos:

a) Los procedimientos de certificación,

b) El acuerdo con suscriptores de certificados de la ACR RA (o sea, los certificadores licenciados),

c) Los términos y condiciones con terceros usuarios de certificados de la ACR RA,

d) La política de privacidad del ente licenciante y de su ACR RA.

1.2. - Identificación

Título del documento:

Política de certificación de la Autoridad Certificante Raíz de la República Argentina:

Versión del documento:	V1.0
Fecha del documento:	12/11/2007
OID de la política de certificación:	2.16.32.1.1.0
Sitio de publicación	http://www.sgp.gov.ar/entelicenciante/

La Oficina Nacional de Tecnologías de Información ("ONTI") como Autoridad de Registro de Identificadores de Objetos ("OID") de la República Argentina es la responsable de la asignación de OIDs a las políticas de certificación licenciadas.

1.3 - Participantes y Aplicabilidad

Los participantes de esta política de certificación son:

a) La ACR RA

b) El Ente Licenciante

c) Los suscriptores de certificados, es decir los Certificadores Licenciados

1.3.1. - Certificador

Para esta política de certificación, la función de certificador la cumplen el ente licenciante,

función ejercida por la Subsecretaría de la Gestión Pública en virtud del Decreto Nº 409/2005, y su Autoridad Certificante Raíz, de acuerdo a lo dispuesto en el inciso 3 del artículo 13 de la DA 06/2007.

1.3.1.1. - Ente licenciante

a) Publica esta política de certificación, el acuerdo con suscriptores de certificados de la ACR RA, los términos y condiciones con terceros usuarios de certificados de la ACR RA y su política de privacidad;

b) Publica los certificados digitales de las Autoridades Certificantes de los certificadores licenciados como así también los certificados digitales de la ACR RA;

c) Publica el estado de los certificados emitidos y provistos por la ACR RA, a través de la Lista de Certificados Revocados (o "CRL" Certificate Revocation List).

1.3.1.2. - Autoridad Certificante Raíz (ACR RA)

a) Emite, renueva y revoca su propio certificado digital;

b) Emite, renueva y revoca los certificados de las Autoridades Certificantes de los certificadores licenciados;

c) Emite su Lista de Certificados Revocados (o "CRL" Certificate Revocation List)

1.3.2 - Autoridad de Registro

Las funciones de Autoridad de Registro son cumplidas por el ente licenciante.

Tendrá sede en:

Subsecretaría de la Gestión Pública

e-mail: licenciamiento@sgp.gov.ar

http://www.sgp.gov.ar/entelicenciante/

1.3.3. –Suscriptores de certificados

Los certificadores licenciados son los suscriptores de los certificados digitales emitidos a favor de sus Autoridades Certificantes que soportan las políticas de certificación licenciadas, otorgadas por el ente licenciante.

1.3.4. - Aplicabilidad

Los certificados emitidos por la ACR RA tienen como único objetivo garantizar la identidad de las Autoridades Certificantes de los certificadores licenciados.

La ACR RA utiliza su clave privada, mantenida en dispositivos criptográficos seguros, para firmar los certificados de las Autoridades Certificantes de los certificadores licenciados, posibilitando que estos últimos emitan certificados digitales a sus suscriptores, en el marco de la Ley Nº 25.506 de firma digital.

1.4 - Contactos

Esta política de certificación es administrada por la Subsecretaría de la Gestión Pública.

Por consultas y sugerencias acerca de este documento se puede obtener información personalmente o por correo en:

Subsecretaría de la Gestión Pública

Jefatura de Gabinete de Ministros

Subsecretaría de la Gestión Pública

e-mail: licenciamiento@sgp.gov.ar

http://www.sgp.gov.ar/entelicenciante/

2. - ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACIÓN

2.1. - Obligaciones

2.1.1. - Obligaciones del certificador

2.1.1.1. - Obligaciones del ente licenciante

Constituyen obligaciones del ente licenciante en relación con la presente política:

a) La generación y administración del par de claves criptográficas de la ACR RA;

b) La entrega de los certificados de Autoridades Certificantes de certificadores licenciados;

c) La renovación de la licencia de las políticas de certificación de certificadores licenciados;

d) La publicación en el Boletín Oficial de:

   1. La Resolución que ordena el otorgamiento, denegación, renovación y/o revocación de licencia de política de certificación de certificador, y

   2. El certificado digital de clave pública correspondiente a esta política de certificación, emitido por la ACR RA.

e) Adoptar las medidas de seguridad y control, previstas en esta política de certificación y en la política de seguridad, abarcando sus procesos, procedimientos y actividades;

f) Mantener los procesos, procedimientos y actividades de conformidad con la legislación

vigente y con las normas, prácticas y reglas establecidas por el ente licenciante;

g) Mantener y garantizar la integridad, confidencialidad y disponibilidad de la información tratada por el ente licenciante;

h) Mantener y probar regularmente el plan de contingencias;

i) Mantener a disposición permanente del público su política de certificación y cumplir fielmente con sus especificaciones;

j) Atender los requerimientos de firma de certificado (CSR - Certificate Signing Requests) generados por las Autoridades Certificantes operadas por los certificadores licenciados al finalizar en forma favorable el respectivo proceso de licenciamiento;

k) Atender los requerimientos de revocación de certificados solicitados por certificadores licenciados o por autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en el presente documento;

l) Autenticar a las entidades que solicitan la revocación de un certificado;

m) Disponer de un servicio de atención que permita responder las consultas de los suscriptores de certificados emitidos por certificadores licenciados y de los terceros usuarios;

n) Garantizar el acceso permanente y gratuito de los suscriptores y terceros usuarios al sitio de publicación que contiene los certificados emitidos a los certificadores licenciados y la lista de certificados revocados;

o) Notificar a los certificadores licenciados, como suscriptores de los certificados de sus

Autoridades Certificantes, acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACR RA y la emisión de un nuevo par de claves criptográficas, como así también del procedimiento a seguir en esa contingencia;

p) Registrar y mantener información de todas las acciones realizadas en el proceso de emisión de certificados.

El ente licenciante cumplirá para con los certificadores licenciados en la República Argentina, las obligaciones que el Art. 21 de la Ley Nº 25.506 asigna al certificador licenciado.

2.1.1.2. - Obligaciones de la ACR RA del Ente Licenciante

Constituyen obligaciones de la ACR RA:

a) La emisión, revocación y renovación de su propio certificado,

b) La emisión, revocación y renovación de los certificados de Autoridades Certificantes de certificadores licenciados,

c) La emisión de su Lista de Certificados Revocados (CRL).

2.1.2. - Obligaciones de la Autoridad de Registro

Las obligaciones de Autoridad de Registro son asumidas por el ente licenciante.

2.1.3. - Obligaciones de los suscriptores de los certificados

Los certificadores licenciados son personas de existencia ideal, registros públicos de contratos u organismos públicos bajo cuya responsabilidad recaerán las obligaciones citadas en este punto.

Toda la información necesaria para la identificación y autenticación del certificador contenida en una solicitud de licencia debe ser provista de forma completa y precisa al iniciar el proceso de licenciamiento.

Al aceptar un certificado emitido por la ACR RA para su Autoridad Certificante, el certificador licenciado es responsable por toda la información por él provista y contenida en ese certificado.

La Autoridad Certificante asociada al certificado emitido por la ACR RA debe operar de acuerdo con su propio manual de procedimientos de certificación (MPC) y su política de certificación (PC), implementado de acuerdo a lo establecido en la Decisión Administrativa 06/2007 y sus Anexos y aprobado por el ente licenciante.

Los certificadores licenciados asumen las siguientes obligaciones*:*

a) Cumplir con las obligaciones que le asigna el Art. 21 de la Ley Nº 25.506 y el Art. 34 del Decreto Nº 2628/02;

b) Cumplir con las obligaciones que le asigna el art. 25 de la ley 25.506, como suscriptor de certificado emitidos por la ACR RA;

c) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso;

d) Utilizar los certificados de sus Autoridades Certificantes de acuerdo con las reglas establecidas en esta política de certificación;

e) Mantener un sitio de publicación con toda la información relativa a su condición de

certificador licenciado, de modo que pueda ser accedida libremente por el público;

f) Publicar en su sitio de publicación los certificados de clave pública asociados a sus Autoridades Certificantes emitidos por la ACR RA;

g) Publicar por el término de un (1) día en el Boletín Oficial, los certificados de clave pública asociados a sus Autoridades Certificantes emitidos por la ACR RA;

h) Cumplir con las obligaciones establecidas en la presente política de certificación y otros documentos aplicables emitidos por el ente licenciante;

i) Firmar el documento "Acuerdo con suscriptores de certificados de la ACR RA", al aceptar su certificado emitido por la ACR RA.

2.1.4. - Obligaciones de terceros usuarios

Sin perjuicio de las responsabilidades que competen al ente licenciante, a la ACR RA y a cada certificador licenciado, los terceros usuarios tienen las siguientes obligaciones:

a) Tomar conocimiento de los términos definidos en el presente documento;

b) Tomar conocimiento de los términos y condiciones con los terceros usuarios de certificados de la ACR RA que se publica en el sito de publicación del ente licenciante;

c) Tomar conocimiento de las obligaciones del tercero usuario establecidas en la política de certificación de la Autoridad Certificante del certificador licenciado;

d) Verificar la validez de los certificados asociados a las Autoridades Certificantes del certificador licenciado consultando la CRL emitida por la ACR RA y publicada por el ente licenciante;

e) Verificar que el certificado de la Autoridad Certificante del certificador licenciado sea utilizado para los propósitos previstos en esta política de certificación;

f) Verificar la validez del certificado de la ACR RA.

El certificado de la ACR RA es considerado válido cuando:

i. Se encuentra dentro de su período de vigencia,

ii. No ha sido revocado, y

iii. Puede ser verificado con el uso del mismo certificado de la ACR RA.

2.1.5. - Obligaciones del servicio de repositorio

Para esta política de certificación son obligaciones del ente licenciante la publicación en los sitios desarrollados a tal fin, de la siguiente información:

a) Esta política de certificación (versión actual y anteriores);

b) El acuerdo con suscriptores de certificados de la ACR RA;

c) Los términos y condiciones con terceros usuarios de certificados de la ACR RA;

d) La política de privacidad de la ACR RA;

e) Los certificados emitidos por la ACR RA;

f) La lista de certificados revocados (CRL) por la ACR RA;

g) La lista de OIDs de políticas de certificación para las Autoridades Certificantes de los certificadores licenciados;

h) Información relevante de los informes de auditoría a que fue objeto el ente licenciante y

su ACR RA;

i) Información relevante de los informes de las auditorías realizadas por el ente licenciante a las Autoridades Certificantes de los certificadores licenciados;

j) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de los contactos del ente licenciante;

k) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos de los certificadores licenciados;

l) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos de los certificadores licenciados cuyas licencias han sido revocadas.

2.2. - Responsabilidades

El ente licenciante asume responsabilidad ante terceros por el incumplimiento de las previsiones de la Ley Nº 25.506, el Decreto Reglamentario Nº 2628/02 y demás normativa aplicable, respecto a los procedimientos que respaldan la emisión de certificados por la ACR RA, por los errores u omisiones que presenten los certificados por ella emitidos y por su falta de revocación en la forma y plazos previstos.

El ente licenciante no asume responsabilidad alguna en caso de utilización no autorizada de un certificado cuya descripción se encuentra establecida en esta política de certificación, tampoco responde por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y procedimientos de la ACR RA, deba ser objeto de verificación.

2.3. - Responsabilidad Financiera

2.3.1. - Responsabilidad financiera del ente licenciante

La responsabilidad del ente licenciante por los incumplimientos previstos en el apartado anterior no compromete en ningún caso la responsabilidad pecuniaria del Estado, de acuerdo con el Art. 31 del Decreto Nº 2628/2002, reglamentario de la Ley Nº 25.506.

2.4. - Interpretación y aplicación de las normas

2.4.1. - Legislación aplicable

La interpretación, obligatoriedad, diseño y validez de esta política de certificación se encuentran sometidos a lo establecido por la Ley Nº 25.506 y demás normas aplicables.

2.4.2. - Forma de interpretación y aplicación

En el caso de que una o más disposiciones de esta política de certificación resulten, por cualquier razón, consideradas nulas, tal nulidad no afectará a la validez de las restantes disposiciones.

Las disposiciones que surgen de la presente política de certificación son de cumplimiento obligatorio.

El Decreto Nº 409/2005 establece que la Subsecretaría de Gestión Pública actúa como Autoridad de Aplicación de la Ley Nº 25.506.

2.4.3. - Procedimientos de resolución de conflictos

Los certificadores licenciados en su calidad de suscriptores de certificados emitidos por la ACR RA y los terceros usuarios podrán interponer recurso administrativo ante la Subsecretaría de la Gestión Pública o el organismo que ésta designe a esos efectos, por conflictos referidos a la prestación del servicio por parte de la ACR RA.

Conforme lo establece el artículo 46 de la Ley Nº 25.506, en los conflictos entre la ACR RA y los certificadores licenciados correspondientes al Sector Público, suscriptores de certificados por ella emitidos, intervendrá la Justicia en lo Contencioso Administrativo Federal, una vez agotada la vía administrativa pertinente.

Si el conflicto se produjere entre la ACR RA y los certificadores licenciados pertenecientes al sector privado, suscriptores de certificados por ella emitidos, entenderá la Justicia en lo Civil y Comercial Federal.

2.5. - Aranceles

No se aplicarán aranceles específicos para la emisión y renovación de certificados bajo esta política de certificación, reservada para los certificados de las Autoridades Certificantes de los certificadores licenciados, dado que se cubre con los aranceles aplicados en el proceso de licenciamiento de políticas de certificación y en el proceso de renovación de licencias, los que están determinados en la Decisión Administrativa Nº 06/2007 y, particularmente, en su Anexo VII.

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

2.6.1. - Publicación de información del certificador

El ente licenciante opera dos sitios de publicación, uno para uso exclusivo de la publicación de la Lista de Certificados Revocados (CRL) y otro para la publicación de la información del ente licenciante.

La publicación de la Lista de Certificados Revocados se encuentra disponible en los sitios http://acraiz.cdp1.gov.ar/ca.crl y http://acraiz.cdp2.gov.ar/ca.crl.

El sitio de publicación del ente licenciante se encuentra disponible en http://www.sgp.gov.ar/entelicenciante/, donde se puede hallar tal información como:

a) El certificado vigente de la ACR RA y los certificados de las Autoridades Certificantes de certificadores licenciados,

b) Los datos de los contactos del ente licenciante como de los certificadores licenciados,

c) El registro de certificadores licenciados conteniendo el número de la Resolución que concede, renueva o revoca las licencias de políticas de certificación que fueron aprobadas (con el correspondiente OID asignado por el ente licenciante), así como el número de la Resolución para las solicitudes de licencia para políticas de certificación que hubieran sido rechazadas durante el proceso de licenciamiento,

d) Esta política de certificación, el acuerdo con suscriptores de certificados de la ACR RA, los términos y condiciones con terceros usuarios de certificados de la ACR RA, la política de privacidad y toda otra documentación técnica de carácter público que se emita, en sus versiones actuales y anteriores.

2.6.2. - Frecuencia de publicación

Los sitios de publicación serán actualizados inmediatamente después de que la información a incluir en ellos haya sido verificada y autorizada por el ente licenciante.

La información respecto a emisiones y revocaciones de certificados será incluida tan pronto como se hayan cumplido los procedimientos de validación de identidad de los solicitantes establecidos en esta política de certificación para cada caso en particular.

La Lista de Certificados Revocados (CRL) será actualizada y la nueva versión será publicada, cuando se produzca la revocación de un certificado o cuando por razones operativas la ACR RA emita un certificado o bien a los seis (6) meses de la última emisión de CRL, si ninguna de las dos condiciones anteriores ocurre antes.

2.6.3. - Controles de acceso a la información

El ente licenciante brinda acceso irrestricto a sus sitios de publicación para consultar a través de la Internet, documentación de carácter público, incluyendo el certificado de la ACR RA, la lista de Certificados Revocados y esta Política de Certificación. El ente licenciante establece controles para restringir la posibilidad de escritura y modificación.

2.6.4. - Repositorios de certificados y listas de revocación

Los sitios de publicación se encuentran disponibles para uso público durante veinticuatro (24) horas diarias siete (7) días a la semana, sujeto a un calendario de mantenimiento.

2.7. - Auditorías

El ente licenciante se encuentra sujeto a auditorias de la Sindicatura General de la Nación

(SIGEN). La información relevante de los informes de las auditorias es publicada en el sitio de publicación del ente licenciante.

2.8. - Confidencialidad

2.8.1. - Información confidencial

Toda información referida a los certificadores licenciados, que haya sido recibida por el ente licenciante durante el proceso de licenciamiento o renovación, es considerada confidencial y no puede hacerse pública sin el consentimiento previo de aquellos, salvo que sea requerida judicialmente por juez competente o por autoridad administrativa. La exigencia se extiende a toda otra información, referida a los certificadores licenciados, a la que el ente licenciante tenga acceso durante el ciclo de vida de los certificados emitidos.

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

La ACR RA no genera ni accede a las claves privadas de las Autoridades Certificantes de los certificadores licenciados. La generación y administración del par de claves criptográficas queda bajo exclusiva responsabilidad de los certificadores licenciados.

En los casos relativos a información personal, resulta de aplicación la Ley Nº 25.326 de protección de datos personales.

2.8.2. - Información no confidencial

No se considerada confidencial lo siguiente:

a) La información incluida en los certificados y en las listas de certificados revocados;

b) La información sobre personas físicas o jurídicas que se encuentre disponible en certificados o en directorios y sitios de publicación de acceso público.

Tampoco se considera confidencial la información incluida en los siguientes documentos emitidos por el ente licenciante:

I. Esta política de certificación;

II. El acuerdo con suscriptores de certificados de la ACR RA;

III. Los términos y condiciones con terceros usuarios de certificados de la ACR RA;

IV. La política de privacidad de la ACR RA.

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

La información referida a la revocación de un certificado no se considera confidencial y se la publica en el sitio de publicación: http://www.sgp.gov.ar/entelicenciante/.

El estado de suspensión de un certificado no es aplicable en el marco de la Ley Nº 25.506.

2.8.4. - Divulgación de información a autoridades judiciales

La información confidencial podrá ser revelada ante un requerimiento judicial emanado de juez competente en el marco de un proceso judicial.

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

La información confidencial en poder del ente licenciante podrá ser revelada ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

2.8.6. - Divulgación de información por solicitud del suscriptor

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del certificador licenciado o de cualquier otra información generada o recibida durante el ciclo de vida del certificado solo podrá efectuarse previa autorización de ese certificador. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público irrestricto.

2.8.7. - Otras circunstancias de divulgación de información

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

2.9. - Derechos de Propiedad Intelectual

La Subsecretaría de la Gestión Pública mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la documentación y aplicaciones pertenecientes al ente licenciante y a su ACR RA. Asimismo, mantiene en forma exclusiva todos los derechos de propiedad intelectual relacionados con sus nombres y claves criptográficas.

3. - IDENTIFICACION Y AUTENTICACION

3.1 - Registro inicial

De acuerdo a la normativa vigente, en el proceso de registración de un certificador interviene el ente licenciante, otorgando o denegando licencias a las políticas de certificación presentadas y asociadas a sus Autoridades Certificantes.

Con la Decisión Administrativa 06/2007 y sus Anexos publicada en el sitio de publicación del ente licenciante http://www.sgp.gov.ar/entelicenciante/, el ente licenciante pone a disposición de los certificadores las condiciones necesarias para la obtención de las licencias de políticas de certificación.

La presentación de solicitud de licencia para una política de certificación, por parte del certificador inicia el proceso de licenciamiento que culmina con el otorgamiento o denegación de licencia por parte del ente licenciante, la publicación en el Boletín Oficial de la Resolución que la otorga o deniega y la asignación de un OID (Identificador de Objeto) para aquella política de certificación licenciada.

Con el otorgamiento de licencia, el ente licenciante a través de la ACR RA, emite un certificado digital para la Autoridad Certificante vinculada a la política de certificación licenciada.

En el acto de emisión del certificado por la ACR RA, el certificador debe confirmar que la información contenida en el certificado sea correcta. Además en ese acto, el certificador firma el acuerdo con suscriptores de certificados de la ACR RA, provisto por el ente licenciante.

3.1.1. - Tipos de Nombres

Las Autoridades Certificantes vinculadas a las políticas de certificación licenciadas son subordinadas de la ACR RA y tendrán un nombre definido por el certificador de acuerdo a la

normativa vigente que será controlado por el ente licenciante para permitir su identificación unívoca en el ámbito de la IFDRA.

Cada certificado tiene un nombre distintivo único (ver punto 3.1.4) en formato X.500 en el campo "Subject" del certificado.

3.1.2. - Necesidad de nombres distintivos

Todos los nombres distintivos son semánticamente significativos dentro del ámbito de la IFDRA. Son de fácil comprensión y asociación con el certificador licenciado y la Autoridad Certificante que representa.

3.1.3.- Reglas para la interpretación de nombres

NO APLICABLE.

3.1.4. - Unicidad de Nombres

Los nombres distintivos (Distinguished Name o DN) son únicos dentro del ámbito de la IFDRA. El ente licenciante es el encargado de controlar la unicidad de los nombres distintivos.

Se podrán emitir varios certificados a favor de un mismo certificador licenciado utilizando el mismo DN cuando así se estime conveniente, ya que la utilización de un mismo DN en varios certificados no afecta la unicidad de dicho nombre dentro de la IFDRA.

3.1.5. - Procedimiento de resolución de disputas sobre nombres

El ente licenciante resolverá los conflictos que pudieran generarse respecto de la utilización

de nombres distintivos que como suscriptores puedan adoptar los certificadores licenciados. En tales casos, corresponde al solicitante del certificado demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

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

No se permite el uso de marcas comerciales, marcas de servicio o nombres de fantasía como nombres distintivos de las Autoridades Certificantes de certificadores licenciados dependientes de la ACR RA.

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

Para formalizar la solicitud de certificado se utiliza el requerimiento de firma de certificado (CSR o "Certificate Signing Request") en formato PKCS#10.

La ACR RA verifica que la clave pública asociada al requerimiento de firma de certificado (CSR) de la Autoridad Certificante del certificador licenciado, se corresponda con la clave privada que el certificador licenciado utilizó para firmarlo.

3.1.8. - Autenticación de la identidad del certificador

Durante el proceso de licenciamiento para política de certificación de un certificador, el ente licenciante procede a identificar fehacientemente la identidad de la persona de existencia ideal, registro públicos de contratos u organismo público solicitante.

Para el caso de organismos públicos, se verifica la identidad de la máxima autoridad del organismo.

Para las personas de existencia ideal, se solicita la documentación constitutiva de la entidad y de acreditación del apoderado o representante legal y si se tratara de registros públicos de contratos, la documentación que acredite su condición. En ambos casos, deben presentar adicionalmente el resto de la documentación indicada en la sección 1.4 del Anexo I de la DA 06/2007.

Toda la documentación relativa a este proceso es mantenida y resguardada por el ente licenciante.

3.1.9. - Autenticación de la identidad de personas físicas

NO APLICABLE.

3.2. - Generación de un nuevo par de claves (rutina de Re-Key)

Se requiere el cumplimiento de los pasos descriptos en el punto 3.1 - Registro inicial.

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

Se requiere el cumplimiento de los pasos descriptos en el punto 3.1 - Registro inicial.

No se admite la utilización del mismo par de claves criptográficas para la renovación de un certificado.

3.4. - Requerimiento de revocación

El procedimiento de revocación de un certificado correspondiente a una Autoridad Certificante de certificador licenciado, se inicia con la recepción de la solicitud de revocación por el ente licenciante y termina cuando una nueva Lista de Certificados Revocados (CRL) conteniendo el número de serie del certificado en cuestión se publica en http://acraiz.cdp1.gov.ar/ca.crl y http://acraiz.cdp2.gov.ar/ca.crl.

Las solicitudes de revocación deberán comunicarse por escrito mediante el formulario diseñado al efecto y disponible en el sitio del ente licenciante.

El ente licenciante realiza la identificación y validación de la identidad del solicitante de la revocación.

Una vez validada la información contenida en la solicitud de revocación, el ente licenciante procederá a la revocación del certificado en un plazo no mayor a las veinticuatro (24) horas. Toda la documentación generada en este proceso es mantenida y resguardada por el ente licenciante.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

Una vez otorgada la licencia de la política de certificación por parte del ente licenciante y publicada la Resolución de otorgamiento en el Boletín Oficial, el certificador licenciado está en condiciones de solicitar el certificado.

El certificador genera en sus instalaciones, el par de claves para la Autoridad Certificante para la política de certificación licenciada, en presencia de personal autorizado del ente licenciante

a quien entrega en ese acto el formulario de solicitud de emisión del certificado debidamente completado junto con el requerimiento de firma de certificado (CSR) en formato PKCS#10.

El certificador licenciado debe seguir los siguientes pasos:

a) Generar el par de claves para la AC vinculada a la política de certificación licenciada, en presencia de personal del ente licenciante,

b) Generar el requerimiento de firma de certificado (CSR), en presencia de personal del ente licenciante,

c) Demostrar que la clave pública presentada al ente licenciante se corresponda con la clave privada utilizada para la firma del requerimiento de firma de certificado (CSR),

d) Presentar la solicitud de emisión de certificado al ente licenciante debidamente firmada por la máxima autoridad en caso de organismo público o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos.

Una vez cumplidos los pasos mencionados, el personal del ente licenciante procederá a verificar la autenticidad del requerimiento de firma de certificado (CSR).

4.2 - Emisión del certificado

Las Autoridades Certificantes de certificadores licenciados integran la IFDRA y dependen de la ACR RA. Por lo tanto la emisión de sus certificados se efectúa en instalaciones de la ACR RA con la participación del certificador licenciado, representado por su máxima autoridad o quien él designe, en caso de organismo público, o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos. Por parte del ente

licenciante, participará el personal debidamente autorizado a dicho efecto.

Los certificados emitidos por la ACR RA a favor de una Autoridad Certificante de certificador licenciado tienen un período de validez de diez (10) años desde su fecha de emisión o hasta su revocación (lo que ocurra primero).

Con la recepción de la solicitud de emisión de certificado remitida por el certificador, la ACR RA del ente licenciante se encuentra en condiciones de generar el certificado digital para la Autoridad Certificante correspondiente.

4.3. - Aceptación del certificado

Un certificado emitido por la ACR RA se considera aceptado por el certificador licenciado después que su apoderado o representante legal, si se trata de una persona de existencia ideal o un registro público de contratos, o la máxima autoridad o quien él designe, si se trata de un organismo público, haya recibido formalmente el certificado digital generado en la ceremonia de emisión y luego de firmado el acuerdo con suscriptores de certificados de la ACR RA.

La ACR RA entrega el certificado emitido al personal de certificador referido en el párrafo precedente, según corresponda.

Una vez recibido el certificado digital emitido por la ACR RA, el certificador licenciado debe instalarlo en su Autoridad Certificante encontrándose en condiciones de emitir certificados a sus suscriptores.

El ente licenciante publica ese certificado digital en su sitio de publicación http://www.sgp.gov.ar/entelicenciante/.

Por otra parte se procederá a publicar en el Boletín Oficial por el término de un (1) día el certificado de clave pública correspondiente a la política de certificación licenciada.

4.4. - Suspensión y Revocación de Certificados

De acuerdo con lo dispuesto por la Ley Nº 25.506, no existe el estado de suspensión de certificados.

La solicitud de revocación de un certificado de Autoridad Certificante debe ser presentada ante el ente licenciante.

4.4.1. - Causas de revocación

El ente licenciante revocará certificados digitales de Autoridad Certificante que hubiera emitido su ACR RA en los siguientes casos:

a) A solicitud del certificador licenciado cuando la clave privada o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo,

b) Si se determina que el certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.

c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por resolución judicial o del mismo ente licenciante debidamente fundada.

e) Por cancelación de la licencia de la política de certificación.

f) En caso de cese de actividades del certificador licenciado.

g) Por condiciones especiales definidas en las Políticas de Certificación.

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

4.4.2. - Autorizados a solicitar la revocación

Se encuentran autorizados a solicitar la revocación de un certificado emitido por la ACR RA:

a) El certificador licenciado, titular del certificado en cuestión, a través de su máxima autoridad en caso de organismo público o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos.

b) Aquellas personas previa y debidamente autorizadas por el certificador licenciado para efectuar tal solicitud.

c) El ente licenciante, o

d) La autoridad judicial competente.

4.4.3. - Procedimientos para la solicitud de revocación

El procedimiento de revocación de un certificado correspondiente a una Autoridad Certificante de certificador licenciado, se inicia con la recepción de la solicitud de revocación por el ente licenciante y termina cuando una nueva Lista de Certificados Revocados (CRL) conteniendo el número de serie del certificado en cuestión se publica en http://acraiz.cdp1.gov.ar/ca.crl y http://acraiz.cdp2.gov.ar/ca.crl.

La solicitud de revocación debe ser completada en papel, firmada y entregada por el solicitante al ente licenciante. El formulario de solicitud se encuentra disponible en el sitio de

publicación del ente licenciante http://www.sgp.gov.ar/entelicenciante/. El ente licenciante verificará la autenticidad de los datos de la solicitud de revocación.

En los casos que la solicitud de revocación surgiera de una decisión judicial o del ente licenciante, se efectuará la notificación al certificador licenciado antes de comenzar el proceso de revocación.

La solicitud de revocación se archiva junto con la documentación recabada en el proceso de licenciamiento de la política de certificación asociada al certificado que se revoca.

Un certificado revocado será válido únicamente para la verificación de firmas generadas durante el período en que el referido certificado era válido.

4.4.4. - Plazo para la solicitud de revocación

El plazo máximo entre la recepción de la solicitud de revocación y la actualización de la lista de certificados revocados, indicando los motivos de la revocación, es de veinticuatro (24) horas.

4.4.5. - Causas de suspensión

De acuerdo con lo dispuesto por la Ley Nº 25.506, no existe el estado de suspensión de certificados.

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

La ACR RA emite y el ente licenciante pública la Lista de Certificados Revocados (CRL) cuando se revoca un certificado o cuando por razones operativas la ACR RA emita un certificado o a los seis (6) meses de la última emisión de CRL, si ninguna de las dos condiciones anteriores ocurre antes.

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

Los certificadores licenciados y terceros usuarios están obligados a verificar la autenticidad y validez de la lista de certificados revocados (CRL) mediante la verificación de la firma digital de la ACR RA y de su período de validez.

La ACR RA del ente licenciante garantizará el acceso permanente, eficiente y gratuito a su lista de certificados revocados

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

NO APLICABLE

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

NO APLICABLE.

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

NO APLICABLE.

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 ente licenciante en su carácter de responsable de la clave privada de la ACR RA, se compromete a comunicar a los certificadores licenciados en caso de compromiso de dicha clave.

4.5. - Procedimientos de Auditoría de seguridad

4.5.1 Tipos de eventos registrados

Con el fin de mantener un ambiente seguro y controlado, se registrará la ocurrencia de los siguientes eventos; registrándose para cada uno, la información relativa al tipo de evento y el tiempo en que el evento ocurrió.

Relacionados con el ente licenciante

a) Cambios en la política de certificación,

b) Cambios en los procedimientos de certificación,

c) Cambios en el acuerdo con suscriptores de certificados de la ACR RA,

d) Cambios en los términos y condiciones con terceros usuarios de certificados de la ACR

RA,

e) Cambios en la política de seguridad,

f) Cambios en el plan de contingencia,

g) Pruebas del plan de contingencia,

h) Cambios en la política de privacidad,

i) Cambios en el personal vinculado al ente licenciante y a la ACR RA,

j) Revisiones de auditoría,

k) Cambios en los procedimientos de licenciamiento.

Relacionados con la ACR RA

a) Ceremonia de generación de claves,

b) Encendido y apagado de los equipos de la Autoridad Certificante y de publicación,

c) Operaciones de mantenimiento, accesos a los sistemas, y cambios y actualizaciones de software y hardware,

d) Entrada en servicio y finalización de las aplicaciones de la ACR RA y del servicio de publicación,

e) Operaciones de lectura y escritura de las aplicaciones de la ACR RA y del servicio publicación,

f) Intentos satisfactorios y fallidos de crear, borrar, acceder, establecer y cambiar contraseñas, permisos y roles del personal afectado a los servicios de certificación,

g) Generación de copias de seguridad,

h) Ciclo de vida de los dispositivos criptográficos incluyendo recepción, instalación, puesta en servicio, uso y finalización del servicio,

i) Generación, almacenamiento, recuperación, activación, desactivación, archivo y destrucción de las claves de la ACR RA,

j) Registro de acceso físico a los diferentes niveles de seguridad,

k) Registros producidos por los elementos de seguridad de las instalaciones (por ej. registro de alarmas, grabaciones de cámaras de vigilancia, etc.),

l) Registro de poseedores de credenciales de activación de los dispositivos criptográficos que contienen las claves privadas de la ACR RA.

Relacionados con el ciclo de vida de los certificados y las listas de revocación

a) Solicitud de emisión de certificado por el certificador licenciado,

b) Aprobación o denegación de solicitud de emisión de certificado,

c) Emisión de certificado por la ACR RA,

d) Aceptación del certificado por el certificador licenciado y firma del acuerdo con suscriptores de certificados de la ACR RA por el certificador licenciado,

e) Asignación del dispositivo criptográfico al responsable poseedor de claves del certificador licenciado,

f) Publicación del certificado en el sitio del ente licenciante,

g) Recepción de solicitud de revocación de certificado,

h) Revocación del certificado,

i) Emisión de la lista de certificados revocados,

j) Publicación de la lista de certificados revocados,

k) Registro de destrucción de material conteniendo información de claves y datos de activación,

l) Renovación de certificados.

4.5.2 Frecuencia de procesamiento del registro de eventos

Los registros de eventos de la ACR RA son analizados periódicamente en relación a su criticidad. Ese análisis es realizado por personal autorizado del ente licenciante.

4.5.3 Período de retención del registro de eventos

Los registros de eventos correspondientes al sistema de la ACR RA se mantienen por un período de doce (12) años a partir de su generación. Los registros de eventos correspondientes al sistema de publicación del ente licenciante se conservan por cinco (5) años.

4.5.4 Protección del registro de eventos

Toda la información pertinente al registro de eventos se mantiene de manera segura y accedida por personal estrictamente autorizado.

4.5.5 Procedimientos de respaldo del registro de eventos

Las copias de respaldo del registro de eventos se realizan acorde a un detallado cronograma.

4.5.6 Sistema de recolección de información acerca de eventos

La información recogida automáticamente es registrada por el sistema operativo y la aplicación. La información sobre eventos manuales es registrada por personal autorizado del ente licenciante.

4.5.7 Notificación al causante del evento

Los sistemas de recolección de eventos no efectúan ninguna notificación al causante del evento sobre el hecho de que sus acciones han sido registradas.

4.5.8 Análisis de vulnerabilidad

Los eventos registrados son utilizados para analizar posibles vulnerabilidades sobre los sistemas y los procedimientos vigentes.

4.6 - Archivo de la información

El ente licenciante mantendrá toda la información relativa a los certificados digitales emitidos por la ACR RA, de acuerdo a lo establecido en el marco legal vigente.

4.6.1 Tipo de información archivada

El ente licenciante almacenará toda la información asociada a los certificados a lo largo de su ciclo de vida incluyendo su renovación. Se registrará:

a) La información obtenida en las diferentes etapas del ciclo de vida del certificado

(solicitud, revocación, renovación, etc.),

b) Los documentos asociados a dichas etapas, incluyendo el licenciamiento,

c) Las diferentes versiones de políticas de certificación, manuales de procedimientos y sus documentos asociados.

4.6.2 Período de retención

El ente licenciante almacenará la información asociada a los certificados digitales emitidos bajo la presente política por un período de diez (10) años, a partir de la fecha de su vencimiento o revocación.

4.6.3 Protección de los archivos de información

El ente licenciante garantiza:

a) la integridad y confidencialidad de la información referente a los certificados digitales emitidos,

b) el almacenamiento de la información en forma completa,

c) la privacidad de los datos obtenidos durante el procedimiento de licenciamiento.

4.6.4 Procedimiento de copia de respaldo (backup)

El ente licenciante efectuará copias de respaldo de la información en soporte electrónico, que serán almacenadas en instalaciones externas. Las copias de respaldo serán:

a) Efectuadas según la política de backup detallada en el manual de procedimientos,

b) Almacenadas en instalaciones que cumplen al menos con los mismos niveles de

protección física y ambiental que las instalaciones principales donde se encuentran instalados los equipos asociados a los procesos de certificación,

c) Verificadas frecuentemente, según lo indica el manual de procedimientos, para asegurar la confiabilidad de los procedimientos de restauración.

4.6.5 Requisitos de sellado de tiempo (Time-Stamping)

NO APLICABLE

4.6.6 Ubicación del archivo de información

El ente licenciante mantiene un esquema distribuido de archivos entre sus instalaciones principales y de respaldo.

4.6.7 Procedimientos de obtención y verificación de la información archivada

Solo las personas autorizadas por el ente licenciante tienen acceso a la información archivada, ya sea en las instalaciones principales como en las de respaldo.

4.7. - Renovación de certificados y cambio de claves criptográficas

La renovación de certificado de Autoridad Certificante deberá seguir el procedimiento indicado en el punto 3.1 de la presente política.

La renovación implica, en todos los casos, la generación de un nuevo par de claves

Transcurrido el periodo de validez del par de claves asociado al certificado, deberán ser retiradas de servicio, de acuerdo a lo indicado en el punto 6.3.2 de esta política.

Únicamente se podrá renovar el certificado de Autoridad Certificante si se cumple alguna de las siguientes condiciones:

a) Para sustituir las claves que van a ser retiradas,

b) Para modificar la información contenida en el certificado, o

c) Por modificaciones realizadas a la política de certificación licenciada.

El ente licenciante realizará una nueva ceremonia de emisión de certificado asociado a la Autoridad Certificante, de acuerdo a su manual de procedimientos.

El trámite de renovación de un certificado digital emitido a favor de un certificador licenciado, debe ser iniciado sesenta (60) días hábiles antes del comienzo del mayor período de validez de los certificados digitales que emite.

Para solicitar un nuevo certificado, se deberá seguir el procedimiento indicado en el punto 4.1 de la presente política.

La clave privada que es objeto de renovación debe ser utilizada para continuar firmando las Listas de Revocación de Certificados (CRLs) hasta la fecha de expiración del último certificado emitido por la Autoridad Certificante utilizando esa clave. En ese momento se debe:

a) solicitar al ente licenciante la revocación de ese certificado, y

b) destruir la clave privada de acuerdo a lo indicado en el punto 6.2.9 de la presente política.

4.8. - Plan de contingencia y recuperación ante desastres

Ante hechos que comprometan la continuidad de sus operaciones, el ente licenciante ha implementado un plan de contingencia y recuperación ante desastres que garantiza el mantenimiento de sus servicios mínimos (recepción de solicitudes de revocación, revocación de certificados, emisión de CRL y consulta de listas de certificados revocados actualizadas).

El plan tiene las siguientes características:

a) es conocido por todo el personal que cumple funciones en el ente licenciante

b) incluye una prueba completa de funcionamiento por lo menos cada seis meses

4.8.1 Compromiso de recursos informáticos, aplicaciones y datos

El ente licenciante utilizará los procedimientos definidos en su plan de contingencia, acorde con su plan de seguridad, para restaurar los recursos informáticos, aplicaciones o datos que hayan sido comprometidos.

4.8.2 Continuidad de las operaciones de la ACR RA

El ente licenciante dispone de procedimientos para asegurar la continuidad de sus operaciones en instalaciones alternativas. El ente licenciante comunicará a los certificadores licenciados si el evento afecta actividades previstas.

4.8.3 Compromiso de la clave privada de la ACR RA

Ante sospecha de compromiso de la clave privada de la ACR RA, el ente licenciante dispone de procedimientos para la revocación de su certificado y el restablecimiento de su infraestructura, contemplándose las siguientes actividades:

a) Ceremonia de generación de un nuevo par de claves,

b) Publicación del nuevo certificado,

c) Emisión de nuevos certificados para los certificadores licenciados.

El ente licenciante tomará las siguientes acciones:

a) Informar a los certificadores licenciados que sus certificados serán revocados, y que las claves privadas asociadas a esos certificados no deben ser utilizadas,

b) Revocar los certificados digitales de las Autoridades Certificantes de los certificadores licenciados,

c) Publicar en su sitio de publicación que se ha revocado el certificado de la ACR RA, notificando a los terceros usuarios que no deben considerarlo como un certificado confiable.

4.9. - Plan de Cese de Actividades

El eventual cese de actividades de la ACR RA queda reservado a una decisión de la Subsecretaria de la Gestión Pública.

En caso de producirse el cese de actividades, el ente licenciante cumplirá con los siguientes procedimientos:

a) Publicará fecha y hora del cese de actividades en el Boletín Oficial durante tres (3) días consecutivos. Esta fecha no podrá ser anterior a los sesenta (60) días contados desde la última publicación en el Boletín Oficial.

b) Notificará a los certificadores licenciados con una antelación no menor a los sesenta (60) días de la fecha prevista de cese.

c) Revocará la totalidad de los certificados que hubiere emitido y que se encontraren vigentes a la fecha de cese de sus actividades.

d) Una vez revocados los certificados de los certificadores licenciados, destruirá la clave privada de la ACR RA mediante un procedimiento que garantice su destrucción total.

5. - CONTROLES DE SEGURIDAD FISICA, FUNCIONALES Y PERSONALES

5.1. - Controles de seguridad física

El ente licenciante ha implementado controles apropiados que restringen el acceso a los equipos, programas y datos utilizados por la ACR RA para la provisión del servicio de certificación, limitándolo a personas debidamente autorizadas.

La ACR RA opera en instalaciones construidas bajo estrictas normas de seguridad física y ambiental internacionales que le brindan una protección adecuada.

5.1.1 Construcción y ubicación de las instalaciones

Para realizar las operaciones de la ACR RA, el ente licenciante cuenta con instalaciones apropiadas que disponen de controles físicos para evitar, prevenir y detectar el acceso indebido a los equipos, programas y datos utilizados. Las instalaciones poseen perímetros de seguridad expresamente definidos.

5.1.2 Niveles de acceso físico

Para ingresar al recinto que contiene los equipos de la ACR RA, el personal autorizado debe atravesar varios niveles de seguridad. Los requisitos de autenticación se incrementan a medida que se accede a los niveles superiores.

5.1.3 Energía eléctrica y aire acondicionado

Los equipos de la ACR RA están alojados en instalaciones que brindan condiciones adecuadas de suministro de energía eléctrica y de aire acondicionado, para permitir una operación segura.

5.1.4 Exposición al agua e inundaciones

Dentro de las instalaciones, los equipos de la ACR RA están alojados en compartimentos estancos a fin de prevenir el impacto producido por inundaciones o filtraciones de líquidos.

5.1.5 Prevención y protección contra incendio

Los equipos de la ACR RA están alojados en instalaciones que cuentan con alarmas de detección y sistemas de extinción de incendios.

5.1.6 Medios de almacenamiento de información

El ente licenciante mantiene los respaldos de información de manera integra y confidencial, almacenándolos en recintos ignífugos y accesibles solo por personal autorizado.

El ente licenciante almacena copias completas de respaldo en instalaciones externas. Además cuenta con procedimientos de recuperación escritos que son verificados periódicamente.

5.1.7 Descarte de medios de almacenamiento de información

El ente licenciante tiene implementado procedimientos para la destrucción de información sensitiva, a fin de imposibilitar su recuperación, acceso o divulgación luego de su eliminación.

5.1.8 Instalaciones de seguridad externas

El ente licenciante dispone de instalaciones externas que tienen niveles de protección física y ambiental similares al de las instalaciones principales.

5.2. - Controles funcionales

El ente licenciante ha establecido una estructura de personal estable con roles específicos definidos para realizar las actividades de licenciamiento y operación de la ACR RA que contempla una adecuada separación de funciones.

5.2.1 Definición de roles afectados al proceso de certificación

El personal del ente licenciante que tenga acceso a los equipos involucrados en los procesos de emisión o revocación de certificados, incluyendo la emisión de la lista de certificados revocados (CRL), es seleccionado y entrenado a los efectos de proporcionar un ambiente de operación seguro y confiable. Este personal deber ser evaluado al menos una vez cada 2 (dos) años para confirmar su continuidad en el puesto.

5.2.2 Separación de funciones

El ente licenciante mantiene un esquema de roles y funciones para establecer una adecuada

segregación y control de las responsabilidades de su personal.

5.2.3 Número de personas requerido por función

Para evitar que una sola persona pueda llevar a cabo operaciones sensitivas, se requiere para las mismas la participación concurrente de varias personas con diferentes roles.

5.2.4 Identificación y autentificación para cada rol

Para ejecutar las funciones pertinentes a su propio rol, todo el personal se debe autenticar de manera segura usando contraseñas y/o certificados digitales.

5.3. - Controles de seguridad del personal del ente licenciante y de la ACR RA

El ente licenciante sigue la política de administración de personal establecida para la Administración Pública Nacional.

5.3.1 Antecedentes laborales, calificaciones, experiencia e idoneidad del personal

El personal del ente licenciante posee experiencia y calificaciones adecuadas para las funciones que desempeñan. Dicho personal tiene pleno conocimiento de las políticas de seguridad y certificación que permiten mantener un ambiente seguro y confiable.

El personal del ente licenciante ha sido cuidadosamente seleccionado y calificado antes de iniciar sus actividades.

5.3.2 Entrenamiento y capacitación inicial

El personal del ente licenciante ha sido entrenado adecuadamente antes de iniciar sus

actividades.

5.3.3 Frecuencias del proceso de actualización técnica

El personal del ente licenciante recibe capacitación constante respecto de los cambios tecnológicos y de procedimientos, que puedan afectar directa o indirectamente las operaciones de certificación.

5.3.4 Frecuencia de rotación de cargos

No aplicable.

5.3.5 Sanciones a aplicar por actividades no autorizadas

El personal del ente licenciante que incumpliere sus funciones y responsabilidades, será sancionado de acuerdo al régimen de sanciones establecido por Administración Pública Nacional.

5.3.6 Requisitos para contratación de personal

El personal del ente licenciante es contratado de acuerdo al régimen de contrataciones establecido por Administración Pública Nacional.

5.3.7 Documentación provista al personal

El ente licenciante proporciona a su personal toda la documentación necesaria para el desempeño de sus funciones y responsabilidades.

6. - CONTROLES DE SEGURIDAD TECNICA

6.1. - Generación e instalación del par de claves criptográficas

6.1.1. - Generación del par de claves criptográficas

Par de claves de la ACR RA

El par de claves criptográficas de la ACR RA es generado por el ente licenciante en instalaciones de la propia ACR RA, en hardware criptográfico seguro que cumple con las características definidas en FIPS 140 Versión 2 para el nivel 3.

El par de claves criptográficas utilizadas por el ente licenciante para emisión y revocación de certificados y emisión de la lista de certificados revocados es de 4096 bits generado con algoritmo RSA.

Par de claves de Autoridad Certificante de certificador licenciado

El par de claves criptográficas de una Autoridad Certificante se genera en las instalaciones del certificador licenciado en presencia de personal del ente licenciante, después de haberle sido otorgada la licencia.

El certificador licenciado, en su carácter de responsable de la Autoridad Certificante a la que la ACR RA le emite un certificado, es el responsable del par de claves criptográficas y, como tal, está obligado a generarlo en un dispositivo criptográfico seguro conforme a la normativa, a no revelar su clave privada a terceros bajo ninguna circunstancia y a almacenarla en un medio que garantice su integridad y confidencialidad. En todo momento la clave privada de la Autoridad Certificante se encuentra bajo el exclusivo y permanente control del certificador licenciado.

Durante la generación y almacenamiento de la clave privada de la Autoridad Certificante, por parte del certificador licenciado debe asegurarse que:

a) la clave privada es única y su seguridad se encuentra garantizada, y

b) no puede ser deducida y se encuentra protegida contra réplicas fraudulentas.

6.1.2. - Entrega de la clave privada al certificador licenciado

De acuerdo al artículo 21, inciso b, de la Ley Nº 25.506 y el artículo 34, inciso i, del decreto Nº 2628/02, el ente licenciante no genera ni toma conocimiento o accede a los datos de generación de firma de las Autoridades Certificantes del certificador licenciado.

6.1.3. - Entrega de la clave pública al ente licenciante

El certificador licenciado, a través del personal designado para representarlo, entrega al ente licenciante copia de su clave pública contenida en un CSR (Certificate Signing Request), en formato PKCS#10, de manera que:

a) No pueda ser alterada, y

b) El certificador posea la clave privada que corresponde a dicha clave pública.

Todas las actividades que se llevan a cabo en el proceso de recepción de la clave pública son registradas para fines de auditoría.

6.1.4. - Disponibilidad de la clave pública

El ente licenciante publica su propio certificado en http://acraiz.gov.ar/ca.crt. Del mismo modo, publicará en http://www.sgp.gov.ar/entelicenciante/ los certificados de las

Autoridades Certificantes de certificadores licenciados que la ACR RA hubiera emitido.

El certificador licenciado es responsable de publicar los certificados de sus Autoridades Certificantes y de sus suscriptores para que terceros usuarios puedan acceder a ellos.

6.1.5. - Tamaño de claves

La ACR RA utiliza un par de claves criptográficas RSA de 4096 bits de longitud para emitir los certificados de las Autoridades Certificantes de los certificadores licenciados.

En caso de tomar conocimiento de técnicas de criptoanálisis que vulneren el algoritmo utilizado para la generación de firma con la longitud indicada, el ente licenciante revocará los certificados emitidos, notificando previamente a los certificadores licenciados y anunciará la implementación de una nueva versión de la presente política de certificación.

6.1.6. - Generación de parámetros de claves asimétricas

NO APLICABLE.

6.1.7. - Verificación de calidad de los parámetros

NO APLICABLE.

6.1.8. - Generación de claves por hardware o software

El par de claves criptográficas se generan en dispositivos criptográficos que cumplan con lo definido en el punto 6.2.1 de la presente política de certificación.

6.1.9. - Propósitos de utilización de claves (Key Usage)

Las claves criptográficas de la ACR RA tienen como exclusivo propósito la firma de su certificado, de su CRL y de los certificados de las Autoridades Certificantes de certificadores licenciado y la firma de sus CRLs.

Las claves criptográficas de las Autoridades Certificantes de certificadores licenciados tienen como exclusivo propósito su utilización para la firma de certificados de sus suscriptores y la firma de sus CRLs.

6.2. - Protección de la clave privada

Las claves privadas de la ACR RA están bajo responsabilidad del ente licenciante y protegidas mediante la utilización de sistemas y procedimientos que incluyen la designación de funcionarios responsables de su control, custodia y activación segura y de su destrucción en caso de compromiso.

Las claves privadas de las Autoridades Certificantes de los certificadores licenciados están bajo su propia responsabilidad, y protegidas mediante la utilización de sistemas y procedimientos confiables que evitan el uso no autorizado o pérdida de las mismas.

6.2.1. - Estándares para dispositivos criptográficos

La ACR RA dispone de un dispositivo criptográfico que cumple con las características definidas en FIPS 140 versión 2, nivel 3, para la generación y almacenamiento de su par de claves criptográficas.

Para la generación y almacenamiento de sus pares de claves criptográficas, el certificador licenciado dispone de dispositivos criptográficos que cumplen con las características

definidas en FIPS 140 versión 1 o 2, de por lo menos:

a) nivel 3, para sus autoridades certificantes, y

b) nivel 2, para sus autoridades de registro.

6.2.2. - Control "M de N" de la clave privada

El ente licenciante utiliza procedimientos que requieren la participación de varias personas para la activación de la clave privada de la ACR RA.

Los certificadores licenciados deben adoptar procedimientos que requieran la participación de varias personas para la activación de las claves privadas de sus Autoridades Certificantes.

Lo indicado anteriormente en este punto no se hace necesariamente extensivo a las Autoridades de Registro de los certificadores licenciados.

6.2.3 Recuperación de la clave privada

El ente licenciante posee procedimientos para la recuperación de su clave privada, detallados en su manual de procedimientos de certificación.

6.2.4. - Copia de seguridad de la clave privada

El ente licenciante mantiene una copia de seguridad de su clave privada. Esta copia es almacenada y protegida con un nivel de seguridad no inferior al establecido para la versión original de la clave y mantenida por el plazo de validez del certificado correspondiente.

El ente licenciante no mantiene copia de las claves privadas de las Autoridades Certificantes de los certificadores licenciados.

Las claves privadas de las Autoridades Certificantes cuentan con al menos una copia de seguridad de manera tal de poder recuperarlas en caso de desastre o malfuncionamiento del sistema.

Estas copias están protegidas bajo las mismas condiciones de acceso físico que se implementan en el ambiente de producción. Están resguardadas en dispositivos criptográficos equivalentes a los que contienen las claves originales.

6.2.5. - Archivo de clave privada

Cuando las claves privadas de las Autoridades Certificantes están desactivadas, los dispositivos criptográficos que las contienen permanecen bajo los controles de seguridad física descriptos en la presente política y el acceso a los mismos es debidamente registrado y solo permitido a personal autorizado.

6.2.6. - Incorporación de claves privadas en módulos criptográficos

Las claves privadas se generan en dispositivos criptográficos conforme lo establecido en la presente política y nunca se extraen de los mismos.

Solo se permite la transferencia de claves en caso de creación de copias de seguridad descriptas en la presente política y se realizan a través de los procedimientos de resguardo propios de los dispositivos criptográficos utilizados.

6.2.7. - Método de activación de claves privadas

La activación de las claves privadas de las Autoridades Certificantes utiliza un esquema de control compartido ("M de N"), por lo que se necesita la intervención simultanea de varias

personas autorizadas.

6.2.8. - Método de desactivación de claves privadas

La desactivación de las claves privadas se realiza a través de procedimientos que garantizan la inhabilitación de esas claves. Para volver a utilizarlas es necesario seguir el procedimiento de activación de claves descriptas en la presente política.

6.2.9. - Método de destrucción de claves privadas

Las claves privadas se destruirán utilizando procedimientos que imposibilitan su posterior recuperación o utilización. Ello se realiza bajo las mismas medidas de seguridad que las empleadas en la Ceremonia de Generación de Claves.

6.3. - Otros aspectos de administración de claves

6.3.1. - Archivo de la clave pública

La clave pública se archiva utilizando métodos que garantizan su integridad. El ente licenciante posee procedimientos para el archivo de su clave privada, detallados en su manual de procedimientos de certificación.

6.3.2. - Período de uso de clave pública y privada

El período de validez del par de claves se corresponde con el período de validez de los certificados emitidos.

El certificado de la ACR RA expira a los veinte (20) años y los certificados de Autoridades Certificantes de certificador licenciado expiran a los diez (10) años o cuando son revocados.

6.4. - Datos de activación

6.4.1. - Generación e instalación de datos de activación

Los datos de activación de las claves privadas utilizan un esquema de control compartido ("M de N").

6.4.2. - Protección de los datos de activación

Los datos de activación son tratados como información confidencial y no deben estar expuestos en medios accesibles por terceros. Asimismo las personas responsables de su custodia no deben divulgar su condición.

6.4.3. - Otros aspectos referidos a los datos de activación

NO APLICABLE

6.5. - Controles de seguridad informática

6.5.1. - Requisitos técnicos específicos

Solo personal debidamente autorizado puede acceder a las instalaciones y sistemas que intervienen en las operaciones de certificación. Acorde a la política de seguridad aprobada por el ente licenciante se garantiza:

a) Una efectiva administración de los accesos para aquellos usuarios involucrados en el ciclo de vida de los certificados,

b) La segregación de funciones según lo especificado en la política de seguridad de la ACR

RA.

c) La correcta identificación y autenticación del personal en las actividades críticas relacionadas con el ciclo de vida de los certificados,

d) El registro de eventos relacionados con el ciclo de vida de los certificados,

e) La protección, integridad y confidencialidad de datos críticos.

6.5.2. - Calificaciones de seguridad computacional

NO APLICABLE.

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

6.6.1. - Controles de desarrollo de sistemas

Para la implementación de los sistemas en el ambiente de producción se consideran los siguientes controles:

a) Análisis de seguridad en todos sus componentes,

b) Entornos separados de desarrollo, prueba y producción,

c) Procedimiento formal de autorización y registro para la actualización de los sistemas,

d) En caso de que el sistema fuera adquirido debe existir un acuerdo de nivel de servicio con el proveedor, que coincida con el ofrecido por el certificador licenciado a sus suscriptores.

6.6.2. - Administración de controles de seguridad

Según el análisis de riesgo efectuado, se clasificaron los activos informáticos de acuerdo a sus

necesidades de protección y se mantiene su inventario. Los sistemas son auditados de forma periódica de acuerdo a lo establecido en el plan de auditoría.

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

NO APLICABLE.

6.7. - Controles de seguridad de red

Los servicios de certificación de la ACR RA se realizan fuera de línea lo que asegura su protección de cualquier ataque a través de redes.

Los servicios de publicación del ente licenciante y de la ACR RA utilizan sistemas debidamente protegidos, garantizando integridad.

6.8. - Controles de ingeniería de dispositivos criptográficos

El dispositivo criptográfico utilizado para el almacenamiento y generación de la clave privada cumple con lo establecido en la presente política de certificación.

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

Tanto el formato del certificado como el de la lista de certificados revocados cumplen con lo especificado en el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile).

7.1. - Perfil del certificado

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de la AC Raíz:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Versión (Version)	V3
Número de serie (Serial Number)	Número asignado por la AC Raíz
Algoritmo de firma (Signature Algorithm)	sha1RSA
Nombre distintivo del emisor (Issuer DN)	CN = AC Raíz O = Infraestructura de Firma Digital C = AR
Validez (desde, hasta) (Valid From / Valid To)	20 años Se especifica desde/hasta
Nombre distintivo del suscriptor (Subject DN)	CN = AC Raíz O = Infraestructura de Firma Digital C = AR
Clave pública del suscriptor (Subject Public Key)	La clave pública RSA es de 4096 bits
Extensiones	
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves (Key Usage)	Los bits deben estar como se indican: DigitalSignature = 0 NonRepudiation =0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	Debe incluir el OID de esta Política (2.16.32.1.1.0) URI: http://acraiz.gov.ar/cps.pdf
Restricciones básicas (Basic Constraints)	cA=TRUE
Punto de distribución de la lista de certificados revocados (CRL Distribution Points)	URI=http://acraiz.cdp1.gov.ar/ca.crl URI=http://acraiz.cdp2.gov.ar/ca.crl

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de ACs de los certificadores licenciados:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión (Version)	V3
Número de serie (Serial Number)	Número asignado por la AC Raíz
Algoritmo de firma (Signature Algorithm)	sha1RSA
Nombre distintivo del emisor (Issuer DN)	CN = AC Raíz O = Infraestructura de Firma Digital C = AR
Validez (desde, hasta) (Valid From / Valid To)	10 años Se especifica desde/hasta
Nombre distintivo del suscriptor (Subject DN)	Según lo especificado en Anexo III de la DA 06/07 en el punto 2.2.6 en lo referente a certificados de certificadores.
Clave pública del suscriptor (Subject Public Key)	Según lo especificado en Anexo III de la DA 06/07 en el punto 4 en lo referente a certificados de certificadores.
Extensiones	
Identificador de la clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un identificador de la clave pública de la ACR RA.
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves (Key Usage)	Los bits deben estar como se indican: DigitalSignature = 0 NonRepudiation =0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	Según lo especificado en Anexo III de la DA 06/07 en el punto 2.3.4,
Restricciones básicas (Basic Constraints)	cA=TRUE pathlen=0

Certificado X.509 v3 Atributos / Extensiones	Contenido
Punto de distribución de la lista de certificados revocados (CRL Distribution Points)	URI=http://acraiz.cdp1.gov.ar/ca.crl URI=http://acraiz.cdp2.gov.ar/ca.crl
Información de Acceso de la Autoridad Certificante (Authority Information Access)	URI=http://acraiz.gov.ar/ca.crt

7.2. - Perfil de la lista de certificados revocados

Se usarán los siguientes campos del formato X.509 versión 2 en la Lista de Certificados Revocados (CRL) de la AC Raíz:

X.509 v2 Certificado Atributos / Extensiones	Contenido
Atributos	
Versión (Version)	V2
Algoritmo de firma (Signature Algorithm)	sha1RSA
Nombre distintivo del emisor (Issuer DN)	CN = AC Raíz O = Infraestructura de Firma Digital C = AR
Día y hora de vigencia (Efective Date)	Día y hora de emisión de esta CRL
Próxima actualización (Next Update)	Día y hora de la próxima emisión de CRL
Certificados revocados (Revoked Certificates)	Lista de los certificados revocados incluyendo número de serie (Serial Number) y fecha de revocación (Revocation Date)
Extensiones	
Identificación de clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Número de CRL (CRL Number)	Número que se incrementa cada vez que cambia una CRL

8. - ADMINISTRACION DE ESPECIFICACIONES

8.1. - Procedimientos de cambio de especificaciones

El ente licenciante cuenta con procedimientos de administración de cambios para efectuar cualquier modificación a la presente política de certificación.

8.2. - Procedimientos de publicación y notificación

El ente licenciante publicará en su sitio de publicación las modificaciones aprobadas a la política de certificación, indicando en cada caso, el texto reemplazado. Asimismo, publicará el texto de la nueva versión del documento modificado.

Lo mismo se aplica al acuerdo con suscriptores de certificados de la ACR RA y a los términos y condiciones de terceros usuarios de certificados de la ACR RA.

Todos los cambios producidos en los documentos antedichos serán notificados a los certificadores licenciados.

8.3. - Procedimientos de aprobación

Esta política de certificación o cualquier documento vinculado, así como sus actualizaciones, serán aprobados por la Subsecretaría de la Gestión Pública.