Jefe de Gabinete de Ministros

ANEXO I

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Requisitos para el licenciamiento de certificadores

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

97

INDICE

Jefe de Gabinete de Ministros

FOLIO 98

Introducción

De acuerdo con el Art. 30 de la Ley 25.506 se establecen a continuación los requisitos que debe cumplir un solicitante para obtener una licencia en el marco de la Infraestructura de Firma Digital de la República Argentina.

El presente documento tiene la siguiente estructura:

- Sección 1: Documentación que debe entregar el solicitante para obtener una licencia para su Política de Certificación
- Sección 2: Pautas de control a que será sometido el solicitante para obtener la licencia
- Sección 3: Registro de eventos
- Sección 4: Controles Físicos

Todas las referencias al certificador, en este documento, se entenderán también válidas para el solicitante en proceso de obtener una licencia, en la medida en que sean aplicables.

Ante cualquier duda en la interpretación del presente documento, podrá dirigirse por escrito al ente licenciante, sito en Av. Roque Sáenz Peña 511 - C1035AAA - Ciudad Autónoma de Buenos Aires - República Argentina, o remitir su consulta firmada digitalmente a la dirección de correo electrónico: licenciamiento@sgp.gov.ar.

Sección 1: Documentación a presentar por el solicitante

Para tramitar su licencia, el solicitante debe presentar ante el ente licenciante los documentos específicos relacionados con su política de certificación, los documentos complementarios descriptivos de sus condiciones de operación y, si se trata de una Persona Jurídica Privada, la documentación correspondiente a esta condición, todo lo cual se describe en detalle más adelante. Cada uno de los documentos deberá estar debidamente firmado.

1.- Responsables de la presentación de la solicitud

El trámite de licenciamiento se inicia con la presentación de la solicitud de licencia firmada:

- En caso de personas jurídicas privadas, por su representante legal
- Si se tratara de un organismo integrante de la Administración Pública Nacional (tal como se define en el Art.8 ley 24.156) se requerirá que la solicitud de licencia esté firmada por la máxima autoridad de la entidad y jurisdicción de que se trate, autorizando el inicio del trámite de licenciamiento.
- En caso de tratarse de un organismo provincial, municipal y de otros poderes del Estado, la solicitud de licencia deberá estar firmada por la máxima autoridad del organismo o jurisdicción.
- Si se tratara de un Registro Público de Contrato, deberá presentar documentación que acredite su condición.

2.- Documentos Específicos

Se deben presentar:

a) Formulario de Solicitud de Licencia completo y firmado por el responsable de la solicitud

b) Política de Certificación (PC) sometida a aprobación

c) Manual de Procedimientos de Certificación (MPC)

d) Acuerdo tipo con suscriptores

e) Términos y condiciones tipo con terceros usuarios ("*relying parties*")

f) Resumen de la PC/MPC para suscriptores ("*PKI Disclosure Statement*") (en caso de existir)

g) Política de Privacidad del certificador

h) Direcciones, protocolos y medios para acceder a la información que se publica, certificados, Lista de Certificados Revocados ("*Certificate Revocation List*" – CRL), etc.

i) Ejemplos de Certificados, CRLs e información de estado de los certificados a emitir (perfil de certificados)

3.- Documentos Complementarios

La documentación complementaria requerida a los efectos de evaluar la consistencia y compatibilidad de las instalaciones, la infraestructura tecnológica, los procedimientos y los controles del solicitante respecto de la Política de Certificación en análisis es la siguiente:

a) Contratos de tercerización, en caso de existir tercerización de servicios, con la especificación del nivel de servicio acordado

b) Plan de Cese de Actividades

c) Plan de Seguridad (política y procedimientos de seguridad)

d) Plan de Contingencia

e) Descripción de la plataforma tecnológica del solicitante

4.- Documentación adicional requerida en caso de Personas Jurídicas Privadas

Se deben presentar:

a) Garantía de Caución (en sus términos y condiciones; su vigencia será constatada en el momento de otorgamiento de la licencia al certificador)

b) Documentación de la constitución de la entidad (Estatuto o Contrato Social) en copia certificada por escribano

c) Última acta de Asamblea, con designación de autoridades, y última acta de Directorio y/o distribución de cargos en copias certificadas por escribano

d) Constancia de inscripción en Inspección General de Justicia o en el registro público de la jurisdicción que corresponda en copia certificada

e) Constancia de inscripción ante la AFIP

f) Últimos estados contables auditados, certificados por Contador Público

g) Comprobante de pago de iniciación del trámite

Sección 2: Pautas de control

Toda la documentación presentada será sometida a controles legales y técnicos y se efectuarán auditorías en instalaciones del certificador, como pasos previos al otorgamiento de la licencia o rechazo de la solicitud de licencia correspondiente a la Política de Certificación.

Por lo tanto el certificador debe permitir el acceso del personal designado por el ente licenciante a sus instalaciones, a la información y a su infraestructura tecnológica a fin de dar cumplimento a las funciones de auditoría, de acuerdo con lo establecido en la Ley N° 25.506, Decreto N° 2628/02 y normas complementarias.

Los controles y auditorías a realizar cubren los siguientes aspectos:

a) Requisitos legales generales
b) Política de Certificación y Manual de Procedimientos de Certificación
c) Plan de Seguridad
d) Plan de Cese de Actividades
e) Plan de Contingencia
f) Plataforma Tecnológica
g) Ciclo de vida de las claves criptográficas del certificador
h) Ciclo de vida de los certificados de suscriptores
i) Estructura y contenido de los certificados y CRLs
j) Mecanismos de acceso a la documentación publicada, certificados y CRLs

Los controles mencionados tienen por objetivo verificar el cumplimiento de los requisitos exigidos a los certificadores para obtener la condición de certificadores licenciados y, en particular, el licenciamiento de la Política de Certificación sometida a aprobación.

a) Requisitos legales generales

1.- Obligación de información

El certificador debe informar a los potenciales suscriptores, terceros usuarios y otros posibles interesados, las condiciones de utilización del certificado digital, su tramitación y revocación así como las condiciones de la Política de Certificación. Dicho mecanismo de información debe constar en la documentación presentada.

2.- Garantías

Las entidades privadas que soliciten licencia de certificador deberán constituir un seguro de caución a fin de garantizar el cumplimiento de sus obligaciones.

3.- Acuerdos entre partes

El certificador debe tener claramente definidos los textos de los modelos de compromisos con suscriptores y terceros usuarios ("relying parties") según los Anexos V y VI que establecen los contenidos mínimos para los siguientes documentos:

a) Acuerdos con suscriptores

b) Términos y condiciones con terceros usuarios

4.- Contratos de Servicios de Tercerización

El certificador debe tener claramente acordados los niveles de servicio que permitan garantizar la correcta prestación del servicio.

5.- Política de Privacidad del certificador

El certificador debe presentar su Política de Privacidad a los efectos de evaluarla en relación con la Política de Certificación que es objeto de análisis para su licenciamiento. Para ello debe tener en cuenta lo expresado en el **Anexo VIII - Contenidos Mínimos de la Política de Privacidad.**

b) Política de Certificación (PC) y Manual de Procedimientos de Certificación (MPC)

1.- Estructura de la Política de Certificación

La Política de Certificación debe responder a la estructura definida en el **Anexo II - Requisitos Mínimos para Políticas de Certificación.**

2.- Contenido de la Política de Certificación

La Política de Certificación debe incluir los contenidos mínimos establecidos en el **Anexo II - Requisitos Mínimos para Políticas de Certificación.**

3.- Compatibilidad de la Política de Certificación y el Manual de Procedimientos de Certificación

El Manual de Procedimientos de Certificación debe ser totalmente compatible con la Política de Certificación y esos documentos no deben contener cláusulas contradictorias o incompatibles entre sí.

4.- Administración de la Política de Certificación y del Manual de Procedimientos de Certificación

El certificador debe mantener procedimientos de administración de la Política de Certificación y del Manual de Procedimientos de Certificación. Esos procedimientos deben asegurar que todo cambio se encuentre debidamente autorizado y difundido.

c) Plan de Seguridad

1.- Normas que debe cumplir el Plan de Seguridad

El Plan de Seguridad debe cumplir con los lineamientos de la Norma IRAM ISO/IEC 17799 y sus correspondientes actualizaciones o reemplazos vigentes al momento de la presentación de la solicitud de licencia, en lo referente a todos aquellos aspectos relacionados directa o indirectamente con las actividades de certificación.

En caso de que alguno de los lineamientos no resultara aplicable a la estructura de la organización, se deberán justificar por escrito y someter a aprobación las razones para no cumplirlo.

Adicionalmente a lo que indica la Norma IRAM ISO/IEC 17799 el certificador debe mantener controles que permitan cumplir con los siguientes puntos:

- **Tercerización**

En ningún caso se podrán tercerizar los servicios asociados a la gestión del ciclo de vida de las claves del certificador.

- **Seguridad física y ambiental**

El certificador debe mantener controles que permitan asegurar que:

a) Las áreas en las cuales se desarrolle cada etapa del ciclo de vida de las claves criptográficas deben ser tratadas como de alta seguridad. El acceso físico a dichas áreas debe limitarse sólo a personal autorizado.

   La **Sección 4** del presente Anexo indica los controles físicos vinculados al proceso de certificación que el certificador debe implementar en sus instalaciones.

b) La infraestructura tecnológica necesaria para la generación de certificados y CRLs del certificador debe encontrarse alojada en servidores físicamente independientes del resto de los servidores utilizados y afectados en forma exclusiva a las tareas de certificación, condiciones que serán controladas durante el proceso de licenciamiento.

- **Intercambios de información y software**

Las comunicaciones entre las Autoridades de Registro (AR) y la Autoridad Certificante (AC) referidas a la aprobación o revocación de certificados deben ser llevadas a cabo mediante un mecanismo que garantice el no repudio.

- **Revisiones de la política de seguridad**

El ente licenciante en sus inspecciones post-licenciamiento solicitará la información relevada por las auditorías encaradas por el certificador que controlen el cumplimiento de su política.

- **Registro de eventos**

El certificador debe dejar evidencia sobre todas las actividades realizadas sobre los registros de eventos actuales y archivados. Además debe implementar procedimientos que determinen:

a) Frecuencia de procesamiento y archivo.
b) Período de retención.
c) Mecanismos de protección contra accesos no autorizados.
d) Mecanismos de resguardo y consulta.
e) Mecanismos para asegurar la integridad de los registros de eventos actuales y archivados.
f) Ubicación de los resguardos.
g) La utilización exclusiva de un par de claves en caso de que los registros de eventos sean firmados.

La **Sección 3** del presente Anexo indica los eventos del proceso de certificación que deben ser registrados por el certificador.

2.- Documentos que componen el Plan de Seguridad

- Una política de seguridad de la información, documentada y aprobada por la alta gerencia de la entidad, en la que se indique cuáles son las acciones que se realizarán para cumplir con sus objetivos.

- Un manual que documente detalladamente los procedimientos para ejecutar las acciones necesarias para cumplir con los objetivos de la política de seguridad.

3.- Conocimiento del Plan de Seguridad

El personal que participa en el proceso de certificación debe conocer la política y los procedimientos con ella relacionados y será responsable de su cumplimiento. El certificador deberá establecer mecanismos de capacitación y de documentación del compromiso de cumplimiento por parte del personal afectado.

d) Plan de Cese de Actividades

1.- Publicación y notificación del cese de actividades

El certificador debe disponer de procedimientos para:

a) la publicación del cese de actividades en el Boletín Oficial, en su sitio de Internet y al menos en otro medio de difusión nacional su notificación al ente licenciante y a los suscriptores con la antelación adecuada.

2.- Prestación de servicios en el período previo al cese

El certificador debe disponer de procedimientos para el mantenimiento de servicios en el período anterior al de cese (revocación de certificados, actualización de repositorios y emisión de CRLs) y la transferencia de la custodia de archivos y de la documentación de soporte de los certificados emitidos.

3.- Administración de los certificados por cese de actividades del certificador

El certificador debe disponer de procedimientos para la revocación de los certificados emitidos al momento del cese de sus actividades.

4.- Destrucción de la clave privada del certificador

El certificador debe implementar procedimientos seguros para la destrucción de las claves privadas, y de sus copias de seguridad, de todas sus autoridades certificantes cuando cesa en sus actividades, una vez que hayan sido revocados todos los certificados emitidos.

e) Plan de Contingencia

1.- Normas que debe cumplir el Plan de Contingencia

El Plan de Contingencia debe cumplir, con los lineamientos de la Norma IRAM ISO/IEC 17799 sobre Administración de la Continuidad de los Negocios y sus correspondientes actualizaciones o reemplazos vigentes al momento de la presentación de la solicitud de licencia.

En caso de que alguno de los lineamientos no resultara aplicable a la estructura de la organización, se deben justificar por escrito y someter a aprobación las razones para no cumplirlo.

Adicionalmente a lo que indica la Norma IRAM ISO/IEC 17799 el certificador debe mantener controles que permitan cumplir con los siguientes puntos:

- **Administración de la continuidad de las operaciones**

El certificador debe tener controles que aseguren:

a) La continuidad de las operaciones en caso de compromiso de su clave privada, y

b) La reducción al mínimo posible de las eventuales interrupciones en el servicio

Se considerarán procesos críticos indispensables para la actividad de certificación:

a) La recepción de solicitudes de revocación

b) La revocación de certificados digitales

c) La emisión de la lista de certificados revocados

d) La publicación de la lista de certificados revocados

e) La respuesta o publicación acerca del estado de un certificado, en caso de que así correspondiese

f) Dependiendo de las características de la Política de Certificación también pueden ser críticos:

- La solicitud, aprobación y emisión de certificados digitales
- La solicitud de renovación, aprobación y emisión de renovaciones de certificados digitales

- **Prueba del plan**

Debe existir un procedimiento de prueba del plan de contingencia. El mismo debe llevarse a cabo con una periodicidad de seis meses y preverse la realización de una prueba durante el periodo de auditoría inicial del ente licenciante.

2.- Documentos que componen el Plan de Contingencia

- El Plan de Contingencia, documentado y aprobado por la alta gerencia de la entidad, en el que se indique cuáles son las acciones que se realizarán para cumplir con los objetivos de este plan.

- Un manual que documente detalladamente los procedimientos para ejecutar las acciones necesarias para cumplir con el objetivo.

- La documentación de todas las pruebas y ejecuciones reales (si las hubo) realizadas del Plan de Contingencia.

3.- Conocimiento del Plan de Contingencia

El personal que participa en el proceso de certificación debe conocer el Plan de Contingencia y los procedimientos con él relacionados y será responsable de su cumplimiento, de acuerdo a los roles asignados. El certificador deberá establecer mecanismos de capacitación y de documentación del compromiso de cumplimiento por parte del personal afectado.

f) Plataforma Tecnológica

Se debe ajustar a estándares tecnológicos vigentes que cubran las necesidades requeridas por el proceso de certificación.

El certificador debe implementar procedimientos que garanticen la confiabilidad de su plataforma tecnológica.

g) Ciclo de vida de las claves criptográficas del certificador

1.- Consideraciones generales respecto de las claves criptográficas

Deben cumplirse los siguientes requerimientos mínimos:

- El par de claves debe ser generado únicamente por el certificador, permaneciendo su clave privada en todo momento bajo su absoluto y exclusivo control.
- El medio de generación y almacenamiento de la clave privada utilizada en la generación de la firma debe asegurar que:
  - La clave privada sea única
  - No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas realizadas con las tecnologías disponibles a la fecha
  - Pueda ser eficazmente protegida por el certificador contra su utilización ilegal
  - El transporte entre el dispositivo de generación y el de almacenamiento se realice en forma segura

2.- Tamaño de las claves criptográficas

Deben respetarse las siguientes longitudes mínimas de claves:

- Las claves criptográficas que el certificador utilice para la firma de certificados, CRLs, y cualquier otro tipo de servicio no podrán ser inferiores a 2048 bits si utilizan los algoritmos RSA o DSA y 210 bits si utiliza el algoritmo ECDSA.
- Para certificados utilizados en servicios relacionados con la firma digital (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.) las claves criptográficas no podrán ser inferiores a 2048 bits si utilizan los algoritmos RSA o DSA y 210 bits si utiliza el algoritmo ECDSA.
- Para los responsables de la Autoridad de Registro, las claves criptográficas que utilicen para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación, deben mantenerse permanentemente bajo su control y no pueden ser inferiores a 1024 bits si utilizan los algoritmos RSA o DSA y 160 bits si utiliza el algoritmo ECDSA.

3.- Estándares para los dispositivos criptográficos

Deben respetarse las siguientes exigencias mínimas:

a) Las claves criptográficas del certificador deben ser generadas y almacenadas en dispositivos que cuenten con certificación emitida FIPS 140 (Versión 1 o 2) para el nivel 3.

b) Las claves criptográficas utilizadas para la firma de información de estado de certificados o servicios relacionados con la firma digital deben ser generadas y

almacenadas en dispositivos que cuenten con certificación emitida FIPS 140 (Versión 1 o 2) para el nivel 3.

c) Las claves criptográficas que los responsables de la Autoridad de Registro utilicen para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación deben ser generadas y almacenadas en dispositivos que cumplan con cuenten con certificación emitida FIPS 140 (Versión 1 o 2) para el nivel 2 o superior.

4.-Generación del par de claves criptográficas del certificador

El certificador debe mantener exclusivo control sobre el proceso de generación de sus claves criptográficas. Esto incluye al personal, equipamiento y sistemas afectados a la operación.

5.- Almacenamiento, respaldo y recuperación de las claves criptográficas del certificador

El certificador debe mantener el control exclusivo sobre las claves criptográficas durante su almacenamiento y sobre sus copias de respaldo.

El certificador debe implementar procedimientos para realizar la recuperación de sus claves a partir de sus copias de respaldo.

6.- Distribución de las claves públicas del certificador

El certificador debe implementar procedimientos seguros para distribuir sus claves públicas.

7.- Custodia de las claves criptográficas del certificador

No está permitida la custodia de claves criptográficas por parte de terceros.

En caso de que el certificador guarde elementos sensitivos vinculados a sus claves criptográficas en dependencias de un tercero, debe garantizar los niveles de resguardo y la imposibilidad de que el tercero en cuestión pueda acceder a ellas y producir su activación.

8.- Utilización de las claves privadas del certificador

El certificador debe mantener procedimientos y controles que aseguren que las claves serán utilizadas exclusivamente para las funciones previstas y en las ubicaciones previamente establecidas.

El control de la utilización de las claves criptográficas del certificador debe estar dividido de forma tal que para activar su uso sea necesaria la presencia de M personas de un total de N posibles, con M mayor o igual a 2.

Debe respetar lo establecido como longitudes mínimas de las claves y estándares para dispositivos criptográficos permitidos.

9.- Destrucción de las claves criptográficas del certificador

El certificador debe mantener procedimientos y controles que aseguren que sus claves se destruyen por completo al finalizar su ciclo de vida.

10.- Almacenamiento (a largo plazo) de las claves del certificador

El certificador debe mantener procedimientos y controles que aseguren la confidencialidad de las claves archivadas, y garantizar que no se podrán reutilizar.

11.- Administración de ciclo de vida de los dispositivos criptográficos del certificador

El certificador debe mantener procedimientos y controles que aseguren que:

a) Solo personal expresamente autorizado pueda acceder al dispositivo criptográfico del certificador,

b) El dispositivo criptográfico funciona adecuadamente

h) Ciclo de vida de los certificados de suscriptores

1.- Registro y procesamiento de la solicitud del suscriptor

El certificador debe implementar procedimientos de solicitud aplicables a los certificados a emitir, que aseguren que los suscriptores sean debidamente identificados y que las solicitudes respondan a un modelo adecuado y se encuentren autorizadas y completas.

El certificador debe implementar procedimientos para asegurar que los suscriptores generen sus claves criptográficas de manera segura y bajo exclusivo control de éstos últimos.

2.- Renovación del certificado

El certificador debe implementar un procedimiento para la renovación del certificado de un suscriptor que deberá contemplar la validación de la solicitud correspondiente.

3.- Requerimiento de certificado con un nuevo par de claves

El certificador debe implementar un procedimiento por el cual un suscriptor pueda solicitar la reemisión de un certificado con un nuevo par de claves que deberá contemplar la validación de la solicitud correspondiente.

4.- Emisión del certificado

El certificador debe mantener controles que aseguren que los certificados nuevos, renovados y reemitidos sean generados de acuerdo con sus políticas, prácticas y procedimientos.

5.- Distribución del certificado

El certificador debe implementar controles que aseguren que los certificados generados sean puestos a disposición de los suscriptores y usuarios.

6.- Aceptación del certificado

El certificador debe implementar procedimientos para la aceptación, por parte de los suscriptores, de los certificados emitidos.

7.- Revocación del certificado

El certificador debe implementar procedimientos y controles que aseguren que:

a) los certificados son revocados conforme a solicitudes de revocación autorizadas y válidas

b) el usuario cuente con medios para solicitar la revocación de sus certificados

c) las vías de comunicación disponibles para recibir la solicitud de revocación operen correctamente

d) se respetan los plazos de revocación establecidos en la Política de Certificación

8.- Suspensión del certificado

El certificador debe informar que el estado de suspensión no es admitido en el marco de la Ley 25.506.

9.- Procesamiento de la información sobre el estado de un certificado

El certificador debe mantener procedimientos que aseguren la puesta a disposición de los suscriptores y usuarios, de información oportuna, completa y adecuada referida al estado de los certificados (incluida la emisión y publicación de Listas de Certificados Revocados y otros mecanismos referidos a dicho estado).

i) Estructura y contenido de los certificados y CRLs

El formato, codificación, contenido e interpretación de los certificados digitales y listas de certificados revocados (CRL) deben cumplir con los contenidos definidos en el **Anexo III- Perfil Mínimo de Certificados y Lista de Certificados Revocados**.

j) Mecanismos de acceso a la documentación publicada, certificados y CRLs

La información a publicar por el certificador en su sitio Web contendrá:

1.- Certificados

El certificador está obligado a publicar los certificados digitales de las autoridades certificantes correspondientes a las políticas de certificación que hayan sido licenciadas y el estado de cada uno de ellos.

2.- Información de estado de certificados

El certificador está obligado a publicar el estado de los certificados por él emitidos. Podrá hacerlo a través de una lista de certificados revocados o algún otro mecanismo que brinde dicha información.

3.- Publicación de documentos

El certificador está obligado a la publicación de las versiones vigentes y anteriores de la Política de Certificación y el Manual de Procedimientos de Certificación (en sus partes públicas), y las versiones vigentes del Resumen PC/MPC para suscriptores (en caso de existir), el acuerdo tipo con suscriptores y los términos y condiciones con terceros usuarios.

4.- Contactos

El certificador está obligado a la publicación de la información sobre la forma de comunicarse tanto con él mismo como con el ente licenciante. Debe proveer como mínimo: nombre, dirección de correo electrónico, número de teléfono y fax.

Periodicidad

El certificador es responsable de actualizar estas publicaciones periódicamente.

Seguridad

El certificador debe implementar mecanismos de seguridad para controlar el acceso a la información publicada y para prevenir accesos o modificaciones no autorizados.

Sección 3: Registro de eventos

El certificador debe mantener la confidencialidad e integridad de los registros de eventos actuales y archivados. Debe indicar los procedimientos utilizados para su tratamiento, registrando, de corresponder, la información y eventos que se indican a continuación para cada uno de ellos.

En el siguiente cuadro de descripción de eventos se entiende por "**entidad**" a toda persona física, jurídica, dispositivo o aplicación que intervenga en el proceso de certificación (tales como, AC, AR, suscriptor, tercero usuario, servidor de aplicación).

	Información Registrada
Contenido mínimos a registrar	a) Fecha y hora del registro. b) Número de serie o secuencia del registro. c) Tipo de registro. d) Fuente del registro (Ej.: terminal, puerto, etc.) e) Identificación de la entidad que efectuó el registro.
	Eventos a Registrar

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 criptográficas del certificador. d) Utilización de las claves criptográficas del certificador. e) Archivo de las claves criptográficas del certificador. f) Retiro de servicio de datos relacionados con las claves criptográficas. g) Destrucción de claves criptográficas del certificador. h) Identificación de la entidad que autoriza una operación de administración de claves criptográficas. i) Identificación de la entidad que administra los datos relativos a las claves criptográficas (tal como, los componentes de claves, o claves almacenadas en dispositivos criptográficos u otros medios). j) Compromiso de la clave privada.
Administración del ciclo de vida de los certificados	a) Recepción de solicitudes de certificados (inicial, de renovación y de generación de un nuevo par de claves). b) Transferencia de claves públicas para la emisión del certificado. c) Cambios en los datos de la solicitud del certificado. d) Generación de certificados. e) Distribución de la clave pública del certificador. f) Solicitudes de revocación de certificados. g) Generación y emisión de listas de certificados revocados. 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 aplicable.

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) Registro 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 sistema y responsables de seguridad. g) Cambios en la relación entre el certificador y sus AC con: • Sus Autoridades de Registro (AR) • 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 o a cualquiera de sus componentes.
	Observaciones generales
Información sensible	a) Los registros de eventos no deben reflejar los valores en texto plano de claves privadas o contraseñas.

Sincronización de eventos	a) Los relojes de las computadoras deben estar sincronizados con un desvío menor a un segundo para permitir un correcto registro de eventos, deben utilizar Hora Universal Coordinada (UTC) y estar configurados según el huso horario oficial de la Ciudad Autónoma de Buenos Aires, que actualmente es UTC-3. b) Toda información de horarios deberá estar expresada en formato: yyyy/mm/dd hh:mm:ss huso-horario.

Sección 4: Controles Físicos

Se deberán detallar los controles físicos referidos a las instalaciones de los sistemas de certificación.

a) Ubicación de las instalaciones

La ubicación de los sistemas de certificación de los certificadores licenciados no debe estar públicamente identificada. No debe haber ambientes compartidos que permitan la visibilidad de las operaciones críticas de emisión o revocación de certificados. Esas operaciones deberán ser realizadas en compartimentos cerrados, que no permitan visibilidad desde el exterior y estar físicamente protegidos.

Los certificadores licenciados deben detallar los aspectos de construcción de las instalaciones de la Autoridad Certificante, referidos a los controles de seguridad física.

b) Acceso Físico a las instalaciones

Todas las Autoridades Certificantes de los certificadores licenciados que componen la Infraestructura de Firma Digital de la República Argentina deberán implementar un sistema de control de acceso físico que garantice la seguridad de sus operaciones, debiendo contar con por lo menos cuatro niveles de acceso físico para llegar al ambiente donde residen los equipos de la Autoridad Certificante. Adicionalmente habrá dos niveles relacionados con la protección de elementos sensitivos vinculados a la clave privada de firma de la Autoridad Certificante.

1.- Nivel de acceso a instalaciones de la Autoridad Certificante

Debe estar ubicado detrás de la primera barrera de control de las instalaciones en donde se encuentre alojada la Autoridad Certificante. Para entrar a un área de este nivel, todo individuo deberá ser identificado y su ingreso registrado por personal autorizado. A partir de ese nivel, toda persona debe transitar con una adecuada identificación a la vista. En este nivel no podrán realizarse operaciones ni procesos administrativos de la Autoridad Certificante.

A partir de aquí, los equipos de grabación, fotográficos, de video, o similares, así como computadoras portátiles, tendrán su entrada registrada y sólo podrán ser utilizadas mediante autorización formal y supervisión.

2.- Nivel de acceso a procesos administrativos de la Autoridad Certificante

Debe ser interno al nivel anterior y deberá requerir, de la misma forma que el primero, la identificación individual de las personas que ingresan en él. Éste será el mínimo nivel de seguridad requerido para la realización de cualquier proceso administrativo de la Autoridad Certificante. El pasaje del primero al segundo nivel deberá exigir la identificación por medio electrónico y uso de tarjeta de identificación.

3.- Nivel operativo de la Autoridad Certificante

Deberá estar comprendido dentro del nivel anterior y será de uso exclusivo del certificador licenciado, en donde se podrán realizar actividades sensibles para las operaciones de la

Autoridad Certificante. Cualquier actividad relativa al ciclo de vida de los certificados digitales deberá ser cumplida a partir de este nivel. Las personas que no estén relacionadas con estas actividades no deberán tener permiso de acceso a este nivel. Las personas que no posean permisos de acceso no podrán permanecer en este nivel si no estuvieran acompañadas por personal autorizado.

En este nivel deberán ser controladas tanto las entradas como las salidas de cada persona. Para la identificación individual se requieren dos tipos distintos de mecanismos de control para la entrada y permanencia en este nivel, como tarjeta de identificación electrónica, contraseña de ingreso o identificación biométrica entre otras posibles.

Los teléfonos celulares, así como otros equipos portátiles de comunicación, excepto aquellos exigidos para las operaciones de la Autoridad Certificante no deberán ser admitidos en este nivel.

4.- Nivel de operaciones críticas de la Autoridad Certificante

Este nivel debe ser interior al nivel anterior, y aquí deberán realizarse todas las actividades sensibles vinculadas a las operaciones de la Autoridad Certificante tales como la emisión o revocación de certificados y la emisión de CRLs. Todos los sistemas y equipamientos necesarios para estas operaciones deberán estar ubicados a partir de este nivel.

Este nivel deberá tener los mismos controles de acceso físico del nivel anterior. Adicionalmente se debe exigir que las personas ajenas a este nivel ingresen acompañadas por al menos 2 personas expresamente autorizadas del certificador.

5.- Nivel de resguardo de elementos sensibles

Este nivel es interior al nivel anterior, y lo constituye una caja de seguridad o gabinete reforzado con cerradura antirrobo. El objetivo principal de este nivel es controlar el acceso a los compartimentos individuales que conforman el nivel siguiente.

6.- Nivel de resguardo de claves

Este nivel es interior al nivel anterior. Está constituido por compartimentos individuales localizados en el interior de la caja de seguridad o gabinete reforzado, cada uno de ellos con cerradura individual. Los datos de activación de la clave privada de la AC deberán estar almacenados en ellos.

Jefe de Gabinete de Ministros

6

131

ANEXO II

Infraestructura de Firma Digital – República Argentina

Ley Nº 25.506

Requisitos mínimos para políticas de certificación

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

CARACTERISTICAS DEL DOCUMENTO

Este documento describe la estructura y los requisitos mínimos que deben cumplir las Políticas de Certificación (PC) de las entidades que soliciten una licencia en el marco de la Infraestructura de Firma Digital de la República Argentina (IFDRA), en los términos de la Ley N° 25.506 de firma digital. Para su elaboración se han tenido en cuenta los lineamientos del RFC 2527, producido por el IETF, el estándar X9.79 de la ANSI (Cap. A), la especificación ITU-T X.509, el estándar ISO 3166 y las recomendaciones RFC 3280 y 3739.

El presente documento establece el formato y los contenidos mínimos para las Políticas de Certificación de los certificadores, las cuales deben ser presentadas ante el ente licenciante para ser sometidas al proceso de licenciamiento.

La Política de Certificación debe estar redactada en idioma castellano y no deben utilizarse siglas o términos que no puedan ser interpretados por usuarios finales. En caso de ser necesario incluir términos en idioma extranjero, dada su aceptación generalizada, deberá incluirse también su significado en idioma castellano.

Las Políticas de Certificación emitidas de los certificadores deben respetar la estructura y ordenamiento (el índice) del presente documento.

Jefe de Gabinete de Ministros

FOLIO 133

INDICE

FOLIO 134

Jefe de Gabinete de Ministros

FOLIO 135

1. - INTRODUCCION

1.1. - Descripción general

Contendrá una introducción a la Política de Certificación.

1.2. - Identificación

Se incluirá la identificación de la Política de Certificación, incorporando información tal como: versión, revisión, fecha de aplicación, lugar o sitio de publicación, etc. e incluirá el identificador de objeto (OID) correspondiente a la Política cuando le sea otorgado por el ente licenciante de manera tal que permita una identificación apropiada.

1.3. - Participantes y aplicabilidad

Se incluirán las distintas entidades que cumplen roles con relación al certificado y cuya integración se encuentre prevista para el cumplimiento de la actividad de certificación.

1.3.1. - Certificador

Se identificará al certificador que presenta la Política de Certificación.

1.3.2. - Autoridad de Registro

Se identificarán las Autoridades de Registro propias o de terceros, utilizadas por el certificador en el proceso de recepción de solicitudes de emisión de certificados, identificación y autenticación de la identidad de los solicitantes de certificados y recepción y validación de solicitudes de revocación. Se deberá indicar el domicilio de cada una de ellas.

1.3.3. - Suscriptores de certificados

Se indicará la comunidad de usuarios (personas físicas o jurídicas) o el tipo de aplicaciones informáticas a quienes se destinarán los certificados emitidos por el certificador.

1.3.4. - Aplicabilidad

Se incluirá la lista de usos o aplicaciones para los que resulten adecuados los certificados emitidos por el certificador, así como de aquellos usos o aplicaciones para las que se prohíba o limite su empleo.

1.4. - Contactos

Se incluirán los datos de un responsable del certificador para actuar como nexo incluyendo como mínimo nombre, dirección de correo electrónico, número de teléfono y fax.

Además debe incluir los datos del responsable del registro, mantenimiento e interpretación de la Política.

2. - ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACIÓN

Se indicarán las disposiciones referidas a las obligaciones del certificador y otros participantes respecto al mantenimiento de repositorios, publicación de certificados y de información sobre sus políticas y procedimientos.

2.1. - Obligaciones

2.1.1. - Obligaciones del certificador

Contendrá como mínimo una descripción detallada de las previsiones para el cumplimiento de:

a) Las obligaciones establecidas en el artículo 21 de la Ley N° 25.506

b) Las obligaciones establecidas en los artículos 34 y 36 del Decreto N° 2628/02

c) La obligatoriedad de notificar a sus suscriptores ante cualquier acontecimiento que pudiera ocasionar el compromiso de su clave privada y la generación de un nuevo par de claves

d) La obligatoriedad de notificar a sus suscriptores y al ente licenciante acerca del cese de sus actividades

e) La obligatoriedad de emitir y distribuir los certificados a sus suscriptores, informándolos acerca de dicha emisión

f) Las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes Anexos

2.1.2. - Obligaciones de la Autoridad de Registro

Incluirá las obligaciones de las Autoridades de Registro operativamente vinculadas al certificador, conteniendo como mínimo:

a) Las obligaciones establecidas en el artículo 35 del Decreto N° 2628/02

b) La obligación de proteger sus claves privadas.

2.1.3. - Obligaciones de los suscriptores de los certificados

Se informarán las obligaciones de los suscriptores de certificados emitidos de acuerdo a lo dispuesto en el marco legal aplicable y sobre la base de las características de la actividad de certificación a desarrollar, conteniendo como mínimo:

a) Las obligaciones establecidas en el artículo 25 de la Ley N° 25.506

b) La obligación de proveer de modo completo y preciso toda la información necesaria para la emisión del certificado

c) La obligación de utilizar sus certificados de forma adecuada, conforme a lo previsto en la Política de Certificación

d) La obligación, como suscriptor de un certificado, de tomar conocimiento de los derechos y obligaciones que se establezcan en la "Política de Certificación", en el "Manual de Procedimientos de Certificación" (en sus aspectos no confidenciales), en el "Acuerdo del Suscriptor" y en todo documento aplicable.

2.1.4. - Obligaciones de los terceros usuarios

Se informarán las obligaciones de los terceros usuarios, incluyendo como mínimo:

a) La obligación de conocer los alcances de la Política de Certificación conforme los "Términos y condiciones con terceros usuarios".

b) La obligación de rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda y de usarlo conforme a los "Términos y condiciones con terceros usuarios".

c) La obligación de verificar la validez del certificado.

2.1.5. - Obligaciones del servicio de repositorio

Para la provisión de los servicios de repositorio, se informarán:

a) Las obligaciones establecidas en el artículo 21 inc. k) de la Ley N° 25.506

b) Las obligaciones establecidas en el artículo 34 incisos g), h) y m) del Decreto N° 2628/02.

c) La obligación de disponer y dedicar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y legal.

2.2. - Responsabilidades

Siempre que sea aplicable, y sin perjuicio de lo determinado por la ley 25.506 al respecto, debe detallarse:

a) Las garantías y sus limitaciones

b) Los tipos de daños cubiertos y las limitaciones de responsabilidad

c) Los límites de cobertura por certificado o por transacción.

2.3. - Responsabilidad Financiera

2.3.1. - Responsabilidad financiera del certificador

Se incluirán las cláusulas que establezcan la responsabilidad por los daños ocasionados a suscriptores de certificados y a terceros usuarios, en razón del incumplimiento de lo dispuesto en las normas legales y reglamentarias y en la Política de Certificación.

En caso de existir seguros de responsabilidad civil debe proveerse información que los respalde.

2.4. - Interpretación y aplicación de las normas

2.4.1. - Legislación aplicable

Se especificará la legislación que respalda la interpretación, aplicación y validez de la Política de Certificación, debiendo indicarse la Ley N° 25.506, el Decreto N° 2628/02, y toda otra norma complementaria dictada por la autoridad competente.

2.4.2. - Forma de Interpretación y aplicación

Se determinarán los procedimientos a seguir en el caso de que existan conflictos respecto a la interpretación de una o más disposiciones de la Política de Certificación.

En esta sección deberá indicarse que el suscriptor o los terceros usuarios podrán accionar ante el ente licenciante, previo agotamiento del procedimiento ante el certificador licenciado

correspondiente, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

2.4.3. - Procedimientos de resolución de conflictos

Deberán indicarse los procedimientos de resolución de conflictos en la Política de Certificación y en los acuerdos en los que el certificador sea parte.

Asimismo, se establecerá que, en ningún caso, la Política de Certificación del certificador prevalecerá sobre lo dispuesto por la normativa vigente de firma digital.

2.5. - Aranceles

Cuando resulte aplicable, se describirán los aranceles asociados a cada uno de los servicios que preste el certificador, relacionados con la Política de Certificación.

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

2.6.1. - Publicación de información del certificador

Se indicará la información a ser publicada por el certificador en el repositorio, la forma, condiciones de acceso y modalidades en que se la pondrá a disposición de terceros.

Debe respetarse lo establecido en el **Anexo I Sección 2** respecto de la información que el certificador debe publicar.

2.6.2. - Frecuencia de publicación

Se indicará la frecuencia de actualización del repositorio. Se garantizará su actualización inmediata después de que la información a incluir se encuentre disponible.

2.6.3. - Controles de acceso a la información

Se incluirán los controles y eventuales restricciones que se impondrán al acceso a la información publicada por el certificador. Se garantizará el acceso al certificado del certificador, a la Lista de Certificados Revocados, a la Política de Certificación correspondiente y a su Manual de Procedimientos, excepto en sus aspectos confidenciales, en sus versiones anteriores y actualizadas.

2.6.4. - Repositorios de certificados y listas de revocación

Se indicarán las entidades que administran los repositorios, indicando si el servicio es propio del certificador o si es provisto por un tercero. En este último caso, se lo identificará y se indicarán las condiciones del servicio.

2.7. - Auditorías

Este componente indicará aspectos específicos del proceso de auditoria, como ser:

a) Denominación de la entidad de auditoría

b) Frecuencia de realización de las auditorías

c) Temas principales a evaluar en las auditorías

d) Medidas a adoptar en caso de dictámenes no favorables

e) Modalidad de comunicación de los informes de auditoría

Son obligatorias las exigencias reglamentarias impuestas por:

a) El artículo 21 Inc. k) de la Ley N° 25.506, relativo a la publicación de informes de auditoria.

b) El artículo 20 del Decreto N° 2628/02, relativos a conflictos de interés.

2.8. -Confidencialidad

Todos los aspectos de confidencialidad de la información estarán sujetos a la normativa vigente en materia de Protección de Datos Personales.

2.8.1. - Información confidencial

Se especificará la información a ser tratada como confidencial por el certificador y por las Autoridades de Registro operativamente vinculadas, de acuerdo con lo establecido por las normas legales y reglamentarias aplicables vigentes.

Como principio general, se establecerá que toda información remitida por el suscriptor de un certificado al momento de efectuar un requerimiento debe ser considerada confidencial y no debe ser divulgada a terceros sin el consentimiento previo del suscriptor, salvo que sea requerida en causa judicial por juez competente. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso el certificador o la Autoridad de Registro durante el ciclo de vida del certificado.

2.8.2. - Información no confidencial

Se especificará la información a ser tratada como no confidencial por el certificador y por las Autoridades de Registro vinculadas operativamente. Se entiende como tal lo siguiente:

a) Contenido de los certificados y de las listas de certificados revocados

b) Información sobre personas físicas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público

c) Políticas de Certificación y Manual de Procedimientos de Certificación, en sus aspectos no confidenciales

d) Versiones públicas de la Política de Seguridad del certificador

e) Política de privacidad del certificador

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

Se deberá considerar como no confidencial la información sobre la revocación de un certificado.

Se deberá informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

2.8.4. - Divulgación de información a autoridades judiciales

Se describirán las condiciones bajo las cuales el certificador deberá revelar información confidencial o privada, si le es requerida judicialmente.

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

Se describirán las condiciones bajo las cuales el certificador deberá revelar información confidencial si es requerida en el marco de procesos judiciales, administrativos u otros procesos legales, tales como citaciones, interrogatorios, solicitud de pruebas, audiencia de posiciones etc.

2.8.6. - Divulgación de información por solicitud del suscriptor

Se describirán las condiciones bajo las cuales el suscriptor del certificado o su representante legal debidamente acreditado podrán tener acceso a sus datos de identificación u otras informaciones generadas durante el ciclo de vida del certificado.

2.8.7. - Otras circunstancias de divulgación de información

En caso de existir otras circunstancias bajo las cuales podrá divulgarse la información anteriormente referida, se deberán describir en este apartado.

2.9. - Derechos de Propiedad Intelectual

Se incluirán especificaciones acerca de los derechos de propiedad intelectual, derechos de autor y patentes relacionadas con los documentos elaborados por el certificador, así como de nombres o claves criptográficas y otras herramientas, de acuerdo con la legislación vigente.

3. - IDENTIFICACION Y AUTENTICACION

3.1. - Registro inicial

Se describirán los procedimientos a utilizar para autenticar, como paso previo a la emisión de un certificado, la identidad y demás atributos del solicitante que se presente ante el certificador o a la Autoridad de Registro operativamente vinculada. Se establecerán los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

El certificador debe cumplir con lo establecido en:

a) El artículo 21 inc. a) de la Ley N° 25.506 y el artículo 34 inc. e) del Decreto N° 2628/02 relativos a la información a brindar a los solicitantes.

b) El artículo 14 inc. b) de la Ley N° 25.506 relativo a los contenidos mínimos de los certificados.

3.1.1. - Tipos de Nombres

Se describirán los tipos de nombres admitidos para los suscriptores de certificados emitidos en función de la Política de Certificación.

3.1.2. - Necesidad de Nombres Distintivos

Se describirán las distintas denominaciones que se utilicen para cada tipo de certificado, debiendo utilizarse como mínimo:

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

- "*commonName*" (OID 2.5.4.3: Nombre común): en caso de existir DEBE corresponder al nombre del servicio (ej. Servicio de Fechado Digital) o al nombre de la unidad operativa responsable del servicio (ej. Unidad de Certificación Digital).
- "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener a las unidades operativas relacionadas con el servicio, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- "*organizationName*" (OID 2.5.4.10: Nombre de la organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio.
- "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

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

"CUIT": Clave única de identificación tributaria para las Personas Jurídicas argentinas.

Para los certificados de **Personas Físicas**:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponder con el nombre que figura en el documento de identidad del suscriptor (DNI, Pasaporte, ...)

- "*serialNumber*" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el tipo y número de documento del titular, expresado como texto y respetando el siguiente formato y codificación: "[tipo de documento]" "[nro. de documento]"

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

- En caso de ciudadanos argentinos o residentes:
  - a) "DU": Documento nacional de identidad
  - b) "LE": Libreta de enrolamiento
  - c) "LC": Libreta cívica
  - d) "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral
- En caso de extranjeros:
  - a) "PA "[país]: Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.
  - b) "EX "[país]: En caso de documento extranjero. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

- "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la suborganización) y "*organizationName*" (OID 2.5.4.10: Nombre de la organización): PUEDEN ser utilizados para guardar la información relativa a la Organización a la cual el suscriptor se encuentra asociado (se deben respetar los criterios definidos para los atributos "*organizationName*" y "*organizationalUnitName*" de personas Jurídicas Públicas o Privadas). El tipo de asociación entre la Organización y el suscriptor debe ser evaluado a partir de la Política de Certificación.

- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar la nacionalidad de la persona física.

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

- *"commonName"* (OID 2.5.4.3: Nombre común): en caso de existir DEBE corresponder al nombre del servicio o aplicación (ej. Sistema de Consulta) o al nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).
- *"organizationalUnitName"* (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener a las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- *"organizationName"* (OID 2.5.4.10: Nombre de la organización): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada.
- *"serialNumber"* (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

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

a) "CUIT": Clave única de identificación tributaria para las Personas Jurídicas argentinas.

b) "ID "[país]: Número de identificación tributario para Personas Jurídicas extranjeras.

El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

- *"countryName"* (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país en el cual está constituida la Persona Jurídica.

En caso de existir información no verificada incluida en el certificado DEBE informarse esta situación utilizando algún campo descriptivo del certificado. Para ello se RECOMIENDA el empleo del atributo *"description"* (OID 2.5.4.13: Descripción).

3.1.3. - Reglas para la interpretación de nombres

Se incluirán las reglas para interpretar los nombres distintivos admitidos por la Política de Certificación.

3.1.4. - Unicidad de nombres

Debe especificarse que el nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias deberá estar basado en la utilización del número de documento de identidad en el caso de personas físicas o el número de identificación tributaria en el caso de personas jurídicas.

3.1.5. - Procedimiento de resolución de disputas sobre nombres

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

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

Se indicará que no se podrán incluir marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados de persona jurídica.

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

Se indicarán los procedimientos que implementarán el certificador o la Autoridad de Registro operativamente vinculada para asegurar que el solicitante se encuentra en posesión de la clave privada correspondiente a la clave pública remitida con el requerimiento del certificado digital, de acuerdo a protocolos de seguridad adecuados y que dicha clave privada es apta para firmar un documento digital.

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

Se describirán los procedimientos de autenticación de la identidad de los suscriptores o responsables de los certificados de personas jurídicas públicas o privadas, debiendo indicarse por lo menos que:

a) El requerimiento deberá efectuarse únicamente por intermedio de un representante autorizado a actuar en nombre del suscriptor.

b) El certificador o la Autoridad de Registro con la que se encuentre operativamente vinculada verificará la identidad del representante del suscriptor y su autorización para utilizar las claves criptográficas en su nombre.

c) El representante autorizado del suscriptor deberá validar su identidad según lo dispuesto en el apartado siguiente.

d) La identidad de la persona jurídica deberá ser verificada mediante documentación que acredite su personería jurídica.

e) Se podrá requerir información de registros oficiales o contratar los servicios de terceros a fin de efectuar la verificación mencionada.

Deben considerarse obligatorias las exigencias reglamentarias impuestas por:

a) El artículo 21 inc. i) de la Ley N° 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21 inc. f) de la Ley N° 25.506 relativo a la recolección de datos personales.

c) El artículo 34 inc. m) del Decreto N° 2628/02 relativo a la protección de datos personales.

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

Adicionalmente, el certificador debe registrar un acuerdo firmado con el suscriptor incluyendo el "Acuerdo del Suscriptor" y la confirmación, por parte del responsable, de que la información incluida en el certificado es correcta.

3.1.9. - Autenticación de la identidad de personas físicas

Se describirán los procedimientos de autenticación de la identidad de los suscriptores de los certificados de personas físicas.

Se exigirá la presencia física del suscriptor del certificado ante el certificador o la Autoridad de Registro con la que se encuentre operativamente vinculada. La verificación se efectuará mediante la presentación de los siguientes documentos:

- De poseer nacionalidad argentina, se requerirá Documento Nacional de Identidad, Libreta de Enrolamiento o Libreta Cívica.
- De tratarse de extranjeros, se requerirá Documento Nacional de Identidad Argentino, Cédula de Identidad Argentina o Pasaporte válido.

En todos los casos, se establecerá la obligatoriedad de la conservación de la documentación de respaldo del proceso de autenticación por parte del certificador o de la Autoridad de Registro operativamente vinculada. Se incluirá la obligatoriedad de la conservación de la información referida al solicitante que no hubiera sido verificada, destacándose dicha condición.

Deben considerarse obligatorias las exigencias reglamentarias impuestas por:

a) El artículo 21 inc. i) de la Ley N° 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21 inc. f) de la Ley N° 25.506 relativo a la recolección de datos personales.

c) El artículo 34 inc. i) del Decreto N° 2628/02 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

d) El artículo 34 inc. m) del Decreto N° 2628/02 relativo a la protección de datos personales.

Adicionalmente, el certificador debe celebrar un acuerdo con el suscriptor y recibir de éste la conformidad de que la información incluida en el certificado es correcta.

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

Se especificarán los procedimientos de identificación y autenticación de la identidad del suscriptor, a seguir para la generación de un nuevo par de claves y su correspondiente certificado:

a) después de la revocación de un certificado por compromiso de claves

b) después de la expiración de un certificado, si la Política de Certificación exigiera que no se use el mismo par de claves

La solicitud del nuevo certificado exigirá el cumplimiento de procedimientos equivalentes a los previstos para el proceso de registro inicial.

Todo cambio a la política de certificación debe ser comunicado al suscriptor y éste debe expresar su consentimiento.

Si alguna información relativa al suscriptor ha sido cambiada, debe ser verificada y registrada.

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

Se establecerán los procedimientos a seguir para validar la identidad del solicitante cuando:

a) Se solicita un nuevo certificado vinculado a uno anterior previamente revocado, sin que hubiera compromiso del par de claves correspondiente.

b) Se solicita un nuevo certificado vinculado a uno anterior que se encuentra expirado, permitiendo la Política de Certificación el uso del mismo par de claves.

El certificador sólo debe emitir un nuevo certificado utilizando una clave pública existente si no hay evidencia de que la correspondiente clave privada ha sido comprometida y el período de vida del par de claves no ha expirado. El certificador debe informar el período de vida del par de claves si correspondiese.

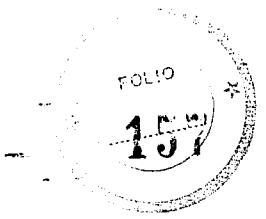
Un certificado revocado cuya clave privada se encuentre comprometida no podrá ser renovado con el mismo par de claves. La solicitud de un nuevo certificado exigirá el cumplimiento de procedimientos equivalentes a los previstos para el proceso de registro inicial.

El certificador debe controlar la existencia y validez del certificado y que la información utilizada para verificar la identidad y atributos del suscriptor sea aún válida.

Todo cambio a la política de certificación debe ser comunicado al suscriptor y éste debe expresar su consentimiento.

Si alguna información relativa al suscriptor ha sido cambiada, debe ser verificada y registrada.

3.4. - Requerimiento de revocación



Se incluirán los procedimientos a seguir para validar la identidad del solicitante de la revocación de un certificado, incluyendo la documentación del proceso.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

Se incluirán los requisitos y procedimientos operativos establecidos por el certificador para recibir los requerimientos de certificados. Estos procedimientos deberán ser cumplidos por el certificador o por la Autoridad de Registro operativamente vinculada y por los solicitantes de certificados.

Adicionalmente, en esta sección debe incluirse una descripción de los procedimientos utilizados para comprobar que el suscriptor se encuentra en poder de la clave privada correspondiente a la clave pública presentada para la generación del certificado.

Los procedimientos deben establecer que los requerimientos sólo podrán ser iniciados por el solicitante o por el representante autorizado de la persona jurídica solicitante.

4.2. - Emisión del certificado

Se establecerán los requisitos y procedimientos establecidos por el certificador para la emisión del certificado y para la notificación de dicha emisión al solicitante.

Adicionalmente, se deberán establecer las condiciones bajo las cuales se determinará la fecha de inicio del periodo de validez del certificado.

4.3. - Aceptación del certificado

Se establecerán los requisitos y procedimientos referidos a la publicación del certificado y a su aceptación por el suscriptor.

4.4. - Suspensión y Revocación de Certificados

El certificador debe asegurar que los certificados sean revocados de manera oportuna y sobre la base de una solicitud de revocación de certificado validada.

Se deberá informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

4.4.1. - Causas de revocación

Se indicarán las circunstancias bajo las cuales un certificado podrá ser revocado y aquellos casos en los cuales la revocación deberá ser obligatoria, conteniendo como mínimo una descripción detallada de:

a) Las obligaciones establecidas en el artículo 19 inc. e) de la Ley N° 25.506

b) Las obligaciones establecidas en el artículo 23 del Decreto N° 2628/02

c) Las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes Anexos (citado en el **Anexo I – Sección 2**)

Asimismo, se especificará que el certificador deberá revocar, en un plazo definido, todo certificado que deje de cumplir con las políticas y normas legales y reglamentarias de la Infraestructura de Firma Digital de la República Argentina (IFDRA).

4.4.2. - Autorizados a solicitar la revocación

Se especificará quiénes son las personas autorizadas para solicitar la revocación de un certificado, debiendo admitirse como mínimo:

a) Al suscriptor del certificado

b) Al responsable autorizado que efectuara el requerimiento, en el caso de certificados de personas jurídicas

c) A la persona jurídica suscriptora del certificado a través de un funcionario debidamente autorizado

d) A aquellas personas habilitadas por el suscriptor del certificado a tal fin.

e) Al certificador o la Autoridad de Registro operativamente vinculada.

f) Al ente licenciante.

g) A la autoridad judicial competente

4.4.3. - Procedimientos para la solicitud de revocación

Se describirán los procedimientos establecidos por el certificador para la revocación de los certificados que emita. Se garantizará que los procedimientos de revocación se encontrarán disponibles en su Política de Certificación, a disposición de los autorizados indicados en el apartado anterior.

Se deberá garantizar que:

a) El solicitante de la revocación será debidamente identificado según se establece en el apartado 3.4

b) Las solicitudes de revocación, así como toda acción efectuada por el certificador o la Autoridad de Registro en el proceso, serán documentadas y conservadas en sus archivos

c) Se documentarán y archivarán las justificaciones de las revocaciones aprobadas

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

e) El suscriptor del certificado revocado deberá ser informado del cambio de estado de su certificado

Deberán indicarse las vías de contacto disponibles para la realización de la solicitud de revocación.

4.4.4. - Plazo para la solicitud de revocación

Se especificará que la solicitud de revocación deberá efectuarse en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado **4.4.1**.

El servicio de recepción de solicitudes de revocación deberá estar disponible en forma permanente (7x24 horas) cumpliendo con lo establecido en el artículo 34 inc. f) del Decreto Nº 2628/02.

El plazo entre la recepción de la solicitud y el cambio de la información de estado del certificado indicando la revocación puesta a disposición de los terceros usuarios debe ser a lo sumo de 24 horas.

4.4.5. - Causas de suspensión

Se deberá informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

4.4.6. - Autorizados a solicitar la suspensión

Se deberá informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

4.4.7. - Procedimientos para la solicitud de suspensión

Se deberá informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

4.4.8. - Límites del periodo de suspensión de un certificado

Se deberá informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

4.4.9. - Frecuencia de emisión de listas de certificados revocados

Se especificará la frecuencia con que se emitirá la lista de certificados revocados asociada a la Política de Certificación.

Para aquellas correspondientes a certificados de personas físicas, personas jurídicas y aplicaciones las Listas de Certificados Revocados deben emitirse como mínimo cada 24 horas.

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

Se establecerá que los terceros usuarios deberán validar el estado de los certificados, mediante el control de la lista de certificados revocados, a menos que utilicen otro sistema con características de seguridad y confiabilidad por lo menos equivalentes.

Asimismo, se especificará que la autenticidad y validez de la lista de certificados revocados también deberá ser confirmada mediante la verificación de la firma digital del certificador que la emite y de su período de validez.

El certificador está obligado a cumplir con lo establecido en el artículo 34 inc. g) del Decreto N° 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes Anexos.

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

La verificación del estado de un certificado podrá efectuarse directamente ante el certificador por medio del acceso a la lista de certificados revocados o de otros medios de verificación de estado en línea.

Se informarán los detalles del servicio de consulta de la lista de certificados revocados. Si el certificador ofrece adicionalmente el servicio de verificación en línea del estado de certificados, deberá informarlo.

El certificador debe poner a disposición de los terceros usuarios:

a) la información relativa a las características de los servicios de verificación de estado

b) la disponibilidad de tales servicios y los procedimientos que se seguirán en caso de no disponibilidad

c) todas las características opcionales de tales servicios

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

Se establecerán los requisitos para la verificación en línea de la información de revocación de certificados por parte de los terceros usuarios.

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

Se describirán, en caso de existir, otras formas utilizadas por el certificador para divulgar la información sobre revocación de certificados.

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

Se establecerán los requisitos para la verificación en línea por parte de los terceros usuarios, de las formas de divulgación de revocación de certificados previstas en el apartado anterior.

4.4.15. - Requisitos específicos para casos de compromiso de claves

Se establecerán los requerimientos específicos aplicables a la revocación de certificados provocada por el compromiso de la correspondiente clave privada. En tal caso, se exigirá que el suscriptor del certificado comunique de inmediato tal circunstancia al certificador.

4.5. - Procedimientos de Auditoría de Seguridad

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

Debe respetarse lo establecido en el **Anexo I Sección 3** respecto del registro de eventos.

4.6. - Archivo de registros de eventos

Se incluirán las políticas de conservación de registros, cuyos procedimientos detallados serán desarrollados en el Manual de Procedimientos.

Los procedimientos deben cumplir con lo establecido por el artículo 21 inc. i) de la Ley N° 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

Debe respetarse lo establecido en el **Anexo I Sección 3** respecto del registro de eventos.

4.7. - Cambio de claves criptográficas

Se incluirán los procedimientos a seguir para distribuir una nueva clave pública a los usuarios de un certificador luego de un cambio de claves. Dichos procedimientos pueden ser los mismos que fueron utilizados para distribuir la clave que se reemplaza. La nueva clave puede ser incluida en un certificado firmado digitalmente con la clave que será reemplazada, salvo que esta última esté comprometida.

4.8. - Plan de contingencia y recuperación ante desastres

Se describirán los requerimientos relativos a la recuperación de recursos del certificador en caso de falla o desastre. Estos requerimientos serán desarrollados en su Plan de Contingencia.

Se incluirán procedimientos referidos a:

a) Recuperación ante falla o sospecha de falla de componentes de hardware, software y datos

b) Revocación del certificado del certificador

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

d) Continuidad de las operaciones en un entorno seguro luego de desastres naturales o de otra naturaleza

e) Identificación, registro, reporte y manejo de incidentes

Los procedimientos deben cumplir con lo establecido por el artículo 33 del Decreto N° 2628/02 en lo relativo a los servicios de infraestructura tecnológicos prestados por un tercero.

4.9. - Plan de Cese de Actividades

Se describirán los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del certificador. Estos requerimientos serán desarrollados en su Plan de Cese de Actividades.

Se especificarán los procedimientos referidos a:

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

b) Revocación del certificado del certificador y de los certificados emitidos

c) Transferencia de la custodia de archivos y documentación

Se establecerá que el responsable de la custodia de archivos y documentación cumplirá con idénticas exigencias de seguridad que las previstas para el certificador que cesó.

Deberá contemplarse lo establecido por el artículo 22 del la Ley N° 25.506 en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos deben cumplir con lo dispuesto por el artículo 33 del Decreto N° 2628/02 en lo relativo a los servicios de infraestructura tecnológicos prestados por un tercero y las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes Anexos.

5. - CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

Se describirán brevemente los procedimientos referidos a los controles de seguridad física, funcionales y personales implementados por el certificador. La descripción detallada se efectuará en el Plan de Seguridad.

5.1. - Controles de seguridad física

Se incluirán referencias a los siguientes aspectos:

a) Construcción y ubicación de instalaciones

b) Niveles de acceso físico

c) Energía y aire acondicionado

d) Exposición al agua

e) Prevención y protección contra incendios

f) Medios de almacenamiento

g) Disposición de material de descarte

h) Instalaciones de seguridad externas

5.2. - Controles Funcionales

Se incluirán referencias a los siguientes temas:

a) Definición de roles afectados al proceso de certificación

b) Separación de funciones

c) Número de personas requeridas por función

d) Identificación y autenticación para cada rol

5.3. - Controles de seguridad del personal

Se especificarán los controles implementados sobre los siguientes aspectos:

a) Antecedentes laborales, calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, seguridad, limpieza, etc.

b) Entrenamiento y capacitación inicial

c) Frecuencia de procesos de actualización técnica

d) Frecuencia de rotación de cargos

e) Sanciones a aplicar por acciones no autorizadas

f) Requisitos para contratación de personal

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

6. - CONTROLES DE SEGURIDAD TECNICA

Se describirán las medidas de seguridad implementadas por el certificador para proteger sus claves criptográficas y otros parámetros de seguridad críticos. Además se incluirán los controles técnicos que se implementarán sobre las funciones operativas del certificador, Autoridades de Registro, repositorios, suscriptores, etc.

6.1. - Generación e instalación del par de claves criptográficas

La generación e instalación del par de claves deben ser consideradas desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro y de los suscriptores. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Responsables de la generación de claves

b) Métodos de generación de claves, indicando si se efectúan por software o por hardware

c) Métodos de entrega de la clave pública de la entidad al certificador en forma segura

d) Métodos de distribución de la clave pública del certificador en forma segura

e) Características y tamaños de las claves y controles efectuados sobre ellas

f) Propósitos para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización

6.1.1. - Generación del par de claves criptográficas

Se describirán todos los aspectos relativos a la generación del par de claves del certificador, de las claves de los responsables de las Autoridades de Registro, y de las claves de los suscriptores.

Debe respetarse lo establecido en el **Anexo I Sección 2** respecto de generación del par de claves.

6.1.2. - Entrega de la clave privada al suscriptor

Deben considerarse las exigencias reglamentarias impuestas por la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firmas de los suscriptores, establecido por la Ley N° 25.506 Art. 21 inc. b) y el Decreto N° 2628/02 Art. 34 inc. i).

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

Se establecerán los procedimientos utilizados para la entrega de la clave pública del suscriptor del certificado al certificador responsable de su emisión.

6.1.4. - Disponibilidad de la clave pública del certificador

Se describirán los medios adoptados para poner el certificado del certificador, y el resto de los certificados que compongan su cadena de certificación, a disposición de todos los suscriptores y terceras partes pertinentes.

6.1.5. - Tamaño de claves

Se definirá el tamaño de las claves criptográficas asociadas con los certificados emitidos según la Política de Certificación.

Debe respetarse lo establecido en el **Anexo I Sección 2** respecto de las longitudes mínimas de las claves.

6.1.6. - Generación de parámetros de claves asimétricas

Se deberán describir los parámetros de generación de claves asimétricas.

6.1.7. - Verificación de calidad de los parámetros

Se deberán describir los procedimientos utilizados para verificar la calidad de los parámetros de generación de claves.

6.1.8. - Generación de claves por hardware o software

Se deberá describir el tipo de soporte utilizado para la generación de claves.

Debe respetarse lo establecido en el **Anexo I Sección 2** respecto de la generación del par de claves.

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

Se establecerán los propósitos para los cuales se utilizarán las claves criptográficas de los suscriptores de los certificados y las posibles restricciones en su uso.

6.2. - Protección de la clave privada

La protección de la clave privada debe ser considerada desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro y de los suscriptores. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Estándares utilizados para la generación del par de claves

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

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

d) En caso de encontrarse archivada la clave privada, modalidad utilizada

e) Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico

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

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

h) Procedimiento de destrucción de la clave privada

6.2.1. - Estándares para dispositivos criptográficos

Se describirán las características de los dispositivos utilizados para la generación y almacenamiento de claves criptográficas.

Debe respetarse lo establecido en el **Anexo I Sección 2** respecto de los estándares para dispositivos criptográficos.

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

Se describirán los controles empleados para la activación de las claves, indicando cuántas personas están involucradas en el control de dicha clave (esquema **M** de **N**).

Debe respetarse lo establecido en el **Anexo I Sección 2** respecto de la utilización de las claves privadas.

6.2.3. - Recuperación de clave privada

Se describirán los procedimientos empleados por el certificador para la recuperación de sus propias claves.

6.2.4. - Copia de seguridad de clave privada

Se describirán los procedimientos y controles de seguridad empleados para la realización de copias de seguridad de las claves privadas del certificador.

En todos los casos deben establecerse procedimientos que garanticen que los niveles de seguridad de las claves no disminuyan por la creación de copias de resguardo.

6.2.5. - Archivo de clave privada

Se describirán los procedimientos y controles de seguridad empleados para el archivo de las claves privadas del certificador.

En todos los casos deben establecerse procedimientos que garanticen que los niveles de seguridad de las claves no disminuyan por el proceso de archivo.

6.2.6. - Incorporación de claves privadas en dispositivos criptográficos

Se describirán los procedimientos para que un suscriptor incorpore su clave privada en un dispositivo criptográfico, detallando bajo qué circunstancias se puede realizar la operación, a quiénes está permitido realizarla y cuál es el formato de la clave privada utilizado durante la transferencia.

6.2.7. - Método de activación de claves privadas

Se describirán los requisitos y procedimientos necesarios para la activación de la clave privada del certificador.

Se exigirá la autenticación de la identidad de los responsables a través de métodos adecuados.

6.2.8. - Método de desactivación de claves privadas

Se describirán los requisitos y procedimientos necesarios para la desactivación de la clave privada del certificador.

Se exigirá la autenticación de la identidad de los responsables a través de métodos adecuados.

6.2.9. - Método de destrucción de claves privadas

Se especificarán los procedimientos a seguir para la destrucción segura de la clave privada y de sus copias de seguridad ante cualquier hecho que motivara el final de la vida útil de un certificado, tales como su revocación o expiración. Se identificarán los responsables de la destrucción, formas de autenticación y acciones a desarrollar.

6.3. - Otros aspectos de administración de claves

6.3.1. - Archivo permanente de la clave pública

El archivo de la clave pública debe ser considerado desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro y de los suscriptores.

Se describirán los procedimientos y controles de seguridad implementados para archivar la clave pública, incluyendo el software y hardware que se deberá preservar, para permitir la posterior utilización de esa clave. Esta sección debe indicar, además, los controles de integridad a utilizar para impedir la adulteración de las claves archivadas. Dichos controles deben incluir mecanismos adicionales a fin de evitar que esas claves sean alteradas durante un período de almacenamiento que puede ser mayor que el período de criptoanálisis de las claves.

6.3.2. - Período de uso de clave pública y privada

Se determinará que las claves privadas correspondientes a los certificados emitidos por el certificador podrán ser utilizadas por su suscriptor únicamente durante el período de validez de los certificados. Las correspondientes claves públicas podrán ser utilizadas durante el período establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su período de validez, según se establece en el apartado anterior.

6.4. - Datos de activación

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

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

6.4.1. - Generación e instalación de datos de activación

Se garantizará que los datos de activación de la clave privada de los suscriptores de certificados sean únicos y generados en forma aleatoria.

6.4.2. - Protección de los datos de activación

Se deben indicar los procedimientos para garantizar la adecuada protección de los datos de activación contra usos no autorizados.

6.4.3. - Otros aspectos referidos a los datos de activación

Se deben incluir controles sobre la protección de los datos de activación, similares a los relacionados con las claves, como se indica en los apartados **6.1** a **6.3**.

6.5. - Controles de seguridad informática

6.5.1. - Requisitos Técnicos específicos

Se establecerán los requisitos de seguridad referidos al computador y software del certificador.

Los requisitos mínimos serán:

a) Control de acceso a los servicios y roles afectados al proceso de certificación

b) Separación de funciones entre los roles afectados al proceso de certificación

c) Identificación y autenticación de los roles afectados al proceso de certificación

d) Utilización de criptografía para las sesiones de comunicación y bases de datos

e) Archivo de datos históricos y de auditoria del certificador y usuarios

f) Registro de eventos de seguridad

g) Prueba de seguridad relativa a servicios de certificación

h) Mecanismos confiables para identificación de roles afectados al proceso de certificación

i) Mecanismos de recuperación para claves y sistema de certificación

Estas funciones pueden ser provistas por el sistema operativo, o bien a través de una combinación del sistema operativo, software de certificación y controles físicos.

6.5.2. - Calificaciones de seguridad computacional

Se describirán las evaluaciones realizadas por terceros calificados respecto a la seguridad en los componentes de hardware y software utilizados.

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

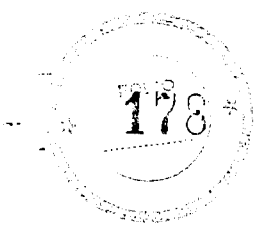
Se describirán los controles de desarrollo y administración de cambios de los sistemas, como así también los asociados a la gestión de la seguridad, en lo relacionado directa o indirectamente con las actividades de certificación.

6.6.1. - Controles de desarrollo de sistemas

Se deberán describir los controles de seguridad asociados a la metodología de desarrollo e implementación de los sistemas utilizados.

6.6.2. – Administración de controles y seguridad

La configuración del sistema, así como toda modificación o actualización debe ser documentada y controlada. El certificador proveerá un método de detección de modificaciones no autorizadas al software o a su configuración.



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

Se describirán, en caso de existir, los resultados de evaluaciones realizadas por terceros calificados respecto del ciclo de vida del software.

6.7. - Controles de seguridad de red

Se asegurará que los servicios de certificación estén protegidos de cualquier ataque a través de redes a las que se encuentre conectado.

6.8. - Controles de ingeniería de dispositivos criptográficos

Se indicarán los requisitos aplicables al dispositivo criptográfico utilizado para el almacenamiento de las claves privadas.

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

Se especificarán los formatos de certificados y de listas de certificados revocados generados según la Política de Certificación.

7.1. - Perfil del certificado

Todos los certificados serán emitidos conforme con lo establecido en la especificación ITU X.509 versión 3 y deben cumplir con las indicaciones establecidas en el sección **"2 - Perfil**

de certificados digitales" del **Anexo III - Perfil Mínimo de Certificados y Listas de Certificados Revocados.**

7.1.1. - Número de versión

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.2. - Extensiones

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.3. - Identificadores de algoritmos

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.4. - Formatos de nombre

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.5. - Restricciones de nombre

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.6. - OID de la Política de Certificación

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.7. - Uso de la extensión "Restricciones de Política" (PolicyConstrains")

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.8. - Sintaxis y semántica de calificadores de Política

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.1.9. - Semántica de procesamiento para extensiones críticas

A completar sobre la base de lo establecido en el documento referido en 7.1.

7.2. - Perfil de la lista de certificados revocados

Las listas de certificados revocados correspondientes a la presente Política de Certificación deberán ser emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 y deben cumplir con las indicaciones establecidas en el sección **"3 - Perfil de CRLs"** del **Anexo III - Perfil Mínimo de Certificados y Listas de Certificados Revocados.**

7.2.1. - Número de versión

A completar sobre la base de lo establecido en el documento referido en 7.2.

7.2.2. - Extensiones de CRL (Lista de Certificados Revocados)

A completar sobre la base de lo establecido en el documento referido en 7.2.

8. - ADMINISTRACIÓN DE ESPECIFICACIONES

Se establecerán los procedimientos para el mantenimiento y administración de la Política de Certificación.

8.1. - Procedimientos de cambio de especificaciones

Se establecerán los procedimientos utilizados para efectuar modificaciones en la Política de Certificación y en el Manual de Procedimientos de Certificación. Toda modificación deberá ser aprobada previamente por el ente licenciante.

8.2. - Procedimientos de publicación y notificación

Se describirán los mecanismos utilizados para notificar a los suscriptores acerca de la Política de Certificación y de sus modificaciones.

8.3. - Procedimientos de aprobación

Toda Política de Certificación deberá ser sometida a aprobación del ente licenciante durante el proceso de licenciamiento.

Toda modificación de la Política de Certificación deberá ser comunicada y aprobada por el ente licenciante conforme con lo establecido por la Ley N° 25.506 Art. 21 inc. q) y por la presente Decisión Administrativa y sus Anexos.

Jefe de Gabinete de Ministros

6

FOLIO 182

ANEXO III

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Perfil mínimo de certificados y listas de certificados revocados

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

Jefe de Gabinete de Ministros

183

INDICE

Jefe de Gabinete de Ministros

184

1 - Estructura básica

1.1 – Conceptos generales

El ente licenciante adhiere a la especificación ITU X.509 "Information Technology – Open Systems Interconnection – The Directory: Public-key and atribute certificate frameworks", en todos los aspectos relacionados con el formato, codificación, contenidos e interpretación de los certificados digitales y las listas de certificados revocados.

1.2 - Notación

Para la interpretación del presente documento deben tenerse en cuenta las siguientes consideraciones:

- OBLIGATORIO, indicado por los términos "debe", "requerido", u "obligatorio";
- RECOMENDADO, donde es altamente aconsejable que los certificadores operen de dicho modo, indicado por los términos "debería" o "recomendado";
- OPCIONAL, donde los certificadores pueden optar por las alternativas que consideren más convenientes, indicado por los términos "opcional" o "puede";
- NO RECOMENDADO, indicado por los términos "no debería" o "no se recomienda"; o,
- NO PERMITIDO, indicado por los términos "no debe" o "no permitido".

2 - Perfil de certificados digitales

2.1 - Formato

El formato de certificados X.509 v3 permite la utilización de una amplia variedad de opciones; por esta razón, es conveniente definir un perfil de los certificados, especificando qué opciones deben aparecer de manera obligatoria, cuáles no están permitidas y cuáles se recomienda que estén incluidas.

En lo referente a los certificados digitales se adhiere al contenido de los documentos:

- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Para aquellos casos en que no se hace una mención explícita sobre un tema en particular, se debe utilizar, con carácter de recomendación, lo establecido en los documentos antes mencionados. Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en estos documentos.

Salvo mención explícita, las siguientes especificaciones deben ser aplicadas tanto a los certificados emitidos a usuarios como aquellos que identifican al certificador o prestador de servicios de certificación.

2.2 - Campos de los certificados

Los siguientes campos DEBEN encontrarse presentes en los certificados:

- Versión (*version*)
- Número de Serie (*serialNumber*)
- Algoritmo de Firma (*signature*)

- Nombre Distintivo del Emisor (*issuer*)
- Validez (Desde, Hasta) (*validity* (*notBefore*, *notAfter*))
- Nombre Distintivo del Suscriptor (*subject*)
- Clave Pública del Suscriptor (*subjectPublicKeyInfo*)

NO DEBEN estar presentes los siguientes campos porque corresponden a la versión 2 de la especificación X.509:

- Identificador único del Emisor (*issuerUniqueID*)
- Identificador único del Suscriptor (*subjectUniqueID*)

2.2.1 – Versión (*Version*)

El campo *"version"* describe la versión del certificado. DEBE tener el valor 2 (correspondiente a versión 3).

2.2.2 – Número de Serie (*Serial Number*)

El campo *"serialNumber"* contiene un número asignado por el certificador a cada certificado. Este número DEBE ser único para cada certificado emitido por cada Autoridad Certificante del certificador.

2.2.3 – Algoritmo de Firma (*Signature*)

El campo *"signature"* DEBE contener el identificador de objeto (OID) del algoritmo y, si fueran necesarios, los parámetros asociados usados por el certificador para firmar el certificado. Este identificador DEBE ser alguno de los definidos en el [RFC3279].

2.2.4 – Nombre Distintivo del Emisor (*Issuer*)

El campo *"issuer"* DEBE identificar a la organización responsable de la emisión del certificado, mediante la utilización de un subconjunto de los siguientes atributos:

- Componente de dominio (OID 0.9.2342.19200300.100.1.25:*domainComponent*)
- Código de país (OID 2.5.4.6: *countryName*)
- Nombre de la organización (OID 2.5.4.10: *organizationName*)
- Nombre de la provincia (OID 2.5.4.8: *stateOrProvinceName*)
- Nombre de la localidad (OID 2.5.4.7: *localityName*)
- Número de serie (OID 2.5.4.5: *serialNumber*)

Otros atributos pueden estar presentes, pero NO DEBEN ser necesarios para identificar a la organización emisora.

Los contenidos y tipos de los atributos deben respetar las mismas pautas establecidas en el punto 2.2.6 para el campo *"subject"* para certificados de certificadores o proveedores de servicios de firma de digital.

El atributo *organizationName* DEBE estar presente.

El atributo "*countryName*" DEBE estar presente y DEBE representar el país en el cual se encuentra establecido el emisor. Este atributo DEBE estar codificado según el estándar [ISO3166].

2.2.5 – Validez (Desde, Hasta) (*Validity* (*notBefore, notAfter*))

El período de la validez del certificado es el intervalo de tiempo durante el cual el suscriptor se encuentra habilitado para utilizarlo.

El campo se representa como una secuencia de dos fechas:

- "*notBefore*": fecha en que el período de validez del certificado comienza.
- "*notAfter*": fecha en que el período de validez del certificado termina.

El período de validez de un certificado es el período de tiempo de *"notBefore"* a *"notAfter"* inclusive.

Se RECOMIENDAN los siguientes periodos de validez para certificados digitales, los cuales DEBEN ser especificados en la Política de Certificación:

- Certificados de certificador: 10 (DIEZ) años.
- Certificados de proveedores de servicios de firma digital: 10 (DIEZ) años.
- Certificados de Personas Jurídicas Públicas o Privadas: 3 (TRES) años.
- Certificados de Personas Físicas: 2 (DOS) años.

Un certificador NO DEBE emitir un certificado digital con vencimiento posterior al de su propio certificado.

2.2.6 – Nombre Distintivo del Suscriptor (*Subject*)

El campo *"subject"* identifica la entidad asociada a la clave pública guardada en el campo *"subjectPublicKeyInfo"*.

DEBE contener un nombre distintivo del suscriptor. Dicho nombre DEBE ser único para cada suscriptor de certificado emitido por un certificador durante todo el tiempo de vida del mismo.

La identidad del suscriptor DEBE quedar especificada utilizando un subconjunto de los siguientes atributos:

- Componente de Dominio (OID 0.9.2342.19200300.100.1.25: *domainComponent*)
- Código de país (OID 2.5.4.6: *countryName*)
- Nombre común (OID 2.5.4.3: *commonName*)
- Cargo o título (OID 2.5.4.12: *title*)
- Nombre de la organización (OID 2.5.4.10: *organizationName*)
- Nombre de la suborganización (OID 2.5.4.11: *organizationalUnitName*)
- Nombre de la provincia (OID 2.5.4.8: *stateOrProvinceName*)
- Nombre de la localidad (OID 2.5.4.7: *localityName*)
- Numero de serie (OID 2.5.4.5: *serialNumber*)

Otros atributos pueden estar presentes, pero los mismos NO DEBEN ser necesarios para identificar al suscriptor.

El atributo "*domainComponent*" se define en el RFC 2247 "Using Domains in LDAP/X.500 Distinguished Names", todos los demás atributos se definen en [RFC3280] y en [X.520].

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

- "*commonName*": en caso de existir DEBE corresponder al nombre del servicio (ej. Servicio de Fechado Digital) o al nombre de la unidad operativa responsable del servicio (ej. Unidad de Certificación Digital).
- "*organizationalUnitName*": en caso de existir PUEDE contener a las unidades operativas relacionadas con el servicio, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- "*organizationName*": DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio.
- "*serialNumber*": DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio, expresado como texto y respetando el siguiente formato y codificación: [código de identificación]" "[nro. de identificación].

  El único valor posible para el campo [código de identificación] es "CUIT": Clave única de identificación tributaria para las Personas Jurídicas argentinas.

Para los certificados de **Personas Físicas**:

- "*commonName*": DEBE estar presente y DEBE corresponder con el nombre que figura en el documento de identidad del suscriptor (DNI, Pasaporte, ...)
- "*serialNumber*" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el tipo y número de documento del titular, expresado como texto y respetando el siguiente formato y codificación: [tipo de documento]" "[nro de documento]
- Los valores posibles para el campo [tipo de documento] son:
  - En caso de ciudadanos argentinos o residentes:
    a) "DU": Documento nacional de identidad

b) "LE": Libreta de enrolamiento

c) "LC": Libreta cívica

d) "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral

- En caso de extranjeros:

a) "PA "[país]: Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

b) "EX "[país]: En caso de documento extranjero. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

- "*organizationalUnitName*" y "*organizationName*": en caso de existir serán utilizados para guardar la información relativa a la Organización a la cual el suscriptor se encuentra asociado (deben respetar los criterios definidos para los atributos "*organizationName*" y "*organizationalUnitName*" de personas Jurídicas Públicas o Privadas). El tipo de asociación entre el organismo y el suscriptor debe ser evaluado a partir de la Política de Certificación.
- "*countryName*": DEBE estar presente y DEBE representar la nacionalidad de la persona física.

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

- "*commonName*": en caso de existir DEBE corresponder al nombre del servicio o aplicación (ej. Sistema de Consulta) o al nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).
- "*serialNumber*" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto

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

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

a) “CUIT”: Clave única de identificación tributaria para las Personas Jurídicas argentinas.

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

- “*organizationalUnitName*”: en caso de existir contendrá las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias ocurrencias de este atributo de ser necesario.
- *“organizationName”*: DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada.
- “*countryName*”: DEBE estar presente y DEBE representar el país en el cual está constituida la Persona Jurídica.

El atributo “*title*”, si está presente, DEBE ser utilizado para guardar la posición o función del suscriptor dentro de la organización especificada por los atributos presentes en el campo “*subject*”. La asociación entre el atributo “*title*”, el suscriptor y la organización debe ser definida en la correspondiente Política de Certificación.

El atributo “*countryName*” DEBE estar codificado según el estándar [ISO3166].

En caso de existir información no verificada incluida en el certificado DEBE informarse esta situación utilizando algún campo descriptivo del certificado. Para ello se RECOMIENDA el empleo del atributo "*description*" (OID 2.5.4.13: Descripción).

Los tipos y longitudes correspondientes a cada atributo DEBEN respetar las definiciones establecidas en [RFC3280] Apéndice A, recomendándose la pauta establecida por este mismo RFC acerca de la utilización de la codificación UTF8String para los atributos de tipo DirectoryString.

2.2.7 – Clave Pública del Suscriptor (*Subject Public Key Info*)

Este campo *"subjectPublicKeyInfo"* se utiliza para transportar la clave pública y para identificar el algoritmo con el cual se utiliza la clave. El identificador utilizado DEBE ser alguno de los definidos en [RFC3279].

2.3 - Extensiones de un Certificado

Las siguientes extensiones DEBEN encontrase presentes en todos los certificados:

- Restricciones Básicas (*BasicConstraint*)
- Uso de Claves (*KeyUsage*)
- Puntos de Distribución de la Lista de Certificados Revocados (*CRLDistributionPoint*)
- Políticas de Certificación (*CertificatePolicies*)

La siguiente extensión DEBE estar presente en todos los certificados que no sean autofirmados:

- Identificador de la Clave de la Autoridad Certificante (*AuthorityKeyIdentifier*)

La siguiente extensión DEBE estar presente en todos los certificados de Autoridad Certificante:

- Identificador de la Clave del Suscriptor (*SubjectKeyIdentifier*)

La siguiente extensión DEBE estar presente en todos los certificados de personas jurídicas públicas o privadas que no identifiquen a un servicio o aplicación:

- Nombres Alternativos del Suscriptor (*SubjectAlternativeName*)

Se RECOMIENDA la presencia de las siguientes extensiones en los certificados:

- Uso de Claves Extendido (*ExtendedKeyUsage*)
- Nombres Alternativos del Suscriptor (*SubjectAlternativeName*)

2.3.1 – Identificador de la Clave de la Autoridad Certificante (*Authority Key Identifier*)

La extensión *"authorityKeyIdentifier"* proporciona un medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado, por ejemplo en los casos en que el emisor tiene múltiples claves de firma.

Esta extensión DEBE estar presente en todos los certificados.

Esta extensión NO DEBE ser marcada como crítica.

2.3.2 – Identificador de la Clave del Suscriptor (*Subject Key Identifier*)

La extensión "*subjectKeyIdentifier*" proporciona un medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.

Esta extensión DEBE estar presente en todos los certificados de Autoridad Certificante.

Esta extensión NO DEBE ser marcada como crítica.

2.3.3 – Uso de Claves (*Key Usage*)

La extensión *"keyUsage"* define el propósito (por ejemplo: cifrado, firma) de la clave contenida en el certificado. DEBE encontrarse presente.

Para certificados de certificadores:

- El bit *"keyCertSign"* DEBE tener valor 1
- El bit *"crlSign"* PUEDE tener valor 1
- El resto de bits DEBEN tener valor 0

Para certificados de Proveedores de servicios de firma digital que emiten información de estado de certificados (por ej. CRLs, OCSP):

- Si emiten CRLs el bit *"crlSign"* DEBE tener valor 1
- Si emiten respuestas OCSP el bit *"nonRepudiation"* DEBE tener valor 1
- El resto de bits DEBEN tener valor 0

Para certificados de otros Proveedores de servicios de firma digital:

- El bit *"nonRepudiation"* DEBE tener valor 1
- El resto de bits DEBEN tener valor 0

Para certificados de Personas Físicas y Jurídicas:

- El bit *"nonRepudiation"* DEBE tener valor 1
- El bit *"digitalSignature"* PUEDE tener valor 1 para propósitos de autenticación.
- Se RECOMIENDA que el resto de bits tengan valor 0

Esta extensión PUEDE ser marcada como crítica.

2.3.4 – Políticas de Certificación (*Certificate Policies*)

El certificador DEBE incluir el OID de su Política de Certificación que utilizará para la emisión de certificados. Ese OID es asignado por el ente licenciante .El documento digital que contiene la Política DEBE ser declarado ante el ente licenciante y la extensión *"CertificatePolicies"* DEBE declarar la URI donde el documento estará disponible.

Adicionalmente al uso que el certificador le de al campo "*userNotice*", DEBE incluir en éste la leyenda "certificado emitido por un certificador licenciado en el marco de la ley 25.506".

La extensión *"CertificatePolicies"* DEBE incluir toda la información sobre la Política necesaria para la validación del certificado. Si la información sobre la Política se incluye en la extensión *"QCStatements"* entonces esta información DEBE definirse en las Políticas indicadas.

Esta extensión DEBE estar presente en todos los certificados.

Esta extensión PUEDE ser marcada como crítica.

2.3.5 – Nombres Alternativos del Suscriptor (*Subject Alternative Name*)

En los certificados de personas jurídicas públicas o privadas que no identifiquen a un servicio o aplicación DEBEN incluirse los datos identificatorios de la persona física a cargo de la custodia de la clave privada del mismo. Los datos a incluir en la extensión DEBEN ser representados mediante la utilización de campos de tipo "*otherName*" y son:

- Nombre y apellido: DEBE ser utilizado, DEBE contener el OID de "*commonName*" (OID 2.5.4.3: Nombre común) y DEBE respetar lo especificado para el atributo "*commonName*" de los certificados de personas físicas (ver punto 2.2.6)
- Tipo y número de documento: DEBE ser utilizado, DEBE contener el OID de "*serialNumber*" (OID 2.5.4.5: Nro de serie) y DEBE respetar lo especificado para el atributo "*serialNumber*" de los certificados de personas físicas (ver punto 2.2.6).
- Posición o función del suscriptor: Cuando corresponda será utilizado para indicar la relación que lo vincula con la persona jurídica titular del certificado, DEBE contener el OID de "*title*" (OID 2.5.4.12: Cargo o título) y DEBE respetar lo especificado para el atributo "*title*" del Nombre Distintivo del Suscriptor (ver punto 2.2.6).

Adicionalmente, esta extensión *"SubjectAlternativeName"* permite asociar identidades adicionales al suscriptor de un certificado. Las opciones definidas incluyen una dirección del correo electrónico, un nombre DNS, una dirección IP, y un identificador uniforme de recurso (URI).

Se RECOMIENDA la utilización de esta extensión para consignar las direcciones de correo electrónico de los suscriptores en lugar del atributo "*email*" del campo "*subject*".

2.3.6 – Atributos de Directorio del Suscriptor (*Subject Directory Attributes*)

La extensión *"SubjectDirectoryAttributes"* PUEDE contener atributos adicionales asociados con el campo *"subject"*, como complemento a la información presente en el mismo y en la extensión *"SubjectAlternativeName"*.

Los atributos adecuados para almacenar en esta extensión son aquellos que no son parte del nombre distintivo del suscriptor pero que PUEDEN ser útiles para otros propósitos (por ejemplo: autorización).

Esta extensión NO DEBE ser marcada como crítica.

Las implementaciones que adhieran a esta especificación DEBEN interpretar como mínimo los siguientes atributos:

- Fecha de nacimiento (*dateOfBirth*)
- Lugar de nacimiento (*placeOfBirth*)
- Sexo (*gender*)
- País de ciudadania (*countryOfCitizenship*)
- País de residencia (*countryOfResidence*)

El valor del atributo *"dateOfBirth"*, si está presente, DEBE contener la fecha de nacimiento del suscriptor.

El valor del atributo *"placeOfBirth"*, si está presente, DEBE contener el lugar de nacimiento del suscriptor.

El valor del atributo *"gender"*, si está presente, DEBE contener el sexo del suscriptor. Para las mujeres se utiliza el valor "F" (o "f") y para los hombres el valor "M" (o "m").

El atributo *"countryOfCitizenship"*, si está presente, DEBE utilizarse para identificar por lo menos uno de los países del que el suscriptor dice ser ciudadano en el momento en que el certificado fue emitido. Si el suscriptor es ciudadano de más de un país, el atributo PUEDE tener más de un valor.

El atributo *"countryOfResidence"*, si está presente, DEBE contener el valor del país de residencia del suscriptor. Si el suscriptor reside en más de un país, el atributo contendrá más de un valor.

2.3.7 – Restricciones Básicas (*Basic Constraints*)

La extensión *"BasicConstraints"* permite identificar si el suscriptor de un certificado es un certificador e indica la longitud máxima de las rutas de certificación válidas que el certificado incluye.

Esta extensión DEBE estar presente en todos los certificados.

Los certificados de certificador DEBEN contener el atributo *"ca"* con valor TRUE y la extensión DEBE ser marcada como crítica.

Para los certificados de usuarios finales DEBEN contener el atributo *"ca"* con valor FALSE y el atributo *"pathLenConstraint"* DEBE ser nulo.

2.3.8 – Uso de Claves Extendido (*Extended Key Usage*)

Esta extensión *"ExtendedKeyUsage"* indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada, además o en lugar de los propósitos básicos indicados en la extensión *"KeyUsage"*.

Esta extensión DEBE ser utilizada al menos en los siguientes casos:

- Certificados para firma de respuestas OCSP DEBEN incluir el valor *"id-kp-OCSPSigning"* (1.3.6.1.5.5.7.3.9)
- Certificados para servicios de certificación digital de fecha y hora DEBEN incluir el valor *"id-kp-timeStamping"* (1.3.6.1.5.5.7.3.8)

No se restringe la utilización de otros propósitos que sean concordantes con lo establecido en la extensión "*KeyUsage*".

2.3.9 – Puntos de Distribución de la Lista de Certificados Revocados (*CRL Distribution Point*)

La extensión *"CRLDistributionPoint"* indica cómo se obtiene la información de CRL.

Esta extensión DEBE estar presente en todos los certificados que no sean autofirmados.

Esta extensión NO DEBE ser crítica.

2.3.10 – CRL más reciente (*Freshest CRL*)

La extensión *"FreshestCRL"* indica cómo puede ser obtenida la "delta CRL".

En caso de que el certificador utilice delta CRL, esta extensión DEBE estar presente.

Esta extensión NO DEBE ser crítica.

2.3.11 – Información Biométrica (*Biometric Information*)

Para la inclusión de información biométrica del suscriptor se RECOMIENDA la extensión *"BiometricInformation"*. Esta información es almacenada como un digesto de una plantilla biométrica.

El propósito de esta extensión es proporcionar los medios para la autenticación de información biométrica. La información biométrica correspondiente al digesto almacenado, no se incluye en la extensión, pero PUEDE incluir una URI que indique el lugar donde esta información puede ser obtenida. La inclusión de la URI no implica que sea la única manera de tener acceso a esta información.

Se RECOMIENDA que la información biométrica de esta extensión se encuentre limitada a tipos de información adecuados para la verificación humana, es decir donde la decisión sobre la exactitud de la representación del suscriptor es realizada por una persona.

Esta extensión NO DEBE ser marcada como crítica.

El tipo de atributo *"picture"*, si está presente, DEBE identificar que la imagen origen es una imagen gráfica (fotografía) del suscriptor. Su valor es el digesto de la imagen y DEBE ser calculado sobre el archivo de la imagen a la que se hace referencia.

El valor del atributo *"handwritten-signature"*, si está presente, DEBE identificar que la imagen origen es una imagen de la firma manuscrita del suscriptor. Su valor es el digesto de la imagen y DEBE ser calculado sobre el archivo de la imagen a la que se hace referencia.

2.3.12 – Declaraciones del Certificado Calificado (*Qualified Certificate Statements*)

En el caso de que el certificador utilice esta extensión, en ésta se DEBE indicar que el certificado ha sido emitido por un certificador licenciado en el marco de la Ley 25.506. El ente licenciante suministrará el OID, que identifica la Política de Certificación.

Se RECOMIENDA la inclusión en esta extensión de las declaraciones que afecten a la utilización del certificado en transacciones, como por ejemplo límites económicos, etc.

Esta extensión puede ser crítica o no crítica. Si es crítica, todas las declaraciones incluidas en la extensión lo son también.

2.3.13 – Información de Acceso de la Autoridad Certificante (*Authority Information Access*)

En caso de que el certificador provea el servicio de OCSP, la extensión *"AuthorityInformationAccess"* DEBE ser utilizada para indicar como se accede a la información.

2.3.14 – Información de Acceso del Suscriptor (*Subject Information Access*)

La extensión *"SubjectInformationAccess"* indica como se accede a la información y servicios del suscriptor del certificado en que la misma aparece.

2.3.15 - Otras extensiones

NO se RECOMIENDA la creación de nuevas extensiones más allá de las definidas en [RFC3280].

3 - Perfil de CRLs

3.1 - Formato

El formato de las Listas de Certificados Revocados X.509 permite la utilización de una amplia variedad de opciones; por esta razón, se hace necesario definir un perfil para las listas de certificados revocados, especificando qué opciones deben aparecer de manera obligatoria, cuáles no está permitido usar y cuáles son recomendables que estén incluidas en ellas.

En lo referente a CRLs se adhiere al contenido del documento:

- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

Para aquellos casos en que no se hace una mención explícita sobre un tema en particular, se recomienda utilizar, lo establecido en el documento antes mencionado. Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en este documento.

3.2 - Campos de una CRL

Los siguientes campos DEBEN encontrarse presentes en todas las CRLs:

- Versión (*version*)
- Algoritmo de Firma (*signature*)

- Nombre Distintivo del Emisor (*issuer*)
- Día y Hora de Vigencia (*thisUpdate*)
- Próxima Actualización (*nextUpdate*)
- Certificados Revocados (*revokedCertificates*) (sólo en caso de que existan certificados revocados)

3.2.1 – Versión (*Version*)

El campo *"version"* describe la versión de la CRL. DEBE tener el valor 1 (correspondiente a Versión 2).

3.2.2 – Algoritmo de Firma (*Signature*)

El campo *"signature"* DEBE contener el identificador de objeto (OID) del algoritmo y, de ser necesarios, los parámetros asociados usados por el certificador para firmar la CRL. Este identificador DEBE ser alguno de los definidos en [RFC3279].

3.2.3 – Nombre Distintivo del Emisor (*Issuer*)

El campo *"issuer"* identifica a la entidad que firma y emite la CRL. Los contenidos y tipos de los atributos DEBEN respetar las pautas establecidas para el campo *"issuer"* de un certificado.

3.2.4 – Día y Hora de Vigencia (*This Update*)

El campo *"ThisUpdate"* indica la fecha de emisión de la CRL. La fecha de revocación de un certificado de la lista no DEBE ser posterior a esta fecha. La CRL DEBE estar disponible para consulta inmediatamente después de emitida.

3.2.5 – Próxima Actualización (*Next Update*)

El campo *"NextUpdate"* indica la fecha límite de emisión de la próxima CRL. Este campo DEBE estar presente en todas las CRL emitidas.

3.2.6 – Certificados Revocados (*Revoked Certificates*)

El campo *"RevokedCertificates"* contiene la lista de certificados revocados indicados por su número de serie, también pueden incluirse extensiones específicas para cada elemento de esta lista.

3.3 - Extensiones de una CRL

3.3.1 – Identificación de Clave de la Autoridad Certificante (*Authority Key Identifier*)

La extensión *"AuthorityKeyIdentifier"* proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL.

Esta extensión DEBE estar presente en todas las listas de revocación de certificados.

3.3.2 - Número de CRL (*CRL Number*)

La extensión *"CRLNumber"* contiene un número de secuencia creciente para una CRL y emisor dado. Esta extensión permite que los usuarios determinen fácilmente cuándo una CRL particular reemplaza otra CRL.

Esta extensión DEBE estar incluida en todas las listas de revocación de certificados.

3.3.3 – Indicador de Delta CRL (*Delta CRL Indicator*)

La extensión *"DeltaCRLIndicator"* permite indicar que una CRL es una CRL incremental o "delta CRL".

El certificador PUEDE utilizar "delta CRL".

De existir esta extensión DEBE ser crítica.

3.3.4 – Punto de Distribución del Emisor (*Issuing Distribution Point*)

La extensión *"IssuingDistributionPoint"* identifica el punto de distribución y el alcance de una CRL particular. Indica, por ejemplo, si la CRL cubre la revocación de certificados del suscriptor solamente, certificados del certificador solamente, etc.

Si existiera esta extensión DEBE ser considerada como crítica.

3.3.5 – CRL más Reciente – Punto de Distribución de la Delta CRL (*Freshest CRL - Delta CRL Distribution Point*)

La extensión *"FreshestCRL"* indica dónde puede obtenerse la información de la "CRL" de una CRL completa.

Esta extensión NO DEBE ser utilizada en "*delta CRL*".

Esta extensión NO DEBE ser crítica.

3.3.6 - Otras extensiones de CRLs

Se RECOMIENDA NO crear nuevas extensiones mas allá de las definidas en [RFC3280].

3.4 - Extensiones de un elemento de la lista "Certificados Revocados" (*Revoked Certificates*)

3.4.1 – Código de motivo (*Reason Code*)

La extensión *"ReasonCode"* indica la razón de revocación de un elemento de la CRL.

Se RECOMIENDA la inclusión del motivo de revocación del certificado.

3.4.2 – Código de instrucción de suspensión (*Hold Instruction Code*)

El estado de suspensión no es admitido en el marco de la Ley 25.506 y lo que sigue en este ítem es sólo a título informativo.

La extensión *"HoldInstructionCode"* indica la acción a seguir el encontrar un certificado suspendido (estado *"hold"*).

Las aplicaciones que encuentren un código *"id-holdinstruction-callissuer"* DEBEN llamar al emisor del certificado o rechazarlo.

Las aplicaciones que encuentren un código *"id-holdinstruction-reject"* DEBEN rechazar el certificado.

3.4.3 – Fecha de invalidez (*Invalidity Date*)

La extensión *"InvalidityDate"* indica la fecha en la cual se sabe o se sospecha que la clave privada fue comprometida o que el certificado pasó a ser inválido.

3.4.4 – Emisor del certificado (*Certificate Issuer*)

La extensión *"CertificateIssuer"* identifica al emisor del certificado asociado con una entrada en una CRL indirecta, es decir una CRL que tenga el indicador *"indirectCRL"* en su extensión *"IssuingDistributionPoint"*.

Esta extensión DEBE ser crítica.

Se RECOMIENDA que las implementaciones reconozcan esta extensión.

3.4.5 - Otras extensiones de entradas de la lista "Certificados Revocados"

NO se RECOMIENDA la creación de nuevas extensiones más allá de las definidas en [RFC3280].

4 - Algoritmos criptográficos

Los algoritmos utilizados DEBEN ser los especificados en RFC 3279 "Algorithms and Identifiers for the Certificate and Certificate Revocation List (CRL) Profile" [RFC3279].

Todos los certificados DEBEN respetar las siguientes longitudes mínimas de claves para los algoritmos de firma:

- Para certificados de certificador o de información de estado de certificados: 2048 bits si se utiliza RSA o DSA y 210 bits en caso de ECDSA.
- Para certificados utilizados en servicios relacionados con la firma digital (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.): 2048 bits si se utiliza RSA o DSA y 210 bits en caso de ECDSA.
- Para certificados de responsables de Autoridades de Registro: 1024 bits si se utiliza RSA o DSA y 160 bits en caso de ECDSA.
- Para certificados de suscriptores (personas físicas o jurídicas): 1024 bits si se utiliza RSA o DSA y 160 bits en caso de ECDSA.

5 – Correspondencia con estándares

A continuación se establece un paralelo entre las definiciones incluidas en esta especificación y los ítems respectivos definidos en los documentos [RFC3279], [RFC3280], [RFC3739], [ISO/IEC 9594-8] y la Ley 25.506, incluyéndose referencias a cada uno de ellos.

Índice de referencia	Estándar
1 - Estructura básica	ISO/IEC 9594-8
1.1 - Conceptos generales	-
1.2 – Notación	-
2 - Perfil de certificados digitales	-
2.1 – Formato	RFC 3280 4
2.2 - Campos de certificados	-
2.2.1 - Versión (*Version*)	RFC 3280 4.1.2.1
2.2.2 - Número de Serie (*Serial Number*)	RFC 3280 4.1.2.2 Ley 25.506 Art. 19.c
2.2.3 - Algoritmo de Firma (*Signature*)	RFC 3280 4.1.2.3 RFC 3279
2.2.4 - Nombre Distintivo del Emisor (*Issuer*)	RFC 3739 3.1.1
2.2.5 - Validez (Desde, Hasta) (*Validity* (*notBefore*, *notAfter*))	RFC 3280 2.1.2.5
2.2.6 - Nombre Distintivo del Suscriptor (*Subject*)	RFC 3739 3.1.2 RFC 3280 Apéndice A
2.2.7 - Clave Pública del Suscriptor (*Subject Public Key Info*)	RFC 3280 4.1.2.7

FOLIO 212

2.3 - Extensiones de un certificado	-
2.3.1 - Identificador de la Clave de la Autoridad Certificante (*Authority Key Identifier*)	RFC 3280 4.2.1.1
2.3.2 - Identificador de la Clave del Suscriptor (*Subject Key Identifier*)	RFC 3280 4.2.1.2
2.3.3 - Uso de Claves (*Key Usage*)	RFC 3739 3.2.4
2.3.4 - Políticas de Certificación (*Certificate Policies*)	RFC 3739 3.2.3 Ley 25.506 Art. 14.b.5
2.3.5 - Nombres Alternativos del Suscriptor (*Subject Alternative Name*)	RFC 3280 4.2.1.7
2.3.6 - Atributos de Directorio del Suscriptor (*Subject Directory Attributes*)	RFC 3739 3.2.2
2.3.7 - Restricciones Básicas (*Basic Constraints*)	RFC 3280 4.2.1.10
2.3.8 - Uso de Claves Extendido (*Extended Key Usage*)	RFC 3280 4.2.1.13
2.3.9 - Puntos de Distribución de la Lista de Certificados Revocados (*CRL Distribution Point*)	RFC 3280 4.2.1.14
2.3.10 - CRL más reciente (*Freshest CRL*)	RFC 3280 4.2.1.16
2.3.11 - Información Biométrica (*Biometric Information*)	RFC 3739 3.2.5
2.3.12 - Declaraciones del Certificado Calificado (*Qualified Certificate Statements*)	RFC 3739 3.2.6
2.3.13 - Información de Acceso de la Autoridad Certificante (*Authority Information Access*)	RFC 3280 4.2.2.1

2.3.14 - Información de Acceso del Suscriptor (*Subject Information Access*)	RFC 3280 4.2.2.2
2.3.15 - Otras extensiones	-
3 - Perfil de CRLs	-
3.1 – Formato	RFC 3280 5
3.2 - Campos de una CRL	-
3.2.1 - Versión (*Version*)	RFC 3280 5.1.2.1
3.2.2 - Algoritmo de Firma (*Signature*)	RFC 3280 5.1.2.2
3.2.3 - Nombre Distintivo del Emisor (*Issuer*)	RFC 3280 5.1.2.3
3.2.4 - Día y Hora de Vigencia (*This Update*)	RFC 3280 5.1.2.4
3.2.5 - Próxima Actualización (*Next Update*)	RFC 3280 5.1.2.5
3.2.6 - Certificados Revocados (*Revoked Certificates*)	RFC 3280 5.1.2.6
3.3 - Extensiones de una CRL	-
3.3.1 - Identificación de Clave de la Autoridad Certificante (*Authority Key Identifier*)	RFC 3280 5.2.1
3.3.2 - Número de CRL (*CRL Number*)	RFC 3280 5.2.3
3.3.3 - Indicador de Delta CRL (*Delta CRL Indicador*)	RFC 3280 5.2.4
3.3.4 - Punto de Distribución del Emisor (*Issuing Distribution Point*)	RFC 3280 5.2.5
3.3.5 - CRL más Reciente - Punto de Distribución de la Delta CRL (*Freshest CRL - Delta CRL Distribution Point*)	RFC 3280 5.2.6
3.3.6 - Otras extensiones de CRLs	-

3.4 - Extensiones de una entrada de la lista "Certificados Revocados" (*Revoked Certificates*)	-
3.4.1 - Código de motivo (*Reason Code*)	RFC 3280 5.3.1
3.4.2 - Código de instrucción de suspensión (*Hold Instruction Code*)	RFC 3280 5.3.2
3.4.3 - Fecha de invalidez (*Invalidity Date*)	RFC 3280 5.3.3
3.4.4 - Emisor del certificado (*Certificate Issuer*)	RFC 3280 5.3.4
3.4.5 - Otras extensiones de entradas de la lista "Certificados Revocados"	-
4 - Algoritmos criptográficos	RFC 3279

6 – Referencias

[RFC2247] Kille, S., Wahl, M., Grimstad, A., Huber, R. and Sataluri, S., "Using Domains in LDAP/X.500 Distinguished Names", RFC 2247, January 1998.

[RFC3279] Polk, W., Housley, R. and Bassham, L., "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" RFC 3279, April 2002.

[RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3739] Santesson, S., Nystrom, M. and Polk, T., "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, March 2004.

[X.509] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[X.520] ITU-T Recommendation X.520 (2001) | ISO/IEC 9594-6:2001, Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types, 2001.

[ISO3166] ISO 3166-1:1997, Codes for the representation of names of countries, 1997.

Jefe de Gabinete de Ministros

FOLIO 216

ANEXO IV

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Contenidos mínimos del resumen de la política de certificación y del manual de procedimientos de certificación para suscriptores

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

El Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación para suscriptores es un documento que presenta en forma concisa y clara toda información crítica relacionada con las políticas y procedimientos de certificación que el certificador ha desarrollado con mayor detalle en su Política de Certificación (PC) y en su Manual de Procedimientos de Certificación (MPC).

Este resumen no es un documento obligatorio y en caso de existir se debe indicar de qué manera se pondrá a disposición de los suscriptores.

El presente documento establece los contenidos mínimos que el certificador debe incluir en dicho resumen.

1. Introducción

Debe contener una descripción del contenido del documento.

2. Contactos

Se incluirán los datos de un responsable del certificador para actuar como nexo incluyendo como mínimo nombre, dirección de correo electrónico, número de teléfono y fax.

3. Política de Certificación

Debe detallar la aplicabilidad y las restricciones de los certificados emitidos bajo la Política de Certificación. La descripción debe incluir el identificador de objeto (OID) de esa política de certificación que forma parte de los certificados emitidos.

218

3.1. Tipos de Certificados

Debe contener una lista y breve descripción de cada uno.

3.2. Aplicabilidad

Descripción de los usos que podrá darse a los certificados (conforme a la Ley Nº 25.506).

3.3. Verificación por terceros usuarios

Debe describir las facilidades que el certificador provee a los terceros usuarios para verificar la validez de los certificados por él emitidos bajo esta Política de Certificación.

4. Limitaciones en el uso del certificado

Debe indicarse toda restricción en el uso en caso de existir.

5. Obligaciones

5.1. Obligaciones del certificador licenciado

Debe reflejar lo especificado al respecto en la Política de Certificación.

5.2. Obligaciones de las Autoridades de Registro

Debe reflejar lo especificado al respecto en la Política de Certificación.

5.3. Obligaciones de los suscriptores

Debe reflejar lo especificado al respecto en la Política de Certificación.

6. Obligaciones de los terceros usuarios ("relying parties")

Deben indicarse las obligaciones de verificación del estado de los certificados a que están sujetos los terceros usuarios según lo especificado en la Política de Certificación.

7. Limitaciones de la responsabilidad

7.1. Fuerza mayor

Debe describir las circunstancias que por ser ajenas a la voluntad de las partes no generan derecho a indemnización a favor del damnificado

7.2. Casos en los cuales el certificador puede limitar su responsabilidad

Deben indicarse las limitaciones de responsabilidad (conforme Artículo 39 de la Ley Nº 25.506) reflejando lo indicado en "Responsabilidades" de su Política de Certificación.

8. Otros acuerdos aplicables

Debe identificar y hacer referencia a los acuerdos con suscriptores, a los términos y condiciones con terceros usuarios, al Manual de Procedimientos de Certificación y a la Política de Certificación. La descripción incorporada en este punto debe reflejar lo indicado en su Política de Certificación y la presente Decisión Administrativa en sus Anexos V y VI.

9. Confidencialidad y Derechos de Propiedad Intelectual

9.1. Confidencialidad

Debe reflejar lo especificado al respecto en la Política de Certificación.

9.2. Derechos de Propiedad Intelectual

Debe reflejar lo especificado al respecto en la Política de Certificación.

9.3. Política de privacidad

Debe reflejar lo especificado al respecto en la Política de Privacidad y en la presente Decisión Administrativa en su Anexo VIII.

10. Legislación Aplicable y Procedimientos de Resolución de Conflictos

Debe reflejar lo especificado al respecto en la Política de Certificación.

11. Auditoría

Debe describir el proceso de auditoría aplicable.

Jefe de Gabinete de Ministros

ANEXO V

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Contenidos mínimos de los acuerdos con suscriptores

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

El acuerdo establecido entre el certificador y el suscriptor determina los derechos y obligaciones de las partes en lo que respecta a la solicitud, aceptación y uso de certificados digitales.

El presente documento identifica los contenidos mínimos que el certificador debe incluir en el acuerdo que establezca con los suscriptores de certificados.

1. Solicitud de Certificado y Descripción de los Certificados

Debe detallar los términos y condiciones relacionados con la solicitud, aceptación y uso del certificado por parte del suscriptor, como así también la generación y uso de las claves criptográficas.

2. Procesamiento de la Solicitud de Certificado del suscriptor

Debe describir los pasos que el certificador sigue desde la recepción de la solicitud hasta la aprobación y emisión del certificado.

3. Obligaciones ante la revocación o expiración

Debe detallar las obligaciones del suscriptor y del certificador respecto del ciclo de vida y de la revocación del certificado reflejando lo que indica la Política de Certificación.

4. Política de Privacidad

La descripción incorporada en este punto debe reflejar lo especificado en la Política de Privacidad y en la presente Decisión Administrativa en su Anexo VIII.

5. Limitaciones de la responsabilidad

5.1. Fuerza mayor

Debe describir las circunstancias que por ser ajenas a la voluntad de las partes no generan derecho a indemnización a favor del damnificado

5.2. Casos en los cuales el certificador puede limitar su responsabilidad

Debe indicar de las limitaciones de responsabilidad (conforme Artículo 39 de la Ley N° 25.506) reflejando lo indicado en "Responsabilidades" de su Política de Certificación.

6. Legislación Aplicable y Procedimientos de Resolución de Conflictos

La descripción incorporada en este punto debe reflejar lo especificado en la Política de Certificación.

7. Cesión de derechos

Debe indicar que ninguno de los derechos del suscriptor bajo los términos del presente acuerdo pueden ser cedidos o transferidos.

Jefe de Gabinete de Ministros

FOLIO 223

8. Contactos

Se incluirán los datos de un responsable del certificador para actuar como nexo incluyendo como mínimo nombre, dirección de correo electrónico, número de teléfono y fax.

9. Vigencia

Indicar la fecha de inicio de vigencia de este acuerdo.

10. Modificaciones a este acuerdo

Descripción de las condiciones bajo las que se pueden cambiar los términos de este acuerdo y como serán refrendadas por el suscriptor.

Jefe de Gabinete de Ministros

6

FOLIO 226

ANEXO VI

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Contenidos mínimos de los términos y condiciones con terceros usuarios

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

Los términos y condiciones establecidos entre el certificador y los terceros usuarios determinan los derechos y responsabilidades de las partes en lo que respecta a la verificación de firmas digitales y otros usos de certificados digitales.

El presente documento identifica los contenidos mínimos que el certificador debe incluir en los términos y condiciones que establezca con los terceros usuarios de certificados.

1. Resumen

Debe contener una breve descripción de los términos y condiciones que rigen este documento.

2. Definiciones

Debe contener un glosario de la terminología utilizada en la política de certificación.

3. Reconocimiento de Información suficiente

Debe contener una descripción de la información relativa al certificado y su política de certificación que debe estar en conocimiento del tercero usuario.

4. Política de Certificación

4.1. Tipos de Certificados

Deben describirse los tipos de Certificados definidos en la política de certificación.

4.2. Aplicabilidad

Debe describir los usos que podrán darse a los certificados (conforme a la Ley Nº 25.506).

4.3. Limitaciones en el uso del certificado

Deben indicarse toda restricción en el uso en caso de existir.

5. Obligaciones del tercero usuario ("relying party")

Deben indicarse las obligaciones de verificación a que están sujetos los terceros usuarios respecto del estado de los certificados. La descripción incorporada en este punto debe reflejar lo especificado en la Política de Certificación.

6. Revocación de los certificados de nivel superior

Debe notificarse de los riesgos a que se ve expuesto el tercero usuario respecto del compromiso de las claves privadas de nivel superior.

7. Limitaciones de Responsabilidad

7.1. Fuerza mayor

Deben describirse las circunstancias que por ser ajenas a la voluntad de las partes no generan derecho a indemnización a favor del damnificado

7.2. Casos en los cuales el certificador puede limitar su responsabilidad

Deben indicarse las limitaciones de responsabilidad (conforme Artículo 39 de la Ley Nº 25.506) reflejando lo indicado en "Responsabilidades" de su Política de Certificación.

8. Legislación Aplicable y Procedimientos de Resolución de Conflictos

La descripción incorporada en este punto debe reflejar lo especificado en la Política de Certificación.

9. Contactos

Se incluirán los datos de un responsable del certificador para actuar como nexo incluyendo como mínimo nombre, dirección de correo electrónico, número de teléfono y fax.

Jefe de Gabinete de Ministros

230

ANEXO VII

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Monto de aranceles y garantías

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

Jefe de Gabinete de Ministros

231

Los trámites ante el ente licenciante están sujetos al pago de los siguientes aranceles a saber:

CONCEPTO	IMPORTE
Por solicitud de licencia única y supervisión del proceso de licenciamiento:	**$ 30.000**
Por obtención de licencias adicionales en caso de infraestructura previamente inspeccionada por el ente licenciante, cuyo nivel de seguridad y prestaciones sean adecuados para las necesidades de las nuevas políticas a licenciar:	**$ 15.000**
Por renovación de licencia:	**$ 15.000**
Monto mínimo a integrarse en concepto de garantía o seguro de caución:	**$ 500.000**

Jefe de Gabinete de Ministros

232

ANEXO VIII

Infraestructura de Firma Digital – República Argentina

Ley 25.506

Contenidos mínimos de la política de privacidad

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

Jefe de Gabinete de Ministros

233

La Política de Privacidad de datos determina el tratamiento que el certificador hará de los datos recibidos de los suscriptores, terceros usuarios de certificados digitales y otros terceros en general, debe estar en un todo de acuerdo con lo establecido al respecto por la ley 25.326 de habeas data.

La Política de Privacidad del certificador deberá como mínimo:

a) Indicar cuál es la información que se solicita a los terceros y/o suscriptores de certificados. En este caso se deberá indicar qué tipo de información personal se requiere para cada uno de los productos o servicios ofrecidos por el certificador.
b) Informar al suscriptor y/o tercero el destino o finalidad de toda información que se recabe y cuál será la forma de utilización de dicha información.
c) Señalar cuál es la información contenida en un certificado digital y la obligación de proceder a su publicación.
d) Precisar la forma de tratamiento de los datos o información adicional opcionalmente remitida por el tercero y/o suscriptor.
e) Detallar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales.
f) Informar que los datos recabados no van a ser objeto de cesión.
g) Proveer la dirección de correo electrónico del contacto a fin que el tercero y/o suscriptor pueda actualizar información, formular las preguntas que considere necesarias, realizar comentarios o sugerencias o bien pedir la supresión, rectificación o actualización de sus datos personales.