FDSL 3.0
FIRMA DIGITAL
DE SAN LUIS

ACUERDO CON SUSCRIPTORES

VERSION 4.0 – FECHA 20/02/2019

DE LA "POLÍTICA DE CERTIFICACIÓN PARA AUTENTICACIÓN DE SERVIDORES Y SERVICIOS"

OID 2.16.32.1.3.2.1.1.1.

INFRAESTRUCTURA DE FIRMA DIGITAL DE SAN LUIS

Versiones y modificaciones de este documento

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	09/06/2009	FDSL	Director	Resolución N° 6090001-ULP-2009
1	1	28/08/2009	FDSL	Director	Resolución N° 8280004-ULP-2009
2	0	15/03/2010	FDSL	Director	Resolución N° 3150004-ULP-2010
3	0	03/10/2016	FDSL	Director	Resolución N° 10-MCyT-2016
3	1	12/01/2017	FDSL	Director	Resolución N° 07-ASLCTyS-2017
4	0	20/02/2019	FDSL	Director	Resolución N° 44-ACTySSL-2019

ÍNDICE

ACUERDO CON SUSCRIPTORES DE UN CERTIFICADO DE CLAVE PÚBLICA DE FIRMA DIGITAL DE SAN LUIS

USTED DEBE LEER EL PRESENTE ACUERDO CON SUSCRIPTORES ANTES DE SOLICITAR, ACEPTAR O UTILIZAR UN CERTIFICADO DIGITAL EN EL MARCO DE LA POLÍTICA DE CERTIFICACIÓN BAJO LA CUAL SE EMITA. SI USTED NO ESTÁ DE ACUERDO CON LOS TÉRMINOS Y CONDICIONES DE ESTE ACUERDO, NO SOLICITE, ACEPTE NI UTILICE EL CERTIFICADO DIGITAL.

El Suscriptor declara que previamente a la aceptación del presente Acuerdo, ha sido notificado de la existencia y ha tenido libre acceso a la Política de Certificación para Autenticación de Servidores y Servicios - bajo la cual se emite el certificado -, a la Política de Privacidad, a la Política de Seguridad, a los Términos y Condiciones con Terceros Usuarios, y demás documentos asociados, declarando que acepta en completa conformidad su contenido.
Dichos documentos son incorporados por referencia y forman parte íntegra de este documento.

1.- SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS

1.1.- SOLICITUD DE CERTIFICADO

El solicitante de un certificado digital se presentará personalmente ante la Autoridad de Registro correspondiente o ante Firma Digital de San Luis (en adelante, FDSL), quién se encargará de asistirlo en el proceso de carga de datos en el Formulario de Solicitud de Emisión de Certificado, además de la aceptación del contenido y alcance de la Política de Certificación y demás documentos asociados a ella.

El Solicitante deberá presentar los requisitos que se detallan a continuación:

a) Documento de Nacional de Identidad o Cédula de Identidad Provincial Electrónica (vigentes al momento de la solicitud), en caso de poseer nacionalidad argentina. De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

b) Una nota firmada digitalmente por el Responsable de Firma Digital designado o bien, por el Superior Jerárquico de la jurisdicción, organismo o dependencia donde desempeña sus funciones (conforme lo pactado en el pertinente Convenio de Constitución de Autoridad de Registro o Acta de Emisión de Certificados Digitales, según corresponda), solicitando se extienda a su favor un certificado de clave pública. En dicha nota de solicitud, deberá especificarse:

- Nombre y Apellido del Solicitante;
- Documento Nacional de Identidad o Cédula de Identidad Provincial Electrónica (CIPE) o Pasaporte, según corresponda;
- Jurisdicción/Organismo, Dependencia y Cargo del Solicitante;
- Correo electrónico del Solicitante del certificado digital, preferentemente institucional.

c) Dispositivo Criptográfico técnicamente confiable. Para la generación, almacenamiento y activación de las claves, los Suscriptores cuentan con dispositivos criptográficos externos removibles que las protegen por medio de dos factores de seguridad:
- Mediante la posesión del dispositivo.
- Mediante un PIN o contraseña definida por el propio Suscriptor, o huella biométrica.
En ningún momento y bajo ninguna circunstancia FDSL ni las Autoridades de Registro toman conocimiento del pin o contraseña del dispositivo que accede a la clave privada del certificado del Suscriptor.

El solicitante se hace completamente responsable de la falsedad de cualquiera de los datos por él facilitados a la Autoridad de Registro, en perjuicio de la Ley Nº 25.326 de Protección de Datos Personales. Asimismo, se obliga a mantener una adecuada protección y confidencialidad de la clave privada asociada a su certificado digital.

1.2.- ACEPTACIÓN DEL CERTIFICADO

La descarga del certificado en el dispositivo del Solicitante importará su aceptación 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.

1.2.1.- Utilización del Certificado

A los fines del correcto funcionamiento de su certificado de clave pública, es importante que realice las siguientes acciones:
1) Para el uso del dispositivo seleccionado será imprescindible la **descarga del driver** respectivo en la PC donde pretenda utilizarlo, los mismos se encuentra a su disposición en www.firmadigital.sanluis.gov.ar
2) Además, es necesario que proceda a la **descarga única de la cadena de confianza de los certificados**. Ello implica descargar en su PC la totalidad de los certificados vinculados a la Política de emisión, disponibles en www.firmadigital.sanluis.gov.ar

1.3.- DESCRIPCIÓN DE LOS CERTIFICADOS

1.3.1.- Alcance del Certificado

El Suscriptor se obliga y acepta utilizar el certificado digital emitido en el marco de la referida Política de Certificación, sólo bajo los propósitos y alcance estipulados a continuación:

➢ **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.
La firma digital, conforme lo establecido precedentemente, garantizará las siguientes características en su aplicación:

*Autenticidad, permitirá atribuir el documento o la comunicación suscripta digitalmente a su autor de manera fehaciente;

*Integridad del documento, permitirá identificar si el contenido del documento o de la comunicación firmada digitalmente fue alterado con posterioridad a su suscripción;

*No repudio.

1.3.2.- Vigencia del Certificado

Todos los certificados emitidos por la Autoridad Certificante de Firma Digital de San Luis, a favor de los Suscriptores en el marco de la Política de Certificación para Autenticación de Servidores y Servicios, tienen un período de vigencia de DOS (2) años, contados a partir de la fecha de emisión - siempre que dicho plazo no exceda el período de uso del certificado del Certificador Licenciado Provincial. Transcurrido el plazo mencionado, 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.

1.3.3.- Contenido

El certificado de clave pública contendrá como mínimo los siguientes datos:
a) Número de versión X.509 del certificado.
b) Nombre y apellido del suscriptor del certificado.
c) Nombre del Organismo, Suborganismo y rol del suscriptor.
d) Dirección de correo electrónico con la extensión institucional respectiva del Organismo al cual pertenece el suscriptor.
e) Clave pública del suscriptor.
f) Algoritmos de firma de la clave pública.
g) Número de serie del certificado.
h) Período de validez del certificado.
i) Nombre de la Autoridad Certificante emisora del certificado.
j) Dirección de consulta de la Lista de Certificados Revocados (CRLs):
http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
y alternativamente, en:
http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
k) URL donde se encuentra disponible la Política de Certificación asociada al presente Manual de Procedimientos.

2.- PROCESAMIENTO DE LA SOLICITUD DE CERTIFICADO DEL SUSCRIPTOR

El solicitante de un certificado digital deberá presentarse personalmente por ante una autoridad de registro o ante Firma Digital de San Luis, quién se encargará de asistirlo en el proceso de carga de datos en el Formulario de Solicitud de Emisión de Certificado, además de la aceptación del contenido y alcance de la Política de Certificación y demás documentos asociados a ella.
La autoridad de registro procederá a realizar la identificación y validación de atributos, conforme las exigencias de la Política bajo la cual se emite el certificado y corroborar que el dispositivo criptográfico del Solicitante es alguno de los homologados por FDSL.
En caso que no se hubieran reunido elementos de juicio suficientes para validar la identidad del solicitante o la pertenencia del Solicitante a la comunidad de Suscriptores conforme lo establece la Política de Certificación, el Responsable de la ARR no iniciará el proceso de Solicitud.
Si hubiera finalizado exitosamente el proceso de validación de la identidad del Suscriptor según los procedimientos indicados, el Responsable de la Autoridad de Registro o FDSL iniciará el proceso de emisión del certificado, el que culminará con la efectiva descarga del certificado de clave pública en el dispositivo criptográfico del Solicitante.

3.- OBLIGACIONES ANTE LA REVOCACIÓN O EXPIRACIÓN

3.1.- OBLIGACIONES DEL SUSCRIPTOR

El Suscriptor acepta dar cumplimiento a todas y cada una de las obligaciones enumeradas en la Política de Certificación para Autenticación de Servidores y Servicios, en lo que respecta al ciclo de vida y revocación del certificado digital emitido por FDSL.

3.1.1.- Pedido de Revocación

El Suscriptor debe pedir la revocación de su certificado de clave pública cuando:
a) Se produzcan cambios en la información que el certificado contiene o ésta se desactualice.
b) La clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
c) Se produzca el cese de su relación laboral con el organismo, dependencia o institución, sin perjuicio de la obligación que le corresponde al Superior Jerárquico -conforme lo prevea el Convenio de Constitución de Autoridad de Registro Remota o Acta de Emisión de Certificados de Clave Pública, según corresponda- y/o al Responsable Máximo de la Jurisdicción, Organismo o Dependencia donde desempeña sus funciones.

Asimismo, el Suscriptor de un certificado puede solicitar su revocación sin necesidad de invocar una causa o motivo en cualquier momento, para lo cual debe comunicarlo a FDSL por cualquiera de los medios previstos en la Política de Certificación asociada al presente Acuerdo.

3.1.2.- Medios de Revocación

El Suscriptor a los fines de la Revocación de su Certificado Digital podrá solicitarlo a través de los siguientes medios:

a) Vía Web: ingresando a www.firmadigital.sanluis.gov.ar, servicio que se encuentra disponible las veinticuatro (24) horas del día los trescientos sesenta y cinco (365) días del año. A cuyo efecto deberá seleccionar la opción “Revocar un Certificado Digital” luego de seleccionar la Política de Certificación para Autenticación de Servidores y Servicios, y conectar su dispositivo criptográfico, o sin conectar su dispositivo criptográfico, puede solicitar la revocación de su certificado ingresando el PIN de revocación que le fue informado mediante correo electrónico al momento de le emisión del mismo certificado.

b) En forma presencial, ante la Autoridad de Registro donde tramito la emisión del Certificado o en su defecto ante FDSL.

3.1.3.- Obligaciones tras la Revocación o Expiración

Tras la expiración o tras tomar conocimiento de la revocación de su certificado, el Suscriptor deberá desinstalar su certificado y no utilizarlo para ningún propósito en lo sucesivo.

3.1.4.- Información Disponible sobre Certificados Revocados

FDSL pone a disposición de los Suscriptores y Terceros usuarios, un servicio de consulta basado en el protocolo de comunicación OSCP (Online Certificate Status Protocol), para la consulta en línea del estado de validez de los certificados emitidos y revocados (CRL) bajo la Política de Certificación para Autenticación de Servidores y Servicios.

Este servicio mantiene una disponibilidad de 24 horas los 7 días de la semana, durante los 365 días del año.
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 Política asociada a este Acuerdo.

3.2.- OBLIGACIONES DE FDSL

FDSL asume dar cumplimiento a todas y cada una de las obligaciones enumeradas en la Política de Certificación para Autenticación de Servidores y Servicios, en lo que respecta al ciclo de vida y revocación del certificado digital.

4.- POLÍTICA DE PRIVACIDAD

El Certificador Licenciado Provincial ha confeccionado la Política de Privacidad la cual debe ser cumplida y respetada por el Suscriptor, por FDSL y por sus Autoridades de Registro, siendo incorporada al presente Acuerdo por referencia y que forma parte integrante de este documento.

5.- LIMITACIONES DE LA RESPONSABILIDAD

5.1.- FUERZA MAYOR

No cabe responsabilidad alguna para FDSL por hechos fortuitos o de fuerza mayor, que éste no pudiera prever, o habiendo sido previsto no pudo evitarlo, conforme el Art 1730 del Código Civil y Comercial de la Nación.

5.2.- CASOS EN LOS CUALES EL CERTIFICADOR PUEDE LIMITAR SU RESPONSABILIDAD

No cabe responsabilidad alguna para Firma Digital de San Luis, en caso de utilización no autorizada de un certificado digital, cuya descripción se encuentra establecida en su 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.
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.

6.- LEGISLACIÓN APLICABLE Y PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS

6.1.- LEGISLACIÓN APLICABLE

La interpretación, obligatoriedad, diseño y validez de este Acuerdo 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 modificada por Decreto N° 6011-MCyT-2018, la Resolución N° 341-ACTySSL-2018, Ley Nacional Nº 25.506, el Decreto Nº 2628/2002 y demás normas complementarias aplicables dictadas por autoridad competente.

6.2.- PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS

La resolución de cualquier controversia y/o conflicto resultante de la aplicación de lo dispuesto en este Acuerdo y/o en cualquiera de sus documentos asociados, será resuelta en sede administrativa ante FDSL.
Agotada la vía administrativa 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.

7.- CESIÓN DE DERECHOS

Ninguno de los derechos del Suscriptor de un Certificado Digital de FDSL, bajo los términos del presente Acuerdo puede ser cedido o transferido.

8.- CONTACTOS

Firma Digital de San Luis funciona en el ámbito de la Agencia de Ciencia, Tecnología y Sociedad San Luis.
Para consultas y sugerencias acerca de este documento se puede obtener información personalmente o por correo en:

Instituto Firma Digital de San Luis
Dirección: Edificio de Descentralización Administrativa “Terrazas del Portezuelo” - Torre III, 3º Piso - Autopista de las Serranías Puntanas Km. 783, Provincia de San Luis, República Argentina. Código Postal 5700.
Teléfono: (0266) 4452000, Internos: 6095 y 3574.
Correo Electrónico: firmadigital@sanluis.gov.ar
Sitio Web: http://www.firmadigital.sanluis.gov.ar

9.- VIGENCIA DEL ACUERDO

Este Acuerdo entra en vigencia desde el mismo momento de haber sido aceptado por el Suscriptor, previo a la solicitud del certificado digital, y hasta la expiración o revocación del certificado digital.

10.- MODIFICACIONES A ESTE ACUERDO

El Suscriptor acepta que el presente Acuerdo y los documentos asociados podrán ser modificados por FDSL, siendo un requisito de validez su aprobación por la Autoridad de Aplicación y su notificación a los Suscriptores que posean certificados vigentes a la fecha de aplicación.

11.- CONSENTIMIENTO INFORMADO

Por la presente declaro que he sido informado y entiendo el alcance y las consecuencias legales del USO DE LA FIRMA DIGITAL expedida por FDSL, las explicaciones me fueron facilitadas en un lenguaje claro y sencillo, permitiéndome realizar todas las observaciones y aclarándome todas las dudas planteadas.

Asimismo, me han explicado detalladamente las obligaciones que como usuario debo observar y que se encuentran contenidas en el presente Acuerdo de Suscriptores.
He tenido oportunidad de corroborar la exactitud de la información y atributos relativos a mi persona, a incluir en el certificado a emitir, confirmando su corrección.

Firma y aclaración del Suscriptor