FDSL 3.0
FIRMA DIGITAL
DE SAN LUIS

POLITICA DE CERTIFICACION PARA AUTENTICACION DE SERVIDORES Y SERVICIOS

OID: 2.16.32.1.3.2.1.1.5

VERSION 3.0 – FECHA 20/02/19

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	15/11/2010	FDSL	Director	Resolución N° 11150008-ULP-2010
2	0	03/10/2016	FDSL	Director	Resolución N° 10-MCyT-2016
2	1	12/01/2017	FDSL	Director	Resolución N° 07-ASLCTyS-2017
3	O	20/02/2019	FDSL	Director	Resolución N° 44-ACTySSL-2019

Contenido

INTRODUCCIÓN

1.1.- DESCRIPCIÓN GENERAL

El presente documento establece las políticas que se aplican a la relación entre un Certificador Licenciado Provincial en el marco de la infraestructura de firma digital de la Provincia de San Luis (Ley N° V-0591-2007 de adhesión a la Ley N° 25.506), las Autoridades de Registro conforme el Convenio que se suscriba a tal efecto, los solicitantes, suscriptores y terceros usuarios de los certificados emitidos por el Certificador Licenciado Provincial, de las clases que se detallan a continuación, a favor de Organizaciones:

- **CLASE I. Autenticación de Servidores**

Los Certificados para la Autenticación de Servidores son certificados expedidos a organizaciones que cuentan con un nombre de dominio debidamente registrado, bajo la responsabilidad del Suscriptor o titular del certificado. La finalidad de este certificado es poder autenticar de forma segura el servidor en la red y permitirles a los usuarios establecer una conexión segura mediante el protocolo SSL (o TLS).

Para esta Clase de certificados de clave pública, en esta Política se establecen las responsabilidades de:

- Firma Digital de San Luis, quien actuará como Certificador Licenciado Provincial;
- Los Solicitantes y Suscriptores de certificados digitales;
- Los Terceros Usuarios, clientes de aplicaciones en el ámbito de la verificación de identidad del servidor al que se conectan y del cifrado del canal de los datos transmitidos entre ellos;
- Las aplicaciones y servicios con capacidades de soporte SSL, en el ámbito de verificación de la identidad de los servidores a los que se conectan y del cifrado del canal de los datos transmitidos entre ellos.

- **CLASE II. Prestación de Servicio de Sellado de Tiempo,**

Este documento describe las Prácticas y la Política de Sellado Digital de Tiempo (Time Stamping) de Firma Digital de San Luis y establece las reglas generales empleadas por la Autoridad de Sellado de Tiempo de la Autoridad de Certificación de FDSL (en adelante TSA - FDSL), para la emisión de sellos de tiempo firmados. Se establecen en este documento los participantes de estos procesos, especificando sus responsabilidades, derechos y ámbito de aplicación.

El sellado de tiempo (Time Stamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. FDSL es Autoridad de Sellado de Tiempo en cuyo carácter actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos, donde el Solicitante realiza una petición de sellado de tiempo según la norma RFC 3161 a una URL de FDSL obteniendo como respuesta una evidencia digital firmada por la TSA de FDSL.

Para esta Clase de certificados de clave pública, en esta Política se establecen las responsabilidades de:

- Firma Digital de San Luis, quien actuará como Autoridad de Sellado de Tiempo
- Los solicitantes del servicio de sellado de tiempo,
- Los Terceros Usuarios.

Esta Política de Certificación será identificada como “Política de Certificación para Autenticación de Servidores y Servicios”, encontrándose su ámbito de aplicación definido en el Punto 1.3 PARTICIPANTES y 1.4.- USO DE LOS CERTIFICADOS.

- **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

Este documento describe las Prácticas y la Política del Servicio de Consulta en Línea del Estado del Certificado (OCSP) de Firma Digital de San Luis y establece las reglas generales empleadas por la Autoridad de Validación OCSP de la Autoridad de Certificación de FDSL (en adelante OCSP - FDSL), para dicho servicio. Se establecen en este documento los participantes de estos procesos, especificando sus responsabilidades, derechos y ámbito de aplicación.

Un certificado vincula los datos de verificación de firma digital de una persona humana o jurídica o de una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

En consecuencia, en esta Política se establecen las responsabilidades de:

- Firma Digital de San Luis (FDSL), quien actuará como Certificador Licenciado Provincial;
- Las Autoridades de Registros, con quienes FDSL haya suscripto un Convenio de Constitución de Autoridad de Registro Delegada;
- Los solicitantes y Suscriptores de certificados digitales;
- Los Terceros Usuarios receptores de documentos firmados por los Suscriptores bajo la presente política.

A los efectos de la presente Política se entenderá que todas las referencias al Suscriptor de un certificado de clave pública también son válidas para los solicitantes en proceso de obtenerlo.

1.2.- NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Título del Documento: "Política de Certificación para autenticación de servidores y servicios"
Versión: 3.0
O.I.D.: 2.16.32.1.3.2.1.1.5
Fecha: 20/02/2019
URL: http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores-cps.pdf
Lugar: Provincia de San Luis, República Argentina.

Esta Política de Certificación se complementa con los siguientes documentos, denominados "Documentos Asociados":

a) El Manual de Procedimientos de Certificación (Parte Pública y Parte Reservada)
b) El Acuerdo con Suscriptores de Certificados
c) Los Términos y Condiciones con Terceros Usuarios
d) La Política de Privacidad del Certificador Licenciado Provincial
e) El Plan de Cese de Actividades
f) El Plan de Seguridad: Política de Seguridad y Manual de Procedimientos de Seguridad
g) El Plan de Contingencia.
h) Tarifario.

1.3.- PARTICIPANTES

Los participantes de esta Política de Certificación para las distintas CLASES de certificados de clave pública:

➢ **CERTIFICADOS CLASE I. AUTENTICACIÓN DE SERVIDORES.**

a) Firma Digital de San Luis, en adelante FDSL, quien actuará como Certificador Licenciado Provincial
b) Los Suscriptores de Certificados, que serán las organizaciones que posean un servidor
c) Los Solicitantes de Certificados, que serán los representantes de las organizaciones que tramiten la emisión del certificado de autenticación de servidores
d) Los Terceros Usuarios.

➢ **CERTIFICADOS CLASE II. SERVICIO DE SELLADO DE TIEMPO.**

a) Firma Digital de San Luis, en adelante FDSL, quien actuará como Certificador Licenciado Provincial;
b) Firma Digital de San Luis, quien actuará como proveedor del servicio de sellado de tiempo, en cuyo rol será denominado TSA – FDSL

c) El Solicitante del servicio de sellado de tiempo
d) Los Terceros Usuarios.

➢ **CERTIFICADOS CLASE III. SERVICIO DE CONSULTA EN LINEA DEL ESTADO DEL CERTIFICADO.**

a) Firma Digital de San Luis, en adelante FDSL, quien actuará como Certificador Licenciado Provincial
b) Firma Digital de San Luis, quien actuará como proveedor del SERVICIO DE CONSULTA EN LÍNEA DEL ESTADO DEL CERTIFICADO, en cuyo rol será denominado OCSP – FDSL
c) El Solicitante del servicio OCSP
d) Los Terceros Usuarios.

1.3.1.- Certificador Licenciado Provincial

Para esta Política de Certificación, la función de Certificador Licenciado Provincial la cumple el Instituto Firma Digital de San Luis (en adelante, FDSL) dependiente de la Agencia de Ciencia, Tecnología y Sociedad San Luis, en virtud de lo dispuesto en el artículo 24 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018, reglamentario de la Ley N° V'0591-2007 y normativa concordante.

Instituto Firma Digital de San Luis (FDSL)
Domicilio: Edificio de Descentralización Administrativa "Terrazas del Portezuelo" – Torre III, piso 3° - Autopista de las Serranías Puntanas Km. 783, Provincia de San Luis. República Argentina. CP 5700
Teléfono: (0266)4452000, Internos 6095/3574
Correo electrónico: firmadigital@sanluis.gov.ar
Sitio web: www.firmadigital.sanluis.gov.ar

1.3.2.- Autoridad de Registro

➢ **CERTIFICADOS CLASE I**

La tarea de validación de la identidad del Solicitante de un certificado de clave pública puede ser realizada por FDSL o por una Autoridad de Registro Delegada, constituida a tal efecto.
La tarea de validación de la identidad del solicitante abarca la identificación y autenticación de los solicitantes, la verificación de la existencia de la persona jurídica a la cual el Solicitante dice pertenecer y la verificación del vínculo con aquella, además de la guarda de la documentación probatoria.
Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación de FDSL.
A los efectos de la constitución de una Autoridad de Registro será indispensable la celebración de un "Convenio de Constitución de Autoridad de Registro Delegada" entre FDSL y quien pretenda constituirse como tal. Dicho convenio deberá ser suscripto por quien tenga facultades suficientes para obligar a la persona jurídica y la autoridad máxima de FDSL, individualizando expresamente la presente Política de Certificación; designando a los Oficiales de Registro de la Autoridad de Registro y detallando sobre quien recaerá la responsabilidad de suscribir la "Nota de Solicitud de Emisión de Certificado" necesaria para tramitar el certificado de clave pública conforme lo previsto en el Punto 3.2.3 de la presente Política de Certificación.
A través del sitio web de internet del Certificador, se identificarán las Autoridades de Registro propias y Delegadas así como sus datos de contacto.

➢ **CERTIFICADOS CLASE II y III**

La tarea de validación de los datos y emisión de un certificado de clave pública debe ser realizada por FDSL. No admite la posibilidad que la tarea de validación y emisión sea realizada por una Autoridad de Registro Remota.

Contacto: Responsable de la Autoridad de Registro Central FDSL

Domicilio: Edificio de Descentralización Administrativa "Terrazas del Portezuelo" – Torre III, piso 3° - Autopista de las Serranías Puntanas Km. 783, Provincia de San Luis. República Argentina. CP 5700
Teléfono: (0266)4452000, Internos 6095/3574
Correo electrónico: firmadigital@sanluis.gov.ar
Sitio web: www.firmadigital.sanluis.gov.ar

1.3.3.- Suscriptores de Certificados
Según los términos de la presente Política de Certificación, se define:

➢ **CLASE I: Autenticación de Servidores**
Podrán ser Suscriptores de certificados de autenticación de servidores todas las personas jurídicas identificadas por medio de un dominio que cumplan los requisitos indicados en el punto 3.2.3 de la presente Política – Autenticación de la Identidad del Solicitante - cuyo trámite deberá ser realizado por el Solicitante de Certificados conforme lo dispuesto en el punto 4.1.1. de esta Política "Solicitantes de Certificados".

➢ **CLASE II: Servicio de Sellado de Tiempo**
Sólo FDSL será suscriptor de certificados de sellado de tiempo en su rol de TSA - FDSL. Quienes soliciten la provisión del servicio se denominan Solicitantes y deben cumplir lo dispuesto en el Punto 1.3 y 1.4 de la presente Política.

➢ **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**
Sólo FDSL será suscriptor de certificados de Servicio de Consulta en Línea del Estado del Certificado en su rol de OCSP - FDSL. Quienes soliciten la provisión del servicio se denominan Solicitantes y deben cumplir lo dispuesto en el Punto 1.3 y 1.4 de la presente Política.

1.3.4.- Terceros Usuarios

Son Terceros Usuarios de los certificados emitidos bajo la presente Política de Certificación, toda persona humana o jurídica que realiza una conexión segura a un servidor que utilice el certificado de autenticación de servidores emitido por FDSL para establecer el canal de comunicación.
Las personas humanas o jurídicas que utilicen el servicio de sellado de tiempo TSA – FDSL.
Las personas humanas o jurídicas que utilicen el Servicio de Consulta en Línea del Estado del Certificado OCSP – FDSL para verificar la validez de un certificado digital.

1.4.- USO DE LOS CERTIFICADOS

1.4.1.- Usos apropiados de los certificados

➢ **CLASE I: Autenticación de Servidores**
Los certificados CLASE I emitidos en el marco de la presente Política de Certificación podrán ser utilizados exclusivamente a los fines de autenticar la identidad de un servidor y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio.

➢ **CLASE II: Servicio de Sellado de Tiempo**
Los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo de FDSL, TSA - FDSL, pueden emplearse para garantizar la fecha y hora de las transacciones y el no repudio en procesos en los cuales intervenga cualquier organismo o entidad con los que FDSL haya formalizado un Convenio de Servicio de Sellado de Tiempo.

➢ **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

Los certificados para el Servicio de Consulta en Línea del Estado del Certificado de FDSL, OCSP – FDSL podrán ser usados exclusivamente a los fines de autenticar la respuesta de la consulta del estado de los certificados que se realiza en línea con el protocolo OCSP.

1.4.2.- Usos prohibidos de los certificados

Todo uso que exceda el ámbito de la presente política establecido por el punto 1.4, se encuentra prohibido.

1.5.- ADMINISTRACION DE LA POLITICA

1.5.1.- Responsable del documento

Para realizar preguntas, efectuar reclamos o enviar sugerencias referidas al presente documento, el interesado deberá dirigirse a:

Contacto: Responsable de Atención al Cliente
Domicilio: Edificio de Descentralización Administrativa "Terrazas del Portezuelo" – Torre III, piso 3° - Autopista de las Serranías Puntanas Km. 783, Provincia de San Luis. República Argentina. CP 5700
Teléfono: (0266) 4452000, Internos 6095/3574
Correo electrónico: firmadigital@sanluis.gov.ar
Sitio web: www.firmadigital.sanluis.gov.ar

1.5.2.- Contacto

El responsable del registro, mantenimiento e interpretación de la Política de Certificación es FDSL, que funciona en el ámbito de la Agencia de Ciencia, Tecnología y Sociedad San Luis.
Contacto: Director
Instituto Firma Digital de San Luis
Dirección: Edificio de Descentralización Administrativa "Terrazas del Portezuelo" – Torre III, piso 3° - Autopista de las Serranías Puntanas Km. 783, Provincia de San Luis. República Argentina. CP 5700
Teléfono: (0266)4452000, Internos 6095/3574
Correo electrónico: firmadigital@sanluis.gov.ar
Sitio web: www.firmadigital.sanluis.gov.ar

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

El Ente Licenciante Provincial es el responsable de acreditar y determinar si una Autoridad de Certificación forma parte de la Infraestructura de Firma Digital de San Luis, en tal sentido, es quien aprueba la Política de Certificación durante el proceso de licenciamiento.

1.5.4.- Procedimiento de aprobación de la Política de Certificación

La Política de Certificación ha sido presentada ante la Autoridad de Aplicación, en su rol de Ente Licenciante Provincial, durante el proceso de licenciamiento y ha sido aprobada mediante el dictado de la **Resolución Nº 44-ACTySSL-2019.**

1.6. – DEFINICIONES Y ACRONIMOS

1.6.1. – Definiciones

Definiciones de los conceptos relevantes utilizados en la presente Política de Certificación:

- Autoridad de Aplicación: AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.
- Ente Licenciante: es el órgano administrativo encargado de otorgar las licenciantes a los Certificadores Licenciado Provinciales y de supervisar su actividad. El INSTITUTO FIRMA DIGITAL DE SAN LUIS y la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS, constituyen el Ente Licenciante del

régimen provincial de firma digital en San Luis (art. 24º y 26° del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018). Cuando el INSTITUTO FIRMA DIGITAL DE SAN LUIS actúa como Certificador Licenciado Provincial, la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS cumple el rol de Ente Licenciante Provincial (art. 18º de Resolución Nº 17-ASLCTyS-2017).

- Certificador Licenciado Provincial: Es el ente público, ente privado u organismo de derecho público no estatal que emite certificados de clave pública, entendiendo por tal al que asocia una clave pública con un suscriptor, durante el período de vigencia del certificado, haciendo plena prueba dentro de la Administración del Sector Público Provincial, los Poderes del Estado Provincial y el sector privado de la veracidad de su contenido y cuenta con una licencia provincial para ello (artículo 31 del Decreto Nº 0428-MP-2008).
- Autoridad de Registro: Es la entidad en quien el Certificador Licenciado Provincial delega las funciones relativas a la verificación de la identidad y demás datos correspondientes al aspirante a suscriptor del servicio, de registro de presentaciones y trámites que le son formuladas, así como la responsabilidad de las comunicaciones con el Ente Licenciante Provincial y/o el Certificador Licenciado Provincial en el proceso técnico de registración (artículo 39 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018). La Autoridad de Registro puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del Certificador Licenciado para hacerlo (artículo 40 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018).
- Autoridad de Certificación: Es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- Suscriptor o Titular de Certificado Digital: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo (art. 36 del Decreto Nº 0428-MP-2008).
- Tercero Usuario: Persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.
- Infraestructura de Firma Digital San Luis: Se entiende por tal al conjunto integrado por las leyes, decretos y normativa legal complementaria que regulen la firma digital en la jurisdicción de la Provincia de San Luis, las obligaciones y deberes de todas aquellas instituciones, organismos y personas que formen parte del circuito de la firma digital tales como la Autoridad de Aplicación Provincial, el Ente Licenciante Provincial, los Certificadores Licenciados Provinciales, las Autoridades de Registro, así como también, a los estándares tecnológicos, los procedimientos de seguridad, el hardware, el software, las redes, los bancos de datos y la infraestructura física de alojamiento, que permitan la utilización de la firma digital en condiciones de seguridad e integridad (artículo 10º del Decreto Nº 0428-MP-2008).
- Firma Digital: Se entiende por Firma Digital al resultado de una transformación de un documento digital empleando una criptografía asimétrica y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza lo siguiente: 1) si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; 2) si el documento digital ha sido modificado desde que se efectuó la transformación, de manera tal de garantizar con esta comprobación la integridad del documento. Todo lo cual conlleva a garantizar las características de “no repudio” y la “integridad” del documento que son requisitos de la firma digital (artículo 7º del Decreto Nº 0428-MP-2008).
- Criptografía Asimétrica: Se entiende por Criptografía Asimétrica al algoritmo que utiliza, por un lado, una clave privada que es utilizada para firmar digitalmente y por otro su correspondiente clave pública para verificar esa firma digital. Debe ser técnicamente confiable (artículo 8º del Decreto Nº 0428-MP-2008).
- Digesto Seguro: es una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, llamada como tal, de forma que se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital (artículo 9º del Decreto Nº 0428-MP-2008).

- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).
- Certificado Digital de Fecha y Hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- Lista de Certificados Revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado Provincial, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: *"Certificate Revocation List"* (CRL).
- Servicio OCSP (PROTOCOLO de Estado de Certificado en Línea): Servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificado de servicio OCSP del Certificador Licenciado Provincial que brinda el servicio. En inglés: *"Online Certificate Status Protocol"* (OCSP)
- Manual de Procedimientos: Conjunto de prácticas utilizadas por el Certificador Licenciado Provincial en la emisión y administración de los certificados. En inglés: *"Certification Practice Statement"* (CPS).
- Plan de Cese de Actividades: Conjunto de actividades a desarrollar por el Certificador Licenciado Provincial en caso de finalizar la prestación de sus servicios.
- Plan de Contingencia o Plan de Continuidad de las Operaciones: Conjunto de procedimientos a seguir por el Certificador Licenciado Provincial ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones. También denominado Plan de Contingencia.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del Certificador Licenciado Provincial.
- Política de Privacidad: Conjunto de declaraciones que el Certificador Licenciado Provincial se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.
- El servicio de emisión de sellos de tiempo de FDSL que podrá ser utilizado con los certificados emitidos en el marco de esta Política está basado en la especificación de los estándares RCF 3161 – "Internet X. 509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities, ETSI TS 101 861, "Time stamping profile" y a su especificación equivalente RFC 3628 – "Requirements for time-stamping authorities".

1.6.2. - Acrónimos

AC	- Autoridad Certificante
ACR-SL	- Autoridad Certificante Raíz San Luis
AR	- Autoridad de Registro
ARD	- Autoridad de Registro Delegada
ACTySSL	- Agencia de Ciencia, Tecnología y Sociedad San Luis
CIPE	- Cédula de Identidad Provincial Electrónica
CLP	- Certificador Licenciado Provincial
CP	- Política de Certificación
CRL	- Lista de Certificados Revocados
CUIL	- Clave Única de Identificación Laboral
CUIT	- Clave Única de Identificación Tributaria
FD	- Firma Digital
FDSL	- Instituto Firma Digita de San Luis
FIPS	- Norma Federal de Procesamiento de la Información
MCyT	- Ministerio de Ciencia y Tecnología de San Luis
MPC	- Manual de Procedimientos de Certificación

OCSP - Protocolo de estado de certificado en línea -Online Certificate Status Protocol
OID - Identificador de Objeto ("Object Identifier").
PKI - Infraestructura de Clave Pública
RFC - Request for Comments.
TSA - Autoridad de sellado de tiempo - Time Stamp Autority
TSP - Protocolo de sellado de tiempo - Time Stamp Protocol

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

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

2.1.- REPOSITORIOS

Los repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por FDSL y son servicios propios.

2.2.- Publicación de información del Certificador Licenciado Provincial

FDSL garantiza el acceso a la información actualizada y vigente publicada en su repositorio de los siguientes elementos:
a) Política de Certificación anteriores y vigente.
b) Acuerdo Tipo con suscriptores.
c) Términos y condiciones Tipo con terceros usuarios (*"relying parties"*).
d) Política de Privacidad.
e) Manual de Procedimientos (parte pública).
f) Información relevante de los informes de su última auditoría.
g) Repositorio de certificados revocados.
h) Certificados del Certificador Licenciado Provincial.
i) Consulta de certificados emitidos (indicando su estado).
j) Listado de Autoridades de Registro (indicando si opera bajo modalidad móvil).
k) Los certificados digitales de clave pública del Ente Licenciante Provincial.
l) Datos de contacto de FDSL.
m) Política de Seguridad y toda otra documentación técnica de carácter público que se emita (en sus versiones vigentes y anteriores),
n) Información relevante de los informes de la última auditoría de sus Autoridades de Registro propias y delegadas.

La publicación de la información de FDSL se realiza en sus servidores, y se puede encontrar en el sitio web identificado como: http://www.firmadigital.sanluis.gov.ar

Se mantiene el repositorio en línea accesible durante las 24 horas, los 7 días de la semana, sujeto a un calendario de mantenimiento.

Adicionalmente, FDSL pone a disposición de los Terceros y de los Suscriptores un servicio de consulta basado en el protocolo de comunicación OCSP, *"Online Certificate Status Protocol"* para la consulta en línea del estado de validez de los certificados emitidos bajo la presente Política.
Dicho servicio de verificación:

1. Cumple con lo señalado en el RFC2560 del registro de estándares para Internet.
2. Utiliza mensajes codificados que son transmitidos sobre el protocolo HTTP.

Este servicio mantiene una disponibilidad de 24x7, durante los 365 días del año.

La AC de FDSL cuenta con una dirección electrónica para llevar a cabo la consulta correspondiente a

través del protocolo OCSP la cual está incluida en todos los certificados digitales emitidos bajo la presente Política: http://ocsp.firmadigital.sanluis.gov.ar/ocsp

2.3.- Frecuencia de publicación

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

2.4.- Controles de acceso a la información

FDSL brinda acceso irrestricto, permanente y gratuito a su sitio de publicación para consultar documentación de carácter público a través de Internet.

Se garantizan los controles de los accesos al certificado del Certificador Licenciado Provincial, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política de Certificación y a su Manual de Procedimientos (en su parte pública).

FDSL establecerá controles para restringir la posibilidad de escritura y modificación de dicha documentación.

Sólo se revelará información confidencial o privada, si es requerida judicialmente o en el marco de un procedimiento administrativo.

En virtud de la Ley de Protección de Datos Personales N° 25.326 y a lo dispuesto por el inciso h) del artículo 21 de la Ley N° 25.506 (conforme artículo 1° de la Ley N° V-0591-2001), el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a las tramitaciones realizadas.

3.- IDENTIFICACIÓN Y AUTENTICACIÓ REGISTRO INICIAL PARA SUSCRIPTORES

Seguidamente se enuncian las características del registro inicial para Suscriptores de esta Política de Certificación para las distintas CLASES de certificados de clave pública:

➢ **CLASE I. Autenticación de Servidores**

El proceso de solicitud debe ser iniciado exclusivamente por el Solicitante y debe cumplir cada uno de los pasos y el procedimiento de validación previsto en el Punto 3.1.10 de la presente Política de Certificación, “Autenticación de la Identidad del Solicitante”.

➢ **CLASE II. Servicio de Sellado de Tiempo**

El proceso de solicitud de esta CLASE de certificado de clave pública sólo podrá ser iniciada por FDSL en su rol de proveedor del servicio de sellado de tiempo

➢ **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

El proceso de solicitud de esta CLASE de certificado de clave pública sólo podrá ser iniciado por FDSL en su rol de proveedor del Servicio de Consulta en Línea del Estado del Certificado.

3.1.- ASIGNACION DE NOMBRES DE SUSCRIPTORES

3.1.1.- Tipos de Nombres

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

➢ **CLASE I. Autenticación de Servidores**

Sólo se admitirá un nombre de dominio.

➢ **CLASE II. Servicio de Sellado de Tiempo**

Sólo se admitirá la denominación del servicio a prestar por FDSL.

➢ **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

Sólo se admitirá la denominación del servicio a prestar por FDSL.

3.1.2.- Necesidad de Nombres distintivos

Todos los nombres distintivos son de fácil asociación con el Suscriptor al que representa.

➢ **CLASE I. Autenticación de Servidores**

Los siguientes atributos son incluidos en los certificados de autenticación de servidores e identifican unívocamente al Suscriptor:

"commonName" (OID 2.5.4.3: Nombre común): Contendrá el nombre de dominio poseedor de las claves.

"organizationName" (OID 2.5.4.10: Nombre de la organización): Identifica el organismo responsable del servidor con el nombre de persona jurídica, pública o privada, suscriptora del certificado de clave pública.

"organizationalUnitName" (OID 2.5.4.11: Nombre de la sub organización): En caso de estar presente en el certificado, identifica en que área, sector o programa se aloja el servidor. Pueden existir varias ocurrencias de este atributo, representando la dependencia jerárquica de las áreas dentro de la organización.

"serialNumber" (OID 2.5.4.5: Número de serie): Contendrá la Clave Única de Identificación Tributaria (CUIT) del Organismo responsable del servidor.

"stateOrProvinceName" (OID 2.5.4.8: Provincia): De estar presente indica el ámbito geográfico de vinculación del Suscriptor.

"countryName" (OID 2.5.4.6: Código de país): Debe indicar el país donde la Persona Jurídica, responsable del certificado de clave pública, se encuentra constituida.

➢ **CLASE II. Servicio de Sellado de Tiempo**

Los siguientes atributos son incluidos en los certificados de sellado de tiempo de FDSL en su rol de proveedor del servicio de sellado de tiempo e identifican unívocamente a dicho Suscriptor:

"commonName" (OID 2.5.4.3: Nombre común): Contendrá el nombre del servicio: "Servicio de Sellado de Tiempo" e indicará las iniciales de FDSL en su rol de unidad operativa relacionada con el servicio "TSA -FDSL" y el número de certificado emitido toda vez que FDSL dispondrá de diversas TSA's para garantizar la alta disponibilidad del servicio de sellado de tiempo.

"organizationalUnitName" (OID 2.5.4.11: Nombre de la sub organización): Contendrá el nombre de la Unidad Operativa relacionada con el servicio y el OID de la Política de Certificación en virtud de la cual fue emitido.

"organizationName" (OID 2.5.4.10: Nombre de la organización): Indicará el nombre de la persona jurídica responsable del servicio de sellado de tiempo

"serialNumber" (OID 2.5.4.5: Número de serie): Contendrá la Clave Única de Identificación Tributaria (CUIT) de la persona jurídica responsable del servicio de sellado de tiempo.

"countryName" (OID 2.5.4.6: Código de país): Debe indicar el país donde la Persona Jurídica, administradora del certificado de clave pública, se encuentra constituida.

➢ **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

Los siguientes atributos son incluidos en los certificados de Servicio de Consulta en Línea del Estado del Certificado de FDSL en su rol de proveedor del servicio de OCSP e identifican unívocamente a dicho Suscriptor:

"commonName" (OID 2.5.4.3: Nombre común): Contendrá el nombre del servicio: "Autoridad de

Validación OCSP" e indicará las iniciales de FDSL en su rol de unidad operativa relacionada con el servicio "OCSP - FDSL" y el número de certificado emitido toda vez que FDSL dispondrá de varios servidores OCSP para garantizar la alta disponibilidad del Servicio de Consulta en Línea del Estado del Certificado.

"organizationalUnitName" (OID 2.5.4.11: Nombre de la sub organización): Contendrá el nombre de la Unidad Operativa relacionada con el servicio y el OID de la Política de Certificación en virtud de la cual fue emitido.

"organizationName" (OID 2.5.4.10: Nombre de la organización): Indicará el nombre de la persona jurídica responsable del servicio de sellado de tiempo

"serialNumber" (OID 2.5.4.5: Número de serie): Contendrá la Clave Única de Identificación Tributaria (CUIT) de la persona jurídica responsable del servicio de sellado de tiempo.

"countryName" (OID 2.5.4.6: Código de país): Debe indicar el país donde la Persona Jurídica, administradora del certificado de clave pública, se encuentra constituida.

3.1.3.- Anonimato o uso de seudónimos

No aplica.

3.1.4.- Reglas para la interpretación de nombres

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con la documentación presentada por el suscriptor.

Las discrepancias o conflictos que puedan generarse si los datos de los solicitantes o suscriptores contienen caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

3.1.5.- Unicidad de nombres

➢ **CLASE I. Autenticación de Servidores**

El nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias se resuelve consultando en el campo "Asunto" del certificado, el atributo correspondiente a *"serialNumber"*, el cual contiene el número de identificación laboral o tributaria.

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

➢ **CLASE I. Autenticación de Servidores**

Los solicitantes de certificados tienen expresamente prohibido el uso de nombres en sus Solicitudes de Certificado que infrinjan los derechos de propiedad intelectual de los demás. FDSL no verifica si el Solicitante tiene un certificado de derechos de propiedad intelectual en la denominación que figura en una Solicitud de Certificado ni arbitra, media o resuelve controversias sobre la propiedad de cualquier nombre de dominio, nombre comercial, marca comercial o marca de servicio. FDSL posee la facultad de rechazar o revocar cualquier Solicitud de Certificado que se encuentra en disputa.

3.2. – REGISTRO INICIAL

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

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

3.2.1.- Métodos para comprobar la posesión de la clave privada
Para la comprobación de la posesión de la clave privada se utiliza el siguiente procedimiento:
a) El solicitante es partícipe directo y necesario para la generación de su par de claves criptográficas asimétricas.
b) Durante el proceso de solicitud, el solicitante es requerido para que realice la generación de un par de claves criptográficas asimétricas.
c) Los datos de la solicitud y el requerimiento con la clave pública del solicitante, en formato PKCS#10, son enviados a la aplicación de la AC de FDSL.
d) La aplicación de la Autoridad Certificante valida el requerimiento PKCS#10, el cual jamás incluye la clave privada.
e) En caso de ser correcto el formato, la aplicación de la AC-FDSL entrega al solicitante un "Formulario de Solicitud" incluyendo el resumen criptográfico.
f) El responsable de la Autoridad de Registro debe imprimir el "Formulario de solicitud/Acuerdo" en el proceso de validación de la identidad para su firma por parte del Suscriptor y del Responsable de la Autoridad de Registro, conservándolo para su archivo oportuno.
La aplicación de la Autoridad Certificante, una vez que emite el certificado, eliminará automáticamente el requerimiento PKCS#10 asociado a ese certificado con el fin de evitar que se genere un nuevo certificado con dicho requerimiento.

3.2.2.- Autenticación de la identidad de personas jurídicas públicas o privadas

➢ CLASE I. Autenticación de Servidores

El proceso de solicitud debe ser iniciado exclusivamente por el Solicitante, quien será la persona debidamente autorizada por su organización para solicitar un certificado y actuar como custodio de las claves privadas del certificado de clave pública CLASE I.
El Solicitante deberá instalar los certificados de la Autoridad Certificante Raíz de la Provincia de San Luis y de la Autoridad Certificante de la presente Política de Certificación en el servidor en donde se instalará el certificado.
El Solicitante deberá ingresar al sitio web de FDSL donde procederá a completar el “Formulario de Solicitud de Certificado para Autenticación de Servidores” y generar una solicitud de firma de certificado (CSR) en el servidor donde se instalará el certificado.
Una vez completado el formulario, el Solicitante recibirá un correo electrónico en el que se le hará saber el Número de Solicitud que le fue asignado y el detalle de la documentación que deberá presentar ante FDSL dentro de los diez (10) días hábiles subsiguientes, la que deberá estar firmada por el representante legal de la organización debidamente legalizada:
a) Documentación que acredita la existencia y personería de la Persona Jurídica Suscriptora del certificado,
b) Documentación que acredita la identidad y designación del Solicitante de Certificados y su documento nacional de identidad, libreta de enrolamiento, libreta cívica o cédula de identidad provincial electrónica,
c) Titularidad del nombre de dominio, certificada por un representante legal de la persona jurídica,
d) Constancia de pago de la tasa de emisión de certificado de clave pública.

FDSL verificará: a) la existencia y personería de la Personas Jurídica, b) la identidad del Solicitante y su autorización para actuar como tal, c) la titularidad del nombre de dominio a cuyo efecto consultará el siguiente servicio WHOIS autenticado https://www.nic.ar para los dominios "*.ar" y para el resto, consultará el servicio WHOIS pertinente, d) el depósito bancario, e) los datos a incluir en el certificado CLASE I, y en el plazo de diez (10) días hábiles deberá a aceptar o rechazar la solicitud de emisión de certificado de clave pública. La aceptación o rechazo de la solicitud es comunicada al Solicitante por correo electrónico.

El Solicitante podrá consultar el estado del trámite a través de la página web de FDSL.

La aprobación de la emisión del certificado por parte de FDSL y su disponibilidad a fin de ser descargado por el Solicitante en el servidor le será notificada a través de un correo electrónico conjuntamente con un código de emisión. El solicitante deberá ingresar a la página web de FDSL donde se le solicitará para la descarga del certificado el número de solicitud y el código de emisión.

Si al momento de la validación de la documentación no se han reunido elementos de juicio suficientes para validar la identidad del Suscriptor o del Solicitante según los procedimientos indicados, o la titularidad del Suscriptor sobre el nombre de dominio, se procederá a la suspensión del trámite. En este caso, se informará al Solicitante acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de la documentación. El Solicitante tendrá un plazo de treinta (30) días para proveer la información complementaria que se le solicite, vencido el cual FDSL rechazará la solicitud de emisión de certificado CLASE I y el Solicitante deberá reiniciar el proceso de solicitud de emisión de certificado, efectuando un nuevo requerimiento de emisión.

En tal caso, FDSL le hará saber al Solicitante a través de un correo electrónico dejando constancia del plazo límite para la presentación de la documentación faltante.

3.2.3.- Autenticación de la identidad de personas humanas

AUTENTICACIÓN DE LA IDENTIDAD DEL SOLICITANTE

➢ **CLASE I. Autenticación de Servidores**

El Solicitante deberá presentar para su validación ante FDSL:

a) Documento de identidad, en original y fotocopia;

b) Documento que acredite fehacientemente su pertenencia a la organización y su autorización para actuar como Solicitante, Custodio de la clave privada del certificado digital y Autorizado para requerir la revocación del certificado digital;

c) Documentación que acredite la existencia y personería de la Persona Jurídica del Suscriptor;

d) Documentación que acredite que la titularidad de la persona jurídica sobre el nombre de dominio;

e) Formulario de Solicitud de Emisión de Certificado de Autenticación de Servidores;

f) Constancia de depósito de la tasa de emisión de certificado de autenticación de servidores.

3.2.4.- Información no verificada del suscriptor

No aplica.

3.2.5.- Validación de autoridad

No aplica.

3.2.6.- Criterios para la interoperabilidad

No aplica.

3.3.- IDENTIFICACION Y AUTENTICACION PARA LA GENERACION DE UN NUEVO PAR DE CLAVES (RUTINA DE RE-KEY)

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

Se requiere el cumplimiento de los pasos descriptos en el punto 3.2.2 de la presente Política de Certificación

3.3.2.- Generación de un certificado con el mismo par de claves
No aplica.

3.4.- REQUERIMIENTO DE REVOCACIÓN
El procedimiento de revocación de un certificado se inicia con la recepción de la solicitud de revocación por FDSL o la Autoridad de Registro correspondiente, y termina cuando se publica una nueva Lista de Certificados Revocados (CRL), conteniendo el número de serie del certificado en cuestión. Dicha CRL se publica en:

http://fd01.firmadigital.sanluis.gov.ar/fds/servidores.crl y alternativamente, en:
http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl

Una vez validada la información contenida en la solicitud de revocación, FDSL procederá a la revocación del Certificado en un plazo no mayor a las veinticuatro (24) horas. Toda la documentación generada en este proceso es mantenida y resguardada por FDSL.
Sólo será posible solicitar la revocación de los certificados a través de alguna de las modalidades previstas en el punto 4.9.3 de esta Política de Certificación.

4.- CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS
4.1.- SOLICITUD DE CERTIFICADO

4.1.1.- Solicitantes de certificados
Sólo podrán ser solicitantes de certificados:

- **CLASE I: Autenticación de Servidores**

Podrán ser Solicitantes de certificados digitales para autenticación de servidores todas las personas debidamente autorizadas por su organización para ello. El Solicitante de los certificados oficiará también como custodio de las claves generadas para la organización.

- **CLASE II: Servicio de Sellado de Tiempo**

Podrá solicitar certificados para el servicio de sellado de tiempo cualquier organismo o entidad con los que el TSA - FDSL haya formalizado un Convenio de Servicio de Sellado de Tiempo siempre que su aplicación cuente con el correspondiente Certificado de Clave Pública para Aplicación.

- **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

Solo FDSL podrá solicitar certificados para el Servicio de Consulta en Línea del Estado del Certificado en su rol de OCSP – FDSL como proveedor del Servicio de Consulta en Línea del Estado del Certificado.

4.1.2.- Solicitud de Certificado
FDSL sólo emite certificados digitales para personas jurídicas identificadas mediante un dominio.
Asimismo, para poder efectuar la solicitud el Solicitante debe:

- Hallarse conectado a internet,
- Ingresar en la página web de FDSL con un navegador adecuado.

Para iniciar el pedido de emisión del certificado el solicitante debe ingresar al sitio web de FDSL y proceder a completar los pasos detallados en el Punto 3.2.2 de la presente Política de Certificación, “Registro Inicial: Autenticación de la Identidad de personas jurídicas públicas o privadas”.

4.2.- PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

➢ **CLASE I: Autenticación de Servidores**

Habiéndose presentado el solicitante ante FDSL o la Autoridad de Registro correspondiente, la aprobación para iniciar el trámite de solicitud de certificado digital queda sujeta a que hubiera verificado la identidad del solicitante y la documentación que presenta.
Si los extremos no fueran corroborados, el Oficial de Registro hará saber al Solicitante que no es posible iniciar el trámite de solicitud e indicará la documentación a presentar o, las correcciones, a realizar.
Generadas las claves, la aplicación de FDSL valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado, que le es enviado al Solicitante al correo que informó en la Solicitud.
El Responsable de la ARR o FDSL procederá a imprimir el Formulario de Solicitud con el Acuerdo con Suscriptores, el que deberá ser firmado ológrafamente tanto por el Suscriptor como por el Oficial de la ARR o FDSL. Dicho Formulario/Acuerdo deberá ser conservado por este último al igual que la documentación de respaldo acompañada por el Solicitante del certificado.
La ARR o FDSL utilizará el sistema de gestión de expedientes digitales a efectos de evidenciar el cumplimiento de todos los extremos para la emisión del certificado solicitado. En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la Autoridad de Registro. El Oficial de Registro arma el expediente digital de respaldo de la identificación del Solicitante. Este contiene el documento de identidad/CIPE/ pasaporte del Solicitante, la nota o documentación que acredita el carácter en virtud del cual ha solicitado el certificado, la Solicitud del Certificado y la actuación de aprobación de emisión, firmada por el propio Oficial de Registro interviniente.
Concluido ello, el Solicitante deberá descargar su certificado en el dispositivo que utilizó para solicitar la emisión conforme lo detallado en el punto 4.3, a cuyo efecto le será requerido que ingrese su pin/contraseña o huella biométrica, según sean las características del mismo.

4.3.- EMISIÓN DEL CERTIFICADO

4.3.1.- Proceso de emisión del certificado

Una vez finalizado exitosamente el proceso de validación de la identidad del Suscriptor, el Oficial de Registro aprobará la solicitud de certificado y seguidamente, la AC FDSL emitirá el certificado digital correspondiente, firmándolo digitalmente y quedará a disposición del Suscriptor para ser descargado en el dispositivo criptográfico utilizado por el Solicitante.
Se emitirá un certificado ante una solicitud de renovación.

4.3.2.- Notificación de emisión

La notificación de la emisión se realiza presencialmente durante el proceso de emisión.

4.4.- ACEPTACIÓN DEL CERTIFICADO

4.4.1.- Conducta constitutiva de la aceptación de un certificado

La descarga del certificado importará su aceptación por parte del Suscriptor asumiendo, en consecuencia, la absoluta y exclusiva responsabilidad por su utilización y por los daños emergentes que la no observancia de la regulación pudiera implicar, desde la fecha de su emisión.

4.4.2.- Publicación del Certificado por el Certificador Licenciado Provincial

Inmediatamente de emitido un certificado digital, el mismo es publicado en el repositorio de FDSL.

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

No aplicable.

4.5.- USO DEL PAR DE CLAVES Y DEL CERTIFICADO

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

Según lo establecido en el artículo 25 de la Ley Nº 25.506 (conforme lo dispuesto en el artículo 1º de la Ley Nº V-0509-2007) y en el artículo 36 del Decreto N° 0428-MP-2008, el suscriptor debe:

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

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

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

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

De acuerdo a lo establecido en la presente Resolución el Suscriptor debe:

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

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

Los Terceros Usuarios deben:

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

b) Rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda y de usarlo conforme a los Términos y Condiciones con Terceros Usuarios;

c) Verificar la validez del certificado digital.

4.6.- RENOVACION DEL CERTIFICADO SIN GENERACION DE UN NUEVO PAR DE CLAVES

No aplica.

4.7.- RENOVACION DEL CERTIFICADO CON GENERACION DE UN NUEVO PAR DE CLAVES

➢ **CLASE I. Autenticación de Servidores**

El proceso de renovación debe ser iniciado exclusivamente por el Solicitante, quien es la persona debidamente autorizada por su organización para solicitar un certificado y actuar como custodio de las claves privadas de dicha organización.

El Solicitante deberá generar una solicitud de firma de certificado (CSR) en el servidor donde se encuentra instalado el certificado a renovar.

Luego deberá realizar el pedido de renovación en el sitio web de FDSL donde deberá indicar el número de serie del certificado a renovar e ingresar la solicitud generada.

El certificado a renovar debe ser válido, debe encontrarse en el período permitido para su renovación y los datos del campo Asunto o Subject deben coincidir con los datos de la solicitud.

Una vez completado el formulario, el Solicitante recibirá un correo electrónico en el que se le hará saber el Número de Solicitud que le fue asignado y el detalle de la documentación que deberá presentar ante FDSL dentro de los diez (10) días hábiles subsiguientes, la que deberá estar firmada por el representante legal de la organización debidamente legalizada.

La validación satisfactoria de la documentación importará la aprobación de la renovación del certificado lo cual le será informado al Solicitante a través de un correo electrónico que contendrá un código de

renovación. El solicitante deberá ingresar a la página web de FDSL donde se le solicitará para la descarga del certificado el número de solicitud y el código de renovación.
En cambio, si al momento de la validación de la documentación resulta que la misma no es completa o es insuficiente, se procederá a la suspensión del trámite. En este caso, se informará al Solicitante acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de la documentación. El Solicitante tendrá un plazo de treinta (30) días para proveer la información complementaria que se le solicite, vencido el cual deberá reiniciar el proceso de solicitud de renovación de certificado, efectuando un nuevo requerimiento de renovación.

4.8.- MODIFICACION DEL CERTIFICADO

El suscriptor se encuentra obligado a notificar al Certificador Provincial cualquier cambio en alguno de los datos contenidos en el certificado digital, que hubiera sido objeto de verificación, de acuerdo a lo dispuesto en el inciso d) del artículo 25 de la Ley N° 25.506 (conforme el art. 1º de Ley Nº V-0591-2007) y en el artículo 36 inciso 4) del Decreto Nº 0428-MP-2008. En cualquier caso procede la revocación de dicho certificado y, de ser requerido, la emisión de uno nuevo.

4.9.- SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS

Los certificados serán revocados de manera oportuna y sobre la base de una solicitud de revocación de certificado validada.
El estado de suspensión de los certificados de clave pública no se encuentra previsto en la normativa que rige la materia, Ley Nº 25.506, de conformidad con lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.9.1.- Causas de la revocación

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

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación (según si, la Política, contempla la emisión de certificados digital a favor de personas humanas o jurídicas).
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por Resolución de la Autoridad de Aplicación.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se hallan comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
- Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política de Certificación, del Manual de Procedimientos, de la normativa provincial vigente en materia de firma digital.
- Por revocación de su propio certificado digital.

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

4.9.2.- Autorizados a pedir revocación

Sólo pueden pedir la revocación de un certificado:

a) El Suscriptor del certificado;
b) Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización;
c) Los Terceros Autorizados: El Responsable de Firma Digital, quien ostenta poder o facultad suficiente en representación de una persona jurídica;
d) FDSL;
e) Las Autoridades de Registro;
f) La Autoridad de Aplicación del régimen de firma digital;
g) La Autoridad judicial competente.
h) Por solicitud de un tercero que ostente un derecho subjetivo o interés legítimo, bajo su exclusiva responsabilidad.

4.9.3.- Procedimiento para la solicitud de revocación

Producida una causa de revocación del certificado, el Suscriptor del certificado, o bien alguno de los autorizados, deben comunicarlo a la Autoridad de Registro ante quien se hubiera realizado la validación de la identidad del Suscriptor o ante FDSL, a través de alguna de las siguientes vías de contacto disponibles:

a) A través del sitio web de FDSL:

Esta vía de revocación estará disponible las veinticuatro (24) horas del día, los siete (7) días de la semana. Sólo podrá ser utilizada por el Suscriptor de un certificado de clave pública. En este caso el suscriptor deberá ingresar al sitio web de FDSL (www.firmadigital.sanluis.gov.ar), seleccionar esta Política de Certificación y entre las opciones disponibles, optar por "Revocar un certificado digital", luego puede solicitar la revocación de su certificado ingresando el número de documento y el PIN de revocación que le fue informado mediante correo electrónico al momento de le emisión del mismo certificado.

b) A través de una nota de solicitud firmada digitalmente, remitida por correo electrónico a FDSL:

Esta vía de revocación podrá ser utilizada por los terceros autorizados conforme lo dispuesto en el Punto 4.9.2 de la Presente Política. El texto de la nota de solicitud debe incluir: los datos de identificación del certificado digital, y la expresión de la causa que origina el pedido de revocación. Tanto el mail como la nota de solicitud, deberá ser dirigido al Responsable de la Autoridad de Registro -quien deberá cumplir el trámite de revocación del certificado-, indicando claramente en el Asunto del correo la leyenda: "Solicitud de Revocación de Certificado de Clave Pública".

Este requerimiento podrá realizarse únicamente en días y horas hábiles de la Administración Pública Provincial. De haber sido remitido el mail en un día o en un horario fuera del establecido, se tendrá por solicitada la revocación la primera hora hábil del primer día hábil siguiente al de realizado el pedido vía correo electrónico.

c) Personalmente:

Esta vía de revocación podrá ser utilizada por el Suscriptor o por los terceros autorizados ante la Autoridad de Registro o FDSL. Deberán acreditar su identidad y rol invocado.

En ambos casos, deberá labrarse un Acta en la que se dejará constancia de los datos del Solicitante que requiere la revocación del certificado y la causa. La misma deberá ser suscripta por el requirente y el responsable de la Autoridad de Registro o FDSL, debiendo cada uno de ellos conservar un ejemplar de la misma.

Este requerimiento podrá realizarse únicamente en días y horarios hábiles, conforme el calendario de la Autoridad de Registro ante la que se presenta el interesado

d) A través de una actuación en el sistema de gestión:

Cuando la revocación es solicitada por personal de FDSL o una Autoridad de Registro porque tomaron

conocimiento que acaeció alguna de las causales de revocación, deberán hacerlo a través del sistema de gestión de expedientes dejando constancia del motivo y firmando digitalmente la actuación con el certificado digital que acredita el rol que enviste.

En todos los casos:
a) El solicitante de la revocación debe identificarse y acompañar la documentación correspondiente.
b) Las solicitudes de revocación, así como toda acción efectuada por FDSL o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.
c) Se documentan y archivan las justificaciones de las revocaciones aprobadas.
d) Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se incluye en la próxima lista de certificados revocados a ser emitida.
e) El suscriptor del certificado revocado es informado del cambio de estado de su certificado.

4.9.4.- Plazo para la solicitud de revocación
El Suscriptor de un certificado debe requerir su revocación en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1 de esta Política de Certificación.

El servicio de recepción de solicitudes de revocación está disponible en forma permanente los siete (7) días de la semana, durante las veinticuatro (24) horas del día a través de la página web.
La solicitud recibida será procesada de inmediato, conforme lo exigido por la normativa vigente.

4.9.5.- Plazo para el procesamiento de la solicitud de revocación
El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado indicando que la revocación ha sido puesta a disposición de los terceros usuarios, no superará en ningún caso las VEINTICUATRO (24) horas.

4.9.6.- Requisitos para la verificación de la Lista de Certificados Revocados
Los terceros usuarios deben verificar la validez de los certificados digitales emitidos por FDSL, utilizados. Para ello los Terceros podrán realizar cualquiera de las siguientes acciones:
a) Utilizando la Lista de Certificados Revocados
Verificar que el certificado digital correspondiente al documento firmado, no se encuentre incluido en la Lista de Certificados Revocados publicada en el siguiente sitio:
http://fd01.firmadigital.sanluis.gov.ar/fds/servidores.crl
y alternativamente, en:
http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl

Verificar la autenticidad de la Lista de Certificados Digitales, mediante la verificación de la firma digital de la AC-FDSL que la emite y de su período de validez.
Si no se pudiera obtener una CRL actualizada, se deberá optar entre rechazar el documento firmado digitalmente o aceptarlo, bajo exclusiva responsabilidad de quien consulta.
b) Utilizando el servicio de consulta basado en el protocolo de comunicación OCSP.

4.9.7.- Frecuencia de emisión de listas de certificados revocados
FDSL mantiene publicada una Lista de Certificados Revocados en forma permanente, efectuando su actualización cada VEINTICUATRO (24) horas.
Sin perjuicio de ello, toda vez que se produce una revocación, FDSL emite una Lista de Certificados Revocados actualizada en un plazo máximo de veinticuatro (24) horas de aceptada la solicitud. Dicha Lista indica claramente la fecha y la hora de la última actualización.
La Lista de Certificados Revocados es suscripta por la AC-FDSL.
El acceso a las Listas de Certificados Revocados es público, no pudiendo establecerse ninguna clase de

restricción. Se encuentra disponible en el sitio web de FDSL en el siguiente:
http://fd01.firmadigital.sanluis.gov.ar/fds/servidores.crl y alternativamente, en:
http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl

4.9.8.- Vigencia de la lista de certificados revocados
La vigencia de cada Lista de Certificados Revocados es de VEINTICUATRO (24) horas.

4.9.9.- Disponibilidad del servicio de consulta sobre revocación y de estado de certificado
La verificación del estado de los certificados puede realizarse indistintamente, a través del servicio de consulta basado en el protocolo de comunicación OCSP (http://ocsp.firmadigital.sanluis.gov.ar/ocsp) o de la consulta de las Listas de Certificados Revocados, disponibles de manera permanente y gratuita en el sitio web:
http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl y alternativamente, en:
http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl

4.9.10.- Requisitos para la verificación en línea del estado de revocación
Para utilizar el servicio de consulta basado en el protocolo de comunicación OCSP es necesario poseer conexión a internet.

4.9.11.- Otras formas disponibles para la divulgación de la revocación
Excepto por los casos mencionados en los apartados anteriores, no existen otras formas utilizadas por FDSL para divulgar la información sobre revocación de certificados.

4.9.12.- Requisitos específicos para casos de compromiso de claves
El Suscriptor debe informar inmediatamente a FDSL ante cualquier situación que involucre el compromiso de su clave privada, o el medio en que se encuentra almacenado, conforme los medios establecidos en el punto 4.9.3. de la presente Política “Procedimiento para la solicitud de revocación”.

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

4.9.14.- Autorizados a solicitar suspensión
El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.9.15.- Procedimientos para la solicitud de suspensión
El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.9.16.- Límites del período de suspensión del certificado
El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

4.10.- ESTADO DEL CERTIFICADO

4.10.1.- Características técnicas
La verificación del estado de los certificados puede realizarse indistintamente a través del servicio de consulta basado en el protocolo de comunicación OCSP (http://ocsp.firmadigital.sanluis.gov.ar/ocsp) o de la consulta de las Listas de Certificados Revocados, disponibles de manera permanente y gratuita en el sitio web:

http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl y alternativamente, en:
http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl

4.10.2.- Disponibilidad del servicio
Se encuentra disponibles de manera permanente y gratuita en el sitio web los siete días de la semana, durante las veinticuatro horas del día, los 365 días del año, sujeto a un calendario de mantenimiento.

4.10.3.- Aspectos operativos
No aplica.

4.11.- DESVINCULACION DEL SUSCRIPTOR
Se dará por desvinculado de los servicios del Certificador al titular de un certificado en los siguientes casos:

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

4.12.– RECUPERACION Y CUSTODIA DE CLAVES PRIVADAS
FDSL no podrá bajo ninguna circunstancia realizar la recuperación o custodia de claves privadas de los titulares de certificados digitales, en virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 25.506 (conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007) y en el inciso 1) del artículo 34 del Decreto Nº 0428-MP-2008.
El suscriptor o el Responsable del certificado se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley nacional antes mencionada.

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

5.1.- CONTROLES DE SEGURIDAD FÍSICA
FDSL cuenta con controles de seguridad relativos a:
a) Construcción y ubicación de instalaciones.
b) Niveles de acceso físico.
c) Comunicaciones, energía y ambientación.
d) Exposición al agua.
e) Prevención y protección contra incendios.
f) Medios de almacenamiento.
g) Disposición de material de descarte.
h) Instalaciones de seguridad externas.

5.2.- CONTROLES DE GESTION
FDSL cuenta con controles de seguridad relativos a:
a) Definición de roles afectados al proceso de certificación.
b) Número de personas requeridas por función.
c) Identificación y autenticación para cada rol.
d) Separación de funciones.

5.3.- CONTROLES DE SEGURIDAD DEL PERSONAL
FDSL cuenta con controles de seguridad relativos a:
a) Calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, de seguridad, limpieza, etcétera.
b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.
d) Frecuencia de procesos de actualización técnica.
e) Frecuencia de rotación de cargos.
f) Sanciones a aplicar por acciones no autorizadas.
g) Requisitos para contratación de personal.
h) Documentación provista al personal, incluidas tarjetas y otros elementos de identificación personal.

5.4.- PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

FDSL mantiene políticas de registro de eventos, cuyos procedimientos se encuentran detallados en el Manual de Procedimientos.

Además, FDSL cuenta con procedimientos de auditoría de seguridad sobre los siguientes aspectos:

a) Tipo de eventos registrados. Debe respetarse lo establecido en el Anexo I Sección 3 de la Resolución N° 341-ACTySSL-2018.
b) Frecuencia de procesamiento de registros.
c) Período de guarda de los registros. Debe respetarse lo establecido en el inciso i) del artículo 21 de la Ley Nº 25.506 (conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007) y en el inciso10) del artículo 34 del Decreto Nº 0428-MP-2008 respecto a los certificados emitidos.
d) Medidas de protección de los registros, incluyendo privilegios de acceso.
e) Procedimientos de resguardo de los registros.
f) Sistemas de recolección y análisis de registros (internos vs. externos).
g) Notificaciones del sistema de recolección y análisis de registros.
h) Evaluación de vulnerabilidades.

5.5.- CONSERVACION DE REGISTRO DE EVENTOS

FDSL cuenta con políticas de conservación de registros, cuyos procedimientos están detallados en el Manual de Procedimientos.

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

Asimismo, FDSL cuenta con procedimientos de conservación y guarda de registros en los siguientes aspectos, que están detallados en el Manual de Procedimientos:

a) Tipo de registro archivado. De conformidad a lo establecido en el Anexo I Sección 3 de la Resolución N° 341-ACTySSL-2018.
b) Período de guarda de los registros.
c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso.
d) Procedimientos de resguardo de los registros.
e) Requerimientos para los registros de certificados de fecha y hora.
f) Sistemas de recolección y análisis de registros (internos vs. externos).
g) Procedimientos para obtener y verificar la información archivada.

5.6.- CAMBIO DE CLAVES CRIPTOGRÁFICAS

El par de claves criptográficas de la AC de FDSL para esta Política tendrá una duración de treinta (30) años.

Las claves criptográficas de la Autoridad Certificante de FDSL son generadas con motivo del licenciamiento de la presente Política de Certificación y tendrán un tiempo operacional que coincide con el descripto en los campos “Válido Desde” y “Válido Hasta” de las mismas.

El cambio de par de claves criptográficas de la Autoridad Certificante de FDSL dará origen a la emisión de un nuevo certificado por parte de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis, operada por la Autoridad de Aplicación.

La publicación de la nueva clave pública de la Autoridad Certificante de FDSL para esta Política de Certificación se realiza en sus servidores, y se puede encontrar en el sitio web:

www.firmadigital.sanluis.gov.ar
Se mantiene el repositorio en línea durante las 24 horas, los 7 días de la semana.
Un año antes del vencimiento previsto del certificado de la Autoridad Certificante de FDSL se solicitará la renovación de la licencia de esta Política de Certificación y del certificado correspondiente.

5.7.- PLAN DE RESPUESTA A INCIDENTES Y RECUPERACION ANTE DESASTRES
Se describen los requerimientos relativos a la recuperación de los recursos del Certificador Licenciado Provincial en caso de falla o desastre. Estos requerimientos son desarrollados en el Plan de Continuidad de las Operaciones o Plan de Contingencia que permiten garantizar el mantenimiento mínimo de la operatoria y la recuperación de los recursos comprometidos dentro de las 24 horas de producida una emergencia. En ese caso, FDSL comunicará a los suscriptores si la infraestructura se encuentra trabajando en esa modalidad.

Se han desarrollado procedimientos referidos a:
a) Identificación, registro, reporte y gestión de incidentes.
b) Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.
c) Recuperación ante compromiso o sospecha de compromiso de la clave privada del certificador.
d) Continuidad de las operaciones en un entorno seguro luego de desastres.

Toda vez que FDSL utiliza servicios de infraestructura tecnológicos prestados por un tercero, prevé dentro de su Plan de Continuidad de Operaciones los procedimientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

5.8.- PLAN DE CESE DE ACTIVIDADES
Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del Certificador Licenciado Provincial o de una o varias de sus autoridades certificantes o de registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:
a) Notificación a la Autoridad de Aplicación Provincial, suscriptores, terceros usuarios, otros Certificadores y otros usuarios vinculados.
b) Revocación del certificado del Certificador Licenciado Provincial y de los certificados emitidos.
c) Transferencia de la custodia de archivos y documentación e identificación de su custodio.

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

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

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

6.1.- GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES CRIPTOGRÁFICAS

La generación e instalación del par de claves deben ser consideradas desde la perspectiva de las Autoridades Certificantes del Certificador Licenciado Provincial, de los repositorios, de las autoridades de registro y de los suscriptores.

6.1.1.- Generación del par de claves criptográficas

A) El par de claves criptográficas de la Autoridad Certificante de FDSL es generado en ambientes seguros, por personal autorizado, sobre dispositivos criptográficos homologados FIPS 140 Versión 2 para el nivel 3.

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

B) El par de claves criptográficas de la Autoridad de Registro es generado por su Responsable, el Oficial de Registro, utilizando un dispositivo criptográfico seguro que cumple con las características definidas en FIPS 140 Versión 2 para el nivel 2 o superior.

La Autoridad de Registro genera su clave mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

C) El par de claves criptográficas de los Suscriptores son generadas, protegidas y activadas en ambientes controlados y seguros.

Los Suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

6.1.2.- Entrega de la clave privada al suscriptor

Las claves privadas de los Suscriptores son generadas por ellos mismos en sus dispositivos criptográficos durante el proceso de solicitud, absteniéndose FDSL y los Oficiales de Registro de las AR de generar, exigir o por cualquier otro medio tomar conocimiento o acceder, a los datos de creación de firma de los suscriptores (incluyendo los roles vinculados a las actividades de registro), establecido por la Ley Nº 25.506, artículo 21, inciso b), conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007, y en el inciso 1) del artículo 34 del Decreto Nº 0428-MP-2008.

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

Durante el proceso de solicitud del certificado, la clave pública del Solicitante es entregada a la Autoridad Certificante de FDSL utilizando técnicas de prueba de posesión de la clave privada asociada. Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión" remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

Previamente, los solicitantes debieron haber probado su identidad y demás extremos requeridos por esta Política, y proceder a completar el "Formulario de Solicitud de Certificado" con la asistencia del Oficial de Registro de la ARR o FDSL, formulario en el cual se identifica la huella criptográfica de la solicitud.

6.1.4.- Disponibilidad de la clave pública del certificador

El certificado de la Autoridad Certificante de FDSL para esta Política de Certificación y los certificados de la Autoridad Certificante Raíz de la Provincia de San Luis, se encuentran disponibles en un repositorio en línea de acceso público a través de internet en la siguiente dirección
http://www.firmadigital.sanluis.gov.ar

La verificación de la validez de los certificados de los suscriptores de la presente Política, se realiza automáticamente a través del siguiente procedimiento:

1. Verificando la cadena de confianza del certificado del suscriptor, que es una cadena de firmas y de certificados, que se realiza de la siguiente manera:

- Verificar el certificado con que se firma el certificado del suscriptor: certificado de la Autoridad Certificante de FDSL para esta Política de Certificación y,

- Verificar el certificado con que se firma el certificado de la Autoridad Certificante de FDSL: certificados de la Autoridad Certificante Raíz de la Provincia de San Luis,

2. Verificando la vigencia y el estado de los certificados, a través de la consulta a las CRLs emitidas por la Autoridad Certificante de FDSL para esta Política de Certificación y por las Autoridades Certificantes Raíz de San Luis.

6.1.5.- Tamaño de claves

a) La Autoridad Certificante de FDSL utiliza claves RSA con un tamaño de 4096 bits.
b) Las Autoridades de Registro utilizan claves RSA con un tamaño mínimo de 2048 bits.
c) Los Suscriptores de certificados utilizan claves RSA con un tamaño mínimo de 2048 bits.

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

Los parámetros son:

Algoritmo: RSA
Exponente: 65537
Longitud: según se indica en el Punto 6.1.5.

No se requieren verificaciones particulares de la calidad de los parámetros de generación de claves, FDSL implementa en su portal de suscriptores estrictos controles de calidad durante el proceso de solicitud, emisión y publicación. El suscriptor deberá solicitar su certificado digital utilizando alguno de los modelos de dispositivos criptográficos homologados por FDSL.

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

Las claves criptográficas de los Certificados Clase I podrán ser utilizadas para firma digital, para firma de claves y para cifrado.
Las claves criptográficas de los Certificados Clase II podrán ser utilizadas para firma digital sin repudio.
Las claves criptográficas de los Certificados Clase III podrán ser utilizadas para firma digital sin repudio.

6.2.- CONTROLES DE INGENIERIA PARA PROTECCIÓN DE LA CLAVE PRIVADA Y DISPOSITIVOS CRIPTOGRAFICOS

La protección de la clave privada, considerada en este punto, se aplica para la Autoridad Certificante de FDSL, las Autoridades de Registro y los suscriptores.

6.2.1.- Controles y estándares para dispositivos criptográficos

a) La clave privada de la Autoridad Certificante de FDSL es generada y almacenada sobre un dispositivo criptográfico diseñado para tal fin que cumple con las características definidas en FIPS 140 versión 2, nivel 3;
b) Las claves privadas de las Autoridades de Registro son generadas y almacenada sobre dispositivos criptográficos diseñados para tal fin que cumplen con las normas FIPS 140-2 Nivel 2;
C) El par de claves criptográficas de los Suscriptores son generadas, protegidas y activadas en ambientes controlados y seguros.

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

La clave privada de la Autoridad Certificante es activada exclusivamente en las instalaciones de FDSL o en su sitio de contingencia, dentro del nivel de seguridad (nivel de operaciones críticas de la Autoridad Certificante). Para su activación deben estar presentes, por lo menos dos (2) funcionarios de la Autoridad de Aplicación del régimen provincial de firma digital, y dos (2), de FDSL.
Las Autoridades de Registro y los suscriptores de certificados deben tener sus propios dispositivos criptográficos y acceden a la clave privada a través de una contraseña que es de su exclusivo conocimiento.

6.2.3.- Recuperación de la clave privada

A) En caso de necesidad, FDSL posee procedimientos para la recuperación de su clave privada a partir de sus copias de respaldo, detallados en su Manual de Procedimientos de Certificación (Reservado).
Esta recuperación solo puede ser realizada por personal autorizado, sobre uno de los dispositivos criptográficos seguros de los que dispone FDSL y exclusivamente en los niveles de seguridad de la Autoridad Certificante en su sitio principal o de contingencia.
B) No se implementan mecanismos de resguardo y recuperación de la clave privada de la Autoridad de Registro, ni de los Suscriptores. En caso de compromiso de la clave privada, éstos deberán proceder a la revocación del certificado y tramitación de una nueva solicitud de emisión de certificado si así correspondiere.

6.2.4.- Copia de seguridad de la clave privada

A) FDSL realiza copias de la clave privada de su Autoridad Certificante inmediatamente después de su generación, por personal autorizado de FDSL y son almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3. Estos dispositivos son resguardados en un lugar de acceso restringido.
B) No se implementan mecanismos de copias de resguardo de la clave privada de las Autoridades de Registro ni de los suscriptores. FDSL garantiza que la seguridad de la clave no disminuye por la creación de copias de seguridad.

6.2.5.- Archivo de clave privada

Las copias de seguridad de la clave privada de la Autoridad Certificante de FDSL son conservadas en lugares seguros, al igual que sus elementos de activación, bajos los niveles de seguridad requeridos por la normativa vigente, garantizándose que su seguridad no disminuye por el proceso de archivo.

6.2.6.- Transferencia de claves privadas en dispositivos criptográficos

Las copias de resguardo de la clave privada de la Autoridad Certificante de FDSL están soportadas en dispositivos criptográficos homologados FIPS 140-2 nivel 3

6.2.7.- Almacenamiento de claves privadas en dispositivos criptográficos

Las claves privadas de las Autoridades de Registro y de los suscriptores son generadas y almacenadas en dispositivos criptográficos homologados FIPS 140-2 nivel 2 y no permiten exportación.

6.2.8.- Método de activación de claves privadas

A) La activación de la clave privada de la Autoridad Certificante de FDSL utiliza un esquema de control compartido (“M de N”), por lo que se necesita la intervención simultanea de varias personas autorizadas.
Para la activación de la clave privada de la Autoridad Certificante deben estar presentes, por lo menos dos (2) funcionarios de la Autoridad de Aplicación del régimen provincial de firma digital y dos (2) de FDSL.
Los responsables necesarios para la activación deberán identificarse frente al sistema según corresponda al rol asignado por medio de distintos mecanismos de autenticación.
B) La Autoridad de Registro tienen acceso a su clave privada y a su certificado contenidos en el dispositivo criptográfico a través de PIN/ contraseña o huella biométrica.
C) Los suscriptores pueden optar por acceder a su clave privada y a su certificado contenidos en el dispositivo criptográfico a través de PIN/contraseña o sin la misma.

6.2.9.- Método de desactivación de claves privadas

La desactivación de las claves privadas de la Autoridad Certificante de FDSL se realiza a través de procedimientos de desactivación de partición ante las siguientes situaciones: cuando se realicen tareas de mantenimiento que lo requieran y cuando sea necesario utilizar un equipamiento de respaldo.
Este procedimiento de excepción debe ser autorizado por el Director y deberá ser realizado por

personal técnico, de seguridad y funcionarios testigos que garanticen la operación.

6.2.10.- Método de destrucción de claves privadas
Una vez concluida la vida útil de la clave privada de la Autoridad Certificante, la partición del dispositivo criptográfico contenedor de esa clave privada será borrada e inicializada a cero. Esta tarea se realizará en el Sitio de Máxima Seguridad en una ceremonia preparada a ese efecto, con personal autorizado y con los procedimientos de seguridad establecidos.

6.2.11.- Requisitos de los dispositivos criptográficos
A) La capacidad del módulo criptográfico de la Autoridad Certificante es expresada en el cumplimiento como mínimo del estándar FIPS 140-2 nivel 3.
B) La capacidad del módulo criptográfico de las Autoridades de Registro es expresada en cumplimiento como mínimo del estándar FIPS 140-2 nivel 2.

6.3.- OTROS ASPECTOS DE ADMINISTRACIÓN DE CLAVES

6.3.1.- Archivo permanente de la clave pública
Los certificados emitidos a Suscriptores y a las Autoridades de Registro, como así también el de la Autoridad Certificante de FDSL, son almacenados y publicados bajo un esquema de redundancia y respaldados en forma periódica.
Todos los certificados son almacenados en soporte magnético, en formato estándar bajo codificación internacional DER. Las políticas y controles de seguridad implementados para recuperar la clave pública archivada, incluyendo el software y hardware, se hallan descriptos en el Plan de Contingencia.

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.
A) La clave privada asociada con el certificado digital de la Autoridad Certificante de FDSL tiene una validez de TREINTA (30) años, y se utilizará para firmar certificados de Suscriptores hasta DOS (2) años antes del vencimiento.
B) Todos los certificados Clase I emitidos por FDSL bajo la presente Política a favor de los Suscriptores tienen un período de vigencia de DOS (2) años, desde su fecha de emisión, siempre que dicho plazo no exceda el período de uso del certificado de la Autoridad Certificante de FDSL actuando como Certificador Licenciado Provincial. Esta información consta expresamente en el certificado.
C) Todos los certificados Clase II emitidos por FDSL bajo la presente Política a favor de los Suscriptores tienen un período de vigencia de DIEZ (10) años, desde su fecha de emisión, siempre que dicho plazo no exceda el período de uso del certificado de la Autoridad Certificante de FDSL actuando como Certificador Licenciado Provincial. Esta información consta expresamente en el certificado.
D) Todos los certificados Clase III emitidos por FDSL bajo la presente Política a favor de los Suscriptores tienen un período de vigencia de VEINTICINCO (25) años, desde su fecha de emisión, siempre que dicho plazo no exceda el período de uso del certificado de la Autoridad Certificante de FDSL actuando como Certificador Licenciado Provincial. Esta información consta expresamente en el certificado.

Transcurrido los plazos mencionados, el certificado expirará automáticamente, perdiendo toda validez.
En tal caso, el Suscriptor debe gestionar uno nuevo, para lo cual iniciará el correspondiente proceso de solicitud de emisión.

6.4.- DATOS DE ACTIVACIÓN
Se entiende por datos de activación, a diferencia de las claves, a los valores requeridos para la operatoria de los dispositivos criptográficos y que necesitan estar protegidos.

Se establecen medidas suficientes de seguridad para proteger los datos de activación requeridos para la operación de los dispositivos criptográficos de los usuarios de certificados

6.4.1.- Generación e instalación de datos de activación

A) Los datos de activación de las claves privadas de la AC FDSL utilizan un esquema de control compartido ("M de N") conforme lo previsto en el Punto 6.2.2.-Control M de N de la clave privada - de la presente Política.

B) Como paso previo a la generación de claves, los Suscriptores y los Responsables de las Autoridades de Registro deberán establecer una clave de seguridad sobre el dispositivo denominado PIN/contraseña o en caso de estar disponible, su huella biométrica. Esta clave de seguridad debe cumplir los requisitos establecidos en la Política de Seguridad y es conocida solo por el Suscriptor, protege su clave privada e impide el acceso a la misma por parte de terceros, incluida la Autoridad Certificante de FDSL.

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. Asimismo, las personas responsables de su custodia no deben divulgar su condición.

Los Suscriptores son responsables de la custodia de sus dispositivos criptográficos y de la no divulgación de sus claves, contraseñas y PIN de acceso.

Ni FDSL, ni la Autoridad de Registro Central, ni las Autoridades de Registro Delegadas implementan mecanismos de respaldo de contraseñas de la clave privada ni de la contraseña de acceso al dispositivo criptográfico de Autoridad de Registro ni de Suscriptores.

Los datos de activación de la clave privada de la Autoridad Certificante de FDSL están protegidos por mecanismos de seguridad implementados en el nivel 6 del Sitio de Máxima Seguridad.

6.4.3.- Otros aspectos referidos a los datos de activación

No es Aplicable.

6.5.- CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1.- Requisitos técnicos específicos

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

Dichos requisitos se vinculan con los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación.
b) Separación de funciones entre los roles afectados al proceso de certificación.
c) Identificación y autenticación de los roles afectados al proceso de certificación.
d) Utilización de criptografía para las sesiones de comunicación y bases de datos.
e) Archivo de datos históricos y de auditoria del certificador y usuarios.
f) Registro de eventos de seguridad.
g) Prueba de seguridad relativa a servicios de certificación.
h) Mecanismos confiables para identificación de roles afectados al proceso de certificación.
i) Mecanismos de recuperación para claves y sistema de certificación.

6.5.2.- Requisitos de seguridad computacional

Los servidores que conforman la Autoridad Certificante de FDSL se encuentran alojados en el "Sitio de Máxima Seguridad" construido con los estándares requeridos para este tipo de ambientes.

Las certificaciones del módulo criptográfico HSM son las siguientes:

- FIPS 140-2 nivel 2 y nivel 3
- Common Criteria EAL4+

- Compatible con ePassport BAC y EAC

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

Por medio de controles llevados a cabo por el personal de FDSL, afectado a tareas de homologación de sistemas informáticos, se controla que el diseño se corresponda con la puesta en producción. Para ello FDSL cuenta con una infraestructura idéntica a la de producción para la prueba de los sistemas informáticos antes de realizar la puesta en producción.

6.6.1.- Controles de desarrollo de sistemas

FDSL utiliza estándares para el desarrollo y mantenimiento de la seguridad de sistemas informáticos basados en el modelo OWASP (Open Web Application Security Project).
FDSL cumple con procedimientos específicos para el diseño, desarrollo y prueba de los sistemas entre los que se encuentran:
- Separación de ambientes de desarrollo, homologación y producción.
- Control de versiones para los componentes desarrollados.
- Pruebas con casos de uso.

6.6.2.- Controles de gestión de seguridad

Se documenta y controla la configuración del sistema, así como toda modificación o actualización.
FDSL cumple con la separación de ambientes de desarrollo, prueba y producción.
Asimismo, FDSL cumple con el control de versiones para los componentes desarrollados y formaliza pruebas con caso de uso.

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

No aplica.

6.7.- CONTROLES DE SEGURIDAD DE RED

Los servicios de certificación de la Autoridad Certificante se realizan fuera de línea lo que asegura su protección de cualquier ataque a través de redes.
Los servicios de publicación de FDSL y de su Autoridad Certificante utilizan sistemas debidamente protegidos, garantizando su integridad.

6.8.- CERTIFICACION DE FECHA Y HORA

El servicio de emisión de sellos de tiempo de FDSL que podrá ser utilizado con los certificados emitidos en el marco de esta Política está basado en la especificación de los estándares RCF 3161 – “Internet X. 509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities, ETSI TS 101 861, “Time stamping profile” y a su especificación equivalente RFC 3628 – “Requirements for time-stamping authorities”.

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 InfrastructureCertificate and CRL Profile).

7.1.- PERFIL DEL CERTIFICADO

Se usarán los siguientes campos del formato X.509 versión 3 en el Certificado de la Autoridad Certificante de FDSL actuando como Certificador Licenciado Provincial:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Versión	V3
Número de Serie	Número asignado por la Autoridad Certificante de la Provincia de San Luis
Algoritmo de firma	Sha2RSA (SHA512)
Nombre distintivo del emisor	CN = ENTE LICENCIANTE SAN LUIS - ACRAIZ02 O = Gobierno de la Provincia de San Luis C = AR
Validez	30 años Se especifica desde/hasta
Nombre Distintivo del Suscriptor	CN = FDSL - AC Servidores y Servicios OU = Firma Digital San Luis O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = 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
Identificador de clave de entidad emisora	Contiene un identificador de la clave pública de la Autoridad Certificante del Ente Licenciante Provincial de la Provincia de San Luis
Uso de Claves Políticas de Certificación	Firma digital, Firma de certificados, Firma CRL sin conexión, Firma CRL
Políticas de Certificación	Política: 2.16.32.1.3.2.1.1.0 CPS: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/cps.pdf Notificación: Infraestructura de Clave Pública de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial Nº V-0591-2007.
Restricciones Básicas	CA = TRUE
Punto 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 del Emisor: http://fd01.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crt http://fd02.firmadigital.sanluis.gov.ar/entelicenciante/acr02.crt

Se usarán los siguientes campos del formato X.509 versión 3 en el **certificado Clase I** de los suscriptores de la Autoridad Certificante de FDSL para la "Política de Certificación para Firma Digital de Servidores Y Servicios - FDSL":

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Número de Serie	Número asignado por FDSL – AC Servidores y Servicios
Algoritmo de firma	sha2RSA (SHA256)
Nombre distintivo del emisor	CN = FDSL - AC Servidores y Servicios OU = Firma Digital San Luis O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = San Luis C = AR
Validez	2 años. Se especifica desde/hasta
Nombre distintivo del Suscriptor	CN = <Nombre de dominio> SERIALNUMBER = <CUIT> + <Número Documento> O = <Nombre de la Organización> OU = <Nombre del Área, Sector o Programa donde se aloja el servidor> S = <Provincia> C= <Nacionalidad del Suscriptor>
Clave pública del Suscriptor	La Clave Pública RSA no debe ser menor a 2048 bits
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la CA del FDSL como Certificador Licenciado
Identificador de la clave del Suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del Suscriptor
Uso de claves	Firma digital, Cifrado de clave, Cifrado de datos
Uso Extendido de Clave	TLS Web Client Authentication TLS Web Server Authentication 2.16.32.1.3.2.1.1.5
Políticas de Certificación	Política: 2.16.32.1.3.2.1.1.5 CPS: http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores - cps.pdf Notificación: Infraestructura de Clave Pública de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial N° V-0591-2007.
Nombre Alternativo del Sujeto	DNS: <Nombre de dominio>
Restricciones básicas	CA = FALSE Pathlen = 0
Puntos de distribución de la Lista de Certificados Revocados	http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
Información de Acceso de la	URL del Emisor:

Autoridad Certificante	http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crt http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crt URL OCSP: http://ocsp.firmadigital.sanluis.gov.ar/ocsp

Se usarán los siguientes campos del formato X.509 versión 3 en el **certificado Clase II** de los suscriptores de la Autoridad Certificante de FDSL para la "Política de Certificación para Firma Digital de Servidores Y Servicios - FDSL":

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Número de Serie	Número asignado por FDSL – AC Servidores y Servicios
Algoritmo de firma	sha2RSA (SHA256)
Nombre distintivo del emisor	CN = FDSL - AC Servidores y Servicios OU = Firma Digital San Luis O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = San Luis C = AR
Validez	10 años. Se especifica desde/hasta
Nombre distintivo del Suscriptor	CN = Servicio de Sellado de Tiempo – TSA FDSL+<número de secuencia> OU = Firma Digital San Luis OID… O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = San Luis C = AR
Clave pública del Suscriptor	La Clave Pública RSA no debe ser menor a 2048 bits
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la CA del FDSL como Certificador Licenciado
Identificador de la clave del Suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del Suscriptor
Uso de claves	Firma digital, Sin repudio
Uso Extendido de Clave	Time Stamping (1.3.6.1.5.5.7.3.8)
Políticas de Certificación	Política: 2.16.32.1.3.2.1.1.5 CPS: http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores - cps.pdf Notificación: Infraestructura de Clave Pública de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial N° V-0591-2007.
Restricciones básicas	CA = FALSE Pathlen = 0

Puntos de distribución de la Lista de Certificados Revocados	http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
Información de Acceso de la Autoridad Certificante	URL del Emisor: http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crt http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crt URL OCSP: http://ocsp.firmadigital.sanluis.gov.ar/ocsp

Se usarán los siguientes campos del formato X.509 versión 3 en el **certificado Clase III** de los suscriptores de la Autoridad Certificante de FDSL para la "Política de Certificación para Firma Digital de Servidores Y Servicios - FDSL":

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Número de Serie	Número asignado por FDSL – AC Servidores y Servicios
Algoritmo de firma	sha2RSA (SHA256)
Nombre distintivo del emisor	CN = FDSL - AC Servidores y Servicios OU = Firma Digital San Luis O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = San Luis C = AR
Validez	25 años. Se especifica desde/hasta
Nombre distintivo del Suscriptor	CN = Autoridad de Validación OCSP–FDSL+<número de secuencia> OU = Firma Digital San Luis O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = San Luis C = AR
Clave pública del Suscriptor	La Clave Pública RSA no debe ser menor a 2048 bits
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la CA del FDSL como Certificador Licenciado
Identificador de la clave del Suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del Suscriptor
Uso de claves	Firma digital, Sin repudio
Uso Extendido de Clave	OCSP Signing (1.3.6.1.5.5.7.3.9)
Extensón	OCSP No Revocation Checking (id-pkix-ocsp-nocheck / 1.3.6.1.5.5.7.48.1.5)
Políticas de Certificación	Política: 2.16.32.1.3.2.1.1.5 CPS: http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores -

	cps.pdf Notificación: Infraestructura de Clave Pública de la Provincia de San Luis, Argentina. Certificado emitido en el marco de la Ley Provincial N° V-0591-2007.
Restricciones básicas	CA = FALSE Pathlen = 0
Puntos de distribución de la Lista de Certificados Revocados	http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
Información de Acceso de la Autoridad Certificante	URL del Emisor: http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crt http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crt URL OCSP: http://ocsp.firmadigital.sanluis.gov.ar/ocsp

7.1.1.- NÚMERO DE VERSION
Todos los certificados emitidos corresponden al estándar X.509 y contienen el valor 2 correspondiente a la versión 3.

7.1.2. EXTENSIONES

7.1.2.1 Key Usage
El "keyUsage" indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Es una EXTENSIÓN CRÍTICA.

7.1.2.2 Extensión Políticas de Certificación
En la extensión de "Certificate Policies" (Politicas de Certificacion) detalla el nombre del dominio de la CA y el directorio creado para el Repositorio de dicho documento. Es una EXTENSIÓN CRÍTICA.
Se incluye OID de la Política de Certificación. Ese OID es asignado por la Autoridad de Aplicación.

7.1.2.3 Nombre Alternativo Del Sujeto
La extensión "subjectAltName", es una EXTENSIÓN NO CRÍTICA. Se define solamente para los certificados de Clase I. El valor contiene los nombres de dominios asociados al certificado.

7.1.2.4 Restricciones Básicas (Basic Constraints)
La extensión "BasicConstraints" permite identificar si el suscriptor de un certificado es un certificador e indica la longitud máxima de las rutas de certificación válidas que el certificado incluye. Esta extensión está presente en todos los certificados.
Los certificados de los suscriptores contienen los atributos "ca" con valor FALSE y PathLenConstraint=Null.

7.1.2.5 Uso de Claves Extendido (Extended Key Usage)
La extensión permite configurar los propósitos de la clave.
Para los certificados de Clase I la extensión NO ES CRÍTICA.
Para los certificados de Clase II la extensión ES CRITICA.
Para los certificados de Clase III la extensión NO ES CRITICA.

7.1.2.6 OCSP No Revocation Checking
La extensión "OCSP No Revocation Checking" es una EXTENSON NO CRITICA. Se define solamente para los certificados de Clase III. Esta extensión le indica al cliente que no revise el estado de revocación del

certificado y de esa forma evitar conflictos de resolución.

7.1.3. IDENTIFICADORES DE ALGORITMOS

El campo "signature" contiene el identificador de objeto (OID) del algoritmo y, si fueran necesarios, los parámetros asociados usados por el certificador para firmar el certificado. Este identificador será de los definidos en el [RFC4055] para RSA.

7.1.4. FORMATOS DE NOMBRE

Los formatos de nombres cumplen con lo establecido en el punto " 3.1.2. Necesidad de Nombres Distintivos" de esta Política de Certificación.

7.1.5. RESTRICCIONES DE NOMBRE

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con "3.1.4. Reglas para la interpretación de nombres" y "3.1.5. Unicidad de nombres" de esta Politica de Certificación.

7.1.6. OID DE LA POLITICA DE CERTIFICACION

La extensión "CertificatePolicies" incluye la información sobre la Política de Certificación necesaria para la validación del certificado.
Esta extensión está presente en todos los certificados y es una EXTENSION CRITICA.

7.1.7. SINTAXIS Y SEMANTICAS DE CERTIFICADORES DE POLITICA

El calificador de la política está incluido en la extensión de "certificate policies" y contiene una referencia al URL con la Politica de Certificación aplicable

7.1.9. SEMANTICA DE PROCESARIMIENTO PARA EXTENSIONES CRITICAS

Sin estipulaciones

7.2.- PERFIL DE LA LISTA DE CERTIFICADOS REVOCADOS

Las Listas de Certificados Revocados (CRL) correspondientes a la presente Política de Certificación serán emitidas conforme lo establecido en la especificación ITU X.509 versión 2:

X.509 v2 Certificado Atributos / Extensiones	Contenido
Atributos	
Versión	V2
Algoritmo de Firma	sha2RSA
Nombre Distintivo del Emisor	CN = FDSL - AC Servidores y Servicios OU = Firma Digital San Luis O = Agencia de Ciencia, Tecnología y Sociedad San Luis SERIALNUMBER = CUIT 30-71547080-9 S = 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 CRL
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 se emite una CRL

7.2.1. Número de Versión

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

7.2.2.1 – Identificación de Clave de la Autoridad Certificante (Authority Key Identifier)

La extensión "AuthorityKeyIdentifier" proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL.
Esta extensión está presente en todas las Listas de Certificados Revocados.

7.2.2.2 - Número de CRL (CRL Number)

La extensión "CRLNumber" contiene un número de secuencia creciente para una CRL y emisor dado. Esta extensión permite que los usuarios determinen fácilmente cuándo una CRL particular reemplaza otra CRL.
Esta extensión se encuentra en todas las Listas de Certificados Revocados.

7.2.2.3 – Punto de Distribución del Emisor (Issuing Distribution Point)

La extensión "IssuingDistributionPoint" identifica el punto de distribución y el alcance de una CRL particular. Esta extensión es CRITICA.

7.3.- PERFIL DE LA CONSULTA EN LINEA DEL ESTADO DEL CERTIFICADO (OCSP)

El formato de las consultas en línea del estado del certificado se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Se implementa conforme a lo indicado en la especificación RFC 5019 Estas consultas se utilizan para determinar el estado de un certificado digital como método alternativo a la Lista de Certificados Revocados.

7.3.1.- Consultas OCSP

Los siguientes datos se encuentran presentes en las consultas:

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

Ejemplo de Consulta:
Obtener la URL de OCSP de un certificado:
openssl x509 -noout -ocsp_uri -in certificate.crt http://prueba-ocsp.firmadigital.sanluis.gov.ar/ocsp
Con el certificado, el certificado de la AC FDSL y la URL realizar la consula
openssl ocsp -no_nonce -issuer servidores.crt -cert certificate.crt -text -url http://prueba-ocsp.firmadigital.sanluis.gov.ar/ocsp
OCSP Request Data:
Version: 1 (0x0)
Requestor List:
Certificate ID:
Hash Algorithm: sha1
Issuer Name Hash: A2EB2E000478EAB40EBB0FBAE6F464A29BDC8E5F
Issuer Key Hash: C8693358E8771A23FED331F26710B67810E62BF8

Serial Number: 65000000057632CEE2AB2F156C000000000005

7.3.2. - Respuestas OCSP

Todas las respuestas OCSP se encuentran firmadas digitalmente por la Autoridad Certificante de FDSL actuando como Certificador Licenciado Provincial para la "Política de Certificación para Firma Digital de Servidores y Servicios".

La respuesta OCSP contiene los siguientes datos:

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

7.4.- PERFIL DE LA CONSULTA DE SELLADO DE TIEMPO (TSA)

7.4.1. – Solicitud de Sellos de tiempo

Las solicitudes de sellos se adherirán a la sintaxis de la especificación "*RFC3161 Time Stamp Protocol (TSP*)".

Los pasos para generar un sello de tiempo son los siguientes:

• El Solicitante calcula el hash utilizando el algoritmo SHA-1 o SHA-256 del documento a sellar

• El Solicitante envía una solicitud de sello de tiempo a una URL determinada de FDSL siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar

• FDSL recibe la petición, revisa si la si la petición está completa y correcta.

• Si el resultado es correcto, la TSA firma la petición generando un Sello de Tiempo (incluyendo el hash del documento, la fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA).

• El sello de tiempo se envía de vuelta al solicitante

• El Solicitante debe validar la firma del sello y custodiarlo debidamente.

La URL del servicio de Sellado de Tiempo se encontrará denunciada en el correspondiente Convenio de Servicio de Sellado de Tiempo.

7.4.2.- Respuesta a la solicitud de Sellos de tiempo

Si la solicitud no se puede procesar, se devuelve una respuesta http indicando un código de error cuando no puede responder con un time stamp. Los posibles errores son:

Causa	Descripción
Cliente envía petición GET	METHOD NOT VALID
Falta el campo content-length	CONTENT_LENGTH REQUIRED
Content-length demasiado grande	REQUEST ENTITY TOO LARGE
Content-type incorrecto	UNSUPORTED MEDIA TYPE
Los datos no son un time stamp request	BAD REQUEST
El servidor no responde	SERVER INTERNAL ERROR

Las respuestas se envían en el siguiente formato:

Content type: application/timestamp-reply
Method: POST
Content-length: required

<< Contiene la respuesta de sello de tiempo en ASN.1, codificado en DER>>

8.- AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

La Agencia de Ciencia, Tecnología y Sociedad San Luis, en su rol de Ente Licenciante, realiza auditorías ordinarias al Certificador, a la Autoridad Certificante de FDSL y a sus Autoridades de Registro, a fin de verificar el cumplimiento de los requisitos de licenciamiento.

Esas auditorías tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener y mantener la condición de Certificador Licenciado Provincial, la correcta aplicación de lo dispuesto en las políticas y procedimientos aprobados por el Ente Licenciante para la presente Política de Certificación. Ello, conforme surge de lo dispuesto en la Ley Provincial Nº V-0591-2007, el Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018, la Resolución Nº 34-ASLCTyS-2017 y la Resolución Nº 341-ACTySSL-2018.

Los principales temas a evaluar en esas auditorías son:

- Requisitos legales generales
- Política de Certificación y Manual de Procedimientos de Certificación
- Plan de Seguridad
- Plan de Cese de Actividades
- Plan de Contingencia
- Plataforma Tecnológica
- Ciclo de vida de las claves criptográficas del Certificador Provincial
- Ciclo de vida de los certificados de suscriptores
- Estructura y contenido de los certificados y CRLs
- Mecanismos de acceso a la documentación publicada, certificados y CRLs
- Guía de Instalación y funcionamiento de las Autoridades de Registro

Asimismo, FDSL conforme la cantidad de certificados emitidos y el nivel de satisfacción en su desempeño, realiza auditorías mensuales, bimestrales o trimestrales a sus Autoridades de Registro Delegadas aplicando el criterio de auditoría: Norma ISO 19011:2011. El objetivo y alcance de estas auditorías es:

- Evaluar la confiabilidad y calidad de los sistemas utilizados; la integridad, confidencialidad y disponibilidad de los datos.
- Evaluar el cumplimiento de las especificaciones del Manual de Procedimientos.
- Evaluar los procedimientos y métodos de la emisión del certificado de Política de Certificación del Instituto Firma Digital de San Luis.
- Identificar áreas potenciales de mejoras en el proceso de emisión.
- Verificar la corrección de las No Conformidades detectadas en auditorias anteriores y verificación de los procedimientos de las nuevas emisiones.

Alcance:

- Verificar el cumplimiento de los procesos y procedimientos, corregir, actualizar y/o modificar aquellos que en la actualidad no se ajustan a la conformidad con la Política de Certificación.
- Se evalúa la totalidad de los Oficiales de Registro de las Autoridades de Registro Delegadas y la totalidad de los expedientes en los que han intervenido.

Los auditores deben considerar si la información entregada en los documentos es:

- completa (todo el contenido esperado se encuentra en el documento);
- correcta (el contenido está conforme con otras fuentes confiables tales como normas y regulaciones);
- consistente(eldocumentoesconsistenteconsigomismoycondocumentosrelacionados);
- actual (el contenido está actualizado);
- los documentos que están siendo revisados cubren el alcance de auditoría y proveen suficiente información para soportar los objetivos de la auditoría;

- el uso de tecnologías de información y comunicación, dependiendo de los métodos de auditoría, promueve una realización eficiente de la auditoría: se debe tener cuidado específico para seguridad de la información debido a regulaciones aplicables sobre protección de datos (en particular para información que está fuera del alcance de la auditoría pero que está contenida en el documento)

En caso de dictámenes no favorables con relación a las Autoridades de Registro, FDSL implementa medidas correctivas. Asimismo, FDSL se reserva en forma exclusiva la facultad de proceder a retirar o suspender la actividad de la Autoridad de Registro que hubiera constituido y que no se allane a la observancia y cumplimiento de la normativa jurídica vigente, mediante una verificación o constatación previa, en la que se acredite la persistencia en la inobservancia y/o inejecución de las medidas correctivas indicadas para sanear las No Conformidades registradas.

El Instituto FDSL realizó la certificación internacional de las Normas ISO 9001:2015, que mantiene anualmente.

Se cumplen las exigencias reglamentarias impuestas por:

- El artículo 33 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma Ley, relativo a la publicación de informes de auditoría.
- Los artículos 19 a 21 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría.

La información relevante de los informes de las últimas auditorías es publicada en el sitio de publicación de FDSL.

9.- ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1.- ARANCELES

La solicitud, emisión y revocación de los certificados de clave pública CLASE I y la prestación de los servicios de Sellado de Tiempo a los que se refiere la presente Política de Certificación se encuentran en el Tarifario de FDSL. Esta Lista se publica en www.firmadigital.sanluis.gov.ar.
La solicitud de revocación de los certificados, por cualquiera de los medios admitidos en esta Política, será gratuita.

9.2.- RESPONSABILIDAD FINANCIERA

El Certificador Licenciado Provincial es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de esta Política de Certificación, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá a FDSL demostrar que actuó con la debida diligencia.
El Certificador Licenciado Provincial es responsable con los alcances establecidos en el apartado anterior, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del Certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisión.

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

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la legislación (de existir, enunciar supuestos);
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

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

9.3.- CONFIDENCIALIDAD

Todos los datos correspondientes a las personas humanas a las cuales alcance esta Política de Certificación, están sujetas a lo establecido en la Ley N° 25.326 de Protección de Datos Personales.
Toda información referida a los Suscriptores de certificados, que haya sido recibida por FDSL durante el proceso de emisión o renovación de un certificado, 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 en un proceso administrativo. La exigencia se extiende a toda otra información, referida a los Suscriptores de certificados, a la que FDSL o la Autoridad de Registro tenga acceso durante el ciclo de vida de los certificados emitidos, así como cualquier otra información vinculada a su operatoria.

9.3.1.- Información Confidencial

La protección abarca a la siguiente información, en la medida en que no sea de conocimiento público:
a) Toda la información remitida por el Suscriptor a la Autoridad de Registro, excepto los datos que figuran en el certificado.
b) Cualquier información almacenada en servidores o bases de datos destinadas a firma digital.
c) Cualquier información impresa o transmitida en forma verbal referida a procedimientos y otros, salvo aquellos que en forma expresa fueran declarados como no confidenciales.
d) Cualquier información referida a planes de contingencia, controles o procedimientos de seguridad, registros de auditoría creados y/o mantenidos por FDSL.
El listado precedente es de carácter meramente enunciativo, resultando confidencial toda información del proceso de firma digital que expresamente no señale lo contrario. La regla general es que toda información que no sea considerada como pública revestirá carácter confidencial.

Durante el ciclo de vida del certificado, FDSL y sus Autoridades de Registro no podrán divulgar los datos de los suscriptores sin su consentimiento. Asimismo, FDSL se compromete a hacer público exclusivamente ellos datos del suscriptor que resulten imprescindibles para el reconocimiento de su firma digital.
Se declaran expresamente confidenciales:
- La clave privada de la Autoridad Certificantes de FDSL.
- Las claves privadas de los solicitantes y suscriptores. Para garantizar su confidencialidad las claves son generadas por el propio solicitante y almacenadas en dispositivos criptográficos que cumplen con los estándares exigidos en la presente Política de Certificación. En ningún caso FDSL ni las Autoridades de Registro tendrán la posibilidad de generar, almacenar, copiar o conservar información que permita reconstruir o activar las claves privadas de los suscriptores.

9.3.2.- Información NO Confidencial

Se considera “No Confidencial” la siguiente información:
a) La información incluida en los certificados y en las Listas de Certificados Revocados;
b) La información sobre personas físicas o jurídicas, que se encuentre disponible en certificados o en directorios y sitios de publicación de acceso público;
c) La información pertinente de los informes de auditorías;

d) La información que hubiera sido previamente conocida por FDSL;
e) La información legítimamente obtenida de terceros;
f) La información publicada por el Suscriptor con posterioridad al momento de su difusión.
g) La causa de revocación de los certificados;

Tampoco se considera confidencial la información incluida en los siguientes documentos emitidos por FDSL:
a) Esta Política de Certificación y el Manual de Procedimientos de Certificación (en sus aspectos públicos);
b) El Acuerdo con los Suscriptores de Certificados;
c) Los Términos y Condiciones con Terceros Usuarios;
d) La Política de Privacidad de FDSL;
e) Secciones Públicas de la Política de Seguridad de FDSL.

9.3.3.- Responsabilidades de los roles involucrados

Los roles del Certificador Licenciado Provincial se hallan descriptos en el documento "Roles y Funciones", que define las principales funciones, responsabilidades, obligaciones y tareas que cubren donde se detalla para aquellos que gestionan información confidencial las responsabilidades pertinentes con el fin de evitar su compromiso o divulgación a personas no autorizadas.

FDSL no es responsable por el uso indebido que los Suscriptores pudieran darle a los certificados de servidor seguro ni el Solicitante del servicio de sellado de tiempo.

9.4. - PRIVACIDAD

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

9.5.- DERECHOS DE PROPIEDAD INTELECTUAL

FDSL es propietaria exclusiva de todos los derechos de propiedad intelectual de la presente Política, acuerdos, declaraciones, procedimientos y documentos auxiliares referidos a la Autoridad Certificante de FDSL, así como la documentación y contenidos del sitio disponible en www.firmadigita.sanluis.gov.ar
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 FDSL.

9.6.- RESPONSABILIDADES Y GARANTIAS

Conforme lo previsto por el artículo 41 del Decreto Nº 0428-MP-2008, FDSL es responsable aun en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho de FDSL de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.
FDSL será responsable, en caso de corresponder, ante terceros por el incumplimiento de las previsiones de la Ley Provincial Nº V-0591-2007, el Decreto Reglamentario Nº 0428-MP-2008 modificado por Decreto N° 6011-MCTyS-2018, y toda otra normativa aplicable, respecto a los procedimientos que respaldan la emisión de certificados, por los errores u omisiones en los certificados por él emitidos y por su falta de revocación en la forma y plazos previstos. Es su responsabilidad demostrar que actuó con la debida diligencia.

Las Autoridades de Registro son responsables por todos los trámites de emisión, renovación y revocación de certificados en los que toman intervención.
Conforme lo previsto por el artículo 41 del Decreto Nº 0428-MP-2008, FDSL es responsable aun en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho de

FDSL de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

Los Suscriptores son responsables por el uso y protección de los certificados de los que son titulares, de proveer información verdadera para su emisión y revocación, de solicitar la revocación de su certificado cuando hubiera acaecido algunas de las causales de revocación previstas expresamente en la normativa vigente, y en esta Política de Certificación, en particular.

Asimismo, los organismos a los que los Suscriptores se encuentran vinculados y dan fe de su relación a través de la Nota de Solicitud de Emisión de Certificados, son responsables de solicitar la revocación del certificado del suscriptor cuando tomaran conocimiento de alguna de las causales de revocación.

Sin perjuicio de lo expuesto cabe aclarar que:
- La relación entre el Certificador Licenciado Provincial y los Suscriptores se rige por el Acuerdo con Suscriptores que ambos celebran además de lo dispuesto en esta Política.
- La relación entre el Certificador Licenciado Provincial y las Autoridades de Registro Delegadas, se rige por los Convenios de Constitución celebrados entre ambos además de lo dispuesto en esta Política.
- La relación entre el Certificador Licenciado Provincial y el organismo que incorpora el uso de certificados de clave pública en su operatoria, se rige por el Convenio o Acta celebrado entre ambos además de lo dispuesto en esta Política.

GARANTIAS

Además de lo previsto en esta Política de Certificación, el Certificador Licenciado Provincial debe garantizar:
- Que no se presenten distorsiones en la información contenida en los certificados o en su emisión,
- Que los certificados reúnen los requerimientos exigidos en esta Política de Certificación.

Además de lo previsto en esta Política de Certificación, la Autoridad de Registro debe garantizar:
- Que no se presenten distorsiones en la información contenida en los certificados o en su emisión,
- Que no se presentan errores en la información del certificado que fue presentada a la AR
- Que los dispositivos, equipamientos y materiales requeridos cumplen con lo dispuestos en esta Política de Certificación.

Además de lo previsto en esta Política de Certificación, los Suscriptores deben garantizar:
- Que cada firma digital creada usando la clave privada corresponde a la clave pública listada en el certificado,
- Que la clave privada está debidamente protegida por un pin/contraseña a la que nadie más que él tiene acceso,
- Que toda la información facilitada a la Autoridad de Registro o a FDSL y contenida en el certificado es verdadera
- Que el certificado es utilizado exclusivamente para los propósitos autorizados.

Asimismo los terceros usuarios deben garantizar:
- Que exclusivamente aceptarán documentos firmados digitalmente siempre que hayan cumplido los recaudos exigidos en el Punto 4.5.2 de la presente Política de Certificación.

9.7.- DESLINDE DE RESPONSABILIDADES

No cabe responsabilidad alguna para FDSL, en caso de utilización no autorizada de un certificado digital, 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 establecidos, deba ser objeto de verificación; ni frente a la omisión de los responsables de revocar un certificado digital cuando éstos no lo hicieran.

9.8.- LIMITACIONES A LA RESPONSABILIDAD FRENTE A TERCEROS

FDSL establece en esta Política de Certificación como en sus documentos asociados cualquier limitación de responsabilidad que pudiera aplicársele, considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación establecidos en este documento.
Asimismo, en el Acuerdo con Suscriptores, Convenios de Constitución de Autoridades de Registro y Actas de Emisión de Certificados se establecerá y limitará las responsabilidades de las partes intervinientes.

9.9.- COMPENSACIONES POR DAÑOS Y PERJUICIOS

No es aplicable.

9.10.- CONDICIONES DE VIGENCIA

Esta Política de Certificación entra en vigencia desde su publicación en el sitio web, previa aprobación del Ente Licenciante Provincial y emisión del nuevo certificado digital para la Autoridad Certificante, que en atención a la actualización en el algoritmo utilizado, su clave pública deberá ser publicado en el Boletín Oficial y Judicial de la Provincia de San Luis.
La Política de Certificación permanecerá vigente hasta que sea reemplazada por la emisión de una nueva versión. Ante ese supuesto, todos los certificados emitidos bajo esta Política de Certificación seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Política disponga que deben ser revocados y la medida se encuentre debidamente fundamentada y aprobada.

9.11.- AVISOS PERSONALES Y COMUNICACIÓN CON LOS PARTICIPANTES

No aplica.

9.12.- GESTION DEL CICLO DE VIDA DEL DOCUMENTO

9.12.1.- Procedimiento de cambio

FDSL cuenta con Procedimientos de Administración de Cambios para efectuar cualquier modificación a la presente Política de Certificación conforme al Procedimiento de Control de los Documentos de la Autoridad de Aplicación.
Toda modificación será sometida a la aprobación de la Autoridad de Aplicación.
Todo cambio aprobado a la Política de Certificación debe ser comunicado al Suscriptor.

9.12.2.- Mecanismo y plazo de publicación y notificación

La Política de Certificación se encuentra permanentemente disponible en forma pública y accesible a través de internet en la dirección: http://fd01.firmadigital.sanluis.gov.ar/fdsl/agentes-cps.pdf

En caso de producirse modificaciones a esta Política de Certificación, inmediatamente de aprobadas serán publicadas en www.firmadigital.sanluis.gov.ar, donde se encontrará la versión actualizada y las versiones anteriores del documento modificado.
Lo mismo se aplica al Acuerdo con Suscriptores, a los Términos y Condiciones con Terceros Usuarios y demás documentos de la AC de FDSL de carácter público.
Todos los cambios producidos en los documentos antedichos serán notificados a los Suscriptores que poseen certificados vigentes a la fecha de aplicación del cambio vía correo electrónico declarado en las correspondientes solicitudes de certificados de clave pública.

9.12.3.- Condiciones de modificación de OID

No aplica.

9.13.- PROCEDIMIENTOS DE RESOLUCION 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 FDSL, la controversia o conflicto será resuelto por la Autoridad de Aplicación conforme a su régimen recursivo.

Pueden recurrir a este procedimiento tanto los Suscriptores como los Terceros Usuarios de certificados de clave pública.

Esta Política de Certificación o cualquier documento asociado, así como sus actualizaciones, serán aprobados por la Autoridad de Aplicación.

9.14.- LEGISLACION APLICABLE

La interpretación, obligatoriedad, diseño y validez de esta Política de Certificación y sus documentos asociados se encuentran sometidos a lo establecido por la Ley Provincial Nº V-0591-2007, el Decreto Reglamentario Nº 0428-MP-2008 modificado por Decreto N° 6011-MCTyS-2018, la Resolución Nº 345-ACTySSL-2018, la Ley Provincial NºII-0947-2016, el Decreto Nº8630-MCyT-2016, la Ley Nacional Nº 25.506, el Decreto Nº 2628/2002, y demás normas complementarias aplicables, dictadas por autoridad competente.

9.15.- CONFORMIDAD CON NORMAS APLICABLES

A los fines de la interpretación y/o aplicación de las disposiciones de esta Política de Certificación y demás documentación asociada, se debe tener en cuenta la normativa que la rige.

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

En caso de reclamos de los usuarios o suscriptores relacionados con la prestación de servicios de FDSL, el suscriptor o tercero deberá realizar el correspondiente reclamo ante FDSL y, en caso de no arribar a una solución, podrá efectuar una denuncia ante la Autoridad de Aplicación.

9.16.- CLAUSULAS ADICIONALES

No se establecen cláusulas adicionales.

9.17.- OTRAS CUESTIONES GENERALES

No aplicable.