Jefe de Gabinete de Ministros

927

FOLIO 811

ANEXO I

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

**Formulario de Adhesión a la Política Única de Certificación**

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 812

**Introducción**

El presente formulario deberá ser completado por todos los certificadores que inicien el proceso de licenciamiento para indicar aquella información particular de su actividad que esté señalada como variable en la Política Única de Certificación, aprobada por el Anexo III de la presente decisión administrativa.

Bajo ningún concepto podrá incluir aspectos no expresamente indicados en este documento, salvo autorización del ente licenciante, mediando justificación suficiente.

La presentación de este formulario por parte del certificador implica la aceptación de la Política Única de Certificación como la aplicable para ejercer sus funciones como parte de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA aprobada por Ley N° 25.506.

Para cada dato solicitado, se referencia la sección de la Política Única de Certificación del Anexo III de la presente decisión.

**Nombre e Identificación de la Política Única de Certificación**

Se deberá indicar la denominación de la Política Única de Certificación presentada, versión, revisión, fecha de aplicación, lugar o sitio de publicación y otros datos de carácter similar que permitan identificar el documento.

*Ref: 1.2. – Nombre e Identificación del Documento.*

**Datos del Certificador**

Se deberán indicar los datos de identificación del certificador, tales como razón social, denominación del organismo/empresa, dirección postal, teléfonos, CUIT y otros datos de carácter similar.

Jefe de Gabinete de Ministros

FOLIO 813

*Ref: 1.3.1. – Certificador.*

**Datos de las Autoridades de Registro**

Se deberán identificar en forma directa o a través de un enlace a un sitio web de Internet, las Autoridades de Registro propias o de terceros, incluyendo el domicilio y datos de contacto de cada una de ellas.

*Ref: 1.3.2. - Autoridad de Registro.*

**Comunidad de Suscriptores y Terceros Usuarios**

Se deberá indicar si los suscriptores serán personas físicas o jurídicas, las aplicaciones o sitios seguros y precisar la comunidad de suscriptores habilitados, como así también los Terceros Usuarios respectivos.

*Ref: 1.3.3. - Suscriptores de certificados y 1.3.4. – Terceros Usuarios.*

**Responsable del Documento**

Se deberán incluir los datos de un responsable del certificador para actuar como nexo incluyendo denominación del servicio de atención de consulta, dirección de correo electrónico institucional y número de teléfono.

*Ref: 1.5.1. – Responsable del documento.*

**Contacto**

Se deberán incluir los datos del responsable del registro, mantenimiento e interpretación de la Política Única de Certificación.

*Ref: 1.5.2. – Contacto.*

**Procedimiento de aprobación de la Política Única de Certificación**

Jefe de Gabinete de Ministros

FOLIO 814

Se deberán especificar los datos completos del acto administrativo, una vez otorgada la licencia.

*Ref: 1.5.3. – Procedimiento de aprobación de la Política Única de Certificación.*

**Repositorios**

Se deberán indicar las entidades que administran los repositorios, señalando 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.

*Ref: 2.1. – Repositorios.*

**Publicación de información del certificador**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 2.2. - Publicación de información del certificador.*

**Controles de acceso a la información**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 2.4. - Controles de acceso a la información.*

**Nombres Distintivos**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 3.1.2. - Necesidad de Nombres Distintivos.*

**Métodos para comprobar la posesión de la clave privada**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 3.2.1. - Métodos para comprobar la posesión de la clave privada.*

**Autenticación de la identidad de personas jurídicas públicas o privadas**

Se deberá indicar la documentación a presentar para acreditar la identidad de la persona jurídica titular del certificado o responsable del servicio, aplicación o sitio web.

*Ref: 3.2.2. - Autentícación de la identidad de personas jurídicas públicas o privadas.*

**Requerimiento de revocación**

Se deberán indicar los procedimientos a seguir para validar la identidad del solicitante de la revocación de un certificado, incluyendo la documentación requerida en el proceso.

*Ref: 3.4. - Requerimiento de revocación.*

**Solicitud de certificado**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 4.1.2. - Solicitud de certificado.*

**Procesamiento de la solicitud del certificado**

Se deberán describir las condiciones, procedimientos y plazos aplicables a la aceptación o rechazo de la solicitud de un certificado, así como toda la información relativa a la tramitación del mismo.

Jefe de Gabinete de Ministros

816

*Ref: 4.2. – Procesamiento de la solicitud del certificado.*

**Proceso de emisión del certificado**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 4.3.1. – Proceso de emisión del certificado.*

**Notificación de emisión**

Se deberán indicar las condiciones para la notificación de la emisión de un certificado a su titular.

*Ref: 4.3.2. – Notificación de emisión.*

**Aceptación del certificado**

Se deberán indicar los requisitos y procedimientos referidos a la publicación del certificado y a su aceptación por el suscriptor y los procedimientos de notificación de emisión a otras entidades, de ser aplicable.

*Ref: 4.4. - Aceptación del certificado.*

**Procedimientos para la solicitud de revocación**

Se deberán indicar las vías de contacto disponibles para la realización de la solicitud de revocación y para la comunicación del cambio de estado del certificado.

*Ref: 4.9.3. - Procedimientos para la solicitud de revocación.*

**Frecuencia de emisión de listas de certificados revocados**

Se deberá indicar la frecuencia de emisión de listas de certificados revocados.

*Ref: 4.9.7. - Frecuencia de emisión de listas de certificados revocados.*

Jefe de Gabinete de Ministros

FOLIO 817

**Vigencia de la lista de certificados revocados**

Se deberá indicar la vigencia de cada lista de certificados revocados.

*Ref: 4.9.8.- Vigencia de la lista de certificados revocados.*

**Disponibilidad del servicio de consulta sobre revocación y de estado del certificado**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

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

**Requisitos para la verificación en línea del estado de revocación**

Se deberán indicar los requisitos para la verificación en línea del estado de revocación de certificados.

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

**Otras formas disponibles para la divulgación de la revocación**

Se deberán indicar, de existir, otras formas disponibles para la divulgación del estado de revocación de certificados y los requisitos para cada una de ellas.

*Ref: 4.9.11. - Otras formas disponibles para la divulgación de la revocación.*

**Características técnicas**

Se deberán describir las características de los servicios disponibles para la verificación del estado de los certificados emitidos, de ser aplicable.

*Ref: 4.10.1. – Características técnicas.*

Jefe de Gabinete de Ministros

FOLIO 818

**Disponibilidad del servicio**

Se deberán detallar, de corresponder, las políticas aplicables para los servicios descriptos en el apartado anterior, incluyendo las consecuencias de la interrupción del servicio.

*Ref: 4.10.2. – Disponibilidad del servicio.*

**Aspectos operativos**

Se deberá indicar cualquier otro aspecto de los servicios de verificación del estado de los certificados.

*Ref: 4.10.3. – Aspectos operativos.*

**Cambio de claves criptográficas**

Se deberán incluir los procedimientos a seguir para distribuir una nueva clave pública a los usuarios de un certificador luego de un cambio de claves.

*Ref: 5.6. - Cambio de claves criptográficas.*

**Generación e instalación del par de claves criptográficas**

Los puntos con referencias a los apartados de la Política Única de Certificación 6.1.1. a 6.1.6. refieren a la generación e instalación del par de claves y deberán ser consideradas en esta sección desde la perspectiva de las autoridades certificantes del certificador, de los repositorios, de las autoridades de registro y de los suscriptores.

*Ref: 6.1. - Generación e instalación del par de claves criptográficas.*

*Ref: 6.1.1. - Generación del par de claves criptográficas.*

*Ref: 6.1.2. – Entrega de la clave privada*

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

*Ref: 6.1.4. - Disponibilidad de la clave pública del certificador.*

*Ref: 6.1.5. - Tamaño de claves.*

*Ref: 6.1.6. - Generación de parámetros de claves asimétricas.*

**Protección de la clave privada y controles sobre los dispositivos criptográficos**

La protección de la clave privada debe ser considerada en esta sección y para cada una de las referencias que siguen desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro y de los suscriptores, siempre que sea aplicable.

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

*Ref: 6.2.1. - Controles y estándares para dispositivos criptográficos.*

*Ref: 6.2.2. – Control "M de N" de clave privada*

*Ref: 6.2.3. - Recuperación de clave privada.*

*Ref: 6.2.4. - Copia de seguridad de clave privada.*

*Ref: 6.2.5. - Archivo de clave privada.*

*Ref: 6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.*

*Ref: 6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos.*

*Ref: 6.2.8. - Método de activación de claves privadas.*

*Ref: 6.2.9. - Método de desactivación de claves privadas.*

*Ref: 6.2.10. - Método de destrucción de claves privadas.*

Jefe de Gabinete de Ministros

FOLIO 820

*Ref: 6.2.11. - Requisitos de los dispositivos criptográficos.*

**Archivo permanente de la clave pública**

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

*Ref: 6.3.1. - Archivo permanente de la clave pública.*

**Generación e instalación de datos de activación**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 6.4.1. - Generación e instalación de datos de activación.*

**Protección de los datos de activación**

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 6.4.2. - Protección de los datos de activación.*

**Otros aspectos referidos a los datos de activación**

Se deberán 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.

*Ref: 6.4.3. - Otros aspectos referidos a los datos de activación.*

**Requisitos de seguridad computacional**

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

Jefe de Gabinete de Ministros

821

*Ref: 6.5.2. - Requisitos de seguridad computacional.*

**Controles Técnicos del ciclo de vida de los sistemas**

Se deberán describir 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.

*Ref: 6.6. - Controles Técnicos del ciclo de vida de los sistemas.*

**Controles de desarrollo de sistemas**

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

*Ref: 6.6.1. - Controles de desarrollo de sistemas.*

**Controles de seguridad del ciclo de vida del software**

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

*Ref: 6.6.3. - Controles de seguridad del ciclo de vida del software.*

**Certificación de fecha y hora**

Se deberán indicar las especificaciones de los servicios de emisión de sellos de tiempo prestados por el certificador, si fuera el caso, según lo establecido en la normativa aplicable.

*Ref: 6.8. – Certificación de fecha y hora.*

**Perfiles de Certificados y de Listas de Certificados Revocados**

Se deberá incluir un perfil tipo para cada clase de certificado que se emita y para las

Jefe de Gabinete de Ministros

FOLIO 822

correspondientes listas de certificados revocados generados según la Política Única de Certificación presentada y al Anexo IV de la presente decisión administrativa.

*Ref: 7. - Perfiles de certificados y de listas de certificados revocados.*

**Auditoría de Cumplimiento y Otras Evaluaciones**

Se deberán indicar los aspectos específicos del proceso de auditoría.

*Ref: 8. – Auditoría de cumplimiento y otras evaluaciones.*

**Aranceles**

Se deberán indicar los aranceles, si fuera aplicable.

*Ref: 9.1. – Aranceles.*

**Responsabilidad Financiera**

Se deberán incluir las cláusulas que establezcan la responsabilidad por daños potenciales que podrían sufrir los suscriptores de certificados y los terceros usuarios, en razón del posible incumplimiento de lo dispuesto en las normas legales y reglamentarias y en la Política Única de Certificación y de los recursos con los que cuenta el certificador para afrontarlos.

*Ref: 9.2. - Responsabilidad Financiera.*

**Confidencialidad**

Se deberán indicar las previsiones en cuanto al tratamiento de información confidencial del certificador.

*Ref: 9.3. - Confidencialidad.*

**Información confidencial**

Jefe de Gabinete de Ministros

FOLIO 823

El certificador podrá utilizar este apartado para incluir información adicional a la establecida en la Política Única de Certificación.

*Ref: 9.3.1. - Información confidencial.*

**Responsabilidades de los roles involucrados**

Se deberán indicar las responsabilidades de los roles que gestionan información confidencial con el fin de evitar su compromiso o divulgación a personas no autorizadas.

*Ref: 9.3.3. – Responsabilidades de los roles involucrados.*

**Derechos de Propiedad Intelectual**

Se deberán incluir 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.

*Ref: 9.5. - Derechos de Propiedad Intelectual.*

**Responsabilidades y garantías**

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, deberán detallarse las garantías para el certificador licenciado, sus autoridades de registro, los suscriptores, los terceros usuarios y para otras entidades participantes y los tipos de daños cubiertos y las limitaciones de responsabilidad.

*Ref: 9.6. – Responsabilidades y garantías.*

**Deslinde de responsabilidad**

FOLIO 824

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, deberán detallarse los distintos tipos de limitaciones de responsabilidad y de daños cubiertos.

*Ref: 9.7. – Deslinde de responsabilidad.*

**Limitaciones a la responsabilidad frente a terceros**

Se deberán detallar las limitaciones de responsabilidad respecto a otras entidades participantes.

*Ref: 9.8. - Limitaciones a la responsabilidad frente a terceros.*

**Compensaciones por daños y perjuicios**

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, se deberán detallar las previsiones relativas a las compensaciones por daños y perjuicios.

*Ref: 9.9. - Compensaciones por daños y perjuicios.*

**Condiciones de vigencia**

Se deberá indicar el período de vigencia de la Política y las condiciones bajo las cuales se extinguirán los términos que rigen su aplicación.

*Ref: 9.10. - Condiciones de vigencia.*

**Gestión del ciclo de vida del documento**

Se deberán establecer las políticas para el mantenimiento y administración de la Política Única de Certificación.

*Ref: 9.12.- Gestión del ciclo de vida del documento.*

Jefe de Gabinete de Ministros

FOLIO 825

**Procedimientos de cambio**

Se deberán establecer las políticas utilizadas para efectuar modificaciones en la Política Única de Certificación.

*Ref: 9.12.1. - Procedimientos de cambio.*

**Mecanismo y plazo de publicación y notificación**

Se deberán describir los mecanismos y plazos utilizados para notificar a los suscriptores acerca de la Política Única de Certificación y de sus modificaciones.

*Ref: 9.12.2 – Mecanismo y plazo de publicación y notificación.*

**Procedimientos de resolución de conflictos**

Se deberán indicar las políticas de resolución de conflictos en la Política Única de Certificación y en los acuerdos en los que el certificador sea parte y las políticas de reclamo aplicables.

*Ref: 9.13. - Procedimientos de resolución de conflictos.*

**Conformidad con normas aplicables**

Se deberá especificar la legislación aplicable a la actividad del certificador, de existir.

*Ref: 9.15. – Conformidad con normas aplicables.*

**Otras cuestiones generales**

Se deberá incluir todo otro aspecto legal o administrativo no incluido en los apartados anteriores.

*Ref: 9.17. – Otras cuestiones generales.*

Jefe de Gabinete de Ministros

FOLIO 826

ANEXO II

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

# Requisitos para el licenciamiento de certificadores

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 827

## ÍNDICE

Jefe de Gabinete de Ministros

FOLIO 828

## INTRODUCCIÓN

De acuerdo con el inciso h) del artículo 30 de la Ley N° 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.
- Sección 2: Pautas de control a las que será sometido el solicitante para obtener la licencia, según sea el caso.
- 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 a la siguiente dirección de correo electrónico: licenciamiento@jefatura.gob.ar.

**SECCIÓN 1: DOCUMENTACIÓN QUE DEBE ENTREGAR EL SOLICITANTE PARA OBTENER UNA LICENCIA**

Para tramitar su licencia, el solicitante debe presentar ante el ente licenciante los documentos específicos relacionados con su Política Única de Certificación y, si se trata de una Persona Jurídica Privada, la documentación correspondiente a esta condición, lo cual se describe en detalle más adelante. Cada uno de los documentos deberán estar debidamente firmados y presentados como documentos electrónicos firmados digitalmente, de acuerdo a las pautas que fije el ente licenciante.

**1.- Responsables de la presentación de la solicitud**

En caso de personas jurídicas privadas, el trámite de licenciamiento, según sea el caso, se inicia con la presentación de la nota de solicitud, firmada por su representante legal o apoderado, en las condiciones establecidas en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

Si se tratara de un organismo integrante de la Administración Pública Nacional (tal como se define en el artículo 8° Ley N° 24.156 y sus modificatorias) se requerirá la presentación de una copia autenticada del acto administrativo correspondiente firmado por la máxima autoridad de la jurisdicción de que se trate, autorizando el inicio del trámite de licenciamiento, e incluyendo la información prevista en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

En caso de tratarse de un organismo provincial, municipal y de otros poderes del Estado, el acto administrativo deberá estar firmado por la máxima autoridad del organismo o jurisdicción, debiendo incluirse la información prevista en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

Si se tratara de un Registro Público de Contrato, deberá presentar documentación que acredite su condición, acompañando nota de solicitud firmada por el máximo responsable del Registro, en las condiciones establecidas en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

**2.- Documentos específicos**

Los certificadores que soliciten una licencia deben presentar:

a) Formulario de Adhesión del Anexo I, debidamente conformado.

b) Política Única de Certificación, con los datos del solicitante.

c) Acuerdo tipo con suscriptores.

d) Términos y condiciones tipo con Terceros Usuarios ("*relying parties*").

e) Política de Privacidad.

f) Contratos con los proveedores de la infraestructura tecnológica, de corresponder.

g) Manual de Procedimientos.

h) Plan de Cese de Actividades.

i) Plan de Seguridad (incluye política y procedimientos de seguridad).

j) Plan de Continuidad de las Operaciones.

k) Descripción de la plataforma tecnológica.

l) Descripción de los servicios que brinda.

**3.- 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 la INSPECCIÓN GENERAL DE JUSTICIA, organismo dependiente del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, o en el registro público de la jurisdicción que corresponda, en copia certificada.

e) Constancia de inscripción ante la ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS, entidad autárquica actuante en el ámbito del MINISTERIO DE ECONOMÍA Y FINANZAS PÚBLICAS.

f) Últimos estados contables auditados, certificados por Contador Público.

g) Comprobante de pago de iniciación del trámite.

h) Copia autenticada del poder que acredita el carácter de representante legal o apoderado de la persona autorizada a iniciar el trámite.

## SECCIÓN 2: PAUTAS DE CONTROL A LAS QUE ESTARÁ SOMETIDO EL SOLICITANTE PARA OBTENER UNA LICENCIA, SEGÚN SEA EL CASO

Toda la documentación presentada será sometida a controles legales y técnicos y se efectuarán revisiones en instalaciones del certificador, según sea el caso, como pasos previos al otorgamiento de la licencia, o el eventual rechazo de la solicitud.

Por lo tanto, el certificador deberá permitir el acceso del personal designado por el ente licenciante y por las entidades de auditoría precalificadas, a sus instalaciones, a la información y a su infraestructura tecnológica a fin de dar cumplimiento a las funciones de auditoría, de acuerdo con lo establecido en la Ley Nº 25.506 y en el Decreto Nº 2628 del 19 de diciembre de 2002 y sus modificatorios.

Los controles y auditorías a realizar, en el caso de los solicitantes de licencia cubrirán los siguientes aspectos:

I. Requisitos legales generales.

II. Política Única de Certificación y Manual de Procedimientos de Certificación.

III. Plan de Seguridad.

IV. Plan de Cese de Actividades.

V. Plan de Continuidad de las Operaciones.

VI. Plataforma Tecnológica.

VII. Ciclo de vida de las claves criptográficas del certificador.

VIII. Ciclo de vida de los certificados de suscriptores.

IX. Estructura y contenido de los certificados y CRLs.

X. Mecanismos de acceso a la documentación publicada, certificados y CRLs.

Los controles mencionados tienen por objetivo verificar el cumplimiento de los requisitos exigidos para obtener la condición de certificador licenciado.

**I) REQUISITOS LEGALES GENERALES**

Los siguientes puntos corresponden al solicitante de una licencia.

**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 Única 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 de la presente decisión administrativa, que establecen los contenidos mínimos para los siguientes documentos:

a) Acuerdos con suscriptores.

b) Términos y condiciones con Terceros Usuarios.

**4.- Política de Privacidad**

El certificador debe presentar su Política de Privacidad a los efectos de evaluarla en relación con la Política Única de Certificación. Para ello debe tener en cuenta lo expresado en el Anexo VIII de la presente decisión administrativa.

**II) POLÍTICA DE CERTIFICACIÓN Y MANUAL DE PROCEDIMIENTOS**

**1.- Contenido de la Política Única de Certificación**

La Política Única de Certificación deberá incluir los contenidos establecidos en el Anexo III de la presente decisión administrativa, excepto en los casos específicamente indicados en el Formulario de Adhesión del Anexo I.

**2.- Compatibilidad de la Política Única de Certificación y el Manual de Procedimientos**

El Manual de Procedimientos deberá adecuarse a la Política Única de Certificación y no deberá contener cláusulas contradictorias o incompatibles con ella.

**3.- Administración de la Política Única de Certificación**

El certificador deberá mantener procedimientos de administración de la Política Única de Certificación de modo de asegurar que todo cambio dispuesto por el ente licenciante o de los datos contenidos en el Formulario de Adhesión del Anexo I de la presente medida, se encuentre debidamente autorizado, aprobado y difundido.

**III) PLAN DE SEGURIDAD**

**1.- Normas que debe cumplir el Plan de Seguridad**


El Plan de Seguridad deberá cumplir con los lineamientos de la Norma IRAM ISO/IEC 27002, no siendo exigible la certificación, 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 27002, el certificador deberá mantener controles que permitan cumplir con los siguientes puntos:

- **Seguridad física y ambiental**

Se deberán mantener controles que permitan asegurar que las áreas en las cuales se desarrolle cada etapa del ciclo de vida de las claves criptográficas sean 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 se deberán implementar en cada instalación.

La infraestructura tecnológica necesaria para la generación de certificados y CRLs del certificador debe encontrarse alojada en servidores preferentemente físicos, o virtuales, 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.

FOLIO 837

- **Intercambios de información y software**

Las comunicaciones entre las autoridades de registro y la autoridad certificante referidas a la aprobación o revocación de certificados deberán ser llevadas a cabo mediante un mecanismo que garantice el no repudio.

- **Revisiones post-licenciamiento**

El ente licenciante y/o las entidades de auditoría en sus auditorías anuales o en las inspecciones extraordinarias que realice dicho ente, de acuerdo a lo establecido en los artículos 58 a 60 de la presente decisión administrativa, podrán solicitar la información relevada en las auditorías previas vinculadas al cumplimiento de la Política Única de Certificación y demás documentación aplicable.

- **Registro de eventos**

Se deberá dejar evidencia de todas las actividades realizadas sobre los registros de eventos actuales y archivados. Además se deberán 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.

FOLIO 838

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 deberán ser registrados por el certificador licenciado.

**2.- Documentos que componen el Plan de Seguridad**

- Una política de seguridad de la información, documentada y aprobada por la máxima autoridad del certificador, en la que se indicará 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 de la Política Única de Certificación y demás documentos relacionados**

El personal que participa en el proceso de certificación y en los servicios relacionados deberá conocer la Política Única de Certificación 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.

**IV) PLAN DE CESE DE ACTIVIDADES**

**1.- Publicación y notificación del cese de actividades**

Se deberá disponer de procedimientos para la publicación del cese de actividades del certificador en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA, en su

sitio web publicado en Internet y en al menos otro medio de difusión nacional y su notificación al ente licenciante, a los suscriptores de certificados y a otras entidades vinculadas, con la antelación correspondiente según lo establecido en el artículo 32 de la presente decisión administrativa.

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

Se deberá 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**

Se deberá 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**

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

**V) PLAN DE CONTINUIDAD DE LAS OPERACIONES**

**1.- Normas que debe cumplir el Plan de Continuidad de las Operaciones**

El Plan de Continuidad de las Operaciones deberá cumplir con los lineamientos de la Norma IRAM ISO/IEC 27002, no siendo exigible la certificación, sobre la

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 27002, el certificador debe mantener controles que permitan cumplir con los siguientes puntos:

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

Se deberán mantener controles que aseguren:

a) La continuidad de las operaciones en caso de compromiso de la clave privada del certificador, y

b) La reducción al mínimo posible de las eventuales interrupciones en el servicio, sobre la base de la matriz de evaluación de riesgo, que se deberá acompañar.

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.

- **Prueba del plan**

Deberá existir un procedimiento de prueba del plan de continuidad de las operaciones. El mismo deberá llevarse a cabo con una periodicidad de UN (1) año y preverse la realización de una prueba durante el período de auditoría inicial previa al licenciamiento.

**2.- Documentos que componen el Plan de Continuidad de las Operaciones**

El Plan de Continuidad de las Operaciones, documentado y aprobado por la máxima autoridad de la entidad, contendrá las acciones que se realizarán para el cumplimiento de sus objetivos y los procedimientos para su ejecución.

Se deberán documentar todas las pruebas y ejecuciones reales efectuadas.

**3.- Conocimiento del Plan de Continuidad de las Operaciones**

El personal del certificador que participa en el proceso de gestión del ciclo de vida de los certificados, deberá conocer el Plan de Continuidad de las Operaciones y los procedimientos con él relacionados y será responsable de su cumplimiento, de acuerdo a los roles asignados. Se deberán establecer mecanismos de capacitación y de documentación del compromiso de cumplimiento por parte del personal afectado.

**VI) PLATAFORMA TECNOLÓGICA**

Se deberá ajustar a los estándares tecnológicos vigentes que cubran las necesidades requeridas por el proceso de gestión del ciclo de vida de los certificados.

Se deberán implementar procedimientos que garanticen la confiabilidad de la plataforma tecnológica.

**VII) CICLO DE VIDA DE LAS CLAVES CRIPTOGRÁFICAS DEL CERTIFICADOR**

**1.- Consideraciones generales respecto de las claves criptográficas**

Deberán cumplirse los siguientes requerimientos mínimos:

- El par de claves deberá ser generado únicamente por el certificador.
- El medio de generación y almacenamiento de la clave privada utilizada en la generación de la firma deberá 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**

Deberán 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 CUATRO MIL

NOVENTA Y SEIS (4096) bits si utilizan los algoritmos RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits si utiliza el algoritmo ECDSA.

- Las claves criptográficas que los certificados utilicen en servicios relacionados con la firma digital, no podrán ser inferiores a DOS MIL CUARENTA Y OCHO (2048) bits si utilizan los algoritmos RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits, si utilizan el algoritmo ECDSA. En el caso particular de autoridades de sello de tiempo, las claves criptográficas no podrán ser inferiores a CUATRO MIL NOVENTA Y SEIS (4096) bits si utilizan los algoritmos RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits si utiliza el algoritmo ECDSA.
- Las claves criptográficas que utilicen las autoridades de registro para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación, deberán mantenerse permanentemente bajo su control, no podrán ser inferiores a DOS MIL CUARENTA Y OCHO (2048) bits si utilizan los algoritmos RSA o DSA; y DOSCIENTOS VEINTICUATRO (224) bits si utiliza el algoritmo ECDSA.

**3.- Estándares para los dispositivos criptográficos vinculados al ciclo de vida de los certificados**

Deberán respetarse las siguientes exigencias mínimas:

a) Las claves criptográficas del certificador deberán ser generadas y almacenadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.

b) Las claves criptográficas que utilicen los responsables de las autoridades de registro para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación deberán ser generadas y almacenadas en dispositivos que cumplan con certificación "overall" FIPS 140 (Versión 2) nivel 2 o superior.

**4.-Generación del par de claves criptográficas del certificador**

El certificador deberá mantener exclusivo control sobre el proceso de generación de sus claves criptográficas.

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

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

El certificador deberá disponer de 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 deberá disponer de procedimientos seguros para distribuir sus claves públicas.

**7.- Custodia de las claves criptográficas del certificador**

En caso de que el certificador guarde elementos críticos vinculados a sus claves criptográficas en dependencias de un tercero, deberá garantizar los niveles de

resguardo y la imposibilidad de que el tercero en cuestión pueda acceder a ellas y producir su activación o alteración.

**8.- Utilización de las claves privadas del certificador**

El certificador deberá disponer de 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 deberá 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 DOS (2).

**9.- Destrucción de las claves criptográficas del certificador**

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

**10.- Almacenamiento de las claves del certificador**

El certificador deberá mantener procedimientos y controles que aseguren la confidencialidad de las claves archivadas.

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

El certificador deberá 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.

## VIII) CICLO DE VIDA DE LOS CERTIFICADOS DE SUSCRIPTORES

### 1.- Registro y procesamiento de la solicitud del suscriptor

El certificador deberá 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 deberá 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 con el mismo par de claves

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

### 3.- Renovación de certificado con un nuevo par de claves

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

FOLIO 847

**5.- Distribución del certificado**

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

**6.- Aceptación del certificado**

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

**7.- Revocación del certificado**

El certificador deberá implementar procedimientos y controles que aseguren que:

a) Los certificados sean revocados conforme a solicitudes autorizadas y válidas de revocación.

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 respeten los plazos de revocación establecidos en la Política Única de Certificación.

**8.- Suspensión del certificado**

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

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

El certificador deberá 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).

El formato, codificación, contenido e interpretación de los certificados digitales y listas de certificados revocados (CRL) deberán ajustarse a los contenidos definidos en el Anexo IV- Perfiles de los Certificados y de las Listas de Certificados Revocados.

## IX) 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 la Política Única de Certificación y a otras políticas que hayan sido aprobadas, 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, debiendo garantizar el acceso permanente, eficiente y gratuito de los titulares al repositorio de certificados revocados, según lo dispuesto por el inciso g) del artículo 34 del Decreto N° 2628/02 y sus modificatorios. Adicionalmente, podrá hacerlo por 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 Única de Certificación y el Manual de Procedimientos de Certificación (en sus partes públicas) y 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 como con el ente licenciante. Debe proveer como mínimo: denominación del servicio de atención de consultas, dirección de correo electrónico y número de teléfono.

**5.- Actualización**

El certificador es responsable de actualizar estas publicaciones cada vez que sean modificadas.

**6.- 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, en los puntos aplicables, deberá mantener la confidencialidad e integridad de los registros de eventos actuales y archivados. Deberá 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 licenciamiento (tales como, autoridad certificante, autoridad de registro, suscriptor, Tercero Usuario, servidor de aplicación, etcétera).

| | Información Registrada |
|---|---|
| Contenido mínimo a registrar | a) Fecha y hora del registro.<br>b) Número de serie o secuencia del registro.<br>c) Tipo de registro.<br>d) Fuente del registro (Ej.: terminal, puerto, etcétera).<br>e) Identificación de la entidad que efectuó el registro. |

| | Eventos a Registrar |
|---|---|
| Administración del ciclo de vida de las claves criptográficas del certificador | a) Generación y almacenamiento de las claves criptográficas.<br>b) Resguardo de las claves criptográficas.<br>c) Recuperación de las claves criptográficas.<br>d) Utilización de las claves criptográficas.<br>e) Archivo de las claves criptográficas.<br>f) Retiro de servicio de datos relacionados con las claves criptográficas.<br>g) Destrucción de las claves criptográficas.<br>h) Identificación de la entidad que autoriza una operación de administración de las claves criptográficas.<br>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).<br>j) Compromiso de la clave privada. |

| | |
|---|---|
| Administración del ciclo de vida de los certificados | a) Recepción de solicitudes de certificados (inicial, de renovación con el mismo o un nuevo par de claves).<br>b) Transferencia de claves públicas para la emisión del certificado.<br>c) Cambios en los datos de la solicitud del certificado.<br>d) Generación de certificados.<br>e) Distribución de la clave pública del certificador.<br>f) Solicitudes de revocación de certificados.<br>g) Generación y emisión de listas de certificados revocados.<br>h) Acciones tomadas en relación con la expiración de un certificado. |
| Administración del ciclo de vida de los dispositivos criptográficos | a) Recepción del dispositivo.<br>b) Ingreso o retiro del dispositivo del lugar de almacenamiento.<br>c) Instalación del dispositivo<br>d) Uso del dispositivo.<br>e) Desinstalación del dispositivo.<br>f) Envío de dispositivos para servicio técnico o reparación.<br>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.<br>b) Otra información de identificación, en caso de ser aplicable.<br>c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación.<br>d) Identificación de la entidad que recibe y acepta la solicitud.<br>e) Método utilizado para validar los documentos de identificación.<br>f) Identificación de la autoridad de registro, de ser aplicable. |

| | |
|---|---|
| Eventos de seguridad | a) Lectura o modificación de archivos o registros críticos de seguridad, incluyendo el registro diario de eventos.<br>b) Borrado de datos críticos.<br>c) Cambios en los perfiles de seguridad.<br>d) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos.<br>e) Caídas del sistema, fallas en el hardware y software, u otras anomalías.<br>f) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad.<br>g) Cambios en la relación entre el certificador o sus autoridades certificantes con:<br>• Sus autoridades de registro.<br>• El personal relacionado con el proceso de certificación.<br>h) Modificaciones en los procesos o procedimientos de cifrado y/o autenticación.<br>i) Accesos al sistema de la autoridad certificante o a cualquiera de sus componentes. |

| | Observaciones generales |
|---|---|
| Información crítica<br><br>Sincronización de eventos | a) Los registros de eventos no deben reflejar los valores en texto plano de claves privadas o contraseñas.<br><br>b) Los relojes de las computadoras deben estar sincronizados con un desvío menor a UN (1) 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.<br><br>c) Toda información de horarios deberá estar expresada en formato: yyyy/mm/dd hh:mm:ss huso-horario. |

FOLIO 856

## SECCIÓN 4: CONTROLES FÍSICOS

En esta sección se definen los niveles de seguridad física mínimos exigidos para las áreas funcionales del certificador que solicite una licencia. Lo dispuesto contempla tanto a las autoridades certificantes como a sus autoridades de registro, cuando sea aplicable.

Los requerimientos de seguridad descriptos a continuación representan la exigencia mínima a cumplir y consideran niveles de acceso físico numerados de UNO (1) a SEIS (6), con características de seguridad crecientes. Toda barrera y control de seguridad que no cumpla con todos y cada uno de los requisitos establecidos en esta sección, no podrá ser considerado como el paso a un área de mayor nivel de seguridad. Se aclara que los niveles CINCO (5) y SEIS (6) se destinan únicamente a la guarda de elementos críticos vinculados a las claves privadas.

Sin perjuicio de los controles que se detallan a continuación, siempre debe estar en condiciones de funcionamiento comprobado la opción de salida de emergencia, con los controles que aseguren su apropiada utilización y eviten cualquier exposición.

### Ubicación de las instalaciones

Los certificadores que soliciten una licencia deben detallar los aspectos de construcción de las instalaciones de sus áreas funcionales, referidos a los controles de seguridad física.

Las autoridades de registro pueden funcionar en una ubicación física diferente a las autoridades certificantes o bien prestar un servicio en una instalación móvil siempre

que no se vulneren los controles de seguridad que garanticen un proceso confiable de aprobación de solicitudes de emisión, renovación o revocación de certificados.

**Seguridad física de una autoridad certificante**

Las autoridades certificantes deberán implementar un sistema de seguridad física que cuente con CUATRO (4) niveles de acceso físico, por lo menos, para llegar desde las áreas de libre circulación al ambiente donde reside su equipamiento informático afectado a la firma de certificados y CRLs. Además cada certificador deberá disponer de DOS (2) niveles adicionales para la protección de los elementos críticos vinculados a la activación de la clave privada de cada autoridad certificante y otros elementos críticos. Estos DOS (2) niveles pueden consistir en cajas de seguridad, gabinetes reforzados o compartimentos, de uso exclusivo de cada certificador. Debe tenerse en cuenta que en el caso que varias autoridades certificantes pertenecientes a distintos certificadores licenciados utilicen la misma infraestructura tecnológica, se deberá contar con N+1 cajas de seguridad, gabinetes o compartimentos, siendo N la cantidad de certificadores licenciados, a los que se agrega un contenedor adicional para el resguardo de otros elementos de operación del dispositivo criptográfico "HSM" (Hardware Security Module), que deban ser compartidos.

Las claves privadas de las autoridades certificantes podrán residir en particiones físicas o lógicas siempre que se garantice la exclusividad en el acceso establecida en la Ley Nº 25.506 (artículo 21, inciso c).

La ubicación del área funcional de las autoridades certificantes no deberá tener identificación visible.

FOLIO 858

Los requerimientos de seguridad física de la autoridad certificante abarcan:

a) Operaciones de baja complejidad.

b) Operaciones de alta complejidad.

c) Resguardo de elementos críticos de activación de la clave privada.

**a. Seguridad Física de las Operaciones de baja complejidad de una autoridad certificante**

Se definen como de baja complejidad a todas las operaciones de la autoridad certificante, con excepción de las vinculadas con el proceso de firma propiamente dicho y de las que requieran el acceso físico a los equipos informáticos asignados a la firma de certificados y CRLs. Estas operaciones de baja complejidad deberán realizarse en un nivel 3 de seguridad física, como mínimo.

Se aclara que todo lo referido a las autoridades de registro se trata en el apartado correspondiente.

El nivel 1 se considera a partir de la primera barrera de control de las dependencias donde se encuentre alojada la autoridad certificante. Para acceder a este nivel, todo individuo deberá ser identificado y su ingreso debidamente registrado.

El nivel 2 debe ser interno al nivel 1. Se deberá exigir el registro de ingreso, por medio electrónico, y el uso de una identificación visible a las personas que permanezcan en él. A partir de este nivel, los equipos de grabación, fotográficos, de video u otros dispositivos electrónicos, así como computadoras portátiles, tendrán su entrada registrada y sólo podrán ser utilizados mediante autorización formal y bajo supervisión.

El nivel 3 debe ser interno al nivel 2, de uso exclusivo de los certificadores que utilicen una misma plataforma tecnológica compartida y únicamente utilizado para tareas específicas de las autoridades certificantes. Por lo tanto, no podrá compartirse con otras áreas funcionales de la organización del certificador o proveedor de la plataforma tecnológica. Para el ingreso de personas que no estén relacionadas con las operaciones de las autoridades certificantes, se requiere autorización expresa de los responsables de los certificadores involucrados y en su permanencia, deberán estar acompañadas por UNA (1) persona designada formalmente para ello. En este nivel deberán ser registradas tanto las entradas como las salidas de cada persona. La identificación deberá realizarse por DOS (2) métodos distintos, tanto para la entrada como para la salida, tales como tarjeta de identificación electrónica, contraseña de ingreso o identificación biométrica.

En este nivel se ubicará el equipamiento destinado a la gestión de la infraestructura de firma digital de los certificadores, tales como la administración del firewall, de los servidores web, bases de datos, etcétera.

Será permitido el acceso lógico al equipamiento descripto en el párrafo anterior desde la intranet o remoto, vía VPN (L2TP, PPTP, IPSEC o los protocolos que los remplacen en el futuro) siempre y cuando se garantice la autenticación de doble vía mediante certificados digitales, dispositivos criptográficos o del tipo OTP (One Time Password), OATH (Initiative for Open Authentication), OCRA (Challenge/Response Algorithms Specification), TOTP (Time-based One-time Password Algorithm) o similar.

Los teléfonos celulares y equipos de comunicación necesarios para las operaciones de las autoridades certificantes, si fuera el caso, sólo se pueden ingresar a este nivel previa autorización expresa y registración.

**b. Seguridad Física de las operaciones de alta complejidad de una autoridad certificante**

Se definen como de alta complejidad aquellas operaciones de una autoridad certificante vinculadas con el proceso de firma y las que requieren acceso físico a los equipos informáticos asignados a la firma de certificados y CRLs. Las mismas se deberán realizar en un nivel 4 de seguridad física.

El nivel 4 debe ser interno al nivel 3 y repetir los mismos controles de acceso físico que los descriptos para ese nivel. Para realizar cualquier actividad en este nivel se requiere la presencia de al menos DOS (2) operadores autorizados por todos los certificadores involucrados. Las personas ajenas al área deberán ingresar acompañadas de por lo menos DOS (2) personas autorizadas formalmente para ello.

Las operaciones críticas de emisión o revocación de certificados deberán ser realizadas en ambientes cerrados, físicamente protegidos, no compartidos con otras áreas de la organización, y exclusivos para funciones vinculadas a los procesos de certificación digital. Se podrán compartir infraestructuras físicas entre autoridades certificantes del mismo o de distintos certificadores, siempre que se implementen adecuados controles que impidan los accesos no autorizados o que pudieran afectar la seguridad de los procesos de certificación.

**c. Seguridad física para el reguardo de los elementos de activación de la clave privada de la autoridad certificante**

La seguridad física para la protección de los elementos críticos de activación de la clave privada de firma de la autoridad certificante corresponde a los niveles 5 y 6.

El nivel 5 debe ser interno al nivel 4 descripto anteriormente y estar constituido por una caja de seguridad, gabinete reforzado con cerradura o compartimento de acceso exclusivo, con una disposición interna de manera tal que permita la protección individual de distintos componentes críticos. Este nivel funciona como un perímetro de seguridad física que permite administrar el acceso a los elementos protegidos contenidos en dicha caja, gabinete o compartimento.

El nivel 6 debe ser interno al nivel 5 y contar con una disposición interna según se describe precedentemente. La función de la disposición interna de la caja o gabinete es almacenar los elementos de activación de la clave privada de la autoridad certificante.

Cada certificador deberá contar con su propio ambiente de nivel 5 y cada autoridad certificante, con su nivel 6 de protección.

**Seguridad física de una autoridad de registro**

Las autoridades de registro deben implementar un sistema de seguridad física que garantice su correcto funcionamiento y la protección adecuada de la información y documentación presentada por el solicitante o titular. En este sentido, deberán extremarse las medidas que impidan el acceso no autorizado al puesto de trabajo de la autoridad de registro y a la documentación que se le confía para su resguardo, así

como a los datos de los solicitantes. Deberán contar asimismo con adecuados procedimientos y mecanismos de recuperación frente a eventos imprevistos.

Las autoridades de registro podrán realizar su actividad en puestos móviles cuando se presenten las condiciones que ameriten tal servicio, siempre que lo haya aprobado el ente licenciante y no se vulneren los controles de seguridad que garanticen un proceso confiable de aprobación de solicitudes de emisión, renovación o revocación de certificados.

**Consideraciones para certificadores licenciados que operen más de UNA (1) autoridad certificante**

En el caso que el certificador licenciado opere más de UNA (1) autoridad certificante, todos los controles físicos definidos en esta sección pueden ser compartidos por las distintas autoridades certificantes, con excepción del nivel 6, donde cada autoridad certificante deberá tener sus propios compartimentos con llave.

**Consideraciones para certificadores licenciados que compartan UNA (1) misma infraestructura tecnológica**

En el caso que DOS (2) o más certificadores licenciados operen sus autoridades certificantes en UNA (1) misma infraestructura tecnológica, podrán compartir todos los controles físicos definidos en esta sección excepto el nivel 5 de protección de los elementos de activación. En este caso cada certificador deberá tener su propia caja de seguridad, gabinete reforzado o compartimento de acceso exclusivo y cada autoridad certificante deberá contar con su propio nivel 6, interno al anterior.

Jefe de Gabinete de Ministros

FOLIO 863

ANEXO III

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley Nº 25.506**

# Política Única de Certificación

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 864

## CARACTERÍSTICAS DEL DOCUMENTO

Este documento describe la estructura y el contenido al que deben adherir las Políticas de Certificación de las entidades que soliciten una licencia en el marco de la Infraestructura de Firma Digital de la República Argentina, en los términos de la Ley de Firma Digital Nº 25.506. Para su elaboración se han tenido en cuenta los lineamientos del RFC 3647, producido por el IETF, el estándar X9.79 de la ANSI, la especificación ITU-T X.509, el estándar ISO 3166 y las recomendaciones RFC 3739 y 5280. Se aclara que para la versión anterior de este Anexo (denominado Anexo II en la Decisión Administrativa N° 6/2007, hoy derogada) se utilizó el RFC 2527, declarado obsoleto por el IETF y reemplazado por el RFC 3647 antes referido.

Las Políticas de Certificación emitidas por los certificadores deben adherir a los contenidos, la estructura y el ordenamiento (índice) del presente documento y solo podrán completar los datos incluidos en el Formulario de Adhesión del Anexo I de la presente decisión administrativa.

Para integrar la Infraestructura antes mencionada, los certificadores deberán presentar el Formulario de Adhesión del Anexo I de la presente decisión administrativa por cada tipo de certificado que emitan, acompañado de toda la documentación requerida en el Anexo II. Una vez cumplidos y aprobados los requisitos para el licenciamiento, el ente licenciante emitirá un acto administrativo otorgando la respectiva licencia.

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 a la dirección de correo electrónico: licenciamiento@jefatura.gob.ar.

Jefe de Gabinete de Ministros

FOLIO 865

## INDICE

Jefe de Gabinete de Ministros

FOLIO 866

Jefe de Gabinete de Ministros

FOLIO 867

Jefe de Gabinete de Ministros

FOLIO 868

Jefe de Gabinete de Ministros

FOLIO 869

**INSTRUCCIONES PARA LA CONFORMACIÓN DE LA POLÍTICA ÚNICA DE CERTIFICACIÓN**

El presente documento contiene lineamientos específicos respecto al texto que deben incluir las Políticas de Certificación de los certificadores licenciados en el marco de la Ley N° 25.506. Su contenido solo debe ser modificado para incluir los aspectos particulares del certificador en los puntos expresamente indicados y referidos en el Anexo I de la presente Decisión Administrativa, no debiéndose agregar o eliminar contenido, excepto donde se señale puntualmente.

De esta manera, se habilita que los certificados digitales que emitan los certificadores licenciados en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, puedan ser utilizados por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción que lo requiera y para realizar procesos, tales como la autenticación o el cifrado, para los cuales han sido habilitados.

La Política Única de Certificación a presentar por cada certificador a los fines del licenciamiento deberá contener las secciones y los contenidos que siguen:

**1. - INTRODUCCIÓN**

**1.1. - Descripción general**

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

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

**1.2. - Nombre e Identificación del Documento**

Se incluirá la identificación de la Política Única de Certificación, incorporando información tal como: versión, revisión, fecha de aplicación, lugar o sitio de publicación, etcétera e incluirá el Identificador de Objeto (OID) correspondiente a la Política cuando le sea otorgado por la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (ONTI) por pedido del ente licenciante, como paso previo a su licenciamiento y de manera tal que permita una identificación apropiada.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**1.3. - Participantes**

Integran la infraestructura del certificador las siguientes entidades:

**1.3.1. - Certificador**

Se identificará al certificador que presenta la Política Única de Certificación correspondiente a su Autoridad Certificante, indicando respectivamente datos de identificación tales como razón social, denominación del organismo, dirección postal, etcétera.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**1.3.2. - Autoridad de Registro**


Se identificarán en forma directa o a través de un enlace a un sitio web de Internet, 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 incluir el domicilio y datos de contacto de cada una de las mismas.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**1.3.3. - Suscriptores de certificados**

Se indicará si los certificados digitales emitidos bajo la presente Política Única de Certificación tienen como suscriptores personas físicas, jurídicas o aplicaciones, especificando para este último caso si se trata de sitios seguros. Se precisará la comunidad de suscriptores habilitados, sin perjuicio de su posible ampliación previa notificación al ente licenciante.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**1.3.4. - Terceros Usuarios**

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**1.4. - Uso de los certificados**

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

### 1.5. - Administración de la Política

#### 1.5.1. - Responsable del documento

Se incluirán los datos de un responsable del certificador para actuar como nexo incluyendo denominación del servicio de atención de consulta, dirección de correo electrónico institucional y número de teléfono.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

#### 1.5.2. - Contacto

Se incluirán los datos del Responsable del registro, mantenimiento e interpretación de la Política Única de Certificación.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

La Política Única de Certificación y el Formulario de Adhesión del Anexo I han sido presentados ante el ente licenciante durante el proceso de licenciamiento aprobado por Acto Administrativo ..... (a completar especificando los datos completos del acto administrativo por el cual se obtuvo la licencia).

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

### 1.6. - Definiciones y Acrónimos

#### 1.6.1. - Definiciones

Se incluirán las definiciones de los conceptos relevantes utilizados en la Política Única de Certificación, incluyendo los siguientes:

- Autoridad de Aplicación: la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.

Jefe de Gabinete de Ministros

FOLIO 873

- Autoridad de Registro: es la entidad que tiene a su cargo las funciones de:

- Recepción de las solicitudes de emisión de certificados.
- Validación de la identidad y autenticación de los datos de los titulares de certificados.
- Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
- Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
- Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
- Identificación y autenticación de los solicitantes de revocación de certificados.
- Archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

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

- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).
- Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. (artículo 17 de la Ley N° 25.506).

FOLIO 874

- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. (Anexo al Decreto N° 2628 de fecha 19 de diciembre de 2002).
- Ente licenciante: la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS es Ente Licenciante.
- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL). (Anexo al Decreto N° 2628/02)
- Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS). (Anexo al Decreto N° 2628/02)
- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02)
- Plan de Continuidad de las operaciones: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado. (Anexo al Decreto N° 2628/02)
- Política de Privacidad: conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

FOLIO 875

- Servicio OCSP (Protocolo en línea del estado de un certificado – "Online Certificate Status Protocol"): servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.
- Suscriptor o Titular de certificado digital: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- Tercero Usuario: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. (artículo 3° del Decreto N° 724/06).

**1.6.2. - Acrónimos**

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

CUIT - Clave Única de Identificación Tributaria

IEC - International Electrotechnical Commission

IETF - Internet Engineering Task Force

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

OID - Identificador de Objeto ("Object Identifier")

ONTI - Oficina Nacional de Tecnologías de Información

RFC - Request for Comments

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

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

FOLIO 876

Se detallan a continuación las responsabilidades del certificador y de todo otro participante respecto al mantenimiento de repositorios, publicación de certificados y de información sobre sus políticas y procedimientos.

**2.1. - Repositorios**

Se indicarán las entidades que administran los repositorios, señalando 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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**2.2. - Publicación de información del certificador**

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

a) Formulario de Adhesión del Anexo I.

b) Política Única de Certificación.

c) Acuerdo Tipo con suscriptores.

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

e) Política de Privacidad.

f) Manual de Procedimientos (parte pública).

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

h) Repositorio de certificados revocados.

i) Certificados del certificador licenciado y acceso al de la Autoridad Certificante Raíz.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**2.3. - Frecuencia de publicación**

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

**2.4. - Controles de acceso a la información**

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

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

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

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**3. - IDENTIFICACIÓN Y AUTENTICACIÓN**

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

**3.1.- Asignación de nombres de suscriptores**

**3.1.1. - Tipos de Nombres**

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

FOLIO 878

**3.1.2. - Necesidad de Nombres Distintivos**

Nota para el certificador: Se indicarán las siguientes denominaciones, según el tipo de certificados que se emitan.

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

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

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

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

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

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

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

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

Para los certificados de **Personas Físicas**:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponderse con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.

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

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

- En caso de ciudadanos argentinos o residentes: "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral.

- En caso de extranjeros:

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

  - "EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.

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

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

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

Jefe de Gabinete de Ministros

FOLIO 880

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

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

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

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

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

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

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

Para los certificados de **sitio seguro**:

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

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

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

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

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

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

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**3.1.3. - Anonimato o uso de seudónimos**

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

**3.1.4. - Reglas para la interpretación de nombres**

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con los correspondientes al documento de identidad del suscriptor o con la documentación presentada por la persona jurídica. Las discrepancias o conflictos que puedan generarse si los datos de los solicitantes o suscriptores contienen caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

**3.1.5. - Unicidad de nombres**

Jefe de Gabinete de Ministros

FOLIO 882

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

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

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

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

**3.2. - Registro Inicial**

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

El certificador DEBE cumplir con lo establecido en:

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

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

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

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

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

Nota para el certificador: se indicará como "No Aplicable" cuando solo se emitan certificados para Personas Físicas.

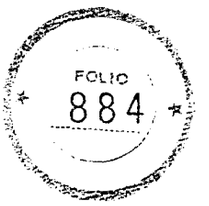
Los procedimientos de autenticación de la identidad de los suscriptores de los certificados de personas jurídicas públicas o privadas comprenden los siguientes aspectos:

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

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

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

d) La identidad de la Persona Jurídica titular del certificado o responsable del servicio, aplicación o sitio web deberá ser verificada mediante documentación que acredite su condición de tal. Estos datos se incluirán en el Formulario de Adhesión del Anexo I.




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

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

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

c) El artículo 34, inciso 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 custodia de las claves criptográficas.

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

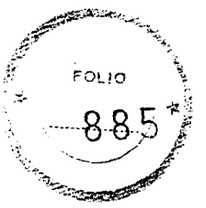
**3.2.3. - Autenticación de la identidad de Personas Físicas**

Nota para el certificador: se indicará como "No Aplicable" cuando solo se emitan certificados para Personas Jurídicas.

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

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

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




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

Se consideran obligatorias las exigencias reglamentarias impuestas por:

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

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

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

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

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

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

**3.2.4. - Información no verificada del suscriptor**

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

**3.2.5. - Validación de autoridad**

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

**3.2.6. - Criterios para la interoperabilidad**

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

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

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

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

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

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

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

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

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

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

**3.3.2. - Generación de UN (1) certificado con el mismo par de claves**

FOLIO 887

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

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

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

**3.4. - Requerimiento de revocación**

Se incluirán los procedimientos a seguir para validar la identidad del solicitante de la revocación de UN (1) certificado, incluyendo la documentación del proceso.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS**

**4.1. - Solicitud de certificado**

**4.1.1. - Solicitantes de certificados**

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

**4.1.2. - Solicitud de certificado**

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

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2. - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas y 3.2.3. - Autenticación de la identidad de Personas Físicas, así como la constancia de C.U.I.T. o

FOLIO 888

C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores de certificados.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**4.2. - Procesamiento de la solicitud del certificado**

En esta sección debe incluirse UNA (1) descripción de las condiciones y procedimientos utilizados para aceptar o rechazar la solicitud de un certificado.

Seindicarán los plazos aplicables para la aceptación o rechazo de una solicitud, así como toda la información relativa a la tramitación de su certificado, de acuerdo al inciso h) del artículo 21 de la Ley N° 25.506.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.3. - Emisión del certificado**

**4.3.1. - Proceso de emisión del certificado**

Cumplidos los recaudos del proceso enunciado en el apartado 4.1.2. Solicitud de certificado y una vez aprobada la solicitud de certificado por la Autoridad de Registro correspondiente, la Autoridad Certificante emitirá el certificado firmándolo digitalmente y lo pondrá a disposición del suscriptor.

En el mismo sentido, se emitirá un certificado ante una solicitud de renovación.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**4.3.2. - Notificación de emisión**

Se deberán establecer las condiciones para la notificación de la emisión de un certificado a su titular.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.4. - Aceptación del certificado**

Se establecerán los requisitos y procedimientos referidos a la publicación del certificado y a su aceptación por el suscriptor. Asimismo, se establecerán los procedimientos de notificación de emisión a otras entidades, de ser aplicable.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

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

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

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;

c) Solicitar la revocación de su certificado al certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

De acuerdo a lo establecido en la presente Decisión Administrativa:

- Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.
- Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la presente Política Única de Certificación.
- Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

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

Los Terceros Usuarios deben:

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

b) Verificar la validez del certificado digital.

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

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

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

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

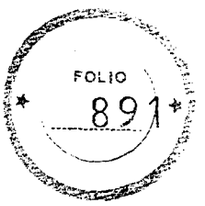
Si la solicitud de UN (1) nuevo certificado se realiza antes de la expiración del anterior, no habiendo sido este revocado, no se exigirá la presencia física, debiendo el solicitante remitir la constancia firmada digitalmente del inicio del trámite de renovación.

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

**4.8. - Modificación del certificado**

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

**4.9. - Suspensión y Revocación de Certificados**




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

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

**4.9.1. - Causas de revocación**

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

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación (Nota para el certificador: se deberá indicar lo que corresponda).
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por Resolución de la Autoridad de Aplicación.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.

- Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, del Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
- Por revocación de su propio certificado digital.

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

**4.9.2. - Autorizados a solicitar la revocación**

Se encuentran autorizados para solicitar la revocación de UN (1) certificado:

a) El suscriptor del certificado.

b) El responsable autorizado que efectuara el requerimiento, en el caso de certificados de persona jurídica o de aplicación.

c) El responsable autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación, en el caso de los certificados de aplicación.

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

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

f) El certificador o la Autoridad de registro operativamente vinculada.

g) El ente licenciante.

h) La autoridad judicial competente.

i) La Autoridad de Aplicación.

**4.9.3. - Procedimientos para la solicitud de revocación**

Jefe de Gabinete de Ministros

FOLIO 893

El certificador garantiza que:

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

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

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

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

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

Deberán indicarse las vías de contacto disponibles para la realización de la solicitud de revocación y para la comunicación del cambio de estado del certificado.

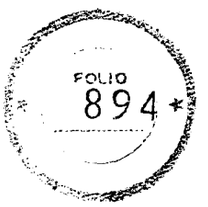
Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**4.9.4. - Plazo para la solicitud de revocación**

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

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

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




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

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

Los Terceros Usuarios deben 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.

La autenticidad y validez de las listas de certificados revocados también debe ser confirmada mediante la verificación de la firma digital del certificador que la emite y de su período de validez.

El certificador cumple con lo establecido en el artículo 34, inciso 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.

**4.9.7. - 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 Única de Certificación, debiendo emitirse como mínimo cada VEINTICUATRO (24) horas.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.9.8.- Vigencia de la lista de certificados revocados**

Se indicará la vigencia de cada lista de certificados revocados, y cada lista indicará la fecha de emisión de la siguiente.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

El certificador pone a disposición de los interesados la posibilidad de verificar el estado de un certificado por medio del acceso a la lista de certificados revocados 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.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**4.9.10. - 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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.9.11. - 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.


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 párrafo anterior.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

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

**4.9.13. - Causas de suspensión**

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

**4.9.14. - Autorizados a solicitar la suspensión**

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

**4.9.15. - Procedimientos para la solicitud de suspensión**

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

**4.9.16. - Límites del período de suspensión de un certificado**

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

**4.10. – Estado del certificado**

**4.10.1. – Características técnicas**

Se describirán las características de los servicios disponibles para la verificación del estado de los certificados emitidos.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.10.2. – Disponibilidad del servicio**

Se detallarán las políticas aplicables para los servicios descriptos en el apartado anterior, incluyendo las consecuencias de la interrupción del servicio.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.10.3. – Aspectos operativos**

Se indicará cualquier otro aspecto de los servicios de verificación del estado de los certificados.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**4.11. – Desvinculación del suscriptor**

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

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

**4.12. – Recuperación y custodia de claves privadas**

El certificador licenciado no podrá bajo ninguna circunstancia realizar la recuperación o custodia de claves privadas de los titulares de certificados digitales, en virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 25.506. El suscriptor se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley antes mencionada.

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

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

**5.1. - Controles de seguridad física**

Se cuenta con controles de seguridad relativos a:

a) Construcción y ubicación de instalaciones

b) Niveles de acceso físico.

c) Comunicaciones, energía y ambientación.

d) Exposición al agua.

e) Prevención y protección contra incendios.

f) Medios de almacenamiento.

g) Disposición de material de descarte.

h) Instalaciones de seguridad externas.

**5.2. - Controles de Gestión**

Se cuenta con controles de seguridad relativos a:

a) Definición de roles afectados al proceso de certificación.

b) Número de personas requeridas por función.

c) Identificación y autenticación para cada rol.

d) Separación de funciones.

**5.3. - Controles de seguridad del personal**

Se cuenta con controles de seguridad relativos a:

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

b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.

d) Frecuencia de procesos de actualización técnica.

e) Frecuencia de rotación de cargos.

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

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

**5.4. - Procedimientos de Auditoría de Seguridad**

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

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

a) Tipo de eventos registrados. Debe respetarse lo establecido en el Anexo II Sección 3.

b) Frecuencia de procesamiento de registros.

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

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

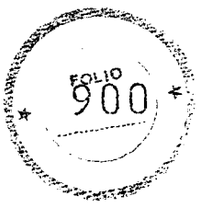
e) Procedimientos de resguardo de los registros.

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

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

h) Evaluación de vulnerabilidades.

**5.5. - Conservación de registros de eventos**




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

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

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

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

a) Tipo de registro archivado. Debe respetarse lo establecido en el Anexo II Sección 3.

b) Período de guarda de los registros.

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

d) Procedimientos de resguardo de los registros.

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

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

g) Procedimientos para obtener y verificar la información archivada.

**5.6. - Cambio de claves criptográficas**

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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

FOLIO 901

**5.7. - Plan de respuesta a incidentes y recuperación ante desastres**

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

Se han desarrollado procedimientos referidos a:

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

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

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

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

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

**5.8. - Plan de Cese de Actividades**

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

Se han implementado procedimientos referidos a:

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

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


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

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

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

**6. - CONTROLES DE SEGURIDAD TECNICA**

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

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

La generación e instalación del par de claves deben ser consideradas desde la perspectiva de las autoridades certificantes 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

f) Controles de calidad de los parámetros de generación de claves.

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.1.1. - Generación del par de claves criptográficas**

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

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

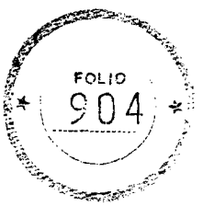
Debe respetarse lo establecido en el Anexo II Sección 2 respecto de generación del par de claves.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.1.2. - Entrega de la clave privada**

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

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




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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**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 II Sección 2 respecto de las longitudes mínimas de las claves.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

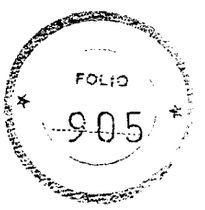
**6.1.6. - Generación de parámetros de claves asimétricas**

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

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




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

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, siempre que sea aplicable. 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) Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico.

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

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

g) Procedimiento de destrucción de la clave privada.

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.1. – Controles y 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 II Sección 2 respecto de los estándares para dispositivos criptográficos.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

Los controles empleados para la activación de las claves se basan en la presencia de M de N con M mayor a 2. Estos controles son desarrollados con mayor detalle en los documentos específicos.

**6.2.3. - Recuperación de clave privada**

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.4. - Copia de seguridad de clave privada**

Se describen los procedimientos y controles de seguridad empleados para la realización de copias de seguridad de las claves privadas del certificador, garantizándose que no disminuyen los niveles de seguridad de dichas claves por la creación de copias de seguridad.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**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, garantizándose que su seguridad no disminuya por el proceso de archivo.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.6. - Transferencia de claves privadas en dispositivos criptográficos**

Si fuera aplicable, se describen los procedimientos para que un suscriptor transfiera 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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos**

Se describen las condiciones bajo las cuales se almacenan las claves privadas en dispositivos criptográficos.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.8. - Método de activación de claves privadas**

Se describen los requisitos, roles y procedimientos necesarios para la activación de la clave privada del certificador y se utilizan métodos adecuados para la autenticación de la identidad de los responsables.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.9. - Método de desactivación de claves privadas**

Se describen los requisitos, roles y procedimientos necesarios para la desactivación de la clave privada del certificador, requiriéndose la autenticación de la identidad de los responsables a través de métodos adecuados.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.10. - Método de destrucción de claves privadas**

Se especifican las políticas 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. Estos controles son desarrollados con mayor detalle en los documentos específicos.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.2.11. – Requisitos de los dispositivos criptográficos**

Se indican las especificaciones de los dispositivos criptográficos, debiendo respetarse lo establecido en el Anexo II Sección 2 respecto de su utilización.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**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 describen las políticas y controles de seguridad implementados para archivar la clave pública, incluyendo el software y hardware que se deberán preservar, para permitir la posterior utilización de esa clave. Dichos controles incluyen 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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

Las claves privadas correspondientes a los certificados emitidos por el certificador podrán ser utilizadas por los suscriptores 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 establecen medidas suficientes de seguridad para proteger los datos de activación requeridos para la operación de los dispositivos criptográficos de los usuarios de certificados.

**6.4.1. - Generación e Instalación de datos de activación**

Se brinda la información suficiente y de ser posible los mecanismos, para promover que los suscriptores utilicen datos robustos de activación de sus claves privadas.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**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.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.5. - Controles de seguridad informática**

**6.5.1. - Requisitos Técnicos específicos**

Se establecen los requisitos de seguridad referidos al equipamiento y al software del certificador, cuyo detalle se encuentra en el Manual de Procedimientos.

Dichos requisitos se vinculan con los siguientes aspectos:

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. - Requisitos de seguridad computacional**

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

Se describen 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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.6.1. - Controles de desarrollo de sistemas**

FOLIO 911

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.6.2. – Controles de gestión de seguridad**

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

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

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.7. - Controles de seguridad de red**

Se describen los mecanismos utilizados para proteger los servicios de certificación de ataques que pudieran ser ejecutados a través de redes a las que se encuentre conectado.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**6.8. – Certificación de fecha y hora**

Se indican las especificaciones de los servicios de emisión de sellos de tiempo prestados por el certificador, según lo establecido en la normativa aplicable.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

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

Nota: Los datos correspondientes a esta sección se incluirán en el Formulario de Adhesión del Anexo I.

Jefe de Gabinete de Ministros

FOLIO 912

Se especifican 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 o la que en su defecto, determine el Ente Licenciante, y deben cumplir con las indicaciones establecidas en la sección "2 - Perfil de certificados digitales" del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados.

**7.1.1. - Número de versión**

A completar sobre la base de lo establecido en el documento referido en el apartado 2.2 del Anexo IV.

**7.1.2. - Extensiones**

A completar sobre la base de lo establecido en el documento referido en 2.3 del Anexo IV.

**7.1.3. - Identificadores de algoritmos**

A completar sobre la base de lo establecido en el documento referido en 2.2 del Anexo IV.

**7.1.4. - Formatos de nombre**

A completar sobre la base de lo establecido en el documento referido en 2.2 del Anexo IV.

**7.1.5. - Restricciones de nombre**

A completar sobre la base de lo establecido en el documento referido en 2.2 del Anexo IV.

**7.1.6. - OID de la Política de Certificación**

A completar sobre la base de lo establecido en el documento referido en 2.3 del Anexo IV.

**7.1.7. - Sintaxis y semántica de calificadores de Política**

A completar sobre la base de lo establecido en el documento referido en 2.3 del Anexo IV.

**7.1.8. - Semántica de procesamiento para extensiones críticas**

A completar sobre la base de lo establecido en el documento referido en 2.3 del Anexo IV.

**7.2. - Perfil de la lista de certificados revocados**

Las listas de certificados revocados correspondientes a la presente Política de Certificación serán emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 o la que en su defecto, determine el Ente Licenciante, y cumplirán con las indicaciones establecidas en la sección "3 - Perfil de CRLs" del Anexo IV – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

**7.2.1. - Número de versión**

A completar sobre la base de lo establecido en el documento referido en el apartado 3.2 del Anexo IV.

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

A completar sobre la base de lo establecido en el documento referido en el apartado 3.3 del Anexo IV.

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

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Deberá ser implementada conforme a lo indicado en la especificación RFC 6960 y cumplir con las indicaciones establecidas en la sección "4 - Perfil de la consulta en línea del estado del certificado" del Anexo IV – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

**7.3.1. – Consultas OCSP**

A completar sobre la base de lo establecido en el documento referido en el apartado 4.1 del Anexo IV.

### 7.3.2. - Respuestas OCSP

A completar sobre la base de lo establecido en el documento referido en el apartado 4.3 del Anexo IV.

## 8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

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

a) Denominación de la entidad de auditoría.

b) Frecuencia y contextos para la realización de las auditorías.

c) Identificación y calificaciones de la entidad evaluadora.

d) Vinculación entre el certificador y la entidad evaluadora

e) Temas principales a evaluar en las auditorías.

f) Medidas a adoptar en caso de dictámenes no favorables.

g) Modalidad de comunicación de los informes de auditoría.

Se cumplen las exigencias reglamentarias impuestas por:

- Los artículos 33 y 34 de la Ley N° 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma Ley, relativo a la publicación de informes de auditoría.
- Los artículos 18 a 21 del Decreto N° 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría y el artículo 20, vinculado a conflicto de intereses.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

## 9. – ASPECTOS LEGALES Y ADMINISTRATIVOS

### 9.1. - Aranceles

Se describen los aranceles asociados a cada uno de los servicios que preste el certificador, relacionados con la Política Única de Certificación, en el caso de las entidades privadas. Según lo dispuesto por el artículo 38 del Decreto N° 2628/02, modificado por el Decreto N° 724/06, los certificados emitidos por las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional deberán ser provistos en forma gratuita.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.2. - Responsabilidad Financiera**

Se incluyen las cláusulas que establezcan la responsabilidad por daños potenciales que podrían sufrir los suscriptores de certificados y los terceros usuarios, en razón del posible incumplimiento de lo dispuesto en las normas legales y reglamentarias y en la Política Única de Certificación y de los recursos con los que cuenta el certificador para afrontarlos.

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.3. - Confidencialidad**

Se indican las previsiones en cuanto al tratamiento de información confidencial del certificador, estableciendo como mínimo los siguientes aspectos:

a) Alcance de la información considerada confidencial.

b) Tipos de información no considerada confidencial.

c) Responsabilidades de los roles involucrados

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.3.1. - Información confidencial**

Jefe de Gabinete de Ministros

FOLIO 916

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

Se especifica 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 vigentes.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**9.3.2. - Información no confidencial**

La siguiente información no se considera confidencial:

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

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

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

d) Secciones públicas de la Política de Seguridad del certificador.

e) Política de privacidad del certificador.

**9.3.3. – Responsabilidades de los roles involucrados**

Se indican las responsabilidades de los roles que gestionan información confidencial en cuanto a evitar su compromiso o divulgación a personas no autorizadas.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.4. - Privacidad**

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

**9.5 - Derechos de Propiedad Intelectual**

Se incluyen 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.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.6. – Responsabilidades y garantías**

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, deben detallarse:

a) Las garantías para el certificador licenciado, sus autoridades de registro y los suscriptores.

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

c) Las garantías para los terceros usuarios.

d) Las garantías para otras entidades participantes.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.7. – Deslinde de responsabilidad**

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley N° 25.506 al respecto, deben detallarse:

a) Las limitaciones de responsabilidad para el certificador licenciado, sus autoridades de registro y los suscriptores.

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

c) Las limitaciones de responsabilidad para los terceros usuarios.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.8. – Limitaciones a la responsabilidad frente a terceros**

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley N° 25.506 al respecto, se detallan las limitaciones de responsabilidad respecto a otras entidades participantes.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.9. – Compensaciones por daños y perjuicios**

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley N° 25.506 al respecto, detallan las previsiones relativas a las compensaciones por daños y perjuicios.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.10. – Condiciones de vigencia**

Se indica el período de vigencia de la Política y las condiciones bajo las cuales se extinguirán los términos que rigen su aplicación.

Se deberán incluir, como mínimo, los siguientes aspectos:

- Fecha de entrada en vigencia y finalización
- Consecuencias de la finalización de la vigencia del documento.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.11.- Avisos personales y comunicaciones con los participantes**

No aplicable.

**9.12.- Gestión del ciclo de vida del documento**

Se establecen las políticas para el mantenimiento y administración de la Política Única de Certificación.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.12.1. - Procedimientos de cambio**

Se establecen las políticas utilizadas para efectuar modificaciones en la Política Única de Certificación. Toda modificación deberá ser aprobada previamente por el ente licenciante conforme a lo establecido por la Ley N° 25.506, artículo 21, inciso q) y por la presente decisión administrativa y sus Anexos respectivos.

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

Todo cambio a la Política Única de Certificación debe ser comunicado al suscriptor.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

**9.12.2 – Mecanismo y plazo de publicación y notificación**

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.12.3. – Condiciones de modificación del OID**

No aplicable.

FOLIO 920

**9.13. - Procedimientos de resolución de conflictos**

Deben indicarse las políticas de resolución de conflictos en la Política Única de Certificación y en los acuerdos en los que el certificador sea parte.

Se detallan las políticas de reclamo aplicables cuando existan conflictos respecto a la interpretación de una o más disposiciones de la Política Única de Certificación, conforme al artículo 27 de la presente Decisión Administrativa.

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

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

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.14. - Legislación aplicable**

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

**9.15. – Conformidad con normas aplicables**

Se especifica la legislación aplicable a la actividad del certificador, de existir.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

**9.16. – Cláusulas adicionales**

No se establecen cláusulas adicionales.

**9.17. – Otras cuestiones generales**

Jefe de Gabinete de Ministros

FOLIO 921

Se incluirá todo otro aspecto legal o administrativo no incluido en los apartados anteriores.

Estos datos se incluirán en el Formulario de Adhesión del Anexo I.

Jefe de Gabinete de Ministros

FOLIO 922

ANEXO IV

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

# Perfiles de los certificados y de las listas de certificados revocados

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 923

## ÍNDICE

Jefe de Gabinete de Ministros

FOLIO 924

FOLIO 925

**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 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 único para los certificados, especificando los campos a completar para integrar la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.

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 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

En lo referente a las consultas en línea del estado de los certificados, se adhiere particularmente al siguiente documento:

RFC 6960 "X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol - OCSP".

Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en los referidos documentos.

Salvo mención explícita, las siguientes especificaciones deben ser aplicadas tanto a los certificados emitidos a usuarios o aplicaciones, como a 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 [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA.

**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*).

FOLIO 928

- 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*).

El contenido de este campo DEBE coincidir con el indicado en el campo del "*distinguishedName*" correspondiente al "*subject*" del certificado emitido por la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.

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 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, es decir la REPÚBLICA ARGENTINA. 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.

FOLIO 929

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

Certificados de certificador: DIEZ (10) años.

Certificados de proveedores de servicios de firma digital: DIEZ (10) años o un plazo inferior determinado teniendo en cuenta la vigencia del certificado de la autoridad certificante del certificador licenciado, utilizada para la emisión, según corresponda.

Certificados de Aplicaciones: TRES (3) años.

Certificados de Personas Físicas: DOS (2) años.

Certificados de Personas Jurídicas Públicas o Privadas: 3 (TRES) 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 los siguientes atributos:

- Código de país (OID 2.5.4.6: *countryName*).
- Nombre común (OID 2.5.4.3: *commonName*).
- Número de serie (OID 2.5.4.5: *serialNumber*).

Para los certificados de **certificadores licenciados,** los campos que integran el nombre distintivo del emisor (issuer DN) deben coincidir con los campos correspondientes del

Jefe de Gabinete de Ministros



nombre distintivo del suscriptor (subject DN), emitido a nombre del certificador licenciado por la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA.

**Para certificados de proveedores de servicios de firma digital**:

"*commonName*": DEBE corresponder al nombre del servicio prestado por el certificador o al nombre de la unidad operativa responsable del servicio.

"*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.

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

FOLIO 931

El valor posible para el campo [tipo de documento] es "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral.

"*countryName*": DEBE estar presente y DEBE indicar el país de nacimiento del suscriptor codificado según el estándar [ISO3166].

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

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

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

- "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.

FOLIO 932

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

**Para los certificados de Aplicaciones:**

"*commonName*": DEBE corresponder al nombre del servicio o aplicación o al nombre de la unidad operativa responsable del servicio o aplicación.

"*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: ["código de identificación"] ["nro. de identificación"]. El valor posible para el campo ["código de identificación"] es "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

"*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 responsable del servicio o aplicación.

"*countryName*": DEBE estar presente y DEBE representar el país en el cual está constituida la Persona Jurídica. El atributo "*countryName*" DEBE estar codificado según el estándar [ISO3166].

**Para los certificados de sitio seguro:**

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

Jefe de Gabinete de Ministros

FOLIO 933

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

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

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

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

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

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

Los tipos y longitudes correspondientes a cada atributo DEBEN respetar las definiciones establecidas en [RFC5280] Apéndice A.

**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 [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA.

**2.3 - Extensiones de un Certificado**

Las siguientes extensiones DEBEN encontrase presentes en todos los certificados:

FOLIO 934

- 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:

- 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:

- 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.

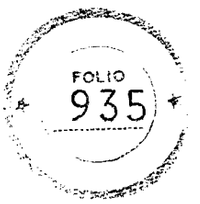
Esta extensión DEBE estar presente en todos los certificados.

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 *"contentCommitment"* DEBE tener valor 1.

El resto de bits DEBEN tener valor 0.

Para certificados de otros Proveedores de servicios de firma digital:

El bit *"contentCommitment"* DEBE tener valor 1.

El resto de bits DEBEN tener valor 0.

Para certificados de Personas Físicas, Jurídicas y Aplicaciones:

El bit *"contentCommitment"* DEBE tener valor 1.

El bit *"digitalSignature"* PUEDE tener valor 1 para propósitos de autenticación.

Los bits correspondientes a *"keyEncipherment"*, *"dataEncipherment"*, *"keyAgreement"*, *"encipherOnly"* y "decipherOnly" DEBEN tener valor 1 **teniendo en cuenta que la pérdida de control de la clave privada correspondiente impedirá descifrar los datos originales.**

FOLIO 936

Los bits "cRLSign" y "CertSign" DEBEN tener valor 0

Esta extensión DEBE 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 la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, a solicitud del ente licenciante. El documento digital que contiene la Política de Certificación DEBE ser declarado ante el ente licenciante y la extensión *"CertificatePolicies"* DEBE declarar la URI donde el documento estará disponible.

El campo "*userNotice*" DEBE incluir la leyenda "certificado emitido por un certificador licenciado en el marco de la Ley N° 25.506".

La extensión *"CertificatePolicies"* DEBE incluir toda la información sobre la Política de Certificación necesaria para la validación del certificado.

Esta extensión DEBE estar presente en todos los certificados.

Esta extensión DEBE 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:

Jefe de Gabinete de Ministros

FOLIO 937

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).

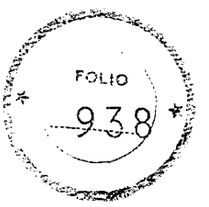
Esta extensión debe utilizarse para consignar las direcciones de correo electrónico de los suscriptores en lugar del atributo "email" del campo "subject".

**2.3.6 – 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"* no DEBE estar presente.

**2.3.7 – 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*".

**2.3.8 – 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.

**2.3.9 – 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.

FOLIO 939

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

La extensión *"AuthorityInformationAccess"* DEBE ser utilizada para indicar como se accede a la información del servicio de OCSP.

Esta extensión NO DEBE ser crítica.

**2.3.11 – Declaración del certificado calificado (Qualified Certificate Statement)**

La extensión *"QCStatement"* DEBE ser utilizada para indicar el módulo criptográfico utilizado para la generación de las claves del suscriptor, debiendo contener uno de los siguientes OIDs:

- 2.16.32.1.10.1, cuando las claves sean generadas por software
- 2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1
- 2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2
- 2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

Esta extensión DEBE ser crítica.

**2.3.12 - Otras extensiones**

NO se DEBEN crear nuevas extensiones más allá de las definidas en el presente Anexo.

**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 y cuáles no está permitido usar.

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

RFC 5280 "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 dicho 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) de los algoritmos y, de ser necesarios, los parámetros asociados usados por el certificador para firmar la CRL. Este identificador DEBE ser alguno de los definidos en el [RFC4055] para RSA, [RFC5480] para curvas elípticas (en el caso de utilizarse) o [RFC5758] para DSA y ECDSA.

**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*)**

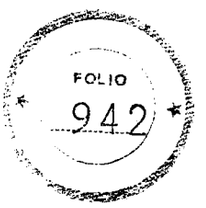
El campo *"ThisUpdate"* DEBE estar presente e indicar la fecha de emisión de la CRL. La fecha de revocación de un certificado de la lista no DEBE ser posterior a esta fecha. La CRL DEBE estar disponible para consulta inmediatamente después de emitida.

**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 indicando su número de serie y su fecha de revocación. Asimismo deben incluirse extensiones específicas para cada elemento de esta lista, de acuerdo a lo establecido a continuación.




**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, etcétera.

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**

No se deben crear nuevas extensiones más allá de las definidas en [RFC5280].

**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 DEBE incluir el motivo de revocación del certificado.

**3.4.2 – 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.

**3.4.3 – 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.

**3.4.4 - Otras extensiones de entradas de la lista "Certificados Revocados"**

NO se RECOMIENDA la creación de nuevas extensiones más allá de las definidas en el presente documento.

**4 - Perfil de la consulta en línea del estado del certificado**

**4.1 - Formato**

El formato de las consultas en línea del estado del certificado se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Estas consultas se utilizan para determinar el estado de un certificado digital como método alternativo a la Lista de Certificados Revocados. En esta sección se especifican los campos a utilizar, adhiriéndose al contenido de los documentos:

RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

RFC 6960 "X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol - OCSP".

Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en dichos documentos.

**4.2 - Consultas OCSP**

Los siguientes datos DEBEN encontrarse presentes en las consultas:

- Versión (version).
- Requerimiento de servicio (service request).
- Identificador del certificado bajo consulta (target certificate identifier).
- Extensiones opcionales (optionals extensions), las cuales podrían ser procesadas por quien responde.

Al recibir la consulta OCSP, quien responde DEBE determinar:

FOLIO 945

- Si el formato de la consulta es adecuado.
- Si quien responde se encuentra habilitado para responder la consulta.
- Si la consulta contiene la información que necesita quien responde.

Si alguna de estas condiciones no se cumpliera, da lugar a un mensaje de error. De lo contrario se devuelve una respuesta.

**4.3 – Respuestas OCSP**

Todas las respuestas OCSP DEBEN ser firmadas digitalmente por la Autoridad Certificante perteneciente al certificador licenciado, que emitió el certificado digital para el cual se hace la consulta.

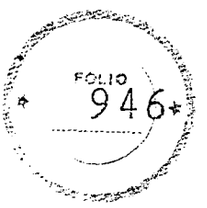
Una respuesta OCSP debe considerar los siguientes datos:

- Versión de la sintaxis de respuesta.
- Identificador de quien responde.
- Fecha y hora en la que se genera la respuesta.
- Respuesta respecto al estado del certificado.
- Extensiones opcionales.
- Identificador (OID) único del algoritmo de firma.
- Firma de la respuesta.

La respuesta a una consulta OCSP consiste en:

- Identificador del certificado.
- Valor correspondiente al estado del certificado.
- Período de validez de la respuesta.
- Extensiones opcionales.

Se especifican las siguientes respuestas posibles para el valor correspondiente al estado del certificado:




- Válido (good), indicando una respuesta positiva a la consulta. Este valor indica que no existe un certificado digital con el número de serie contenido en la consulta, que haya sido revocado durante su vigencia.
- Revocado (revoked), indicando que el certificado ha sido revocado.
- Desconocido (unknown), indicando que quien responde no reconoce el número de serie incluido en la consulta, debido comúnmente a la inclusión de un emisor desconocido.

**5 - Perfil de sellos de competencia**

**5.1 - 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 único para los sellos de competencia, especificando los campos a completar para integrar la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.

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

RFC 5755, "An Internet Attribute Certificate Profile for Authorization".

Para una completa implementación de esta especificación se recomienda la consulta de los formatos y definiciones especificadas en los referidos documentos.

**5.2 - 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) (*attrCertValidityPeriod* (*notBefore*, *notAfter*)).
- Nombre Distintivo del Titular (*holder*).
- Competencia (attributes).

Los sellos de competencia podrán incluir las extensiones establecidas en los estándares indicados precedentemente.

**5.2.1 – Versión (*Version*)**

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

**5.2.2 – Número de Serie (*Serial Number*)**

El campo *"serialNumber"* contiene un número asignado por la Autoridad de Competencia a cada certificado. Dicho número DEBE ser único para cada certificado emitido por dicha Autoridad.

**5.2.3 – 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 la Autoridad de Competencia para firmar el certificado. Este identificador DEBE ser alguno de los definidos en el [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA.

**5.2.4 – Nombre Distintivo del Emisor (*Issuer*)**

El campo *"issuer"* DEBE identificar a la organización responsable de la emisión del sello de competencia.

FOLIO 948

El contenido de este campo DEBE coincidir con el indicado en el campo del "*distinguishedName*" correspondiente al "*subject*" del certificado de la Autoridad de Competencia que fuera emitido por la Autoridad Certificante del certificador licenciado.

**5.2.5 – Validez (Desde, Hasta) (*attrCertValidityPeriod* (*notBefore, notAfter*))**

El período de la validez es el intervalo de tiempo durante el cual el sello de competencia se considera válido. Este intervalo dependerá de la validez del atributo correspondiente.

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 desde *"notBefore"* hasta *"notAfter"* inclusive.

Una autoridad de competencia NO DEBE emitir un certificado con vencimiento posterior al de su propio certificado.

**5.2.6 – Nombre Distintivo del Titular (*holder*)**

El campo *"subject"* identifica la entidad asociada a la competencia contenida en el certificado. DEBE contener un nombre distintivo del titular. Dicho nombre DEBE ser único para cada titular de certificado emitido por una autoridad de competencia durante todo el tiempo de vida del mismo.

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

- Nombre común (OID 2.5.4.3: *commonName*).
- Número de serie (OID 2.5.4.5: *serialNumber*).

**Para certificados de personas jurídicas:**

"*commonName*": DEBE corresponder al nombre 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"].

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.

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

El valor posible para el campo [tipo de documento] es "CUIT/CUIL": Clave Única de Identificación Tributaria o Laboral.

**5.2.7 – Competencia (*attributes*)**

Este campo contiene las competencias asociadas al titular, que se está certificando. Pueden tratarse de competencias profesionales, relaciones laborales o similar.

**6 - Algoritmos criptográficos**

- Los algoritmos utilizados DEBEN ser los especificados en el [RFC4055] para RSA, [RFC5480] para curvas elípticas o [RFC5758] para DSA y ECDSA o los que en su defecto, determine el Ente Licenciante.

- 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: CUATRO MIL NOVENTA Y SEIS (4096) bits si se utiliza RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits en caso de ECDSA.
    - Para certificados utilizados en servicios relacionados con la firma digital : DOS MIL CUARENTA Y OCHO (2048) bits si se utiliza RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits en caso de ECDSA, excepto en el caso de las autoridades de sello de tiempo, cuyas claves DEBEN ser de CUATRO MIL NOVENTA Y SEIS (4096) bits si se utiliza RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits en caso de ECDSA.
    - Para certificados de responsables de Autoridades de Registro: DOS MIL CUARENTA Y OCHO (2048) bits si se utiliza RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits en caso de ECDSA.
    - Para certificados de suscriptores (personas físicas o jurídicas): DOS MIL CUARENTA Y OCHO (2048) bits si se utiliza RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits en caso de ECDSA.

**7 – Correspondencia con estándares**

A continuación se establece un paralelo entre las definiciones incluidas en esta especificación y los ítems respectivos definidos en los documentos [RFC4055], [RFC5480], [RFC5758], [RFC5280], [RFC3739], [ISO/IEC 9594-8] y la Ley N° 25.506, incluyéndose referencias a cada uno de ellos.

Jefe de Gabinete de Ministros

FOLIO 951

| 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 5280 4 |
| 2.2 - Campos de certificados | - |
| 2.2.1 - Versión (*Version*) | RFC 5280 4.1.2.1 |
| 2.2.2 - Número de Serie (*Serial Number*) | RFC 5280 4.1.2.2<br>Ley 25.506 Art. 19.c |
| 2.2.3 - Algoritmo de Firma (*Signature*) | RFC 5280 4.1.2.3<br>RFC 4055, 5480 o 5758 |
| 2.2.4 - Nombre Distintivo del Emisor (*Issuer*) | RFC 3739 3.1.1 |
| 2.2.5 - Validez (Desde, Hasta) (*Validity* (*notBefore*, *notAfter*)) | RFC 5280 4.1.2.5 |
| 2.2.6 - Nombre Distintivo del Suscriptor (*Subject*) | RFC 3739 3.1.2<br>RFC 5280 Apéndice A |
| 2.2.7 - Clave Pública del Suscriptor (*Subject Public Key Info*) | RFC 5280 4.1.2.7 |
| 2.3 - Extensiones de un certificado | - |

Jefe de Gabinete de Ministros

FOLIO 952

| | |
|---|---|
| 2.3.1 - Identificador de la Clave de la Autoridad Certificante (*Authority Key Identifier*) | RFC 5280 4.2.1.1 |
| 2.3.2 - Identificador de la Clave del Suscriptor (*Subject Key Identifier*) | RFC 5280 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<br>Ley 25.506 Art. 14.b.5 |
| 2.3.5 - Nombres Alternativos del Suscriptor (*Subject Alternative Name*) | RFC 5280 4.2.1.6 |
| 2.3.6 - Restricciones Básicas (*Basic Constraints*) | RFC 5280 4.2.1.9 |
| 2.3.7 - Uso de Claves Extendido (*Extended Key Usage*) | RFC 5280 4.2.1.12 |
| 2.3.8 - Puntos de Distribución de la Lista de Certificados Revocados (*CRL Distribution Point*) | RFC 5280 4.2.1.13 |
| 2.3.9 - CRL más reciente (*Freshest CRL*) | RFC 5280 4.2.1.15 |
| 2.3.10 - Información de Acceso de la Autoridad Certificante (*Authority Information Access*) | RFC 5280 4.2.2.1 |
| 2.3.11 - Declaración del certificado calificado (Qualified Certificate Statement) | RFC 3739 3.2.6 |
| 2.3.12 - Otras extensiones | - |
| **3 - Perfil de CRLs** | - |
| 3.1 – Formato | RFC 5280 5 |

FOLIO 953

| | |
|---|---|
| 3.2 - Campos de una CRL | - |
| 3.2.1 - Versión (*Version*) | RFC 5280 5.1.2.1 |
| 3.2.2 - Algoritmo de Firma (*Signature*) | RFC 5280 5.1.2.2 |
| 3.2.3 - Nombre Distintivo del Emisor (*Issuer*) | RFC 5280 5.1.2.3 |
| 3.2.4 - Día y Hora de Vigencia (*This Update*) | RFC 5280 5.1.2.4 |
| 3.2.5 - Próxima Actualización (*Next Update*) | RFC 5280 5.1.2.5 |
| 3.2.6 - Certificados Revocados (*Revoked Certificates*) | RFC 5280 5.1.2.6 |
| 3.3 - Extensiones de una CRL | - |
| 3.3.1 - Identificación de Clave de la Autoridad Certificante (*Authority Key Identifier*) | RFC 5280 5.2.1 |
| 3.3.2 - Número de CRL (*CRL Number*) | RFC 5280 5.2.3 |
| 3.3.3 - Indicador de Delta CRL (*Delta CRL Indicador*) | RFC 5280 5.2.4 |
| 3.3.4 - Punto de Distribución del Emisor (*Issuing Distribution Point*) | RFC 5280 5.2.5 |
| 3.3.5 - CRL más Reciente - Punto de Distribución de la Delta CRL (*Freshest CRL - Delta CRL Distribution Point*) | RFC 5280 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 5280 5.3.1 |

Jefe de Gabinete de Ministros

FOLIO 954

| | |
|---|---|
| 3.4.2 - Fecha de Invalidez (*Invalidity Date*) | RFC 5280 5.3.2 |
| 3.4.3 - Emisor del certificado (*Certificate Issuer*) | RFC 5280 5.3.3 |
| 3.4.4 - Otras extensiones de entradas de la lista "Certificados Revocados" | - |
| **4 - Perfil de la consulta en línea del estado del certificado** | - |
| 4.1 - Formato | RFC 6960 |
| 4.2 – Consulta OCSP | RFC 6960 |
| 4.3 – Respuesta OCSP | RFC 6960 |
| **6- Algoritmos criptográficos** | RFC 4055, 5480 o 5758 |

Jefe de Gabinete de Ministros

FOLIO 955

ANEXO V

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

**Contenidos mínimos de los Acuerdos con Suscriptores**

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 956

## Contenidos mínimos de los Acuerdos con Suscriptores

El acuerdo establecido entre el certificador licenciado 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 y en su caso, los de su posterior renovación.

### 3. Obligaciones ante la revocación o expiración

Debe detallar las obligaciones del suscriptor y del certificador licenciado ante la revocación y expiración del certificado reflejando lo que indica la Política Única de Certificación.

### 4. Política de Privacidad

La descripción incorporada en este punto debe reflejar lo especificado en la Política de Privacidad (Anexo VIII) y en la presente decisión administrativa.

### 5. Limitaciones de la responsabilidad

#### 5.1. Fuerza mayor

FOLIO 957

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 las limitaciones de responsabilidad, conforme el Artículo 39 de la Ley Nº 25.506 de Firma Digital, reflejando lo indicado en "Responsabilidades" de su Política Única de Certificación.

**6. Legislación Aplicable y Procedimientos de Resolución de Conflictos**

La descripción incorporada en este punto debe reflejar lo especificado en la Política Única de Certificación (Anexo III).

**7. Cesión de derechos**

Debe indicar que ninguno de los derechos del suscriptor bajo los términos del presente acuerdo puede ser cedido o transferido.

**8. Contactos**

Se incluirán los datos de un responsable del certificador licenciado para actuar como nexo incluyendo como mínimo denominación del servicio de atención de consultas, dirección de correo electrónico institucional y número de teléfono.

**9. Vigencia**

Indicar el plazo de vigencia de este acuerdo y la fecha a partir de la cual se hará efectivo el mismo.

**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

FOLIO 958

ANEXO VI

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

# Contenidos mínimos de los términos y condiciones con terceros usuarios

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 959

## Contenidos mínimos de los términos y condiciones con terceros usuarios

Los términos y condiciones establecidos entre el Certificador Licenciado 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 licenciado 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 la relación entre el Certificador licenciado y los Terceros Usuarios.

### 2. Definiciones

Debe contener el glosario de terminología incluido en la Política Única de Certificación.

### 3. Reconocimiento de Información Suficiente

Debe contener una descripción de la información relativa al certificado y su Política Única 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 Única de Certificación aplicable.

Jefe de Gabinete de Ministros

FOLIO 960

**4.2. Aplicabilidad**

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

**4.3. Limitaciones en el uso del certificado**

Debe indicarse que no existen restricciones en el uso del certificado, excepto aquellas indicadas en la Ley N° 25.506, su Decreto Reglamentario N° 2628/02 y sus modificatorios y demás normativa aplicable.

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

De acuerdo a lo establecido en la Política Única de Certificación correspondiente, los Terceros Usuarios deben:

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

b) Verificar la validez del certificado digital.

**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**

De acuerdo a lo establecido en el CÓDIGO CIVIL DE LA NACIÓN, los casos de fuerza mayor vinculados a circunstancias ajenas a la voluntad de las partes, no generan derecho a indemnización a favor del damnificado.

Jefe de Gabinete de Ministros

FOLIO 961

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

Deben indicarse las limitaciones de responsabilidad, conforme el Artículo 39 de la Ley Nº 25.506 de Firma Digital, reflejando lo indicado en "Responsabilidades" de su Política Única de Certificación.

## 8. Legislación Aplicable y Procedimientos de Resolución de Conflictos

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

## 9. Contactos

Se incluirán los datos de un responsable del certificador licenciado para actuar como nexo incluyendo como mínimo, la denominación del servicio de atención de consultas, la dirección de correo electrónico institucional y el número de teléfono.

Jefe de Gabinete de Ministros

FOLIO 962

ANEXO VII

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

**Fórmula para establecer los montos de aranceles y seguros de caución**

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 963

## Fórmula para establecer los montos de aranceles y seguros de caución

Los trámites ante el ente licenciante están sujetos al pago de aranceles en base a la fórmula y detalle que a continuación se consignan:

La fórmula para cada caso se basa en un número fijo (cantidad de horas de trabajo estimado) por el valor en pesos a la fecha de pago de los montos correspondientes de las Unidades Retributivas (UR) estipulado en el Decreto N° 2098 del 3 de diciembre de 2008 y sus modificatorios (SISTEMA NACIONAL DE EMPLEO PÚBLICO).

| TIPO | Monto a Pagar |
|---|---|
| Por solicitud de licencia de certificador licenciado (Sector Privado) | 4000 (UR) |
| 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 | 2400 (UR) |
| Por renovación de licencia para el certificador licenciado | 2000 (UR) |
| Monto mínimo a integrarse en concepto de garantía o seguro de caución | 8000 (UR) |

Los costos de auditorías, soluciones de software o hardware necesarios para operar en la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, serán afrontados por los interesados con las Instituciones precalificadas para tal fin por el ente licenciante.

Jefe de Gabinete de Ministros

FOLIO 964

ANEXO VIII

**Infraestructura de Firma Digital – REPÚBLICA ARGENTINA**

**Ley N° 25.506**

# Contenidos mínimos de la Política de Privacidad

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 965

## Contenidos mínimos de la Política de Privacidad

La Política de Privacidad de datos determina el tratamiento que el certificador licenciado hará de los datos recibidos de los suscriptores, Terceros Usuarios de certificados digitales y otros terceros en general, debiendo estar en un todo de acuerdo con lo establecido al respecto por la Ley N° 25.326 de Protección de Datos Personales y sus modificatorias.

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.

Jefe de Gabinete de Ministros

FOLIO 966

En particular y con relación al cumplimiento de la Ley de Protección de Datos Personales N° 25.326 y sus modificatorias, debe tenerse en cuenta que la misma establece en forma expresa la siguiente obligación:

*"ARTICULO 21. — (Registro de archivos de datos. Inscripción).*

*1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.*

*2. El registro de archivos de datos debe comprender como mínimo la siguiente información:*

*a) Nombre y domicilio del responsable;*

*b) Características y finalidad del archivo;*

*c) Naturaleza de los datos personales contenidos en cada archivo;*

*d) Forma de recolección y actualización de datos;*

*e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;*

*f) Modo de interrelacionar la información registrada;*

*g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;*

*h) Tiempo de conservación de los datos;*

*i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.*

*3. Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.*

Jefe de Gabinete de Ministros

927

FOLIO 967

*El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley."*

Asimismo se recomienda tener en cuenta la normativa reglamentaria, aclaratoria y técnica de la Ley de Protección de Datos Personales N° 25.326 y sus modificatorias.