ANEXO III

INFRAESTRUCTURA DE FIRMA DIGITAL REPÚBLICA ARGENTINA

LEY N° 25.506

POLÍTICA ÚNICA DE CERTIFICACIÓN

SECRETARÍA DE INNOVACIÓN PÚBLICA

JEFATURA DE GABINETE DE MINISTROS

ANEXO III

CARACTERÍSTICAS DEL DOCUMENTO

Este documento describe la estructura y el contenido que debe poseer la Política Única de Certificación de las entidades y jurisdicciones del sector Público o Privado 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, su modificatorias y normas complementarias.

Para su elaboración se han tenido en cuenta los lineamientos del RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*", 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 "*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*" y RFC 5280 "*Internet X.509 Public Key Infrastructure Certificate and Certificate RevocationList (CRL) Profile*" producido por el IETF.

Las Políticas Únicas de Certificación emitidas por los Certificadores se encuentran sujetas a los contenidos, la estructura y los lineamientos del presente documento.

Para integrar la Infraestructura antes mencionada, los Certificadores deberán presentar toda la documentación requerida en el Anexo II. Una vez cumplidos y aprobados los requisitos para el licenciamiento, la Autoridad de Aplicación procederá al dictado del acto administrativo correspondiente, ordenando su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

Toda consulta acerca de la interpretación del presente documento debe ser presentada por los interesados a través del trámite "Presentación ante el Ente Licenciante" de la plataforma de Trámites a Distancia (TAD), o, en caso de

corresponder, a través del sistema de Gestión Documental Electrónica (GDE) o por escrito en Mesa de Entrada ante el Ente Licenciante, sito en Av. Pres. Roque Sáenz Peña 788 8° Piso - C1035AAP - CIUDAD AUTÓNOMA DE BUENOS AIRES - REPÚBLICA ARGENTINA, o remitir su consulta a la siguiente dirección de correo electrónico: licenciamiento@jefatura.gob.ar.

INSTRUCCIONES PARA LA CONFORMACIÓN DE LA POLÍTICA ÚNICA DE CERTIFICACIÓN

El presente documento contiene lineamientos específicos respecto al texto que deben incluir las Políticas Únicas de Certificación de los Certificadores Licenciados en el marco de la Ley N° 25.506 y su modificatoria.

Los certificados digitales que emitan los Certificadores Licenciados en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, pueden 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:

ANEXO III

1. - INTRODUCCIÓN

1.1. - Descripción general

Se indicará que el documento establece las políticas que se aplican a la relación entre un Certificador Licenciado y los solicitantes, suscriptores y terceros usuarios de los certificados que éste emita en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley N° 25.506 y normativa complementaria).

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. Incluirá el Identificador de Objeto (OID) correspondiente a la política cuando le sea otorgado por la DIRECCIÓN NACIONAL DE FIRMA DIGITAL E INFRAESTRUCTURA TECNOLÓGICA de la SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS o la que la reemplace en el futuro, 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 Licenciado que presenta la Política Única de Certificación correspondiente a su Autoridad Certificante, indicando los datos de

identificación tales como razón social o denominación del organismo, CUIT, dirección postal, dirección electrónica, teléfono y sitio web.

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, 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, renovación, 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 Política Única de Certificación tienen como suscriptores personas humanas, jurídicas o aplicaciones.

1.3.4. - Terceros Usuarios

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

1.4. - Uso de los certificados

Se indicará que las claves correspondientes a los certificados digitales que se emitan bajo la 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. - Organización administradora del documento

Se incluirán los datos de la organización responsable de la Política Única de Certificación 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 de Única Certificación.

1.5.3. – Organismo encargado de aprobar la Política Única de Certificación

Se indicará que la Política Única de Certificación ha sido presentada ante el Ente Licenciante durante el proceso de licenciamiento y ha sido aprobada mediante 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**: Es quien tiene por función el dictado de las normas reglamentarias de aplicación de la Ley N° 25.506 y lo establecido en la normativa regulatoria de Firma Digital de la REPÚBLICA ARGENTINA.
- **AUTORIDAD DE REGISTRO**: Es la entidad que tiene a su cargo las siguientes funciones, delegadas por el Certificador Licenciado:
  a) Recepción de las solicitudes de emisión de certificados.
  b) Validación de la identidad y autenticación de los datos de los titulares de certificados.
  c) Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
  d) Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
  e) Recepción y validación de las solicitudes de revocación de certificados y su direccionamiento al Certificador Licenciado con el que se vinculen.
  f) Identificación y autenticación de los solicitantes de revocación de certificados.
  g) 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.

h) Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

i) 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.

- **CERTIFICADO DIGITAL**: Se entiende por certificado digital al documento digital firmado digitalmente por un Certificador Licenciado, que vincula los datos de verificación de firma a su titular.
- **CERTIFICADOR LICENCIADO**: Se entiende por Certificador Licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.
- **AUTORIDAD DE SELLO DE TIEMPO**: Entidad que acredita la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- **AUTORIDAD DE SELLO DE COMPETENCIA**: Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.
- **ENTE LICENCIANTE**: Es el encargado de aprobar las Políticas Únicas de Certificación, el Manual de Procedimiento, el Plan de Seguridad, el Plan de Cese de Actividades y el Plan de Contingencia, presentados por los Certificadores solicitantes de la licencia o licenciados en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.

ANEXO III

- **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).
- **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).
- **PLAN DE CESE DE ACTIVIDADES**: Conjunto de actividades a desarrollar por el Certificador Licenciado en caso de finalizar la prestación de sus servicios.
- **PLAN DE CONTINGENCIA**: 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.
- **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 Certificados de Revocados (CRL).

- **SUSCRIPTOR O TITULAR DE CERTIFICADO DIGITAL**: Persona, jurisdicción 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 humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

1.6.2. - Acrónimos

Se deberá detallar los acrónimos utilizados en la Política Única de Certificación.

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

Se detallarán 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

Se indicará que el Certificador garantiza 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 con Suscriptores.

c) Términos y condiciones con Terceros Usuarios.

d) Política de Privacidad.

e) Manual de Procedimientos.

f) Información sobre las auditorias e inspecciones que le fueron efectuadas (fecha y organismo que efectuara la auditoria o inspección).

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).

2.3. Listado de Autoridades de Registro - Frecuencia de publicación

Se indicará que el Certificador 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 indicará que el Certificador garantiza los controles de los accesos a su certificado, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política Única de Certificación y a su Manual de Procedimientos.

Se indicará que el Certificador solo podrá revelar información confidencial o privada, si es requerida judicialmente o por autoridad competente en el marco de procedimientos administrativos.

Se indicará que, en virtud de lo dispuesto por la Ley de Protección de Datos Personales N° 25.326 y por el artículo 21 inciso h) de la Ley N° 25.506, el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a su tramitación.

3. - IDENTIFICACIÓN Y AUTENTICACIÓN

Se describirán 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 describirán 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

Se indicarán las siguientes denominaciones, según el tipo de certificado que se emita.

Para los **certificados de Aplicaciones**:

- "*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 posible 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 [ISO 3166] 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 número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

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

  En el caso que el suscriptor sea extranjero:

  "PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [IS0 3166] 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 [IS0 3166] 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 [ISO 3166] de 2 (DOS) caracteres.

ANEXO III

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.
- "*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 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 Tributaria para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO 3166] de DOS (2) caracteres.
- "*countryName"* (OID 2.5.4.6: Código de país): DEBE estar presente y representar el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

ANEXO III

Para los **Certificados de Autoridad de Sello de Tiempo.**

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE indicar el nombre del servicio.
- "*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 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 tributaria para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO 3166] de DOS (2) caracteres.
- "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y representar el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los **Certificados de Autoridad de Sello de Competencia**:

- "*commonName*" (OID 2.5.4.3: Nombre común): DEBE indicar el nombre de la Autoridad de Competencia.
- "*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.
- "*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 [ISO 3166] de DOS (2) caracteres.

3.1.3. - Anonimato o uso de seudónimos

No se emitirán certificados anónimos o cuyo Nombre Distintivo contenga un seudónimo.

3.1.4. - Reglas para la interpretación de nombres

Todos los nombres representados dentro de los certificados emitidos coincidirán 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 humanas como jurídicas.

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

No se admitirá 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 reservará el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores. En caso de conflicto, la parte que solicite el certificado debe

demostrar su interés legítimo o su derecho subjetivo a la utilización de un nombre en particular.

3.2. - Registro inicial

El Certificador 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 la Autoridad de Registro operativamente vinculada al Certificador. Indicando los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

El Certificador DEBE cumplir con lo establecido en los artículos 14, inciso b) y 21, inciso a) de la Ley de Firma Digital Nº 25.506, y normas complementarias.

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

El Certificador comprobará 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, exigir o acceder bajo ninguna circunstancia a la clave privada de los solicitantes o titulares de los certificados, conforme el artículo 21 inciso b) de la Ley N° 25.506, y del artículo 21 inciso 3 del Anexo al Decreto Reglamentario N° 182/2019 y complementarias.

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

Se indicará como “No Aplicable” cuando solo se emitan certificados para Personas Humanas.

Los procedimientos de autenticación de identidad de los suscriptores responsables de los certificados de personas jurídicas públicas o privadas deberán cumplir los siguientes aspectos:

a) El requerimiento debe efectuarse únicamente por intermedio del responsable autorizado a actuar en nombre de la persona jurídica del suscriptor para el caso de certificados de personas jurídicas, el responsable del servicio o aplicación.

b) La Autoridad de Registro, 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 mediante documentación que acredite su condición de persona jurídica.

d) La identidad de la Persona Jurídica titular del certificado, responsable del servicio o aplicación deberá ser verificada mediante documentación que acredite su condición de tal.

El Certificador DEBE cumplir con las siguientes exigencias reglamentarias impuestas por el artículo 21, inciso i) de la Ley Nº 25.506, relativo a la conservación de la documentación de respaldo de los certificados emitidos e inciso f) de la misma ley, relativo a la recolección de datos personales necesarios para su emisión.

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

El responsable autorizado a cargo del servicio o aplicación debe prestar su consentimiento expresando la confirmación de que la información incluida en el certificado es correcta.

Los Oficiales de Registro de las Autoridades de Registro, en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, deberán capturar la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital.

3.2.3. - Autenticación de la identidad de Personas Humanas

Se indicará como “No Aplicable” cuando solo se emitan certificados para Personas Jurídicas.

El Certificador describirá los procedimientos de autenticación de la identidad de los suscriptores de los Certificados de Personas Humanas.

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

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

Se conservará registro biométrico y/o la documentación de respaldo del proceso de autenticación por parte de la Autoridad de Registro.

Se deberán tener en consideración las exigencias reglamentarias impuestas por la Ley Nº 25.506, su modificatoria y complementarias, en particular, lo establecido en el artículo 21, inciso i) de la mencionada ley relativo a la conservación de la documentación de respaldo de los certificados emitidos e inciso f) de la misma ley, relativo a la recolección de datos personales.

Adicionalmente, el Certificador debe celebrar UN (1) acuerdo con el solicitante o suscriptor, conforme el Anexo V de la presente resolución.

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 Autoridad de Aplicación. Los Oficiales de Registro de las Autoridades de Registro, en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, deberán capturar la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital.

3.2.4. - Información no verificada del suscriptor

Se deberá conservar la información referida al solicitante que no hubiera sido verificada, para lo cual, se deberá cumplir con lo establecido en el artículo 14 apartado 3 del inciso b) de la Ley N° 25.506 y su modificatoria.

3.2.5. - Validación de autoridad

Según lo dispuesto en el punto 3.2.2., la Autoridad de Registro verificará la autorización del responsable 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 humanas 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 Humanas.

En el caso c) si la solicitud de la renovación se realiza antes de la expiración del

certificado, no habiendo sido este revocado, no se exigirá la presencia física del suscriptor, debiendo el solicitante remitir la constancia del inicio del trámite de renovación firmada digitalmente con el certificado a renovar.

La renovación sin presencia física del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y las contraseñas necesarias para el acceso a su clave privada (PIN/OTP)

Sin perjuicio de ello en el caso de certificados de personas jurídicas o de aplicaciones, el solicitante deberá presentar nuevamente la documentación requerida 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 humanas, jurídicas o de aplicaciones, 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.

A los fines de la renovación del certificado, no se exigirá la presencia física del suscriptor, debiendo éste remitir la constancia del inicio del trámite de renovación firmada digitalmente con el certificado a renovar. La renovación sin presencia física del solicitante se podrá realizar, una sola vez, siempre y cuando no se modifique ningún dato del certificado y el suscriptor posea un certificado vigente y los datos necesarios para el acceso a su clave privada (PIN/OTP)

Sin perjuicio de ello, en el caso de certificados de personas jurídicas o de aplicaciones, el solicitante deberá presentar nuevamente la documentación requerida en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

3.4. - Requerimiento de revocación

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

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

4.1.1. - Solicitantes de certificados

Se describirán las condiciones y procedimientos que deben cumplir los solicitantes de certificados.

4.1.2. - Solicitud de certificado

En el caso de certificados de personas humanas las solicitudes sólo podrán ser iniciadas por el solicitante.

En el caso de certificados de personas jurídicas, las solicitudes serán presentadas por el representante legal o apoderado acreditando poder suficiente a dichos efectos.

En el caso de certificados de aplicación las solicitudes serán presentadas por el responsable del servicio.

El 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 la constancia de C.U.I.T./C.U.I.L.

4.2. - Procesamiento de la solicitud del certificado

En esta sección se incluirá la descripción de las condiciones y procedimientos utilizados para aceptar o rechazar la solicitud de un certificado. De corresponder se indicarán los plazos aplicables, así como toda la información relativa a la tramitación de su certificado, de acuerdo al artículo 21, inciso h) de la Ley N° 25.506 y del artículo 21, inciso 7 del Anexo al Decreto 182/2019.

4.3. - Emisión del certificado

4.3.1. - Proceso de emisión del certificado

Se deberán indicar los recaudos del proceso enunciado en el apartado 4.1.2. Solicitud de certificado, como así también el proceso de emisión del certificado y de su puesta a disposición del suscriptor.

4.3.2. - Notificación de emisión

Se establecerán los procedimientos y condiciones para la notificación de la emisión de un certificado a su titular.

4.4. - Aceptación del certificado

Asimismo, se establecerán los procedimientos de notificación de emisión a otras entidades y jurisdicciones, de ser aplicable.

Se establecerán los requisitos y procedimientos de aceptación del certificado por el suscriptor.

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

Se indicará que el suscriptor deberá cumplir con las obligaciones establecidas en el artículo 25 de la Ley Nº 25.506 y su modificatoria:

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.

Asimismo, se indicará que el suscriptor debe cumplir con las siguientes obligaciones:

a) Resguardar y no divulgar aquellos factores de autenticación (contraseñas de usuario, OTP, PIN) que permitan utilizar la clave privada.
b) Proveer toda la información que le sea requerida a los fines de la emisión del

certificado de modo completo y preciso.

c) Utilizar los certificados de acuerdo a lo establecido en la Política de Única Certificación.

d) 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

Se indicará que los Terceros Usuarios deberán:

a) Conocer los alcances de la 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 deberán aplicar los procedimientos previstos 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

Se deberán aplicar los procedimientos previstos en el punto 3.3.1.- Renovación con generación de nuevo par de claves.

4.8. - Modificación del certificado

Se indicará que 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 tal caso procede la revocación de dicho certificado y de ser requerido, la solicitud de uno nuevo.

4.9. - Suspensión y Revocación de Certificados

Se indicará que las revocaciones de certificados se efectuarán en los plazos previstos en el apartado 4.9.4 y sobre la base de una solicitud de revocación validada según los procedimientos mencionados en el apartado 4.9.3.

Asimismo, se indicará que el estado de suspensión no se encuentra contemplado en la legislación vigente aplicable a Firma Digital.

4.9.1. - Causas de revocación

Se deberá indicar que el Certificador procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

a) A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación.
b) Si se determina que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
c) Si determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por resolución judicial.

e) Por acto administrativo de la Autoridad de Aplicación debidamente fundado.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

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

j) Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.

k) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.

l) 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 y su modificatoria, sus normas reglamentarias.

4.9.2. - Autorizados a solicitar la revocación

Se indicará que se encuentran autorizados para solicitar la revocación de un certificado:

a) En el caso de los certificados de personas humanas, el suscriptor del certificado.

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

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

d) El Certificador o la Autoridad de Registro.

e) El Ente Licenciante.

f) La Autoridad Judicial.

g) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación

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.

Se indicará que 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 causales 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.

4.9.4. - Plazo para la solicitud de revocación

Se indicará que en caso de producirse alguna de las circunstancias previstas en el apartado 4.9.1 se debe requerir su revocación en forma inmediata.

El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE DÍAS POR VEINTICUATRO HORAS (7x24) cumpliendo con lo establecido en el artículo 21, inciso 8 del Anexo al Decreto Nº 182/2019.

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

Se indicará que el Certificador, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) HORAS de recibido el requerimiento de revocación.

4.9.6. - Requisitos para la verificación de la Lista de Certificados Revocados

Se indicará 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, como mínimo, equivalentes.

Se indicará que la autenticidad y validez de las Listas de Certificados Revocados está confirmada mediante la verificación de la firma digital del Certificador que la emite y de su período de validez.

El Certificador deberá, asimismo, indicar, que cumple con lo establecido en el artículo 21, inciso 9 del Anexo al Decreto Nº 182/2019 relativo al acceso al

repositorio de certificados revocados y las obligaciones establecidas en la presente resolución.

4.9.7. - Frecuencia de emisión de listas de certificados revocados

Se deberá especificar 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. Cada una de ellas indicará la fecha de emisión de la siguiente.

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

Se indicará que el Certificador pondrá 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 de estado de certificados (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.

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

Se establecerán los requisitos para la verificación en línea de estado de certificados (servicio OCSP) 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, 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

Se 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 medios previstos en el apartado 4.9.3. - Procedimientos para la solicitud de revocación.

4.9.13. - Causas de suspensión

El estado de suspensión no se encuentra contemplado en el marco de la Ley Nº 25.506 y modificatoria.

4.9.14. - Autorizados a solicitar la suspensión

El estado de suspensión no se encuentra contemplado en el marco de la Ley Nº

25.506 y modificatoria.

4.9.15. - Procedimientos para la solicitud de suspensión

El estado de suspensión no se encuentra contemplado en el marco de la Ley Nº 25.506 y modificatoria.

4.9.16. - Límites del periodo de suspensión de un certificado

El estado de suspensión no se encuentra contemplado en el marco de la Ley Nº 25.506 y modificatoria.

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, garantizando su disponibilidad.

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

Se indicará que, en caso de expiración o revocación del certificado, su titular se considera desvinculado de los servicios del Certificador, excepto en el caso en que se tramite un nuevo certificado.

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

4.12. – Recuperación y custodia de claves privadas

Se indicará que 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 artículo 21, inciso b) de la Ley N° 25.506 y del artículo 21, inciso 3 del Anexo al Decreto N° 182/2019. Asimismo, 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 artículo 25, inciso a) de la ley antes mencionada.

5. CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN

En esta Sección se describirán los procedimientos referidos a los controles de seguridad física, operativos y de gestión implementados por el Certificador. La descripción detallada se efectuará en el Plan de Seguridad.

5.1. - Controles de seguridad física

Se indicará que el Certificador 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 indicará que el Certificador 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 indicará que el Certificador 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, etc.

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

Los procedimientos de auditoría de seguridad deberán contar con los siguientes aspectos:

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

b) Frecuencia de procesamiento de registros.

c) Período de guarda de los registros. Debe respetarse lo establecido en el artículo 21, inciso i) 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.

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

h) Evaluación de vulnerabilidades.

5.5. - Conservación de registros de eventos

Se indicará que 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 II Sección 3 respecto del registro de eventos.

Se establecerán procedimientos de conservación y guarda de registros en los siguientes aspectos, los que se detallarán en el Manual de Procedimientos:

a) Tipo de registro archivado. Debe respetarse lo establecido en el Anexo II Sección 3.
b) Período de guarda de los registros.
c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso.
d) Procedimientos de resguardo de los registros.
e) Sistemas de recolección y análisis de registros
f) Procedimientos para obtener y verificar la información archivada.

5.6. - Cambio de claves criptográficas

Se indicarán 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. Si la clave privada se encontrase comprometida, se procederá a la revocación del certificado y esa clave no podrá ser usada en el proceso de emisión de certificados.

5.7. - Compromiso y recuperación ante desastres

Se describirán 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 Contingencia.

Se deberán desarrollar procedimientos referidos a los siguientes aspectos:

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 20 del Anexo al Decreto Nº 182/2019, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8. - Plan de Cese de Actividades

El Certificador describirá los requisitos y procedimientos a ser adoptados en caso de finalización de sus servicios como certificador o de una o varias de sus Autoridades Certificantes. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se indicará la implementación de procedimientos referidos a:

a) Notificación al Ente Licenciante, Suscriptores, Terceros Usuarios, otros Certificadores y otros usuarios vinculados.

b) Custodia de archivos y documentación e identificación de su custodio.

Se deberá contemplar que se podrá aplicar la sanción de caducidad de la licencia, ante los casos previstos en el artículo 44 de la Ley Nº 25.506. Asimismo, se deberán cumplir los procedimientos dispuestos por el artículo 20 del Anexo al Decreto Nº 182/2019, 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 describirán las medidas de seguridad implementadas por el Certificador para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además, se incluirán los controles técnicos que se implementen sobre las funciones operativas del Certificador, Autoridades de Registro y suscriptores.

6.1. - Generación e instalación del par de claves criptográficas

La generación e instalación del par de claves serán consideradas desde la perspectiva de las Autoridades Certificantes del Certificador, 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 y distribución de la clave pública en forma segura.

d) Características y tamaños de las claves.

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

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

6.1.1. - Generación del par de claves criptográficas

Se describirán los aspectos relativos a la generación del par de claves de las Autoridades Certificantes del Certificador, de las claves de los Oficiales de Registro 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.

Se deberá respetar lo establecido en el Anexo II Sección 2 respecto de generación del par de claves.

6.1.2. - Entrega de la clave privada

Se indicará que el Certificador cumple con la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia a los datos de creación de firma de los suscriptores (incluyendo los roles vinculados a las actividades de registro), de conformidad a lo establecido por artículo 21, inciso b) de la Ley Nº 25.506 y el artículo 21, inciso 3 del Anexo al Decreto Nº 182/2019.

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

Se indicarán 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 a disposición de todos los suscriptores y terceras partes, el certificado del Certificador y el resto de los certificados que compongan su cadena de confianza.

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.

Se deberá respetar lo establecido en el Anexo II 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)

Se indicará que las claves criptográficas de los suscriptores de los certificados pueden ser utilizadas para firmar digitalmente, para funciones de autenticación y/o para cifrado.

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

La protección de la clave privada será considerada desde la perspectiva del Certificador y sus 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.

Se deberá respetar lo establecido en el Anexo II Sección 2 respecto de los estándares para dispositivos criptográficos.

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

Se indicará que 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 deben ser desarrollados con mayor detalle en el Plan de Seguridad.

6.2.3. - Recuperación de clave privada

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

6.2.4. - Copia de seguridad de clave privada

Se describirán los procedimientos y controles de seguridad empleados para la realización de copias de seguridad de las claves privadas del Certificador, garantizando que los niveles de seguridad de dichas claves no disminuyen 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. Se garantizará que su seguridad no disminuya por el proceso de archivo.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos

Si fuera aplicable, se describirán 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 describirán las condiciones bajo las cuales se almacenan las claves privadas en dispositivos criptográficos.

6.2.8. - Método de activación de claves privadas

Se indicarán los procedimientos necesarios para la activación de la clave privada del Certificador, utilizando métodos adecuados para la autenticación de la identidad de los responsables involucrados. Su descripción detallada se indicará en los documentos específicos.

6.2.9. - Método de desactivación de claves privadas

Se indicarán los procedimientos necesarios para la desactivación de la clave privada del Certificador, utilizando métodos adecuados para la autenticación de la identidad de los responsables involucrados. Su descripción detallada se indicará en los documentos específicos.

6.2.10. - Método de destrucción de claves privadas

Se especificarán las políticas a seguir para la destrucción segura de la clave privada del certificador 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 deberán ser desarrollados con mayor detalle en los documentos específicos.

6.2.11. – Requisitos de los dispositivos criptográficos

Se indicarán las especificaciones de los dispositivos criptográficos, debiendo respetarse lo establecido en el Anexo II 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 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.

6.3.2. - Período de uso de clave pública y privada

Se indicará que 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. Asimismo, se indicará que 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.

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 indicará que 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 indicará la 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

Se indicarán 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 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. 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.

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

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

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

6.6.1. - Controles de desarrollo de sistemas

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

6.7. - Controles de seguridad de red

Se describirán 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.

Los análisis deberán realizarse como mínimo cada SEIS (6) MESES.

6.8. – Servicios de emisión de Sellos de Tiempo

En caso de corresponder, se indicarán las especificaciones de los servicios de emisión de sellos de tiempo prestados por el Certificador, según lo establecido en el RFC 3161 "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*".

6.9. – Servicio de emisión de Sello de Competencia y/o Atributo

En caso de corresponder, se indicarán las especificaciones de los servicios de emisión de sellos de competencia y/o atributo prestados por el Certificador, según

lo establecido en el RFC 5755 "*An Internet Attribute Certificate Profile for Authorization*".

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

Se deberán especificar 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 el Ente Licenciante, y deben cumplir con las indicaciones establecidas en el apartado 2 del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados.

7.1.1. - Número de versión

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.1.2. - Extensiones

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.1.3. - Identificadores de algoritmos

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.1.4. - Formatos de nombre

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.1.5. - Restricciones de nombre

A completar sobre la base de lo establecido en el aparatado 2 del Anexo IV.

7.1.6. - OID de la Política Única de Certificación

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.1.7. - Sintaxis y semántica de calificadores de Política

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.1.8. - Semántica de procesamiento para extensiones críticas

A completar sobre la base de lo establecido en el apartado 2 del Anexo IV.

7.2. - Perfil de la Lista de Certificados Revocados

Se indicará que las Listas de Certificados Revocados serán emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 o la que, en su defecto, determine el Ente Licenciante, y cumplirán con las indicaciones establecidas el apartado **"**3 - Perfil de CRLs" del Anexo IV – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

7.2.1. - Número de versión

A completar sobre la base de lo establecido en el apartado 3 del Anexo IV.

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

A completar sobre la base de lo establecido en el apartado 3 del Anexo IV.

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

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (*On-Line Certificate Status Protocol*). Deberá ser implementada conforme a lo indicado en la especificación RFC 6960 "*X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol – OCSP*" y cumplir con las indicaciones establecidas en el apartado "4 - Perfil de la consulta en línea del estado del certificado" del Anexo IV – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

7.3.1. – Consultas OCSP

A completar sobre la base de lo establecido en el apartado 4 del Anexo IV.

7.3.2. - Respuestas OCSP

A completar sobre la base de lo establecido en el apartado 4 del Anexo IV.

ANEXO III

8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

En este componente se indicarán los aspectos específicos del proceso de auditoría.

Se indicará el cumplimiento de las exigencias impuestas por:

a) El artículo 33 de la Ley Nº 25.506 y su modificatoria, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma ley, relativo a la publicación de la información relevante de los informes de auditoría.

b) Los artículos 6° y 7° del Anexo al Decreto Nº 182/2019.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1. - Aranceles

Se describirán los aranceles asociados a cada uno de los servicios que preste el Certificador, relacionados con la Política Única de Certificación.

Los certificados emitidos por las entidades y jurisdicciones pertenecientes al Sector Público deberán ser provistos en forma gratuita.

9.2. - Responsabilidad Financiera

Se incluirán 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 indicarán 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

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

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no podrá ser divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente o por autoridad administrativa competente en el marco de un procedimiento administrativo. 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.

9.3.2. - Información no confidencial

Se indicará que la siguiente información no se considera confidencial:

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) Política Únicas de Certificación y Manual de Procedimientos.

d) Secciones públicas del Plan de Seguridad del Certificador.

e) Política de privacidad del Certificador.

f) Acuerdo con suscriptores.

g) Términos y condiciones con terceros usuarios.

9.3.3. – Responsabilidades de los roles involucrados

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

9.4. - Privacidad

Se 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

Se incluirán especificaciones acerca de los derechos de propiedad intelectual, donde se incluyan los derechos de autor y los derechos de patentes de invención relacionados con los documentos elaborados por el Certificador, así como denominación de herramientas y aplicaciones, de acuerdo con la legislación vigente.

9.6. – Responsabilidades y garantías

Sin perjuicio de lo determinado por el artículo 38 de la Ley N° 25.506 y su decreto reglamentario, se determinará la responsabilidad de los Certificadores Licenciados ante terceros. Asimismo, el Certificador deberá cumplir con la exigencia que la Autoridad de Aplicación establezca en cumplimiento con lo dispuesto en el artículo 23, inciso 16 del Anexo al Decreto N° 182/2019 en relación a las garantías y seguros de caución necesarias para prestar el servicio previsto.

9.7. – Deslinde de responsabilidad

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, se deberá detallar:

a) Las limitaciones de responsabilidad para el Certificador Licenciado, sus Autoridades de Registro y los suscriptores.
b) Los tipos de daño cubiertos.
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 detallarán las limitaciones de responsabilidad respecto a terceros y 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, se detallarán las previsiones relativas a las compensaciones por daños y perjuicios.

9.10 – Condiciones de vigencia

Se indicará el período de vigencia de la Política Única 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 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 establecerán las políticas para el mantenimiento y administración de la Política Única de Certificación.

9.12.1. - Procedimientos de cambio

Se establecerán las políticas utilizadas para efectuar modificaciones en la Política Única de Certificación. Toda modificación deberá ser aprobada previamente por el Ente Licenciante conforme a lo establecido por el artículo 21 inciso q) de la Ley Nº 25.506, el Decreto Nº 182/2019 y por la presente resolución.

Toda Política Única de Certificación será sometida a la aprobación del Ente Licenciante durante el proceso de licenciamiento.

9.12.2 – Mecanismo y plazo de publicación y notificación

Se describirán 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

Deberán indicarse las políticas de resolución de conflictos respecto a la aplicación de la Política Única de Certificación y a los acuerdos en los que el Certificador sea parte.

Se deberán detallar las políticas de reclamo aplicables cuando existan conflictos respecto a la interpretación de una o más disposiciones de la Política Única de Certificación, conforme a lo establecido en el artículo 17 del Anexo I 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 la Autoridad de Aplicación, 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

Se indicará que la legislación que respalda la interpretación, aplicación y validez de la Política Única de Certificación, es la Ley Nº 25.506 y su modificatoria, el Decreto Nº 182/2019 y su modificatorio, y su normativa complementaria.

9.15. – Conformidad con normas aplicables

Se especificará 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.

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Anexo

Número: IF-2021-61068088-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Jueves 8 de Julio de 2021

Referencia: ANEXO III: POLÍTICA ÚNICA DE CERTIFICACIÓN

El documento fue importado por el sistema GEDO con un total de 61 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.07.08 11:01:18 -03:00

Luis Mariano PAPAGNI
Subsecretario
Subsecretaría de Innovación Administrativa
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2021.07.08 11:01:19 -03:00