

FDSL 3.0

FIRMA DIGITAL DE SAN LUIS

ACUERDO CON SUSCRIPTORES

VERSION 3.0 – FECHA 19/02/2019

DE LA “POLÍTICA DE CERTIFICACIÓN PARA
CERTIFICADOS DIGITALES DE PERSONAS HUMANAS”

OID 2.16.32.1.3.2.1.1.2.

INFRAESTRUCTURA DE FIRMA DIGITAL DE SAN LUIS

Versiones y modificaciones de este documento

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	15/11/2010	FDSL	Director	Resolución N° 1150004-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
2	2	28/04/2017	FDSL	Director	Resolución N° 33-ASLCTyS-2017
3	0	19/02/2019	FDSL	Director	Resolución N° 41-ACTySSL-2019

ÍNDICE

1.- SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS.....	4
1.1.- SOLICITUD DE CERTIFICADO	4
1.2.- ACEPTACIÓN DEL CERTIFICADO	5
1.2.1.- Utilización del Certificado	5
1.3.- DESCRIPCIÓN DE LOS CERTIFICADOS	5
1.3.1.- Alcance del Certificado	5
1.3.2.- Vigencia del Certificado	6
1.3.3.- Contenido.....	6
2.- PROCESAMIENTO DE LA SOLICITUD DE CERTIFICADO DEL SUSCRIPTOR	6
3.- OBLIGACIONES ANTE LA REVOCACIÓN O EXPIRACIÓN	7
3.1.- OBLIGACIONES DEL SUSCRIPTOR	7
3.1.1.- Pedido de Revocación	7
3.1.2.- Medios de Revocación	7
3.1.3.- Obligaciones tras la Revocación o Expiración	7
3.1.4.- Información Disponible sobre Certificados Revocados	7
3.2.- OBLIGACIONES DE FDSL	8
4.- POLÍTICA DE PRIVACIDAD	8
5.- LIMITACIONES DE LA RESPONSABILIDAD	8
5.1.- FUERZA MAYOR.....	8
5.2.- CASOS EN LOS CUALES EL CERTIFICADOR PUEDE LIMITAR SU RESPONSABILIDAD	8
6.- LEGISLACIÓN APLICABLE Y PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS	8
6.1.- LEGISLACIÓN APLICABLE	8
6.2.- PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS	8
7.- CESIÓN DE DERECHOS	9
8.- CONTACTOS	9
9.- VIGENCIA DEL ACUERDO	9
10.- MODIFICACIONES A ESTE ACUERDO	9
11.- CONSENTIMIENTO INFORMADO	9

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 Certificados Digitales de Personas Humanas - 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

Teniendo en cuenta que la Política de Certificación de referencia contempla la posibilidad de emitir certificados digitales para Personas Humanas en un procedimiento integrado con la emisión de la Cédula de Identidad Provincial Electrónica (CIPE), en el marco de lo previsto en la Ley N° V-0698-2009, debe diferenciarse si el Solicitante tramita su certificado digital en un Centro de Expedición CIPE/LC:

- En un Centro de Expedición CIPE/LC

Se podrá solicitar la emisión de un certificado digital para persona humana ante un Centro de Expedición CIPE/LC utilizando exclusivamente como dispositivo criptográfico una CIPE. La identificación y autenticación del habitante seguirá un proceso integrado con el registro para la expedición de la CIPE.

1. Por lo tanto, si se trata de una **primera solicitud**, el requirente deberá comparecer en una Oficina de Expedición de CIPE con la documentación que se indica en su sitio web, la cual incluye:

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

La Autoridad de Registro verificará la identidad del solicitante y la documentación que presenta. Es condición necesaria para la aprobación de la emisión del certificado de digital para personas humanas, el poseer aprobada la solicitud de emisión de la Cédula de Identidad Provincial Electrónica.

2. Si el Solicitante requiere **la emisión de un nuevo certificado digital para persona humana en el dispositivo contenido en su CIPE**, deberá presentarse ante la Oficina de Expedición de CIPE con su CIPE o con su Documento Nacional de Identidad vigente, si posee nacionalidad argentina o, de tratarse de extranjeros, su Documento Nacional de Identidad Argentino o pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

Siempre que un Suscriptor solicite la emisión de su certificado digital en un Centro de Expedición CIPE constará, entre los datos obrantes en su certificado, el documento que utilizó para identificarse al solicitar la expedición de su CIPE y el número correspondiente.

Concluido el trámite de emisión de CIPE, el titular deberá suscribir digitalmente una actuación con la que quedará acreditado que solicitó la emisión de su certificado de clave pública, la aceptación del mismo y la aceptación del Acuerdo con Suscriptores

- Ante la Autoridad de Registro Central de FDSL u otra Autoridad de Registro Delegada que no sea un Centro de Expedición CIPE

El futuro suscriptor podrá tramitar la emisión de un certificado digital para persona humana en el marco de la presente Política ante la Autoridad de Registro Central de FDSL u otra Autoridad de Registro Delegada que no sea un Centro de Expedición CIPE, a cuyo efecto, el solicitante deberá presentar:

- Si posee nacionalidad argentina, Documento Nacional de Identidad o Cédula de Identidad Provincial Electrónica (CIPE) expedida por la Provincia de San Luis.
- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

El solicitante podrá tramitar su firma utilizando cualquier dispositivo criptográfico homologado por la autoridad.

En este supuesto, el Solicitante deberá firmar ológrafamente el Formulario de Solicitud de Certificado y el Acuerdo con Suscriptores. La aceptación del certificado se configurará con la descarga del certificado de clave pública en su dispositivo criptográfico.

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 N° 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:

- a) Suscribir todo tipo de documento actuaciones contenidas en un sistema de gestión de expedientes;
- b) Suscribir todo tipo de comunicación realizada a través de correo electrónico denunciado a los efectos de la solicitud del certificado.

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.

- c) Brindar autenticación de cliente seguro en aplicaciones telemáticas.
- d) Cifrado.

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 Certificados Digitales de Personas Humanas, tienen un período de vigencia de DIEZ (10) 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) Número de documento / CIPE / Pasaporte del Suscriptor.
- d) Provincia donde reside
- e) País de Nacimiento
- f) Dirección de correo electrónico
- g) Fecha de nacimiento.
- h) Clave pública del suscriptor.
- i) Algoritmos de firma de la clave pública.
- j) Número de serie del certificado.
- k) Período de validez del certificado.
- l) Nombre de la Autoridad Certificante emisora del certificado.
- m) Dirección de consulta de la Lista de Certificados Revocados (CRLs):
<http://fd01.firmadigital.sanluis.gov.ar/fdsl/humanas.crl> y alternativamente, en:
<http://fd02.firmadigital.sanluis.gov.ar/fdsl/humanas.crl>
- n) 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 Certificados Digitales de Personas Humanas, 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.

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 Certificados Digitales de Personas Humanas, 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 la emisión del mismo certificado.
- b) En forma presencial, ante la Autoridad de Registro donde tramita 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 Certificados Digitales de Personas Humanas.

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 Certificados Digitales de Personas Humanas, 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 N° V-0591-2007, el Decreto Reglamentario N° 0428-MP-2008 modificada por Decreto N° 6011-MCyT-2018, la Resolución N° 341-ACTySSL-2018, Ley Nacional N° 25.506, el Decreto N° 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