Ministerio de Modernización

ANEXO II

INFRAESTRUCTURA DE FIRMA DIGITAL
REPÚBLICA ARGENTINA
LEY N° 25.506

POLÍTICA ÚNICA DE CERTIFICACIÓN

SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA
MINISTERIO DE MODERNIZACIÓN

IF-2016-01339408-APN-SECMA#MM

ANEXO II

CARACTERÍSTICAS DEL DOCUMENTO

Este documento describe la estructura y el contenido de 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.

Las Políticas de Certificación emitidas por los certificadores se encuentran alcanzadas a los contenidos, la estructura y el ordenamiento (índice) del presente documento.

Para integrar la Infraestructura antes mencionada, los certificadores deberán presentar toda la documentación requerida en el Anexo I. Una vez cumplidos y aprobados los requisitos para el licenciamiento, la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA y el MINISTERIO DE MODERNIZACIÓN procederán al dictado de los actos administrativos correspondientes, aprobando la Política Única de Certificación y otorgando la respectiva licencia, ordenando en sendos casos su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

Ante cualquier duda en la interpretación del presente documento, podrá dirigirse por escrito a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, 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@modernizacion.gob.ar.

ANEXO II

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, 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 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 el MINISTERIO DE MODERNIZACIÓN, siendo dicho organismo y la SECRETARÍA DE

MODERNIZACIÓN ADMINISTRATIVA, quienes entienden 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 DIRECCIÓN NACIONAL DE SISTEMAS DE ADMINISTRACIÓN Y FIRMA DIGITAL de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN por pedido de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, como paso previo a su licenciamiento y de manera tal que permita una identificación apropiada.

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.

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.

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 a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN.

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.

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.

1.5.2. - Contacto

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

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

La Política Única de Certificación ha sido presentada ante la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN durante el proceso de licenciamiento y ha sido aprobada por el correspondiente Acto Administrativo.

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**: El MINISTERIO DE MODERNIZACIÓN es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.
- **AUTORIDAD DE REGISTRO**: Es la entidad que tiene a su cargo las funciones de:

- Recepción de las solicitudes de emisión de certificados.
- Validación de la identidad 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 de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN.

- **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 MINISTERIO DE MODERNIZACIÓN. (artículo 17 de la Ley N° 25.506).

- **CERTIFICACIÓN DIGITAL DE FECHA Y HORA**: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. (Anexo al Decreto N° 2628 de fecha 19 de diciembre de 2002).
- **ENTE LICENCIANTE**: El MINISTERIO DE MODERNIZACIÓN y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA constituyen el Ente Licenciante.
- **LISTA DE CERTIFICADOS REVOCADOS**: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL). (Anexo al Decreto N° 2628/02)
- **MANUAL DE PROCEDIMIENTOS**: Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS). (Anexo al Decreto N° 2628/02)
- **PLAN DE CESE DE ACTIVIDADES**: Conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02)
- **PLAN DE CONTINUIDAD DE LAS OPERACIONES**: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- **PLAN DE SEGURIDAD**: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado. (Anexo al Decreto N° 2628/02)

- **POLÍTICA DE PRIVACIDAD**: Conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.
- **SERVICIO OCSP (PROTOCOLO EN LÍNEA DEL ESTADO DE UN CERTIFICADO – "ONLINE CERTIFICATE STATUS PROTOCOL")**: Servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.
- **SUSCRIPTOR O TITULAR DE CERTIFICADO DIGITAL**: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- **TERCERO USUARIO**: Persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. (artículo 3° del Decreto N° 724/06).

1.6.2. - Acrónimos

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

CUIT - Clave Única de Identificación Tributaria.

DNSAFD – Dirección Nacional de Sistemas de Administración y Firma Digital.

IEC - International Electrotechnical Commission.

IETF - Internet Engineering Task Force.

MM – Ministerio de Modernización.

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

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

RFC - Request for Comments.

SMA – Secretaría de Modernización Administrativa.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección.

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

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.

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) Política Única de Certificación anteriores y vigente.

b) Acuerdo Tipo con suscriptores.

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

d) Política de Privacidad.

e) Manual de Procedimientos (parte pública).

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

g) Repositorio de certificados revocados.

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

i) Consulta de certificados emitidos (indicando su estado).

j) Listado de Autoridades de Registro (indicando si opera bajo modalidad móvil).

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección.

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.

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.

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.

ANEXO II

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.
- "organizationName" (OID 2.5.4.10: Nombre de la organización): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada.
- "serialNumber" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

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

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

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

"countryName" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país 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.

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

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 titularidad del par de claves

El certificador comprueba que el solicitante es el titular del par de claves mediante la verificación de la solicitud del certificado digital en formato PKCS#10, la cual no incluye la clave privada. 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.

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

a) El artículo 21, inciso i) de la Ley Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21, inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.

c) El artículo 34, inciso m) del Decreto Nº 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 Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21, inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.

c) El artículo 34, inciso i) del Decreto Nº 2628/02 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

d) El artículo 34, inciso m) del Decreto Nº 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 IV de la presente Resolución, 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 la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN.

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

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.

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 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.

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.

Se indicará 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.

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.

4.3.2. - Notificación de emisión

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

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.

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 Resolución:

- 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

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.

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 Nº 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la presente Resolución 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.

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.

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 y de la verificación de estado en línea (OCSP), aclarando la obligatoriedad de este último servicio.

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.

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.

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.

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 Nº 25.506.

4.9.14. - Autorizados a solicitar la suspensión

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

4.9.15. - Procedimientos para la solicitud de suspensión

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

4.9.16. - Límites del periodo de suspensión de un certificado

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

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.

4.10.3. – Aspectos operativos

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

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 I 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 Nº 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

Se respeta lo establecido en el Anexo I 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 I 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.

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 a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, 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 Resolución y sus correspondientes Anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA

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.

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 I Sección 2 respecto de generación del par de claves.

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.

6.1.4. - Disponibilidad de la clave pública del certificador

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

6.1.5. - Tamaño de claves

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

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

6.1.6. - Generación de parámetros de claves asimétricas

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

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.

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 I Sección 2 respecto de los estándares para dispositivos criptográficos.

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.

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.

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.

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.

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.

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 a través de métodos adecuados.

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.

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.

6.2.11. – Requisitos de los dispositivos criptográficos

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

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.

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.

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.

6.4.3. - Otros aspectos referidos a los datos de activación

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

6.5. - Controles de seguridad informática

6.5.1. - Requisitos Técnicos específicos

Se 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.

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.

6.6.1. - Controles de desarrollo de sistemas

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

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.

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.

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.

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

Se especifican los formatos de certificados y de listas de certificados revocados generados según la Política Única 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 la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, y deben cumplir con las indicaciones establecidas en la sección **"**2 - Perfil de certificados digitales" del Anexo III - 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 III.

7.1.2. - Extensiones

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

7.1.3. - Identificadores de algoritmos

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

7.1.4. - Formatos de nombre

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

7.1.5. - Restricciones de nombre

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

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 III.

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 III.

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 III.

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 la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, y cumplirán con las indicaciones establecidas en la

sección **"**3 - Perfil de CRLs" del Anexo III – "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 III.

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 III.

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 III – "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 III.

7.3.2. - Respuestas OCSP

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

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:

- El artículo 33 de la Ley Nº 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 19 a 21 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección.

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.

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.

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

9.3.1. - Información confidencial

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.

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.

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.

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.

9.7. – Deslinde de responsabilidad

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 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.

9.8. – Limitaciones a la responsabilidad frente a terceros

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, se detallan las limitaciones de responsabilidad respecto a otras entidades participantes.

9.9. – Compensaciones por daños y perjuicios

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

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 deberá incluir, como mínimo, los siguientes aspectos:

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

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.

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 la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN conforme a lo establecido por la Ley Nº 25.506, artículo 21, inciso q) y por la presente Resolución y sus Anexos respectivos.

Toda Política Única de Certificación es sometida a aprobación de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN 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.

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.

9.12.3. – Condiciones de modificación del OID

No aplicable.

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 26 de la presente Resolución.

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 MINISTERIO DE MODERNIZACIÓN, previo agotamiento del procedimiento ante el certificador licenciado correspondiente, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

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.

9.16. – Cláusulas adicionales

No se establecen cláusulas adicionales.

9.17. – Otras cuestiones generales

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