INFRAESTRUCTURA DE FIRMA DIGITAL DE LA PROVINCIA DE SAN LUIS

LEY N° V-0591-2007

REQUISITOS MINIMOS PARA POLÍTICAS DE CERTIFICACIÓN

Contenido

CARACTERÍSTICAS DEL DOCUMENTO

Este documento describe la estructura y los requisitos mínimos que deben cumplir las Políticas de Certificación de las entidades que soliciten una licencia en el marco de la Infraestructura de Firma Digital de la Provincia de San Luis, en los términos de la Ley Nº V-0591-2007. 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.

El presente documento establece el formato y los contenidos mínimos para las Políticas de Certificación de los Certificadores Licenciados Provinciales, las cuales deben ser presentadas ante el Ente Licenciante de San Luis para ser sometidas al proceso de licenciamiento.

Las Políticas de Certificación emitidas por los Certificadores Licenciados Provinciales deben respetar 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 de la presente Resolución. Una vez cumplidos y aprobados los requisitos para el licenciamiento, la AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS conjuntamente con el INSTITUTO FIRMA DIGITAL DE SAN LUIS procederán al dictado de los actos administrativos correspondientes, aprobando la Política de Certificación y otorgando la respectiva licencia, ordenando en sendos casos su publicación en el BOLETÍN OFICIAL DE LA PROVINCIA DE SAN LUIS.

Ante cualquier duda en la interpretación del presente documento, podrá dirigirse al Ente Licenciante Provincial: INSTITUTO FIRMA DIGITAL DE SAN LUIS dependiente de la AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS, en Edificio de Descentralización Administrativa “Terrazas del Portezuelo” - Torre III Piso 3º - Autopista de las Serranías Puntanas Km. 783, Ciudad de San Luis, Provincia de San Luis, o remitir su consulta a la siguiente dirección de correo electrónico: entelicenciante@sanluis.gov.ar

1. - INTRODUCCIÓN

Este documento contiene lineamientos específicos respecto al texto que deben incluir las Políticas de Certificación de los Certificadores Licenciados Provinciales en el marco de la Ley N° 0591-2007 de adhesión a la Ley N° 25.506. Su contenido solo debe ser modificado para incluir los aspectos particulares del Certificador Provincial en los puntos expresamente indicados, no debiéndose agregar o eliminar contenido, excepto donde se señale puntualmente.

De este modo, se habilita a los certificados digitales, que emitan los Certificadores Licenciados Provinciales en el marco de la Infraestructura de Firma Digital de San Luis, a que 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 y cifrado, para los cuales han sido habilitados.
Asimismo, esta norma sigue los lineamientos de la Política Única de Certificación de la Infraestructura de Firma Digital de la República Argentina con el objetivo de permitir la interoperabilidad de los certificados digitales que emitan los Certificados que hubiesen sido Licenciados por la Provincia de San Luis y por la República Argentina.
La Política de Certificación a presentar por los potenciales Certificadores Provinciales, a los fines del licenciamiento, deberá contener las siguientes secciones y contenidos:

1.1. - Descripción general

El documento establecerá las políticas que se aplican a la relación entre un Certificador Licenciado Provincial en el marco de la Infraestructura de Firma Digital de la Provincia de San Luis (Ley Nº V-0591-2007 de adhesión a la Ley Nº 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 humana o jurídica o de una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

1.2. - Nombre e Identificación del Documento

Incluirá la identificación de la Política 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 otorgada por la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS de manera tal que permita una identificación apropiada.

1.3. – Participantes

Incluirá las distintas entidades que integran la infraestructura del Certificador:

1.3.1. – Certificador Licenciado Provincial

Identificará al Certificador Licenciando Provincial que presenta la Política 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

Identificará 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 Licenciado Provincial en el proceso de recepción de solicitudes de emisión de certificados, identificación y autenticación de la identidad de los solicitantes de certificados y demás requisitos conforme la aplicabilidad de la Política de Certificación o los usos de los 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

Indicará si los certificados digitales emitidos bajo la Política de Certificación tienen como suscriptores personas humanas, jurídicas o aplicaciones, especificando para este último caso si se trata de sitios seguros.

1.3.4. - Terceros Usuarios

Indicará que son Terceros Usuarios de los certificados emitidos bajo la Política de Certificación, toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

En el caso de los certificados de sitio seguro, serán Terceros Usuarios quienes verifiquen el certificado del servidor.
En el caso de los certificados de autenticación, serán Terceros Usuarios quienes verifiquen el certificado de autenticación.

1.4. - Uso de los certificados

1.4.1. Usos apropiados de los certificados

Detallará la lista de usos o aplicaciones para los que resulten adecuados los certificados emitidos por el Certificador Licenciado Provincial en el marco de la Política de Certificación, pudiendo especificarse además los usos y aplicaciones para los que se prohíba su empleo.

1.4.2. Usos prohibidos de los certificados

Detallará la lista de usos o aplicaciones para los que el certificado se encuentra prohibido, pudiendo expresar que todos los usos no enumerados en el 1.4.1 se encuentran prohibidos.

1.5. - Administración de la Política

1.5.1. - Responsable del documento

Incluirá los datos de un responsable del Certificador Licenciado Provincial 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

Incluirá los datos del Responsable del registro, mantenimiento e interpretación de la Política de Certificación.

1.5.3. Persona que determina la conformidad de la Política de Certificación

Indicará que el Ente Licenciante Provincial es el responsable de acreditar y determinar si una autoridad de certificación forma parte de la Infraestructura de Firma Digital de San Luis, asimismo, señalará que es quien aprueba la Política de Certificación durante el proceso de licenciamiento.

1.5.4. Procedimiento de aprobación de la Política de Certificación

Deberá referir que la Política de Certificación ha sido presentada ante el Ente Licenciante Provincial durante el proceso de licenciamiento y ha sido aprobada por el correspondiente Acto Administrativo, el cual deberá ser individualizado.

1.6. - Definiciones y Acrónimos

1.6.1. - Definiciones

Contendrá las definiciones de los conceptos relevantes utilizados en la Política de Certificación, incluyendo los siguientes:

- Autoridad de Aplicación: AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.
- Ente Licenciante: es el órgano administrativo encargado de otorgar las licenciantes a los Certificadores Licenciado Provinciales y de supervisar su actividad. El INSTITUTO FIRMA DIGITAL DE SAN LUIS y la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS, constituyen el Ente Licenciante del régimen provincial de firma digital en San Luis (art. 24º y 26° del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018).
- Cuando el INSTITUTO FIRMA DIGITAL DE SAN LUIS actúa como Certificador Licenciado Provincial, la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS cumple el rol de Ente Licenciante Provincial (art. 18º de Resolución Nº 17-ASLCTyS-2017).
- Certificador Licenciado Provincial: Es el ente público, ente privado u organismo de derecho público no estatal que emite certificados de clave pública, entendiendo por tal al que asocia una clave pública con un suscriptor, durante el período de vigencia del certificado, haciendo plena prueba dentro de la Administración del Sector Público Provincial, los Poderes del Estado Provincial y el sector privado de la veracidad de su contenido y cuenta con una licencia provincial para ello (artículo 31 del Decreto Nº 0428-MP-2008).
- Autoridad de Registro: Es la entidad en quien el Certificador Licenciado Provincial delega las funciones relativas a la verificación de la identidad y demás datos correspondientes al aspirante a suscriptor del servicio, de registro de presentaciones y trámites que le son formuladas, así como la responsabilidad de las comunicaciones con el Ente Licenciante Provincial y/o el Certificador Licenciado Provincial en el proceso técnico de registración (artículo 39 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018).
- La Autoridad de Registro puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del Certificador Licenciado para hacerlo (artículo 40 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018).
- Autoridad Certificadora: Es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o 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 (art. 36 del Decreto Nº 0428-MP-2008).
- Tercero Usuario: Persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.
- Infraestructura de Firma Digital San Luis: Se entiende por tal al conjunto integrado por las leyes, decretos y normativa legal complementaria que regulen la firma digital en la jurisdicción de la Provincia de San Luis, las obligaciones y deberes de todas aquellas instituciones, organismos y personas que formen parte del circuito de la firma digital tales como la Autoridad de Aplicación Provincial, el Ente Licenciante Provincial, los Certificadores Licenciados Provinciales, las Autoridades de Registro, así como también, a los estándares tecnológicos, los procedimientos de seguridad, el hardware, el software, las redes, los bancos de datos y la infraestructura física de alojamiento, que permitan la utilización de la firma digital en condiciones de seguridad e integridad (artículo 10º del Decreto Nº 0428-MP-2008).
- Firma Digital: Se entiende por Firma Digital al resultado de una transformación de un documento digital empleando una criptografía asimétrica y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza lo siguiente: 1) si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; 2) si el documento digital ha sido modificado desde que se efectuó la transformación, de manera tal de garantizar con esta comprobación la integridad del documento. Todo lo cual conlleva a

garantizar las características de “no repudio” y la “integridad” del documento que son requisitos de la firma digital (artículo 7º del Decreto Nº 0428-MP-2008).

- Criptografía Asimétrica: Se entiende por Criptografía Asimétrica al algoritmo que utiliza, por un lado, una clave privada que es utilizada para firmar digitalmente y por otro su correspondiente clave pública para verificar esa firma digital. Debe ser técnicamente confiable (artículo 8º del Decreto Nº 0428-MP-2008).
- Digesto Seguro: es una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, llamada como tal, de forma que se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital (artículo 9º del Decreto Nº 0428-MP-2008).
- 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).
- Certificado 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.
- Lista de Certificados Revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado Provincial, la cual ha sido firmada digitalmente y publicada por el mismo.
- En inglés: *“Certificate Revocation List”* (CRL).
- Servicio OCSP (PROTOCOLO de Estado de Certificado en Línea): 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 certificado de servicio OCSP del Certificador Licenciado Provincial que brinda el servicio.
- En inglés: *“Online Certificate Status Protocol”* (OCSP)
- Manual de Procedimientos: Conjunto de prácticas utilizadas por el Certificador Licenciado Provincial en la emisión y administración de los certificados.
- En inglés: *“Certification Practice Statement”* (CPS).
- Plan de Cese de Actividades: Conjunto de actividades a desarrollar por el Certificador Licenciado Provincial en caso de finalizar la prestación de sus servicios.
- Plan de Continuidad de las Operaciones: Conjunto de procedimientos a seguir por el Certificador Licenciado Provincial ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones. También denominado Plan de Contingencia.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del Certificador Licenciado Provincial.
- Política de Privacidad: Conjunto de declaraciones que el Certificador Licenciado Provincial se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

1.6.2. - Acrónimos

AC	- Autoridad Certificante
ACR-SL	- Autoridad Certificante Raíz San Luis
AR	- Autoridad de Registro
ARR	- Autoridad de Registro Remoto
ACTySSL	- Agencia de Ciencia, Tecnología y Sociedad San Luis
CIPE	- Cédula de Identidad Provincial Electrónica
CLP	- Certificador Licenciado Provincial
CP	- Política de Certificación

CRL	- Lista de Certificados Revocados
CUIL	- Clave Única de Identificación Laboral
CUIT	- Clave Única de Identificación Tributaria
FD	- Firma Digital
FDSL	- Instituto Firma Digita de San Luis
FIPS	- Norma Federal de Procesamiento de la Información
MCyT	- Ministerio de Ciencia y Tecnología de San Luis
MPC	- Manual de Procedimientos de Certificación
OCSP	- Protocolo de estado de certificado en línea -Online Certificate Status Protocol
OID	- Identificador de Objeto (“Object Identifier”).
PKI	- Infraestructura de Clave Pública
RFC	- Request for Comments.

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

Detallará las responsabilidades del Certificador Licenciado Provincial y de todo otro participante respecto al mantenimiento de repositorios, publicación de certificados y de información sobre sus políticas y procedimientos.

2.1. - Repositorios

Indicará las entidades que administran los repositorios, señalando si el servicio es propio del Certificador Licenciado Provincial o si es provisto por un tercero. En este último caso, lo deberá identificar e indicar las condiciones del servicio.

2.2. - Publicación de información del Certificador Licenciado Provincial

El Certificador Licenciado Provincial deberá garantizar el acceso a la información actualizada y vigente publicada en su repositorio de los siguientes elementos:

a) Política 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 Provincial, acceso a la Autoridad Certificante Raíz del Ente Licenciante de San Luis.
i) Consulta de certificados emitidos (indicando su estado).
j) Listado de Autoridades de Registro (indicando si opera bajo modalidad móvil).

2.3. - Frecuencia de publicación

El Certificador Licenciado Provincial deberá garantizar la actualización inmediata del repositorio cada vez que cualquiera de los documentos publicados sea modificado.

2.4. - Controles de acceso a la información

Deberá garantizar los controles de los accesos al certificado del Certificador Licenciado Provincial, 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).

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

Señalará que 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 (conforme artículo 1º de Ley Nº V-0591-2007), el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a las tramitaciones realizadas.

3. - IDENTIFICACIÓN Y AUTENTICACIÓN

En esta sección se describirán los procedimientos empleados, previamente a la emisión de un certificado, para autenticar la identidad y demás atributos de los solicitantes utilizados por las Autoridades Certificantes o sus Autoridades de Registro. También se describirán los pasos para la autenticación de la identidad y demás atributos de los solicitantes de renovación y revocación de certificados.

3.1.- Asignación de nombres de suscriptores

Se describirán los nombres de los suscriptores siguiendo las siguientes reglas:

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

Se indicarán las siguientes denominaciones, según el tipo de certificados que se emitan en el marco de la Política de Certificación.

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 Humanas:

- "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).
- "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:

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

3.1.3. - Anonimato o uso de seudónimos

Especificará que no se emitirán certificados anónimos o cuyo Nombre Distintivo contenga un seudónimo.

3.1.4. - Reglas para la interpretación de nombres

Especificará que todos los nombres representados dentro de los certificados emitidos bajo la Política deben coincidir 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

Especificará que el nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor.

Además, enunciará que frente a una situación de homonimia quedará resuelta, tanto en el caso de personas humanas como personas jurídicas, consultando en el campo "Asunto" del certificado el atributo correspondiente a *"serialNumber"*. El cual, contiene el número de identificación laboral o tributaria, tanto en el caso de las personas físicas como jurídicas.

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

Especificará que 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.

Asimismo, enunciará que el Certificador Licenciado Provincial 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 deberá demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2. – Registro Inicial

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

El Certificador Licenciado Provincial DEBE cumplir con lo establecido en:

a) El artículo 21, inciso a) de la Ley Nº 25.506 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y el artículo 34, incisos 7 y 9 del Decreto Nº 0428-MP-2008 modificado por el Decreto N° 6011-MCyT-2018, relativos a la información a brindar a los solicitantes.
b) El artículo 14, inciso b) de la Ley Nº 25.506 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y el artículo 37 del Decreto Nº 0428-MP-2008, relativo a los contenidos mínimos de los certificados.

3.2.1. - Métodos para comprobar la posesión del par de claves

Indicará los procedimientos que implementarán el propio Certificador Licenciado Provincial o la autoridad de registro operativamente vinculada para asegurar que el solicitante se encuentra en posesión de la clave privada correspondiente a la clave pública remitida con el requerimiento del certificado digital, de acuerdo a protocolos de seguridad adecuados y que dicha clave privada es apta para firmar un documento.

Enunciará que el Certificador Licenciado Provincial procede a comprobar 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 debe incluir la clave privada. Las claves siempre deben ser generadas por el solicitante.

Asimismo, señalará que en ningún caso el Certificador Licenciado Provincial 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, de conformidad con el art. 1º de Ley Nº V-0591-2007.

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

Nota: El Certificador Licenciado Provincial indicará que el presente punto resulta “No Aplicable” cuando solo se emitan certificados para Personas Humanas.

De ser aplicable, describirá los procedimientos de autenticación de la identidad de los suscriptores o responsables de los certificados de personas jurídicas públicas o privadas, debiendo indicarse que:

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

El Certificador Licenciado Provincial DEBE cumplir con las siguientes exigencias reglamentarias impuestas por:

a) El artículo 21, inciso i) de la Ley Nº 25.506 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y el artículo 34, inciso 10 del Decreto Nº 0428-MP-2008, relativos a la conservación de la documentación de respaldo de los certificados emitidos.
b) El artículo 21, inciso f) de la Ley Nº 25.506 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y el artículo 34, inciso 8 del Decreto Nº 0428-MP-2008, relativos a la recolección de datos personales.
c) El artículo 14 de la Ley Nº V-0591-2007 y el artículo 40, inciso 8) del Decreto Nº 0428-MP-2008, relativos a la protección de datos personales.

Debe conservar 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 documento que contenga la confirmación de que la información incluida en el certificado es correcta y que presta su conformidad con relación al Acuerdo de Suscriptores.

3.2.3. - Autenticación de la identidad de Personas Humanas

Nota: El Certificador Licenciado Provincial indicará que el presente punto resulta “No Aplicable” cuando solo emita certificados para Personas Jurídicas.

De ser aplicable, describirá los procedimientos de autenticación de la identidad de los suscriptores de los certificados de Personas Humanas.

El Certificador Licenciado Provincial 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.

Se exige la presencia física del solicitante o suscriptor del certificado ante el Certificador Licenciado Provincial o la Autoridad de Registro con la que se encuentre operativamente vinculada. Asimismo, se autoriza la autenticación remota mediante la utilización de certificados de clave pública expedidos a ese sólo efecto. La verificación se efectúa mediante la presentación de los siguientes documentos:

- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad o Cédula de Identidad Provincial Electrónica (CIPE) expedida por la Provincia de San Luis.
- 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 Licenciado Provincial 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 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y el artículo 34, inciso 10) del Decreto Nº 0428-MP-2008, relativos a la conservación de la documentación de respaldo de los certificados emitidos.
b) El artículo 21, inciso f) de la Ley Nº 25.506 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y artículo 34, inciso 8) del Decreto Nº 0428-MP-2008, relativos a la recolección de datos personales.
c) El artículo 34, inciso i) de la Ley Nº 25.506 (de conformidad con el art. 1º de Ley Nº V-0591-2007) y artículo 34, inciso 1) del Decreto Nº 0428-MP-2008 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.
d) El artículo 14 de la Ley Nº V-0591-2007 y el artículo 40, inciso 8) del Decreto Nº 0428-MP-2008, relativos a la protección de datos personales.

El Solicitante deberá firmar un documento que contenga la confirmación de que la información incluida en el certificado es correcta y que presta su conformidad con relación al Acuerdo de Suscriptores (ver Anexo IV de la presente Resolución).

La Autoridad de Registro deberá verificar que el dispositivo criptográfico utilizado por el solicitante cumple con las especificaciones técnicas exigidas por la normativa vigente en la materia en la jurisdicción provincial.

Para el supuesto de autenticación remota del Solicitante mediante la utilización de certificados de clave pública expedidos a ese sólo efecto, el sistema deberá contemplar la verificación del dispositivo, la suscripción digital de la Solicitud y del Acuerdo con Suscriptores.

3.2.4. - Información no verificada del suscriptor

Se indicará que el Certificador Licenciado Provincial 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, conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

3.2.5. - Validación de autoridad

Indicará que según lo dispuesto en el punto 3.2.2., el Certificador Licenciado Provincial o la Autoridad de Registro con la que se encuentre operativamente vinculado, verificará la autorización de la Persona Humana que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente.

3.2.6. - Criterios para la interoperabilidad

Los certificados emitidos por todo Certificador Licenciado Provincial pueden ser utilizados por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, así como para autenticación o cifrado conforme lo establezca la respectiva Política de Certificación.

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)

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

- después de la revocación de un certificado.
- después de la expiración de un certificado.
- antes de la expiración de un certificado.

En los dos primeros supuestos se exigirá el cumplimiento de los procedimientos previstos en el Punto 3.2.3. – Autenticación de la Identidad de Personas Humanas.
Si la solicitud del nuevo certificado se realiza antes de la expiración del certificado, no habiendo sido este revocado, podrá no exigirse la presencia física del suscriptor, debiendo cumplirse con cada uno de los extremos que aseguran la correcta emisión de un certificado digital.

En los certificados de personas jurídicas o de aplicaciones, incluyendo los de servicios, se deberá tramitar un 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 certificado con el mismo par de claves

De aplicar, especificará los procedimientos de identificación y autenticación de la identidad del suscriptor a seguir para la renovación de un certificado digital, es decir, para la generación de un nuevo certificado sin que hayan operado cambios en la clave pública o en los datos del suscriptor. La renovación se podrá realizar siempre que el certificado se encuentre vigente.

A los fines de la obtención del certificado de personas humanas, podrá no exigirse la presencia física del suscriptor, debiendo cumplirse los extremos que aseguran la correcta emisión de un certificado digital.

En los certificados de personas jurídicas o aplicaciones, incluyendo los de servidores, se deberá tramitar un nuevo certificado.

3.4. – Requerimiento de Revocación

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

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

4.1.1. - Solicitantes de certificados

Describirá las condiciones que deben cumplir los solicitantes de certificados.

4.1.2. – Solicitud de Certificado

Señalará que las solicitudes sólo podrán ser iniciadas:

- En el caso de certificados de personas humanas, por el Solicitante.
- En el caso de personas jurídicas, 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.

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 Humanas, así como su documento nacional de identidad, CIPE y la constancia de C.U.I.T. o C.U.I.L.
Asimismo, el Solicitantes debe demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores de certificados.

4.2. - Procesamiento de la solicitud del certificado

Incluirá una descripción de las condiciones y procedimientos utilizados para aceptar o rechazar la solicitud de un certificado.

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 Nº 25.506 (conforme el artículo 1º de la Ley Nº V-0591-2007) y al inciso 9) del artículo 34 del Decreto Nº 0428-MP-2008.

4.3. - Emisión del certificado

4.3.1. - Proceso de emisión del certificado

Especificará que 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.

Indicará que, en el mismo sentido, se emitirá un certificado ante una solicitud de renovación.

4.3.2. - Notificación de emisión

Establecerá las condiciones para la notificación de la emisión de un certificado a su titular.

4.4. - Aceptación del certificado

4.4.1. Conducta constitutiva de la aceptación de un certificado

Detallará la conducta que configura la aceptación del certificado por parte de su titular.

4.4.2. Publicación del Certificado por el Certificador Licenciado Provincial

Establecerá los requisitos y procedimientos referidos a la publicación del certificado

4.4.3. Notificación del Certificador Licenciado Provincial a otras entidades respecto a la emisión de un certificado

Establecerá 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

Indicará que según lo establecido en el artículo 25 de la Ley Nº 25.506 (conforme lo dispuesto en el artículo 1º de la Ley Nº V-0509-2007), y en el artículo 36 del Decreto Nº 0428-MP-2008, 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 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.
e) Asimismo, indicará que de acuerdo a lo establecido en la presente Resolución el Suscriptor debe:

    i. Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.
    ii. Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la Política de Certificación.
    iii. Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política de Certificación, del Manual de Procedimientos (en su parte pública), 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

Indicará que los Terceros Usuarios deben:

a) Conocer los alcances de la presente Política de Certificación;
b) Rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda y de usarlo conforme a los Términos y Condiciones con Terceros Usuarios;
c) Verificar la validez del certificado digital.

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

Indicará si corresponde la aplicación de lo dispuesto en el punto 3.3.2.- Generación de un certificado con el mismo par de claves.

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

Indicará que, en el caso de certificados digitales de Personas Humanas, la generación 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., es decir su re emisión.

Asimismo, indicará que, si la solicitud de un nuevo certificado se realiza antes de la expiración del anterior, no habiendo sido este revocado, podrá no exigirse la presencia física, debiendo cumplirse los extremos que acreditan la correcta emisión de certificados digitales.

Referirá que, para los certificados de aplicaciones, incluyendo los de servidores, los responsables deben tramitar un 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

Indicará que el suscriptor se encuentra obligado a notificar al Certificador Licenciado Provincial 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 artículo 25 inciso d) de la Ley Nº 25.506 (conforme el art. 1º de Ley Nº V-0591-2007) y en el artículo 36 inciso 4) del Decreto Nº 0428-MP-2008. 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

Indicará que los certificados serán revocados de manera oportuna y sobre la base de una solicitud de revocación de certificado validada.
Referirá, además, que el estado de suspensión no es admitido en el marco de la Ley Nº 25.506 (de conformidad con lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007).

4.9.1. - Causas de revocación

Especificará que el Certificador Licenciado Provincial 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 (según si, la Política, contempla la emisión de certificados digital a favor de personas humanas o jurídicas).
- 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 hallan 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 de Certificación, del Manual de Procedimientos, de la normativa provincial vigente en materia de firma digital.
- Por revocación de su propio certificado digital.

Expresará además que el Certificador Licenciado Provincial 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

Especificará que se encuentran autorizados para solicitar la revocación de un 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 Licenciado Provincial o la Autoridad de registro operativamente vinculada.
g) El Ente Licenciante Provincial.
h) La autoridad judicial competente.
i) La Autoridad de Aplicación Provincial del régimen de firma digital.

4.9.3. - Procedimientos para la solicitud de revocación

Describirá los procedimientos establecidos por el Certificador Licenciado Provincial para la revocación de los certificados que emita, debiendo garantizar 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 Licenciado Provincial 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.

Asimismo, indicará las vías de contacto disponibles para la realización de la solicitud de revocación y para la comunicación del cambio de estado del certificado.

4.9.4. - Plazo para la solicitud de revocación

Indicará que 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 deberá estar disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas.

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

Expresará que 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

Especificará que 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 Licenciado Provincial que la emite y de su período de validez.

El Certificador Licenciado Provincial debe cumplir con lo establecido en el artículo 34, inciso 11) del Decreto Nº 0428-MP-2008 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

Especificará la frecuencia con que se emitirá la lista de certificados revocados asociada a la Política de Certificación, debiendo emitirse como mínimo cada VEINTICUATRO (24) horas.

4.9.8.- Vigencia de la lista de certificados revocados

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

Indicará que el Certificador Licenciado Provincial 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 en línea del estado del certificado (OCSP).

El Certificador Licenciado Provincial debe poner a disposición de los terceros usuarios:

a) La información relativa a las características de los servicios de verificación de estado.
b) La disponibilidad de tales servicios y los procedimientos que se seguirán en caso de no disponibilidad.
c) Todas las características opcionales de tales servicios.

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

Indicará 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

Describirá, en caso de existir, otras formas utilizadas por el Certificador Licenciado Provincial para divulgar la información sobre revocación de certificados.

Establecerá, además, 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

Indicará que, 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

Indicará que el estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.9.14. - Autorizados a solicitar la suspensión

Indicará que el estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.9.15. - Procedimientos para la solicitud de suspensión

Indicará que el estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.9.16. - Límites del periodo de suspensión de un certificado

Indicará que el estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.10. – Estado del certificado

4.10.1. – Características técnicas

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

4.10.2. – Disponibilidad del servicio

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

4.10.3. – Aspectos operativos

Indicará cualquier otro aspecto de los servicios de verificación del estado de los certificados.

4.11. – Desvinculación del suscriptor

Indicará que se dará por desvinculado de los servicios del certificador al titular de un certificado en los siguientes casos:

- Por caducidad de la vigencia del certificado digital, si no tramitara uno nuevo,
- Por revocación del certificado digital, si no tramitara uno nuevo,
- Ante el cese de las operaciones del Certificador Licenciado Provincial.

.

4.12. – Recuperación y custodia de claves privadas

Indicará que el Certificador Licenciado Provincial 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 (conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007) y en el inciso 1) del artículo 34 del Decreto Nº 0428-MP-2008. 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 nacional antes mencionada.

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

Describirá los procedimientos referidos a los controles de seguridad física, de gestión y operativos implementados por el Certificador Licenciado Provincial. La descripción detallada se efectuará en el Plan de Seguridad.

5.1. - Controles de seguridad física

Indicará que el Certificador Licenciado Provincial 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

Indicará que el Certificador Licenciado Provincial 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

Indicará que el Certificador Licenciado Provincial 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

Indicará que el Certificador Licenciado Provincial mantiene políticas de registro de eventos, cuyos procedimientos detallados serán desarrollados en el Manual de Procedimientos.

Se indicará que el Certificador Licenciado Provincial 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 Nº 25.506 (conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007) y en el inciso10) del artículo 34 del Decreto Nº 0428-MP-2008 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

Indicará que el Certificador Licenciado Provincial cuenta con políticas de conservación de registros, cuyos procedimientos detallados serán desarrollados en el Manual de Procedimientos.

Los procedimientos deben cumplir lo establecido en el inciso i) del artículo 21 de la Ley Nº 25.506 y en el inciso 10) del artículo 34 del Decreto Nº 0428-MP-2008 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

Se debe respetar lo establecido en el Anexo I Sección 3 respecto del registro de eventos.

Señalará que existen procedimientos de conservación y guarda de registros en los siguientes aspectos, que serán 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

Incluirá 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

Describirá los requerimientos relativos a la recuperación de los recursos del Certificador Licenciado Provincial en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Continuidad de las Operaciones.

Se deberá indicar que 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.

En los casos en que el Certificador Licenciado Provincial requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Continuidad de las Operaciones los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Los contratos entre el Certificador Licenciado Provincial y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades.

El Certificador Licenciado Provincial o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Continuidad de las Operaciones.

La contratación de servicios o infraestructura no exime al prestador de la presentación de los informes de auditoría, los cuales deberán incluir los sistemas y seguridades del prestador contratado

5.8. - Plan de Cese de Actividades

Describirá los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del Certificador Licenciado Provincial o de una o varias de sus autoridades certificantes o de registro. Estos requerimientos deben ser desarrollados en su Plan de Cese de Actividades.

Indicará que se han implementado procedimientos referidos a:

a) Notificación a la Autoridad de Aplicación Provincial, al Ente Licenciante Provincial, suscriptores, terceros usuarios, otros certificadores y otros usuarios vinculados.
b) Revocación del certificado del Certificador Licenciado Provincial 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 debe cumplir con idénticas exigencias de seguridad que las previstas para el Certificador o su autoridad certificante o de registro que cesó.

En los casos en que el Certificador Licenciado Provincial requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, los contratos entre aquel y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades.

El Certificador Licenciado Provincial o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la implementación del Plan de Cese de actividades.

6.- CONTROLES DE SEGURIDAD TÉCNICA

Describirá las medidas de seguridad implementadas por el Certificador Licenciado Provincial para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además, incluirá 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 Licenciado Provincial, 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

Describirá todos los aspectos relativos a la generación del par de claves de las autoridades certificantes del Certificador Licenciado Provincial, de las claves de los responsables de las Autoridades de Registro, y de las claves de los suscriptores.

Además, describirá 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 al Suscriptor

Indicará que 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), conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007, y en el inciso 1) del artículo 34 del Decreto Nº 0428-MP-2008.

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

Establecerá los procedimientos utilizados para la entrega de la clave pública del solicitante del certificado al Certificador Licenciado Provincial responsable de su emisión.

6.1.4. - Disponibilidad de la clave pública del certificador

Describirá los medios adoptados para poner el certificado del Certificador Licenciado Provincial, 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

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

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

6.1.6. - Generación de parámetros de claves asimétricas y verificación de la calidad

Describirá 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)

Establecerá que las claves criptográficas de los suscriptores de los certificados podrán ser utilizados para firmar digitalmente, para funciones de autenticación y para cifrado.

6.2.- Controles de ingeniería para protección de la clave privada y dispositivos criptográficos

La protección de la clave privada debe ser considerada desde la perspectiva del Certificador Licenciado Provincial, 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 establecida 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

Describirá 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

Describirá los controles empleados para la activación de las claves que deben basarse en la presencia de M de N con M mayor a 3. Estos controles son desarrollados con mayor detalle en los documentos específicos.

6.2.3. - Recuperación de clave privada

Describirá los procedimientos empleados por el Certificador Licenciado Provincial para la recuperación de sus propias claves.

6.2.4. - Copia de seguridad de clave privada

Describirá los procedimientos y controles de seguridad empleados para la realización de copias de seguridad de las claves privadas del Certificador Licenciado Provincial, 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

Describirá los procedimientos y controles de seguridad empleados para el archivo de las claves privadas del Certificador Licenciado Provincial, garantizándose que su seguridad no disminuya por el proceso de archivo.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos

Indicará la prohibición que el Suscriptor transfiera su clave privada.

6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos

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

6.2.8. - Método de activación de claves privadas

Describirá los requisitos, roles y procedimientos necesarios para la activación de la clave privada del Certificador Licenciado Provincial y señalará que 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

Describirá los requisitos, roles y procedimientos necesarios para la desactivación de la clave privada del Certificador Licenciado Provincial, requiriéndose la autenticación de la identidad de los responsables a través de métodos adecuados.

6.2.10. - Método de destrucción de claves privadas

Especificará 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 serán desarrollados con mayor detalle en los documentos específicos.

6.2.11. – Requisitos de los dispositivos criptográficos

Indicará 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 Licenciado Provincial, de los repositorios, de las Autoridades de Registro y de los suscriptores.

Se describirán 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 deben incluir mecanismos adicionales a fin de evitar que esas claves sean alteradas durante un período de almacenamiento que puede ser mayor que el período de criptoanálisis de las claves.

6.3.2. - Período de uso de clave pública y privada

Determinará que las claves privadas correspondientes a los certificados emitidos por el Certificador Licenciado Provincial 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

Indicará que 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.

Señalará que se establecerán 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

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

6.4.2. - Protección de los datos de activación

Indicará los procedimientos para garantizar la adecuada protección de los datos de activación contra usos no autorizados.

6.4.3. - Otros aspectos referidos a los datos de activación

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

6.5. - Controles de seguridad informática

6.5.1. - Requisitos Técnicos específicos

Se establecerán los requisitos de seguridad referidos al equipamiento y al software del Certificador Licenciado Provincial, 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

Describirá 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

Describirá 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

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

6.6.2. – Controles de gestión de seguridad

Señalará la necesidad de documentar y controlar la configuración del sistema, así como toda modificación o actualización, implementado además un método de detección de modificaciones no autorizadas.

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

Describirá, 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

Describirá 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

Especificará los servicios de donde se toman la fecha y hora utilizadas para la información publicada en los repositorios (directores, CRLs, copias de seguridad, entre otros).

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

Especificará 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 la Agencia de Ciencia, Tecnología y Sociedad San Luis, y deben cumplir con las indicaciones establecidas en la sección “2 - Perfil de certificados digitales” del Anexo III y sección 3 “Perfil de CRLs” del mismo Anexo.

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 Política de Certificación deberán ser emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 o la que en su defecto determine la Agencia de Ciencia, Tecnología y Sociedad San Luis, y cumplirán con las indicaciones establecidas en el Anexo III, Sección “3 - Perfil de CRLs”.

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 (OCSP)

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 el Anexo III, Sección “4 - Perfil de la consulta en línea del estado del certificado”.

7.3.1. – Consultas OCSP

A completar sobre la base de lo establecido en el documento referido en el apartado 4.2 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:

- Los artículos 22 y 23 del Decreto Nº 0428-MP-2008, respecto al sistema de auditoría y el artículo 21, inciso k) de la Ley Nº 25.506 (conforme art. 1º de la Ley Nº V-0591-2007), relativo a la publicación de informes de auditoría.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1. - Aranceles

De corresponder, describirá los aranceles asociados a cada uno de los servicios que preste el Certificador Licenciado Provincial, relacionados con la Política de Certificación.

9.2. - Responsabilidad Financiera

Incluirá 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 de Certificación y de los recursos con los que cuenta el Certificador Licenciado Provincial para afrontarlos.

Además, expresará que el Certificador Licenciado Provincial es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones legales, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles.

Los Certificadores Licenciados Provinciales no son responsables en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la legislación (de existir, enunciar supuestos);
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos,

deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

Asimismo, indicará que, en ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un Certificador Licenciado Provincial, público o privado, comprometerá la responsabilidad pecuniaria del Estado de San Luis en su calidad de Ente Administrador de la Infraestructura de Firma Digital Provincial.

Señalará que el Certificador Licenciado Provincial es responsable con los alcances establecidos en los apartados anteriores, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisión.

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

9.3. - Confidencialidad

Indicará las previsiones en cuanto al tratamiento de información confidencial del Certificador Licenciado Provincial, 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

Establecerá, como principio general, que toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no será 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 Licenciado Provincial o la Autoridad de Registro durante el ciclo de vida del certificado.

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

9.3.2. - Información no confidencial

Especificará la información a ser tratada como no confidencial por el Certificador Licenciado Provincial y por las Autoridades de Registro vinculadas operativamente. Entendiéndose como tal la siguiente:

a) Contenido de los certificados y de las listas de certificados revocados.
b) Información sobre personas humanas 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

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

9.4. - Privacidad

Indicará que 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

Incluirá especificaciones acerca de los derechos de propiedad intelectual, derechos de autor y patentes relacionadas con los documentos elaborados por el Certificador Licenciado Provincial, 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 legislación en materia de responsabilidad en firma digital, detallará:

a) Las garantías para el Certificador Licenciado Provincial, 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 legislación en materia de responsabilidad en firma digital, detallará:

a) Las limitaciones de responsabilidad para el Certificador Licenciado Provincial, 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 legislación en materia de responsabilidad en firma digital, se detallarán 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 legislación en materia de responsabilidad en firma digital, se detallarán las previsiones relativas a las compensaciones por daños y perjuicios.

9.10.- Condiciones de vigencia

Indicará el período de vigencia de la Política de Certificación 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
- 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

Establecerá las políticas para el mantenimiento y administración de la Política de Certificación.

9.12.1.- Procedimientos de cambio

Establecerá las políticas utilizadas para efectuar modificaciones en la Política de Certificación aprobada. Toda modificación deberá ser aprobada previamente por el Ente Licenciante Provincial conforme a lo establecido por la Ley Nº 25.506, artículo 21, inciso q), (conforme artículo 1º de la Ley Nº V-0591-2007), por la presente Resolución y sus Anexos respectivos.

Asimismo, referirá que toda Política de Certificación debe ser sometida a aprobación del Ente Licenciante Provincial durante el proceso de licenciamiento.

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

Adicionalmente, el Certificador Licenciado Provincial incluirá la información específica correspondiente a esta sección.

9.12.2.- Mecanismo y plazo de publicación y notificación

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

9.12.3.- Condiciones de modificación del OID

No aplicable.

9.13.- Procedimientos de resolución de conflictos

Indicará los procedimientos de resolución de conflictos, como así también lo hará en los acuerdos en los que el Certificador Licenciado Provincial sea parte.

Detallará las políticas de reclamo aplicables cuando existan conflictos respecto a la interpretación de una o más disposiciones de la Política de Certificación, conforme lo dispuesto en el Capítulo IV del Decreto Nº 0428-MP-2008.

En ningún caso, la Política de Certificación del Certificador Licenciado Provincial prevalecerá sobre lo dispuesto por la normativa vigente de firma digital.

Asimismo, informará que el suscriptor o los terceros usuarios podrán accionar ante la Agencia de Ciencia, Tecnología y Sociedad San Luis, previo agotamiento del procedimiento ante el Certificador Licenciado Provincial correspondiente, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

9.14.- Legislación aplicable

Especificará la legislación que respalda la interpretación, aplicación y validez de la Política de Certificación, debiendo indicarse la Ley Nº V-0591-2007 de adhesión a la Ley Nº 25.506, el Decreto Provincial Nº 0428-MP-2008 y sus modificatorios, y toda otra norma complementaria dictada por la autoridad competente.

9.15.- Conformidad con normas aplicables

Especificará la legislación aplicable a la actividad del Certificador Licenciado Provincial.

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.