POLITICA DE CERTIFICACION

DE LA AUTORIDAD CERTIFICANTE RAIZ DE SAN LUIS

OID 2.16.32.1.3.2.1.1.0

INFRAESTRUCTURA DE FIRMA DIGITAL DE LA PROVINCIA DE SAN LUIS

Versiones y modificaciones de este documento

V	R	Fecha	Elaborado por	Revisado por	Descripción
1	0	2009/02/24	FDSL	Dirección	Resolución Rectoral N° 2240005-ULP-2009
1	1	2009/08/28	FDSL	Dirección	Resolución Rectoral N° 8280003-ULP-2009
2	0	2010/10/28	FDSL	Dirección	Resolución Rectoral N° 10280006-ULP-2010
3	0	2019/01/09	FDSL	Dirección	Resolución 03-ACTySSL-2019

Contenido

1- INTRODUCCION

1.1.- DESCRIPCIÓN GENERAL

La **Infraestructura de Firma Digital de la Provincia de San Luis** funciona en el ámbito del INSTITUTO FIRMA DIGITAL DE SAN LUIS dependiente de la AGENCIA DE CIENCIA TECNOLOGÍA Y SOCIEDAD SAN LUIS. A los efectos de fortalecer la seguridad de la cadena de confianza, característica en la operatoria de la tecnología de clave pública, San Luis ha optado por utilizar una jerarquía de tres niveles. Por tal motivo, el ENTE LICENCIANTE PROVINCIAL posee una AUTORIDAD CERTIFICANTE compuesta por una Autoridad Certificante Raiz**,** en adelante denominada, "ACR01 – SL", y una Autoridad Certificante Intermedia, en adelante denominada, "ACR02 – SL", ambas denominadas en conjunto **AUTORIDAD CERTIFICANTE RAIZ DE SAN LUIS** o **ACR-SL**. Éstas serán administradas por la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS y el INSTITUTO FIRMA DIGITAL DE SAN LUIS con la función de emitir certificados digitales a los Certificadores que obtengan licencias provinciales para sus Políticas de Certificación, una vez verificado el cumplimiento de los requisitos legales vigentes. Todo ello en cumplimiento a lo dispuesto en el Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018, reglamentario de la Ley Provincial Nº V-0591-2007 que adhiere a la Ley Nacional Nº 25.506 de Firma Digital, y la Ley N°II-0947-2016, modificada por Ley N° II-0975-2017 y el Decreto N° 8630-MCyT-2016.

La ACR01-SL, emite, renueva y revoca su propio certificado digital, firma la Lista de Certificados Revocados que ha emitido y emite, renueva y revoca el certificado de la ACR02-SL; mientras que la ACR02-SL, emite renueva y revoca el certificado de las Autoridades Certificante Subordinadas de los Certificadores Licenciados Provinciales y firma la Lista de Certificados Revocados que ha emitido. Esta Política de Certificación denominará a ambas en conjunto AUTORIDAD CERTIFICANTE RAIZ SAN LUIS, salvo cuando fuera necesario diferenciarlas específicamente.

La **POLITICA DE CERTIFICACION DE LA AUTORIDAD CERTIFICANTE DE SAN LUIS** tiene por objeto estalecer el empleo de la firma digital tanto en el ámbito público como en el privado en la **Provincia de San Luis**, por ello a través del Decreto Nº 8630-MCyT-2016 se designó a la **Agencia San Luis Ciencia, Tecnología y Sociedad** como Autoridad de Aplicación del régimen de firma digital, y se creó en su órbita, el **Instituto Firma Digital de San Luis**, con la finalidad de actuar como Ente Licenciante Provincial y Certificador Licenciado Provincial conforme el régimen previsto en la Ley Nº V-0591-2007. La Autoriad de Aplicación establece los manuales de procedimiento del Ente Licenciante, lo lineamientos de los Manuales de Procedimientos de los Certificadores Licenciados y las normas de auditoría.

Las relaciones entre el Ente Licenciante Provincial de la Provincia de San Luis con los Certificadores que soliciten licencias para sus Políticas de Certificación, se rigen por la Ley Provincial N° V-0591-2007, su Decreto Reglamentario N° 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018, la Resolución Nº 341-ACTySSL-2018 y demás normas complementarias.

La AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS dicta la presente Política de Certificación indicando la aplicabilidad de los certificados emitidos por el Ente Licenciante Provincial a través de sus Autoridades Certificantes, conforme lo dispuesto en el artículo 11 del Decreto N° 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018.

Esta Política de Certificación se complementa con los siguientes documentos:

a) Los procedimientos de licenciamiento,
b) El Manual de Procedimientos de Certificación,
c) La Política de Privacidad del Ente Licenciante Provincial y de sus Autoridades Certificantes,
d) El Plan de Cese de Actividades,
e) El Plan de Seguridad y Política de Seguridad,
f) El Plan de Contingencia,

1.2. - IDENTIFICACIÓN

Título del Documento: "Política de Certificación de la Autoridad Certificante Raíz de la Provincial de San Luis"

Versión del documento: 3.0

Fecha del documento: 09/01/2019

OID de la política de certificacion: 2.16.32.1.3.2.1.1.0

Sitio de Publicacion: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/cps.pdf

Lugar: Provincia de San Luis. República Argentina.

La AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD es la responsable de la asignación de OIDs para las Políticas de Certificación. Ello, toda vez que mediante Resolución Ministerial Nº 0038-MP-2009 del 14/08/09, conforme la facultad conferida por Nota O.N.T.I. Nº 104/09 de fecha 6/07/09, se asignó el OID 2.16.32.1.3.2.1.1 para la Infraestructura de Firma Digital de la Provincia de San Luis, disponiendo que la adjudicación y uso de niveles inferiores al OID asignado para la referida infraestructura es de exclusiva administración de la Autoridad de Aplicación de la Ley N° V-0591-2007.

1.3 - PARTICIPANTES Y APLICABILIDAD

Son las partes esenciales de la Infraestructura de Firma Digital de la Provincia de San Luis:

a) La Autoridad Certificante Raíz de San Luis (ACR01-SL y ACR02-SL),
b) El Ente Licenciante Provincial de la Provincia de San Luis (AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS y el INSTITUTO FIRMA DIGITAL DE SAN LUIS),
c) Los Certificadores Licenciados Provinciales (Suscriptores de Certificados).

1.3.1. – Certificador

Para esta Política de Certificación, la función de Certificador la cumple el Ente Licenciante Provincial de la Provincia de San Luis, es decir, la AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS y el INSTITUTO FIRMA DIGITAL DE SAN LUIS quienes administran la **ACR-SL**.

Cuando el INSTITUTO FIRMA DIGITAL DE SAN LUIS, en ejercicio de lo dispueso en el art. 24 del Decreto N° 0428-MP-2008 actúe como Certificador Licenciado Provincial, la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS asumirá exclusivamente el rol de administrador de la **ACR-SL**, conforme lo establece el artículo 18° la Resolución N° 17-ACTySSL-2018.

1.3.1.1. Ente Licenciante Provincial de la Provincia de San Luis

El Ente Licenciante Provincial de la Provincia de San Luis es el órgano administrativo encargado de otorgar las licencias a los Certificadores Licenciados Provinciales y de supervisar su actividad.

En tal carácter, administra la **ACR-SL**, emitiendo certificados digitales a las Autoridades Certificantes de los Certificadores Licenciados correspondientes a sus Políticas de Certificación aprobadas, es decir, a las Autoridades Certificantes Subordinadas.

a) Publica la presente Política de Certificación, el Acuerdo con Suscriptores de certificados de la **ACR-SL**, los Términos y Condiciones con Terceros Usuarios de certificados de la **ACR-SL**, su Política de Privacidad y Política de Seguridad;
b) Publica los certificados digitales de las Autoridades Certificantes de los Certificadores Licenciados Provinciales como así también los certificados digitales de la **ACR-SL**;
c) Publica el estado de los certificados emitidos y provistos por la **ACR-SL**, a través de la Lista de Certificados Revocados (o “CRL” Certificate Revocation List).

1.3.1.2.- Autoridad Certificante Raíz de San Luis

a) Emite, renueva y revoca su propio certificado digital;
b) Emite, renueva y revoca los certificados de las Autoridades Certificantes de los Certificadores Licenciados Provinciales;
c) Emite su Lista de Certificados Revocados (o “CRL” Certificate Revocation List).

1.3.2.- Autoridad de Registro

En el marco de la presente Política, la función de Autoridad de Registro será cumplida por el Ente Licenciante Provincial de la Provincia de San Luis, es decir, el INSTITUTO FIRMA DIGITAL DE SAN LUIS dependiente de la AGENCIA DE CIENICA, TECNOLOGIA Y SOCIEDAD SAN LUIS.

Tendrá sede en: **Data Center**, sito en Av. Universitaria s/n, Ciudad de la Punta (5710) – San Luis. República Argentina.

Correo: entelicenciante@sanluis.gov.ar

http://www.acraiz.sanluis.gov.ar

1.3.3.- Suscriptores de Certificados

Serán Suscriptores de los certificados emitidos por la **ACR-SL** el ente público, ente privado u organismo de derecho público no estatal que se constituya como Certificador Licenciado Provincial conforme lo dispuesto en la legislación vigente. En tal carácter, podrá emitir certificados de clave pública, entendiendo por tal, al que asocia una clave pública con el 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.

El Certificador Licenciado Provincial podrá proveer el servicio de sellado digital de fecha y hora.

1.3.4.- Aplicabilidad

Los certificados a emitirse por la **ACR-SL** tienen como único objetivo garantizar la identidad de las Autoridades Certificantes de entes u organismos que sean constituidos en Certificadores Licenciados Provinciales, de conformidad con la Resolución que al efecto dictará en cada caso la Autoridad de Aplicación de la Ley Nº V-0591-2007.

La **ACR-SL** utiliza su clave privada, mantenida en dispositivos criptográficos seguros, para firmar los certificados de las Autoridades Certificantes de los Certificadores Licenciados Provinciales, posibilitando que estos últimos emitan certificados digitales a sus suscriptores, en el marco de la Ley de Firma Digital de la Provincia Nº V-0591-2007.

1.4.- CONTACTOS

La presente Política de Certificación es administrada por el INSTITUTO FIRMA DIGITAL DE SAN LUIS dependiente de la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.

Para consultas y sugerencias acerca de este documento se puede obtener información personalmente o por correo en:

Agencia de Ciencia, Tecnología y Sociedad San Luis

INSTITUTO FIRMA DIGITAL DE SAN LUIS

Edificio de Descentralización Administrativa, “Terrazas del Portezuelo”

Autopista Serranías Puntanas KM 783 – Torre III - Piso 3°

Ciudad de San Luis (5700) – San Luis. República Argentina

Teléfono: 0266 4452000 int. 6095/3574

entelicenciante@sanluis.gov.ar

www.acraiz.sanluis.gov.ar

2.- ASPECTOS GENERALES DE LA POLITICA DE CERTIFICACION

2.1. - OBLIGACIONES

2.1.1. – Obligaciones del Certificador

2.1.1.1. Obligaciones del Ente Licenciante Provincial de la Provincia de San Luis

Son obligaciones del Ente Licenciante:

a) Generar y administrar el par de claves criptográficas de la **ACR-SL**.

b) Otorgar las licencias habilitantes a los Certificadores Provinciales, y emitir los correspondientes certificados de Autoridades de Certificantes de certificadores licenciados.

c) Publicar en el Boletín Oficial:
   - las Resoluciones que ordenan el otorgamiento, denegación, renovación y/o revocación de licencia y la aprobación de la Política de Certificación del Certificador, y
   - El certificado digital de clave pública correspondiente a esta Política de Certificación emitido por la **ACR-SL**

d) Denegar las solicitudes de licencias a los Certificadores que no cumplan con los requisitos establecidos para su aprobación.

e) Revocar las licencias otorgadas a los Certificadores Licenciados Provinciales que dejen de cumplir con los requisitos establecidos para su ejercicio.
f) Verificar que los Certificadores Licenciados Provinciales utilicen sistemas técnicamente confiables, entendiéndose por tales a los que cumplan con los estándares tecnológicos que al efecto dicte la Autoridad de Aplicación de la Provincia de San Luis.
g) Considerar para su aprobación, Politica de Certificacion, Manual de Procedimientos, los Planes de Seguridad y los de Cese de Actividades presentados por los Certificadores Provinciales.
h) Generar un Plan de Auditoría para los Certificadores Licenciados Provinciales.
i) Disponer de oficio la realización de auditorías.
j) Resolver los conflictos individuales que se susciten entre el suscriptor de un certificado y un Certificador Licenciado Provincial, emisor del mismo.
k) Renovar la licencia de las Políticas de Certificación de Certificadores Licenciados Provinciales.
l) Adoptar las medidas de seguridad y control, previstas en la presente Política de Certificación y en la Política de Seguridad, abarcando sus procesos, procedimientos y actividades.
m) Mantener los procesos, procedimientos y actividades de conformidad con la legislación vigente y con las normas, prácticas y reglas establecidas por el ente licenciante.
n) Mantener y garantizar la integridad, confidencialidad y disponibilidad de la información tratada por el Ente Licenciante.
o) Mantener y probar regularmente el plan de contingencias.
p) Mantener a disposición permanente del público su Política de Certificación y cumplir fielmente con sus especificaciones.

El Ente Licenciante Provincial cumplirá para con los Certificadores Licenciados Provinciales, las obligaciones que el Art. 21 de la Ley Nº 25.506 asigna al Certificador Licenciado.

En su calidad de suscriptor de certificado y de Certificador Licenciado Provincial, el Ente Licenciante, tiene idénticas obligaciones que los Certificadores Licenciados Provinciales, y además debe:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la clave privada de cualquier suscriptor de los certificados que emita.
b) Mantener el control de su propia clave privada e impedir su divulgación.
c) Revocar su propio certificado de clave pública frente al compromiso de su clave privada.
d) Permitir el acceso público permanente a los certificados de clave pública que ha emitido en favor de los Certificadores Licenciados Provinciales, a la Lista de Certificados Revocados y a la información sobre direcciones y números telefónicos de los Certificadores Licenciados Provinciales, por medio de conexiones de telecomunicaciones públicamente accesibles.
e) Permitir el ingreso de los auditores, debidamente acreditados, a su local operativo. Poner a disposición de aquellos toda la información necesaria y proveer la asistencia del caso.
f) Publicar su propio certificado de clave pública en el Boletín Oficial Provincial y Nacional.
g) Revocar los certificados emitidos en favor de los Certificadores Licenciados Provinciales incursos en causales de revocación de licencia, o que han cesado sus actividades.

h) Revocar los certificados emitidos en favor de los Certificadores Licenciados Provinciales, cuando las claves públicas que en ellos figuran dejan de ser técnicamente confiables.

i) Supervisar la ejecución del Plan de Cese de Actividades de los Certificadores Licenciados Provinciales que discontinúan sus funciones.

j) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

2.1.1.2. Obligaciones de la ACR-SL

Son obligaicones de la **ACR-SL**:

a) La emisión, revocación y renovación de su propio certificado.

b) La emisión, revocación y renovación de los certificados de Autoridades Certificantes de Certificadores Licenciados Provinciales.

c) La emisión de su Lista de Certificados Revocados (CRL).

2.1.2.- Obligaciones de la Autoridad de Registro

Las obligaciones de Autoridad de Registro son asumidas por el Ente Licenciante Provincial de la Provincia de San Luis.

2.1.3. - Obligaciones de los Suscriptores de los certificados

En el marco de la presente Política de Certificación serán Suscriptores los Certificadores Licenciados Provinciales, y en tal carácter asumen las siguientes obligaciones:

a) Proveer toda la información necesaria en forma completa y precisa para su identificación y autenticación contenida en su Solicitud de Licencia al iniciar el proceso de licenciamiento.

b) Al aceptar un certificado emitido por la **ACR-SL**, será responsable por toda la información por él provista y contenida en el mismo.

c) Utilizar los certificados de sus Autoridades Certificantes de acuerdo con las reglas establecidas en la presente Política de Certificación.

d) Operar conforme con su propio Manual de Procedimientos de Certificación y su Política de Certificación, implementados de acuerdo a lo establecido en la normativa vigente y aprobada por el Ente Licenciante Provincial de la Provincia de San Luis.

e) Abstenerse de generar, exigir, o por cualquier otro medio, tomar conocimiento o acceder, bajo ninguna circunstancia, a la clave privada del suscriptor.

f) Mantener el control de su clave privada e impedir su divulgación.

g) Solicitar inmediatamente la revocación de su certificado, cuando tuviera sospechas fundadas de que su clave privada ha sido comprometida.

h) Solicitar al Ente Licenciante Provincial la revocación de su certificado cuando la clave pública, en él contenida, deje de ser técnicamente confiable.

i) Informar inmediatamente al Ente Licenciante Provincial sobre cualquier cambio en los datos contenidos en su certificado o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo;

j) Operar utilizando un sistema técnicamente confiable.

k) Notificar al solicitante de un certificado sobre las medidas necesarias que deberá obligatoriamente adoptar, para crear firmas digitales seguras y para su verificación confiable

y de las obligaciones que aquel asume, por el sólo hecho de ser suscriptor de un certificado de clave pública.

l) Recabar únicamente aquellos datos personales del suscriptor del certificado, que sean necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el certificado, será de trato confidencial por parte del Certificador Licenciado Provincial.

m) Poner a disposición del suscriptor de un certificado emitido por éste Certificador Licenciado Provincial, toda la información relativa a la tramitación del certificado.

n) Mantener la documentación de respaldo de los certificados emitidos durante diez (10) años, contados a partir de su fecha de vencimiento o revocación.

o) Mantener un sitio de publicación con toda la información relativa a su condición de Certificador Licenciado Provincial, de modo que pueda ser accedida libremente por el público.

p) Publicar en su sitio de publicación los certificados de clave pública asociados a sus Autoridades Certificantes emitidos por la **ACR-SL**.

q) Permitir el acceso público permanente a los certificados que ha emitido y a la Lista de Certificados Revocados, por medio de conexiones de telecomunicaciones públicamente accesibles.

r) Publicar su dirección y sus números telefónicos.

s) Permitir el ingreso de los auditores acreditados a su local operativo, poner a su disposición toda la informuzación necesaria, y proveer la asistencia del caso.

t) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

u) En caso de Cese de Actividades los certificados emitidos por un Certificador Licenciado se revocarán a partir del día y la hora en que cesa su actividad, a menos que sean transferidos a otro Certificador Licenciado. El Certificador Licenciado notificará la fecha y hora de cese de sus actividades, mediante la publicación durante un (1) día, sesenta (60) días hábiles antes de la suspensión efectiva o cese de las operaciones en el Boletín Oficial y Judicial de la Provincia de San Luis y en el Boletín Oficial de la Nación. La notificación, también, deberá hacerse individualmente al Ente Licenciante.

   Cuando se hayan emitido certificados a entes, entidades o personas ajenas al Sector Público Provincial, el Certificador Licenciado publicará en un diario de difusión provincial durante un (1) día, el cese de sus actividades.

   Si el alcance de la Política de Certificación permitiera la emisión de certificados a personas de otras jurisdicciones, el Certificador Licenciado publicará el cese de sus actividades en un diario de difusión nacional durante un (1) día.

   El Certificador Licenciado podrá disponer de medios adicionales de comunicación del cese de sus actividades para notificar a los suscriptores de certificados que son ajenos al Sector Público Provincial. Si los certificados son transferidos a otro Certificador Licenciado, toda la documentación pertinente también deberá ser transferida a aquel

v) Revocar los certificados de clave pública por él emitidos ante las siguientes circunstancias: por solicitud de su suscriptor; por solicitud de un tercero que ostente un derecho subjetivo o interés legítimo; si llegara a determinar que un certificado fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación; si llegara a determinar que las claves públicas contenidas en los certificados dejan de ser técnicamente confiables; si cesa en sus actividades y no transfiere los certificados emitidos por él a otro Certificador Licenciado Provincial.

2.1.4.- Obligaciones de los Terceros Usuarios:

Son obligaciones de los Terceros Usuarios de certificados de clave pública:

a) Conocer los alcances de la presente Política de Certificación.
b) Conocer los Términos y Condiciones con los terceros usuarios de la **ACR-SL** que se publican en el sitio de publicación del Ente Licenciante.
c) Conocer las obligaciones de terceros usuarios establecidas en la Política de Certificación de los Certificadores Licenciados Provinciales.
d) Rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda.
e) Verificar la validez de los certificados asociados a las Autoridades Certificantes del Certificador Licenciado Provincial consultando la CRL emitida por la **ACR-SL** y publicada por el Ente Licenciante.
f) Vertificar la validez del certificado de la **ACR-SL**.

El certificado de la **ACR-SL** es considerado válido cuando:

a) Se encuentra dentro de su período de vigencia
b) No ha sido revocado, y
c) Puede ser verificado con el uso del mismo certificado de la **ACR-SL**.

2.1.5.- Obligaciones del Servicio de Repositorio

Para esta Política de Certificación, el Ente Licenciante Provincial tiene la obligación de publicar en los sitios desarrollados a tal fin, la siguiente información:

a) Esta Política de Certificación (última versión y anteriores, de existir).
b) El Acuerdo con Suscriptores de certificados de la **ACR-SL**.
c) Los Términos y Condiciones con Terceros Usuarios de certificados de la **ACR-SL**.
d) La Política de Privacidad de la **ACR-SL**.
e) La Política de Seguridad de la **ACR-SL**.
f) Los certificados emitidos por la **ACR-SL**.
g) La Lista de Certificados Revocados por la **ACR-SL**.
h) Información relevante de los informes de auditoría a que fue objeto el Ente Licenciante Provincial y la **ACR-SL**.
i) Información relevante de los informes de las auditorías realizadas por el Ente Licenciante Provincial a los Certificadores Licenciados Provinciales.
j) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de los contactos del Ente Licenciante.

k) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos de los Certificadores Licenciados Provinciales.

l) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos de los Certificadores Licenciados Provinciales cuyas licencias han sido revocadas.

m) La lista de OIDs de Políticas de Certificación para las Autoridades Certificantes de los Certificadores Licenciados Provinciales.

2.2.- RESPONSABILIDADES

El Ente Licenciante Provincial será responsable, en caso de corresponder, ante terceros por el incumplimiento de las previsiones de la Ley Provincial Nº V-0591-2007, Decreto Reglamentario Nº 0428-MP-2008, y demás normativa aplicable, respecto a los procedimientos que respaldan la emisión de certificados por la **ACR-SL**, por los errores u omisiones en los certificados emitidos por ella y por su falta de revocación en la forma y plazos previstos.

El Ente Licenciante Provincial no sume responsabilidad alguna, en caso de utilización no autorizada de un certificado, cuya descripción se encuentra establecida en esta Política de Certificación, como tampoco responde por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y procedimientos de la **ACR-SL** deba ser objeto de verificación.

2.3.- RESPONSABILIDAD FINANCIERA

2.3.1. - Responsabilidad Financiera del Ente Licenciante Provincial

La responsabilidad del Ente Licenciante Provincial por los incumplimientos previstos en el apartado anterior no compromete, en ningún caso, la responsabilidad pecuniaria del Estado Provincial.

2.4.- INTERPRETACIÓN Y APLICACIÓN DE LAS NORMAS

2.4.1.- Legislación Aplicable

La interpretación, obligatoriedad, diseño y validez de esta Política de Certificación se encuentran sometidos a lo establecido por la Ley Provincial Nº V-0591-2007 y demás normas complementarias aplicables.

2.4.2.- Forma de Interpretación y Aplicación

En el caso de que una o más disposiciones de esta Política de Certificación resulten consideradas nulas por cualquier razón, tal nulidad no afectará a la validez de las restantes disposiciones.

Las disposiciones que surgen de la presente Política de Certificación son de cumplimiento obligatorio para los participantes detallados en el **apartado 1.3** del presente documento.

2.4.3.- Procedimientos de Resolución de Conflictos

La resolución de cualquier controversia y/o conflicto resultante de la aplicación de lo dispuesto en esta Política y/o en cualquiera de sus documentos asociados, será resuelta en sede administrativa de acuerdo a lo dispuesto a continuación:

Previo agotamiento del procedimiento administrativo ante el Ente Licenciante, la controversia o conflicto será resuelto por la Autoridad de Aplicación conforme el régimen recursivo de la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.

Pueden recurrir a este procedimiento tanto los Suscriptores como los Terceros Usuarios de certificados de clave pública.
La Autoridad de Aplicación de la Provincia de San Luis evaluará el accionar de todos los partícipes de la Infraestructura de Firma Digital y recibirá las denuncias que contra cualquiera de ellos se presentase.

En su carácter de Órgano de Control aplicará sanciones de apercibimiento, suspensión, multa, clausura o cancelación para funcionar como tal, a los Certificadores Licenciados Provinciales o a las Autoridades de Registro.

Las multas aplicables por la Autoridad de Aplicación van de un mínimo de una (1) Unidad de Multa y hasta un máximo de un mil (1000) Unidades de Multa. La Unidad de Multa, será un importe equivalente a un (1) salario mínimo vital y móvil vigente a la fecha de comisión del hecho.

La cuantía de las sanciones se graduará atendiendo a:

a) la naturaleza de los derechos afectados,
b) los beneficios obtenidos,
c) el grado de intencionalidad,
d) la reincidencia,
e) los daños y perjuicios causados a las personas interesadas y a terceros,
f) y cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

Se considerará reincidente a quien habiendo sido sancionado por una infracción incurriera en otra de similar naturaleza dentro del término de tres (3) años, a contar desde la aplicación de la sanción.

El procedimiento se ajustará a las siguientes disposiciones:

a) La Autoridad de Aplicación de la Provincia de San Luis iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Provincial de Firma Digital, a su Decreto Reglamentario y/o a las demás normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, o asociaciones de consumidores o usuarios.
b) Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida. En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de cinco (5) días hábiles, presente su descargo por escrito o por vía telemática con firma digital. En su primera presentación, el presunto infractor deberá constituir domicilio y acreditar personería.
c) La constancia del acta labrada conforme a lo previsto en este artículo, así como las comprobaciones técnicas que se dispusieran, constituirán prueba suficiente de los hechos así comprobados, salvo en los casos en que resultaren desvirtuados por otras pruebas.
d) Las pruebas se admitirán solamente en caso de existir hechos controvertidos y siempre que no resulten manifiestamente inconducentes. Contra la resolución que deniegue medidas de prueba sólo se concederá recurso de reconsideración. La prueba deberá producirse dentro del término de diez (10) días hábiles, prorrogables cuando haya causas justificadas,

teniéndose por desistidas aquellas no producidas dentro de dicho plazo por causa imputable al infractor.

e) Concluidas las diligencias sumariales, se dictará la resolución definitiva dentro del término de veinte (20) días hábiles.

2.5.- ARANCELES

A los fines del cumplimiento de lo establecido en la Ley Provincial Nº V-05912007, su Decreto Reglamentario, y en las Resoluciones complementarias específicas, la Autoridad de Aplicación de la Provincia de San Luis se encuentra facultada para fijar en la oportunidad que lo considere pertinente, el monto de los aranceles a abonarse por los diferentes servicios a prestar a fin de efectivizar la operatoria de la Firma Digital en el ámbito público y privado.

Asimismo, el Ente Licenciante Provincial podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos.

2.6.- PUBLICACIÓN Y REPOSITORIOS DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRLs)

2.6.1.- Publicación de Información del Certificador

El Ente Licenciante Provincial opera dos repositorios para uso exclusivo de la publicación de la Lista de Certificados Revocados (CRL) y un sitio web para la publicación de la información del Ente Licenciante Provincial de la Provincia de San Luis.

La publicación de la Lista de Certificados Revocados (CRL), está disponible en:

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

y alternativamente en:

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

El sitio de publicación del Ente Licenciante Provincial se encuentra disponible en http:// www.acraiz.sanluis.gov.ar donde se puede consultar la siguiente información:

a) El certificado vigente de la **ACR01-SL**, el certificado vigente de la **ACR02-SL** y los certificados de las Autoridades Certificantes de los Certificadores Licenciados Provinciales.

b) Los datos de los contactos del Ente Licenciante Provincial como de los Certificadores Licenciados Provinciales.

c) El Registro de Certificadores Licenciados Provinciales conteniendo el número de la Resolución que concede, renueva o revoca las licencias de Políticas de Certificación que fueron aprobadas (con el correspondiente OID asignado a la Política de Certificación), así como el número de la Resolución que rechaza la aprobación de las Políticas de Certificación durante el proceso de licenciamiento.

d) Esta Política de Certificación, el Acuerdo con Suscriptores de Certificados de la **ACR-SL**, los Términos y Condiciones con Terceros Usuarios de certificados de la **ACR-SL**, la Política de Privacidad, la Política de Seguridad y toda otra documentación técnica de carácter público que se emita, en sus versiones actuales y anteriores.

e) La Lista de Certificados Revocados.

2.6.2.- Frecuencia de Publicación

La información alojada en los sitios de publicación será actualizada inmediatamente después de que la información a incluir en ellos haya sido verificada y autorizada por el Ente Licenciante Provincial Provincial.

La información respecto a emisiones y revocaciones de certificados será incluida tan pronto como se hayan cumplido los procedimientos de validación de identidad de los solicitantes establecidos en esta Política de Certificación para cada caso en particular.
La Lista de Certificados Revocados (CRL) será actualizada y la nueva versión será publicada cuando se produzca la revocación de un certificado o bien a los seis (6) meses de la última emisión de la Lista de Certificados Revocados, si ninguna de las dos condiciones anteriores ocurre antes.

2.6.3.- Controles de Acceso a la Información

El Ente Licenciante Provincial de la Provincia de San LuisEnte Licenciante Provincial brinda acceso irrestricto a sus sitios de publicación para consultar, a través de Internet, documentación de carácter público, incluyendo la clave pública del certificado de la **ACR-SL**, la Lista de Certificados Revocados y esta Política de Certificación. El Ente Licenciante Provincial establecerá controles para restringir la posibilidad de escritura y modificación.

2.6.4.- Repositorios de Certificados y Listas de Revocación

El sitio de publicación se encontrará disponibles para uso público durante las veinticuatro (24) horas diarias, siete (7) días a la semana, sujeto a un calendario de mantenimiento.

2.7.- AUDITORÍAS

El Ente Licenciante Provincial se encuentra sujeto a auditorias de la Autoridad de Aplicación de la Provincial de San Luis conforme lo dispuesto en el Capítulo V del Decreto Provincial Nº 0428-MP-2008 y las resoluciones específicas que se dictaren al respecto. La información relevante de los informes de las auditorias, es publicada en el sitio de publicación del Ente Licenciante.

2.8.- CONFIDENCIALIDAD

2.8.1.- Información Confidencial

Toda información referida a los Certificadores Licenciados Provinciales, que haya sido recibida por el Ente Licenciante Provincial durante el proceso de licenciamiento o renovación, es considerada confidencial y no puede hacerse pública sin el consentimiento previo de aquellos, salvo que sea requerida judicialmente por juez competente o por autoridad administrativa. La exigencia se extiende a toda otra información, referida a los Certificadores Licenciados Provinciales, a la que el Ente Licenciante Provincial tenga acceso durante el ciclo de vida de los certificados emitidos.

Lo indicado no es aplicable cuando se trate de información que se transcriba al certificado o sea obtenida de fuentes públicas.

La **ACR-SL** no generarán ni accederán a las claves privadas de las Autoridades Certificantes de los Certificadores Licenciados Provinciales. La generación y administración del par de claves criptográficas queda bajo exclusiva responsabilidad de los Certificadores Licenciados Provinciales.

En los casos relativos a información personal, resulta de aplicación lo dispuesto en la Ley Nº 25.326 de Protección de Datos Personales.

2.8.2.- Información No Confidencial

No se considerada confidencial lo siguiente:

a) La información incluida en los certificados y en las Listas de Certificados Revocados;
b) La información sobre personas humanas o jurídicas, que se encuentre disponible en certificados o en directorios y sitios de publicación de acceso público.

Tampoco se considera confidencial la información incluida en los siguientes documentos emitidos por el Ente Licenciante:

a) Esta Política de Certificación,
b) El Acuerdo con Suscrirptores de certificados de la **ACR-SL**,
c) Los Términos y Condiciones con Terceros Usuarios de certificados de la **ACR-SL**,
d) La Política de Privacidad de la **ACR-SL**,
e) La Política de Seguridad de la **ACR-SL**.

2.8.3.- Publicación de Información sobre la Revocación o Suspensión de un Certificado

La información referida a la Revocación de un Certificado no se considera confidencial y se la publica en el sitio de publicación:

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl
http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl
y alternativamente en:
http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

El estado de suspensión de un certificado no es aplicable en el marco de la Ley N° V-0591.2007, de adhesión a la Ley N° 25.506.

2.8.4.- Divulgación de Información a Autoridades Judiciales

La información confidencial podrá ser revelada ante un requerimiento judicial emanado de juez competente en el marco de un proceso judicial.

2.8.5.- Divulgación de Información como parte de un Proceso Judicial o Administrativo

La información confidencial en poder del Ente Licenciante Provincial podrá ser revelada ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

2.8.6.- Divulgación de Información por Solicitud del Suscriptor

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del Certificador Licenciado Provincial o de cualquier otra información generada o recibida durante el ciclo de vida del certificado, solo podrá efectuarse previa autorización de ese Certificador. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público irrestricto.

2.8.7.- Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales el Ente Licenciante Provincial pueda divulgar la información.

2.9.- DERECHOS DE PROPIEDAD INTELECTUAL

La AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la documentación y aplicaciones pertenecientes al Ente Licenciante Provincial y a su **ACR-SL**. Asimismo, mantiene, en forma exclusiva, todos los derechos de propiedad intelectual relacionados con sus nombres y claves criptográficas.

Ninguna parte de este documento se puede reproducir o distribuir sin que la previa notificación de derechos de propiedad intelectual aparezca en forma precisa, completa y sin modificaciones, atribuyendo su autoría a la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.

3.- IDENTIFICACION Y AUTENTICACION

3.1.- Registro Inicial

De acuerdo a la normativa vigente, en el proceso de registración de un Certificador Licenciado Provincial interviene el Ente Licenciante, otorgando o denegando licencias a las Políticas de Certificación presentadas y asociadas a sus Autoridades Certificantes.

A través de la Resolución N° 341-ACTySSL-2018 y sus Anexos, la AGENCIA DE CIENICA TECNOLOGÍA Y SOCIEDAD SAN LUIS publica, en su sitio www.acraiz.sanluis.gov.ar, y pone a disposición las condiciones necesarias para la obtención de las licencias de las Políticas de Certificación. a quienes pretendan constituirse en Certificadores Licenciados Provinciales.

La presentación de solicitud de licencia para una Política de Certificación por parte del Certificador, inicia el proceso de licenciamiento que culmina con la aprobación o rechazo de la Política, y el otorgamiento o denegación de la licencia por parte del Ente Licenciante, además de la publicación en el Boletín Oficial de la Resolución que la otorga o deniega.

Con el otorgamiento de la licencia, el Ente Licenciante Provincial a través de la **ACR-SL**, emite un certificado digital para la Autoridad Certificante vinculada a la Política de Certificación licenciada.

En el acto de emisión del certificado por la **ACR-SL**, el Certificador Licenciado Provincial debe confirmar que la información contenida en el certificado sea correcta. Además, en ese acto, el Certificador Licenciado Provincial firma el Acuerdo con Suscriptores de certificados de la **ACR-SL** provisto por el Ente Licenciante.

3.1.1.- Tipos de Nombres

Las Autoridades Certificantes vinculadas a las Políticas de Certificación licenciadas son subordinadas de la **ACR-SL** y tendrán un nombre definido por el Certificador Licenciado Provincial de acuerdo a la normativa vigente, que será controlado por el Ente Licenciante Provincial para permitir su identificación unívoca en el ámbito de la Infraestructura de Firma Digital de la Provincia de San Luis.

Cada Certificado tiene un nombre distintivo único (ver punto 3.1.4) en formato X.500 en el campo “Subject” del Certificado.

3.1.2.- Necesidad de Nombres Distintivos

Todos los nombres distintivos son semánticamente significativos dentro del ámbito de la Infraestructura de Firma Digital de la Provincia de San Luis. Son de fácil comprensión y asociación con el Certificador Licenciado Provincial y la Autoridad Certificante que representa.

3.1.3. – Reglas para la Interpretación de nombres

No aplica.

3.1.4 Unicidad de Nombres

Los nombres distintivos (Distinguished Name o DN) son únicos dentro del ámbito de la Infraestructura de Firma Digital de la Provincia de San Luis. El Ente Licenciante Provincial es el encargado de controlar la unicidad de los nombres distintivos.

Se podrán emitir varios certificados a favor de un mismo Certificador Licenciado Provincial utilizando el mismo DN, cuando así se estime conveniente, ya que la utilización de un mismo DN en varios certificados, no afecta la unicidad de dicho nombre dentro de la Infraestructura de Firma Digital de la Provincia de San Luis.

3.1.5.- Procedimiento de Resolución de Disputas sobre Nombres

El Ente Licenciante Provincial resolverá los conflictos que pudieran generarse respecto de la utilización de nombres distintivos que como suscriptores puedan adoptar los Certificadores Licenciados Provinciales.

En tales casos, corresponde al solicitante del certificado demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.1.6.- Reconocimiento, Autenticación y Rol de las Marcas Registradas

No se permite el uso de marcas comerciales, marcas de servicio o nombres de fantasía como Nombres Distintivos de las Autoridades Certificantes de Certificadores Licenciados Provinciales dependientes de la **ACR-SL**.

3.1.7.- Métodos para comprobar la posesión de la Clave Privada

Para formalizar la solicitud de certificado se utiliza el requerimiento de firma de certificado (CSR o “Certificate Signing Request”) en formato PKCS#10.

La **ACR-SL** verifica que la clave pública asociada al requerimiento de firma de certificado (CSR) de la Autoridad Certificante del Certificador Licenciado Provincial, se corresponda con la clave privada que el Certificador Licenciado Provincial utilizó para firmarlo.

3.1.8.- Autenticación de la Identidad del Certificador

Durante el proceso de licenciamiento el Ente Licenciante Provincial procede a identificar fehacientemente la identidad de la persona de existencia ideal, registros públicos de contratos u organismo público solicitante.

Para el caso de organismos públicos, se verifica la identidad de la máxima autoridad del organismo.

Para las personas de existencia ideal, se solicita la documentación constitutiva de la entidad y de acreditación del apoderado o representante legal y si se tratara de registros públicos de contratos, la documentación que acredite su condición.

Asimismo, deberán presentar adicionalmente la documentación indicada en la la Resolución Nº 341-ACTySSL-2018.

Toda la documentación relativa a este proceso mencionado es mantenida y resguardada por el Ente Licenciante.

3.1.9. - Autenticacion de la identidad de personas humanas

No aplica.

3.2.- GENERACIÓN DE UN NUEVO PAR DE CLAVES (RUTINA DE RE-KEY)

Se requiere el cumplimiento de los pasos descriptos en el punto **3.1 - Registro Inicial**.

3.3.- GENERACIÓN DE UN NUEVO PAR DE CLAVES DESPUÉS DE UNA REVOCACIÓN - SIN COMPROMISO DE CLAVE

Se requiere el cumplimiento de los pasos descriptos en el punto **3.1 - Registro Inicial**.

No se admite la utilización del mismo par de claves criptográficas para la renovación de un certificado.

3.4.- REQUERIMIENTO DE REVOCACIÓN

El procedimiento de revocación de un certificado correspondiente a una Autoridad Certificante de Certificador Licenciado Provincial se inicia con la recepción de la solicitud de revocación por el Ente Licenciante, y termina cuando una nueva Lista de Certificados Revocados (CRL) conteniendo el número de serie del certificado en cuestión, se publica en:

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

y alternativamente en:

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crtl

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

Las solicitudes de revocación deberán comunicarse por escrito mediante el formulario diseñado al efecto y disponible en el sitio del Ente Licenciante.

El Ente Licenciante Provincial realiza la identificación y validación de la identidad del solicitante de la revocación.

Una vez validada la información contenida en la solicitud de revocación, el Ente Licenciante Provincial procederá a la revocación del certificado en un plazo no mayor a las veinticuatro (24) horas de recibida y validada. Toda la documentación generada en este proceso es mantenida y resguardada por el Ente Licenciante.

4.- CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - SOLICITUD DE CERTIFICADO

Una vez otorgada la licencia de la Política de Certificación por parte del Ente Licenciante Provincial y publicada la Resolución de otorgamiento en el Boletín Oficial, el Certificador Licenciado Provincial está en condiciones de solicitar el certificado.

El Certificador Licenciado Provincial genera en sus instalaciones, el par de claves para la Autoridad Certificante para la Política de Certificación licenciada, en presencia de personal autorizado del Ente Licenciante Provincial a quien entrega en ese acto el Formulario de Solicitud de Emisión del

Certificado debidamente completado junto con el requerimiento de firma de Certificado (CSR) en formato PKCS#10.

El Certificador Licenciado Provincial debe seguir los siguientes pasos:

a) Generar el par de claves para la Autoridad Certificante vinculada a la Política de Certificación Licenciada, en presencia de personal del Ente Licenciante;
b) Generar el Requerimiento de Firma de Certificado (CSR), en presencia de personal del Ente Licenciante;
c) Demostrar que la Clave Pública presentada al Ente Licenciante Provincial se corresponda con la Clave Privada utilizada para la firma del Requerimiento de Firma de Certificado (CSR);
d) Presentar la solicitud de emisión de certificado al Ente Licenciante Provincial debidamente firmada por la máxima autoridad en caso de organismo público o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos. La mencionada nota debe contener el hash del CSR.

Una vez cumplidos los pasos mencionados, el personal del Ente Licenciante Provincial procederá a verificar la autenticidad del Requerimiento de Firma de Certificado (CSR).

4.2.- EMISIÓN DEL CERTIFICADO

Las Autoridades Certificantes de Certificadores Licenciados Provinciales integran la Infraestructura de Firma Digital de la Provincia de San Luis y dependen de la **ACR-SL**. Por lo tanto, la emisión de sus certificados se efectúa en instalaciones de la **ACR-SL** con la participación del Certificador Licenciado Provincial, representado por su máxima autoridad o quien él designe, en caso de organismo público, o por su apoderado o representante legal, para el caso de personas de existencia ideal o registros públicos de contratos. Por parte del Ente Licenciante, participará el personal debidamente autorizado a dicho efecto.

Los certificados emitidos por la **ACR-SL** a favor de una Autoridad Certificante de Certificador Licenciado Provincial tienen un período de validez treinta (30) años desde su fecha de emisión, siempre que dicho plazo no exceda el período de uso del certificado de la **ACR-SL**, o hasta su revocación (lo que ocurra primero).

Con la recepción de la Solicitud de Emisión de Certificado remitida por el Certificador Licenciado Provincial, la **ACR-SL** se encuentra en condiciones de generar el certificado digital para la Autoridad Certificante correspondiente.

4.3.- ACEPTACIÓN DEL CERTIFICADO

Un Certificado emitido por la **ACR-SL** se considera aceptado por el Certificador Licenciado Provincial después que su apoderado o representante legal, si se trata de una persona de existencia ideal o un registro público de contratos, o la máxima autoridad o quien él designe, si se trata de un organismo público, haya recibido formalmente el certificado digital generado en la ceremonia de emisión y luego haya firmado el Acuerdo con Suscriptores de certificados de la **ACR-SL**.

La **ACR-SL** entrega el certificado emitido al personal del Certificador Licenciado Provincial referido en el párrafo precedente, según corresponda.

Una vez recibido el certificado digital emitido por la **ACR-SL**, el Certificador Licenciado Provincial debe instalarlo en su Autoridad Certificante, encontrándose en condiciones de emitir certificados a sus suscriptores.

El Ente Licenciante Provincial publicará ese certificado digital en su sitio de publicación www.acraiz.sanluis.gov.ar

Por otra parte, se procederá a publicar en el Boletín Oficial de la Provincia y de la Nación, por el término de un (1) día el certificado de clave pública correspondiente a la Política de Certificación Licenciada.

4.4.- SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS

De acuerdo con lo dispuesto por la Ley Nº V-0591-2007, que adhiere a la Ley Nº 25.506, no existe el estado de suspensión de certificados.

La solicitud de revocación de un certificado de Autoridad Certificante de Certificador Licenciado Provincial debe ser presentada ante el Ente Licenciante.

4.4.1.- CAUSAS DE REVOCACIÓN

El Ente Licenciante Provincial revocará el certificado digital de la Autoridad Certificante de Certificador Licenciado Provincial que hubiera emitido la **ACR-SL** en los siguientes casos:

a) A solicitud del Certificador Licenciado Provincial cuando la clave privada o el medio en que se encuentre almacenada, se hallen comprometidos o corran peligro de estarlo;
b) Si se determina que el certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación;
c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros;
d) Por resolución judicial o del mismo Ente Licenciante Provincial debidamente fundada;
e) Por cancelación de la licencia de la Política de Certificación;
f) En caso de cese de actividades del Certificador Licenciado Provincial;
g) Por condiciones especiales definidas en las Políticas de Certificación;
h) Si se determina que la información contenida en el certificado ha dejado de ser válida.

4.4.2.- Autorizados a Solicitar la Revocación

Se encuentran autorizados a solicitar la revocación de un certificado emitido por la **ACR-SL**:

a) El Certificador Licenciado Provincial, titular del certificado en cuestión, a través de su máxima autoridad en caso de organismo público o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos;
b) Aquellas personas previa y debidamente autorizadas por el Certificador Licenciado Provincial para efectuar tal solicitud;
c) El Ente Licenciante;
d) La Autoridad de Aplicación del presente régimen;
e) La autoridad judicial competente.

4.4.3.- Procedimientos para la Solicitud de Revocación

El procedimiento de revocación de un certificado correspondiente a una Autoridad Certificante de Certificador Licenciado Provincial, se inicia con la recepción de la solicitud de revocación por ante el

Ente Licenciante Provincial y termina cuando una nueva Lista de Certificados Revocados (CRL) conteniendo el número de serie del certificado en cuestión se publica en:

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl

http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

y alternativamente en:

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl

La solicitud de revocación debe ser completada, firmada y entregada por el solicitante al Ente Licenciante. El Ente Licenciante Provincial verificará la autenticidad de los datos de la solicitud de revocación.

En los casos que la solicitud de revocación surgiera de una decisión judicial o del Ente Licenciante, se efectuará la notificación al Certificador Licenciado Provincial antes de comenzar el proceso de revocación.

La solicitud de revocación se archiva, junto con la documentación recabada en el proceso de licenciamiento de la Política de Certificación asociada al certificado que se revoca.

Un certificado revocado será válido, únicamente, para la verificación de firmas generadas durante el período en que el referido certificado era válido.

4.4.4.- Plazo para la Solicitud de Revocación

El plazo máximo entre la recepción de la solicitud de revocación y la actualización de la Lista de Certificados Revocados, indicando los motivos de la revocación, es de veinticuatro (24) horas.

4.4.5.- Frecuencia de Emisión de Listas de Certificados Revocados

La **ACR-SL** emite y pública la Lista de Certificados Revocados (CRL) cuando se revoca un certificado o a los seis (6) meses de la última emisión de CRL, si la condición anterior no ocurre antes.

4.4.6.- Requisitos para la Verificación de la Lista de Certificados Revocados

Los Certificadores Licenciados Provinciales y terceros usuarios están obligados a verificar la autenticidad y validez de la Lista de Certificados Revocados (CRL) mediante la verificación de la firma digital de la **ACR-SL** y de su período de validez.

Los Terceros Usuarios, además de ello, están obligados a verificar la utenticidad y validez de los certificados en la Lista de Certificados Revocados (CRL) mediante la verificación de la Firma Digital de las Autoridades Certificantes de los Certificadores Licenciados Provinciales.

La **ACR-SL** del Ente Licenciante Provincial garantizará el acceso permanente, eficiente y gratuito a su Lista de Certificados Revocados.

4.4.7. - Disponibilidad en línea del servicio de revocación y verificación del estado del certificado

No aplicable.

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

No aplicable.

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

No aplicable.

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

No aplicable.

4.4.11.- Requisitos Específicos para Casos de Compromiso de Claves

El Ente Licenciante Provincial en su carácter de responsable de la clave privada de la **ACR-SL**, se compromete a comunicar a los Certificadores Licenciados Provinciales en caso de compromiso de dichas claves.

4.4.12. – Causas de suspensión

De acuerdo con lo dispuesto por la Ley N° V-0591-2007, de achesión a la Ley Nº 25.506, no existe el estado de suspensión de certificados.

4.4.13. - Autorizados a solicitar la suspensión

No aplicable.

4.4.14. - Procedimientos para la solicitud de suspensión

No aplicable.

4.4.15. - Límites del periodo de suspensión de un certificado

No aplicable.

4.5.- PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

4.5.1.- Tipos de eventos registrados

Con el fin de mantener un ambiente seguro y controlado, se registrará la ocurrencia de los siguientes eventos, registrándose para cada uno, la información relativa al tipo de evento y el tiempo en que el evento ocurrió.

1.- Relacionados con el Ente Licenciante:

a) Cambios en la Política de Certificación,
b) Cambios en los Procedimientos de Certificación,
c) Cambios en el Acuerdo con Suscritpreso de certificados de la **ACR-SL**,
d) Cambios en los Términos y Condiciones con Terceros Usuarios de certificados de la **ACR-SL**,
e) Cambios en la Política de Seguridad,
f) Cambios en el Plan de Contingencia,
g) Pruebas del Plan de Contingencia,
h) Cambios en la Política de Privacidad,
i) Cambios en el personal vinculado al Ente Licenciante Provincial y a la **ACR-SL**,
j) Revisiones de auditoría,
k) Cambios en los Procedimientos de Licenciamiento,

2.- Relacionados con la **ACR-SL**:

a) Ceremonia de generación de claves,
b) Encendido y apagado de los equipos de las Autoridades Certificantes y de publicación,
c) Operaciones de mantenimiento, accesos a los sistemas, y cambios y actualizaciones de software y hardware,

d) Entrada en servicio y finalización de las aplicaciones de la **ACR-SL** y del servicio de publicación,
e) Operaciones de lectura y escritura de las aplicaciones de la **ACR-SL** y del servicio publicación,
f) Intentos satisfactorios y fallidos de crear, borrar, acceder, establecer y cambiar contraseñas, permisos y roles del personal afectado a los servicios de certificación,
g) Generación de copias de seguridad,
h) Ciclo de vida de los dispositivos criptográficos incluyendo recepción, instalación, puesta en servicio, uso y finalización del servicio,
i) Generación, almacenamiento, recuperación, activación, desactivación, archivo y destrucción de las claves de la **ACR-SL**,
j) Registro de acceso físico a los diferentes niveles de seguridad,
k) Registros producidos por los elementos de seguridad de las instalaciones (por ej. registro de alarmas, grabaciones de cámaras de vigilancia, etc.),
l) Registro de poseedores de credenciales de activación de los dispositivos criptográficos que contienen las claves privadas de la **ACR-SL**.

3.- Relacionados con el Ciclo de Vida de los Certificados y las Listas de Revocación de Certificados:

a) Solicitud de emisión de certificado por el Certificador Licenciado Provincial,
b) Aprobación o denegación de solicitud de emisión de certificado,
c) Emisión de certificado por la **ACR-SL**,
d) Aceptación del certificado por el Certificador Licenciado Provincial y firma del Acuerdo con Suscriptores de certificados de **ACR-SL**,
e) Asignación del dispositivo criptográfico al responsable poseedor de claves del Certificador Licenciado Provincial,
f) Publicación del certificado en el sitio del Ente Licenciante,
g) Recepción de solicitud de revocación de certificado,
h) Revocación del certificado,
i) Emisión de la Lista de Certificados Revocados,
j) Publicación de la Lista de Certificados Revocados,
k) Registro de destrucción de material conteniendo información de claves y datos de su activación,
l) Renovación de certificados.

4.5.2.- Frecuencia de Procesamiento del Registro de Eventos

Los registros de eventos de la **ACR-SL** son analizados periódicamente en relación a su criticidad.

Ese análisis es realizado por personal autorizado del Ente Licenciante.

4.5.3.- Período de Retención del Registro de Eventos

Los registros de eventos correspondientes al sistema de la **ACR-SL** se mantienen por un período de diez (10) años a partir de su generación. Los registros de eventos correspondientes al sistema de publicación del Ente Licenciante Provincial se conservan por un (1) año.

4.5.4.- Protección del Registro de Eventos

Toda la información pertinente al registro de eventos se mantiene de manera segura y accedida por personal estrictamente autorizado.

4.5.5.- Procedimientos de Respaldo del Registro de Eventos

Las copias de respaldo del registro de eventos se realizan acorde a un detallado cronograma que será confeccionado por el Ente Licenciante.

4.5.6.- Sistema de recolección de información acerca de eventos

La información recogida automáticamente es registrada por el sistema operativo y el software de aplicación. La información sobre eventos manuales es registrada por personal autorizado del Ente Licenciante.

4.5.7.- Notificación al Causante del Evento

Los sistemas de recolección de eventos no efectúan ninguna notificación al causante del evento sobre el hecho de que sus acciones han sido registradas.

4.5.8.- Análisis de Vulnerabilidad

Los eventos registrados son utilizados para analizar posibles vulnerabilidades sobre los sistemas y los procedimientos vigentes.

4.6.- ARCHIVO DE LA INFORMACIÓN

El Ente Licenciante Provincial mantendrá toda la información relativa a los certificados digitales emitidos por la **ACR-SL**, de acuerdo a lo establecido en el marco legal vigente.

4.6.1.- Tipo de Información Archivada

El Ente Licenciante Provincial almacenará toda la información asociada a los certificados a lo largo de su ciclo de vida incluyendo su renovación. Se registrará:

a) La información obtenida en las diferentes etapas del ciclo de vida del certificado (solicitud, revocación, renovación, etc.),
b) Los documentos asociados a dichas etapas, incluyendo el licenciamiento,
c) Las diferentes versiones de Políticas de Certificación, Manuales de Procedimientos y sus documentos asociados.

4.6.2.- Período de Retención

El Ente Licenciante Provincial almacenará la información asociada a los certificados digitales emitidos bajo la presente Política, por un período de diez (10) años contados a partir de la fecha de su vencimiento o revocación.

4.6.3.- Protección de los Archivos de Información

El Ente Licenciante Provincial garantiza:

a) La integridad y confidencialidad de la información referente a los certificados digitales emitidos,
b) El almacenamiento de la información en forma completa,
c) La privacidad de los datos obtenidos durante el procedimiento de licenciamiento.

4.6.4.- Procedimiento de Copia de Respaldo (Backup)

El Ente Licenciante Provincial efectuará copias de respaldo de la información en soporte electrónico, que serán almacenadas en instalaciones externas. Las copias de respaldo serán:

a) Efectuadas según procedimientos de backup detallada en el Plan de Contingencia.
b) Almacenadas en instalaciones que cumplen al menos con los mismos niveles de protección física y ambiental que las instalaciones principales donde se encuentran instalados los equipos asociados a los procesos de certificación,
c) Verificadas frecuentemente, según lo indica el Plan de Contigencia.

4.6.5.- Ubicación del Archivo de Información

El Ente Licenciante Provincial mantiene un esquema distribuido de archivos entre sus instalaciones principales y de respaldo.

4.6.6.- Procedimientos de Obtención y Verificación de la Información Archivada

Solo las personas autorizadas por el Ente Licenciante Provincial tienen acceso a la información archivada, ya sea en las instalaciones principales como en las de respaldo.

4.7.- RENOVACIÓN DE CERTIFICADOS Y CAMBIO DE CLAVES CRIPTOGRÁFICAS

La renovación de certificado de la Autoridad Certificante de Certificador Licenciado Provincial deberá seguir el procedimiento indicado en el **punto 3.1** de la presente Política.

La renovación implica, en todos los casos, la generación de un nuevo par de claves. Transcurrido el periodo de validez del par de claves asociado al certificado, deberán ser retiradas de servicio, de acuerdo a lo indicado en el **punto 6.3.2** de esta Política.

Únicamente se podrá renovar el certificado si se cumple alguna de las siguientes condiciones:

a) Para sustituir las claves que van a ser retiradas,
b) Para modificar la información contenida en el certificado,
c) Por modificaciones realizadas a la Política de Certificación licenciada que así lo ameriten.

El Ente Licenciante Provincial realizará una nueva ceremonia de emisión de certificado asociado a la Autoridad Certificante, de acuerdo a su Manual de Procedimientos.

El trámite de renovación de un certificado digital emitido a favor de un Certificador Licenciado Provincial, debe ser iniciado sesenta (60) días hábiles antes del comienzo del mayor período de validez de los certificados digitales que emite.

Para solicitar un nuevo certificado, se deberá seguir el procedimiento indicado en el **punto 4.1** de la presente Política.

La clave privada que es objeto de renovación debe ser utilizada para continuar firmando las Listas de Revocación de Certificados (CRLs) hasta la fecha de expiración del último certificado emitido por la Autoridad Certificante utilizando esa clave. En ese momento se debe:

a) Solicitar al Ente Licenciante Provincial la revocación de ese certificado, y
b) Destruir la clave privada de acuerdo a lo indicado en el punto 6.2.9 de la presente Política.

4.8.- PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE DESASTRES

Ante hechos que comprometan la continuidad de sus operaciones, el Ente Licenciante Provincial deberá implementar un Plan de Contingencia y Recuperación ante Desastres que garantice el

mantenimiento de sus servicios mínimos (recepción de solicitudes de revocación, revocación de certificados, emisión de CRL y consulta de Listas de Certificados Revocados actualizadas).

El plan deberá tener las siguientes características:

a) Ser conocido por todo el personal que cumple funciones en el Ente Licenciante,
b) Incluir pruebas completas de funcionamiento periódicamente.

4.8.1.- Compromiso de Recursos Informáticos, Aplicaciones y Datos

El Ente Licenciante Provincial utilizará los procedimientos definidos en su Plan de Contingencia, acorde con su Plan de Seguridad, para restaurar los recursos informáticos, aplicaciones o datos que hayan sido comprometidos.

4.8.2.- Continuidad de las Operaciones de la ACR-SL

El Ente Licenciante Provincial dispone de procedimientos para asegurar la continuidad de sus operaciones en instalaciones alternativas. El Ente Licenciante Provincial comunicará a los Certificadores Licenciados Provinciales si el evento afecta actividades previstas.

4.8.3.- Compromiso de la Clave Privada de la ACR-SL

Ante sospecha de compromiso de la clave privada de la **ACR-SL**, el Ente Licenciante Provincial dispone de procedimientos para la revocación de su certificado y el restablecimiento de su infraestructura, contemplándose las siguientes actividades:

a) Ceremonia de generación de un nuevo par de claves,
b) Publicación del nuevo certificado,
c) Emisión de nuevos certificados para los Certificadores Licenciados Provinciales.

El Ente Licenciante Provincial tomará las siguientes acciones:

a) Informar a los Certificadores Licenciados Provinciales que sus certificados serán revocados, y que las claves privadas asociadas a esos certificados no deben ser utilizadas,
b) Revocar los certificados digitales de las Autoridades Certificantes de los Certificadores Licenciados Provinciales,
c) Publicar en su sitio de publicación que se ha revocado el certificado de la **ACR-SL**, notificando a los terceros usuarios que no deben considerarlo como un certificado confiable.

4.9.- PLAN DE CESE DE ACTIVIDADES

El eventual cese de actividades de la **ACR-SL** queda reservado a una decisión de la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.

En caso de producirse el cese de actividades, el Ente Licenciante Provincial cumplirá con los siguientes procedimientos:

a) Publicará fecha y hora del cese de actividades en el Boletín Oficial y Judicial de la Provincial y en el Boletín Oficial Nacional NOVENTA (90) DÍAS hábiles antes de la fecha del efectivo cese.
b) Notificará a los Certificadores Licenciados Provinciales con una antelación no menor a los NOVENTA (90) días hábiles de la fecha prevista de cese.

c) Publicará en un medio de difusión provincial durante un día, 90 días hábiles antes de la suspensión efectiva o cese de las operaciones, si sus Certificadores Provinciales han emitido certificados digitales a personal ajeno al Sector Público Provincial.

d) Publicará en un medio de difusión nacional durante un día, 90 días hábiles antes de la suspensión efectiva o cese de las operaciones, si sus Certificadores Provinciales han emitido certificados digitales a personas de otras jurisdicciones.

e) Revocará la totalidad de los certificados que hubiere emitido y que se encontraren vigentes a la fecha de cese de sus actividades;

f) Una vez revocados los certificados de los Certificadores Licenciados Provinciales, publicará la CRL y conservará la clave privada de la **ACR-SL** al sólo efecto de firmar la última CRL.

5.- CONTROLES DE SEGURIDAD FISICA, FUNCIONALES Y PERSONALES

5.1.- CONTROLES DE SEGURIDAD FÍSICA

El Ente Licenciante Provincial ha implementado controles apropiados que restringen el acceso a los equipos, programas y datos utilizados por la **ACR-SL** para la provisión del servicio de certificación, limitándolo a personas debidamente autorizadas.

La **ACR-SL** opera en instalaciones construidas bajo estrictas normas de seguridad física y ambiental internacionales que les brindan una protección adecuada.

5.1.1.- Construcción y Ubicación de las Instalaciones

Para realizar las operaciones de la **ACR-SL**, el Ente Licenciante Provincial cuenta con instalaciones apropiadas que disponen de controles físicos para evitar, prevenir y detectar el acceso indebido a los equipos, programas y datos utilizados. Las instalaciones poseen perímetros de seguridad expresamente definidos.

5.1.2.- Niveles de Acceso Físico

Para ingresar al recinto que contiene los equipos de la **ACR-SL**, el personal autorizado debe atravesar varios niveles de seguridad. Los requisitos de autenticación se incrementan a medida que se accede a los niveles superiores.

5.1.3.- Energía Eléctrica y Aire Acondicionado

Los equipos de la **ACR-SL** están alojados en instalaciones que brindan condiciones adecuadas de suministro de energía eléctrica y de aire acondicionado, para permitir una operación segura.

5.1.4.- Exposición al agua e inundaciones

Dentro de las instalaciones, los equipos de la **ACR-SL** están alojados en compartimentos estancos a fin de prevenir el impacto producido por inundaciones o filtraciones de líquidos.

5.1.5.- Prevención y Protección contra Incendio

Los equipos de la **ACR-SL** están alojados en instalaciones que cuentan con alarmas de detección y sistemas de extinción de incendios.

5.1.6.- Medios de Almacenamiento de Información

El Ente Licenciante Provincial mantiene los respaldos de información de manera íntegra y confidencial, almacenándolos en recintos ignífugos y accesibles solo por personal autorizado.

El Ente Licenciante Provincial almacena copias completas de respaldo en instalaciones externas. Además, cuenta con procedimientos de recuperación escritos que son verificados periódicamente.

5.1.7.- Descarte de Medios de Almacenamiento de Información

El Ente Licenciante Provincial tiene implementado procedimientos para la destrucción de información sensitiva, a fin de imposibilitar su recuperación, acceso o divulgación luego de su eliminación.

5.1.8.- Instalaciones de Seguridad Externas

El Ente Licenciante Provincial dispone de instalaciones externas que tienen niveles de protección física y ambiental similares al de las instalaciones principales.

5.2.- CONTROLES FUNCIONALES

El Ente Licenciante Provincial ha establecido una estructura de personal estable con roles específicos definidos para realizar las actividades de licenciamiento y operación de la **ACR-SL** que contempla una adecuada separación de funciones.

5.2.1.- Definición de Roles Afectados al Proceso de Certificación

El personal del Ente Licenciante Provincial que tenga acceso a los equipos involucrados en los procesos de emisión o revocación de Certificados, incluyendo la emisión de la Lista de Certificados Revocados (CRL), es seleccionado y entrenado a los efectos de proporcionar un ambiente de operación seguro y confiable. Este personal deber ser evaluado al menos una vez cada 2 (dos) años para confirmar su continuidad en el puesto.

5.2.2.- Separación de Funciones

El Ente Licenciante Provincial mantiene un esquema de roles y funciones para establecer una adecuada segregación y control de las responsabilidades de su personal.

5.2.3.- Número de Personas Requerido por Función

Para evitar que una sola persona pueda llevar a cabo operaciones sensitivas, se requiere para las mismas la participación concurrente de varias personas con diferentes roles.

5.2.4.- Identificación y Autentificación para cada Rol

Para ejecutar las funciones pertinentes a su propio rol, todo el personal se debe autenticar de manera segura usando contraseñas y/o certificados digitales.

5.3.- Controles de Seguridad del Personal de La ACR-SL

El Ente Licenciante Provincial sigue la política de administración de personal establecida para la AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS.

5.3.1.- Antecedentes Laborales, Calificaciones, Experiencia e Idoneidad del Personal

El personal del Ente Licenciante Provincial posee experiencia y calificaciones adecuadas para las funciones que desempeñan. Dicho personal tiene pleno conocimiento de las Políticas de Seguridad y Certificación que permiten mantener un ambiente seguro y confiable.

El personal del Ente Licenciante Provincial ha sido cuidadosamente seleccionado y calificado antes de iniciar sus actividades.

5.3.2.- Entrenamiento y Capacitación Inicial

El personal del Ente Licenciante Provincial ha sido entrenado adecuadamente antes de iniciar sus actividades.

5.3.3.- Frecuencias del Proceso de Actualización Técnica

El personal del Ente Licenciante Provincial recibe capacitación constante respecto de los cambios tecnológicos y de procedimientos, que puedan afectar directa o indirectamente las operaciones de certificación.

5.3.4. - Frecuencia de rotación de cargos

No aplicable.

5.3.5.- Sanciones a aplicar por Actividades No Autorizadas

El personal del Ente Licenciante Provincial que incumpliere sus funciones y responsabilidades, será sancionado de acuerdo al régimen de sanciones establecido por la AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS.

5.3.6.- Requisitos para Contratación de Personal

El personal del Ente Licenciante Provincial es contratado de acuerdo al régimen de la AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS.

5.3.7.- Documentación Provista al Personal

El Ente Licenciante Provincial proporciona a su personal toda la documentación necesaria para el desempeño de sus funciones y responsabilidades.

6.- CONTROLES DE SEGURIDAD TECNICA

6.1. - GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES CRIPTOGRÁFICAS

6.1.1.- Generación del Par de Claves Criptográficas

Par de Claves de la ACR-SL

El par de claves criptográficas de la **ACR-SL** es generado por el Ente Licenciante Provincial en instalaciones de la propia **ACR-SL**, en hardware criptográfico seguro que cumple con las características definidas en FIPS 140 Versión 2 para el nivel 3.

El par de claves criptográficas utilizadas por el Ente Licenciante Provincial para emisión y revocación de certificados y emisión de la Lista de Certificados Revocados es de 4096 bits generado con algoritmo RSA.

Par de Claves de Autoridad Certificante de Certificador Licenciado Provincial

El par de claves criptográficas de una Autoridad Certificante Subordinada se genera en las instalaciones del Certificador Licenciado Provincial, en presencia de personal del Ente Licenciante, después de haberle sido otorgada la licencia.

El Certificador Licenciado Provincial, en su carácter de responsable de la Autoridad Certificante a la que la **ACR-SL** le emite un certificado, es el responsable del par de claves criptográficas y, como tal, está obligado a generarlo en un dispositivo criptográfico seguro conforme a la normativa, a no revelar su clave privada a terceros bajo ninguna circunstancia y a almacenarla en un medio que garantice su integridad y confidencialidad. En todo momento, la clave privada de la Autoridad

Certificante se encuentra bajo el exclusivo y permanente control del Certificador Licenciado Provincial.

Durante la generación y almacenamiento de la clave privada de la Autoridad Certificante, por parte del Certificador Licenciado Provincial debe asegurarse que:

a) La clave privada sea única y su seguridad se encuentre garantizada, y
b) No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas.

6.1.2.- Entrega de la Clave Privada al Certificador Licenciado

De acuerdo al artículo 28, punto 1 del Decreto N° 0428-MP-2008, reglamentario de la Ley N° V-0591-2007 que adhiere a la Ley Nacional Nº 25.506, el Ente Licenciante Provincial no genera ni toma conocimiento o accede a los datos de generación de firma de las Autoridades Certificantes del Certificador Licenciado Provincial.

6.1.3.- Entrega de la Clave Pública al Ente Licenciante Provincial

El Certificador Licenciado Provincial, a través del personal designado para representarlo, entrega al Ente Licenciante Provincial copia de su Clave Pública contenida en un CSR (Certificate Signing Request), en formato PKCS#10, de manera que:

a) No pueda ser alterada, y
b) El Certificador Licenciado Provincial posea la clave privada que corresponde a dicha clave pública.

Todas las actividades que se llevan a cabo en el proceso de recepción de la clave pública son registradas para fines de auditoría.

6.1.4.- Disponibilidad de la Clave Pública

El Ente Licenciante Provincial publica el certificado de la **ACR01-SL** y de la **ACR02-SL**, en:
http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crt
http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crt
y alternativamente en:
http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crt

http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crt

Asimismo, publica los certificados de las Autoridades Certificantes de los Certificadores Licenciados Provinciales que su Autoridad Certificante hubiera emitido en: www.acraiz.sanluis.gov.ar
El Certificador Licenciado Provincial es responsable de publicar los certificados de sus Autoridades Certificantes y de sus suscriptores para que terceros usuarios puedan acceder a ellos.

6.1.5.- Tamaño de Claves

La **ACR-SL** utiliza un par de claves criptográficas RSA de 4096 bits de longitud para emitir el certificado de las Autoridades Certificantes.En caso de tomar conocimiento de técnicas de criptoanálisis que vulneren el algoritmo utilizado para la generación de firma con la longitud indicada, el Ente Licenciante Provincial revocará los certificados emitidos, notificando previamente a los Certificadores Licenciados Provinciales y anunciará la implementación de una nueva versión de la presente Política de Certificación.

6.1.6. - Generación de parámetros de claves asimétricas

No aplicable.

6.1.7. - Verificación de calidad de los parámetros

No aplicable.

6.1.8.- Generación de Claves por Hardware o Software

El par de claves criptográficas se generan en dispositivos criptográficos que cumplan con lo definido en el **punto 6.2.1** de la presente Política de Certificación.

6.1.9.- Propósitos de Utilización de Claves (Key Usage)

Las claves criptográficas de la **ACR01-SL** tienen como exclusivo propósito la firma de su certificado, la CRL que emite y del certificado de la **ACR02-SL**.

Las claves criptográficas de la **ACR02-SL** tienen como exclusivo propósito la firma de los certificados de las Autoridades Certificantes Subordinadas correspondientes a los Certificadores Licenciados Provinciales y la firma de la Lista de Certificados Revocados (CRL) que emitie.

Las claves criptográficas de las Autoridades Certificantes de Certificadores Licenciados Provinciales tienen como exclusivo propósito su utilización para la firma de certificados de sus suscriptores, la firma de sus Listas de Certificados Revocados (CRL), y de poseer, la firma del servicio de estado de certificado en línea (OCSP).

6.2.- PROTECCIÓN DE LA CLAVE PRIVADA

Las claves privadas de la **ACR-SL** está bajo responsabilidad del Ente Licenciante Provincial y protegidas mediante la utilización de sistemas y procedimientos que incluyen la designación de funcionarios responsables de su control, custodia y activación segura y de su destrucción en caso de compromiso.

Las claves privadas de las Autoridades Certificantes de los Certificadores Licenciados Provinciales están bajo su propia responsabilidad, y protegidas mediante la utilización de sistemas y procedimientos confiables que evitan el uso no autorizado o pérdida de las mismas.

6.2.1.- Estándares para dispositivos criptográficos

La **ACR-SL** cumple con las características definidas en FIPS 140 versión 2, nivel 3, para la generación y almacenamiento de su par de claves criptográficas en dispositivos criptográficos seguros.

Para la generación y almacenamiento de sus pares de claves criptográficas, el Certificador Licenciado Provincial dispone de dispositivos criptográficos que cumplen con las características definidas en FIPS 140 versión 2, de por lo menos:

a) Nivel 3, para sus Autoridades Certificantes, y
b) Nivel 2, para sus Autoridades de Registro.

6.2.2.- Control “M de N” de la Clave Privada

El Ente Licenciante Provincial utiliza procedimientos que requieren la participación de varias personas para la activación de la clave privada de la **ACR-SL**.

Los Certificadores Licenciados Provinciales deben adoptar procedimientos que requieran la participación de varias personas para la activación de las claves privadas de sus Autoridades Certificantes.

6.2.3.- Recuperación de la clave privada

El Ente Licenciante Provincial posee procedimientos para la recuperación de la clave privada de la **ACR-SL**, detallados en su Manual de Procedimiento Reservado.

6.2.4.- Copia de seguridad de la clave privada

El Ente Licenciante Provincial mantiene una copia de seguridad de la clave privada de la **ACR-SL**. Estas copias son almacenadas y protegidas con un nivel de seguridad no inferior al establecido para la versión original de las claves y mantenidas por el plazo de validez del certificado correspondiente.

El Ente Licenciante Provincial no mantiene copia de las claves privadas de las Autoridades Certificantes de los Certificadores Licenciados Provinciales.

Las claves privadas de las Autoridades Certificantes de Certificadores Licenciados Provinciales cuentan con al menos una copia de seguridad de manera tal de poder recuperarlas en caso de desastre o mal funcionamiento del sistema.

Estas copias están protegidas bajo las mismas condiciones de acceso físico que se implementan en el ambiente de producción. Están resguardadas en dispositivos criptográficos equivalentes a los que contienen las claves originales.

6.2.5.- Archivo de Clave Privada

Cuando las claves privadas de las Autoridades Certificantes están desactivadas, los dispositivos criptográficos que las contienen permanecen bajo los controles de seguridad física descriptos en la presente Política y el acceso a los mismos es debidamente registrado y solo permitido a personal autorizado.

6.2.6.- Incorporación de Claves Privadas en Módulos Criptográficos

Las claves privadas se generan en dispositivos criptográficos conforme lo establecido en la presente Política y nunca se extraen de los mismos.

Solo se permite la transferencia de claves en caso de creación de copias de seguridad descriptas en la presente Política y se realizan a través de los procedimientos de resguardo propios de los dispositivos criptográficos utilizados.

6.2.7.- Método de Activación de Claves Privadas

La activación de las claves privadas de las Autoridades Certificantes utiliza un esquema de control compartido (“M de N”), por lo que se necesita la intervención simultanea de varias personas autorizadas.

6.2.8.- Método de Desactivación de Claves Privadas

La desactivación de las claves privadas se realiza a través de procedimientos que garantizan la inhabilitación de esas claves. Para volver a utilizarlas es necesario seguir el procedimiento de activación de claves descriptas en la presente Política.

6.2.9.- Método de Destrucción de Claves Privadas

Las claves privadas se destruirán utilizando procedimientos que imposibilitan su posterior recuperación o utilización. Ello se realiza bajo las mismas medidas de seguridad que las empleadas en la Ceremonia de Generación de Claves.

6.3.- OTROS ASPECTOS DE ADMINISTRACIÓN DE CLAVES

6.3.1.- Archivo de la Clave Pública

La clave pública se archiva utilizando métodos que garantizan su integridad. El Ente Licenciante Provincial posee procedimientos para el archivo de su clave privada, y se encuentran detallados en su Manual de Procedimiento (Reservado).

6.3.2.- Período de Uso de Clave Pública y Privada

El período de validez del par de claves se corresponde con el período de validez de los certificados emitidos.

El certificado de la **ACR01-SL** expira a los sesenta (60) años de su emisión y el certificado de la **ACR02-SL** expira a los cincuenta y nueve (59) años desde su emisión. Los certificados de Autoridades Certificantes de Certificador Licenciado Provincial expiran a los treinta (30) años, siempre que dicho plazo no exceda el período de vigencia del certificado de la **ACR-SL**, o cuando sean revocados.

6.4.- DATOS DE ACTIVACIÓN

6.4.1.- Generación e Instalación de Datos de Activación

Los datos de activación de las Claves Privadas utilizan un esquema de control compartido (“M de N”).

6.4.2.- Protección de los Datos de Activación

Los datos de activación son tratados como información confidencial y no deben estar expuestos en medios accesibles por terceros. Asímismo las personas responsables de su custodia no deben divulgar su condición.

6.4.3. - Otros aspectos referidos a los datos de activación

No aplicable.

6.5.- CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1.- Requisitos Técnicos Específicos

Solo personal debidamente autorizado puede acceder a las instalaciones y sistemas que intervienen en las operaciones de certificación. Acorde a la Política de Seguridad aprobada por el Ente Licenciante Provincial se garantiza:

a) Una efectiva administración de los accesos para aquellos usuarios involucrados en el ciclo de vida de los certificados,
b) Una adecuada segregación de funciones,
c) La correcta identificación y autenticación del personal en las actividades críticas relacionadas con el ciclo de vida de los certificados,
d) El registro de eventos relacionados con el ciclo de vida de los certificados,
e) La protección, integridad y confidencialidad de datos críticos.

6.5.2. - Calificaciones de seguridad computacional

No aplicable.

6.6.- CONTROLES TÉCNICOS DEL CICLO DE VIDA DE LOS SISTEMAS

6.6.1.- Controles de Desarrollo de Sistemas

Para la implementación de los sistemas en el ambiente de producción se consideran los siguientes controles:

Análisis de seguridad en todos sus componentes,

a) Entornos separados de desarrollo, prueba y producción,
b) Procedimiento formal de autorización y registro para la actualización de los sistemas,
c) En caso de que el sistema fuera adquirido debe existir un acuerdo de nivel de servicio con el proveedor, que coincida con el ofrecido por el Certificador Licenciado Provincial a sus suscriptores.

6.6.2.- Administración de Controles de Seguridad

Según el análisis de riesgo efectuado, se clasificaron los activos informáticos de acuerdo a sus necesidades de protección y se mantiene su inventario. Los sistemas son auditados de forma periódica de acuerdo a lo queestablezca el Plan de Auditoría.

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

No aplicable.

6.7.- CONTROLES DE SEGURIDAD DE RED

Los servicios de certificación de la **ACR-SL** se realizan fuera de línea lo que asegura su protección de cualquier ataque a través de redes.

Los servicios de publicación del Ente Licenciante Provincial y de la **ACR-SL** utilizan sistemas debidamente protegidos, garantizando integridad.

6.8.- CONTROLES DE INGENIERÍA DE DISPOSITIVOS CRIPTOGRÁFICOS

El dispositivo criptográfico utilizado para el almacenamiento y generación de la clave privada cumple con lo establecido en la presente Política de Certificación.

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

Tanto el formato del certificado como el de la Lista de Certificados Revocados cumplen con lo especificado en el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile).

7.1.- PERFIL DEL CERTIFICADO

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de la **ACR01-SL**:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Versión	V3
Número de Serie	Número Asignado por la AC Raíz de San Luis
Algoritmo de firma	Sha2RSA

Nombre distintivo del emisor	CN = ENTE LICENCIANTE SAN LUIS – ACRAIZ01 O = Gobierno de la Provincia de San Luis C =AR
Validez	60 años Se especifica desde xx/xx/xx hasta xx/xx/xx
Nombre distintivo del suscriptor	CN = ENTE LICENCIANTE SAN LUIS – ACRAIZ01 O = Gobierno de la Provincia de San Luis C = AR
Clave pública del suscriptor	La clave pública RSA es de 4096 bits
Extensiones	
Identificador de la clave del suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves	Los bits deben estar como se indican Digital Signature = 0 Non Repudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Restricciones básicas	CA=TRUE
Políticas de Certificación	Política: OID 2.16.32.1.3.2.1.1.0 CPS: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/cps.pdf Notificación: Infraestructura de clave públilca de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial N° V-0591-2007

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de la ACR02-SL:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Numero de Serie	Número asignado por la Autoridad Certificante Raíz 01 de San Luis ….
Algoritmo de firma	sha2RSA
Nombre distintivo del emisor	CN = ENTE LICENCIANTESAN LUIS - ACRAIZ01 O = Gobierno de la Provincia de San Luis C = AR
Validez	59 años Se especifica desde xx/xx./xx hasta xx/xx/xx

Nombre distintivo del suscriptor	CN = ENTE LICENCIANTE SAN LUIS – ACRAIZ02 O = Gobierno de la Provincia de San Luis C = AR
Clave pública del suscriptor	La clave pública RSA es de 4096 bits
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la Autoridad Certificante Raíz 01 de San Luis
Identificador de la clave del suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves	Firma digital, Firma de Certificados, Firma de CRL sin conexión, Firma CRL
Políticas de Certificación	Política: OID 2.16.32.1.3.2.1.1.0 CPS: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/cps.pdf Notificación: Infraestructura de clave públilca de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial N° V-0591-2007
Restricciones básicas	CA=TRUE
Puntos de distribución de la Lista de Certificados Revocados	URL: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crl
Información de Acceso de la Autoridad Certificante	URL: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crt http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr01.crt

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de las Autoridades Certificantes de los Certificadores Licenciados Provinciales:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Numero de Serie	Número asignado por la Autoridad Certificante Raíz 02 del Ente Licenciante Provincial de San Luis
Algoritmo de firma	Sha2RSA
Nombre distintivo del emisor	CN = ENTE LICENCIANTE PROVINCIAL SAN LUIS – ACRAIZ02 O = Gobierno de la Provincia de San Luis C = AR

Validez	30 años Se especifica desde/hasta
Nombre distintivo del suscriptor	Según lo especificado en la Resolución N° 341-ACTySSL-2018 en lo referente a certificados de certificadores. Si el certificado digital no incluyera la extensión Políticas de Certificación, deberá incluir en el presente la URL donde se encuentra publicada la correspondiente Política de Certificación.
Clave pública del suscriptor	Según lo especificado en la Resolución Nº 341-ACTySSL-2018 en lo referente a certificados de certificadores.
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la Autoridad Certificante del Ente Licenciante Provincial de la Provincia de San Luis
Identificador de la clave del suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves	Los bits deben estar como se indican Digital Signature = 0 Non Repudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación	Política: Completar con OID CPS: Completar con URI donde el documento estará disponible conforme lo exigido en el Anexo III de la Resolución Nº 341-ACTySSL-2018 Requisitios de licenciamiento Notificación: Infraestructura de clave públilca de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial N° V-0591-2007
Restricciones básicas	cA=TRUE pathlen=0
Puntos de distribución de la lista de certificados revocados	URL: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crl
Información de Acceso de la Autoridad Certificante	URL: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crt http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crt

7.2. - Perfil de la Lista de Certificados Revocados

Se usarán los siguientes campos del formato X.509 versión 2 en la Lista de Certificados Revocados (CRL) de la ACR01-SL:

X.509 v2 Certificado Atributos / Extensiones	Contenido
Atributos	
Versión	V2
Algoritmo de firma	Sha2RSA
Nombre distintivo del emisor	CN = ENTE LICENCIANTE DE SAN LUIS – ACRAIZ01 O = Gobierno de la Provincia de San Luis C = AR
Día y hora de vigencia	Día y hora de emisión de esta CRL
Próxima actualización	Día y hora de la próxima emisión de
Certificados revocados	Lista de los certificados revocados incluyendo número de serie y fecha de revocación
Extensiones	
Identificación de clave de la Autoridad Certificante	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Número de CRL	Número que se incrementa cada vez que cambia una CRL

Se usarán los siguientes campos del formato X.509 versión 2 en la Lista de Certificados Revocados (CRL) de la ACR02-SL:

X.509 v2 Certificado Atributos / Extensiones	Contenido
Atributos	
Versión	V2
Algoritmo de firma	Sha2RSA
Nombre distintivo del emisor	CN = ENTE LICENCIANTE DE SAN LUIS – ACRAIZ02 O = Gobierno de la Provincia de San Luis C = AR
Día y hora de vigencia	Día y hora de emisión de esta CRL
Próxima actualización	Día y hora de la próxima emisión de
Certificados revocados	Lista de los certificados revocados incluyendo número de serie y fecha de revocación
Extensiones	
Identificación de clave de la Autoridad Certificante	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Número de CRL	Número que se incrementa cada vez que cambia una CRL

8.- ADMINISTRACION DE ESPECIFICACIONES

8.1.- PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIONES

El Ente Licenciante Provincial cuenta con Procedimientos de Administración de Cambios para efectuar cualquier modificación a la presente Política de Certificación.

8.2.- PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN

El Ente Licenciante Provincial publicará, en su sitio de publicación, las modificaciones aprobadas a la Política de Certificación, indicando en cada caso, el texto reemplazado. Asimismo, publicará el texto de la nueva versión del documento modificado. Lo mismo se aplica a los demás documentos públicos asociados.

Todos los cambios producidos en los documentos antedichos serán notificados a los Certificadores Licenciados Provinciales.

8.3.- PROCEDIMIENTOS DE APROBACIÓN

Esta Política de Certificación o cualquier documento vinculado, así como sus actualizaciones, serán aprobados por la Autoridad de Aplicación de la Provincia de San Luis.