

ACS-005	ACUERDO CON SUSCRITORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 1 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

ANEXO III
Resolución Rectoral N° 11150007-ULP-2010

ACUERDO CON SUSCRITORES

correspondiente a

**“POLÍTICA DE CERTIFICACIÓN PARA FIRMA DIGITAL DE PERSONAS
VINCULADAS - FDSL”**

OID 2.16.32.1.3.2.1.1.4.

INFRAESTRUCTURA DE FIRMA DIGITAL DE SAN LUIS

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 2 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

Contenido

1. DESCRIPCIÓN DE LOS CERTIFICADOS.....	3
1.1. Alcance	3
1.2. Vigencia.....	3
1.3. Contenido	4
2. SOLICITUD DE CERTIFICADO Y PROCESAMIENTO DE LA SOLICITUD	4
2.1. Solicitud de Certificado	4
2.2. Aceptación del Certificado	6
2.3. Utilización del Certificado.....	6
3. OBLIGACIONES DEL SUSCRIPTOR	6
3.1. Pedido de Revocación.....	6
3.2. Medios para solicitar la Revocación	7
3.3. Obligaciones tras la revocación o expiración	7
3.4. Información disponible sobre certificados Emitidos y Revocados....	7
4. RESPONSABILIDAD DEL SUSCRIPTOR.....	7
5. OBLIGACIONES DE FDSL.....	7
6. POLÍTICA DE PRIVACIDAD.....	7
7. LIMITACIONES DE LA RESPONSABILIDAD	7
8. LEGISLACIÓN APLICABLE Y PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS.....	8
8.1. Legislación Aplicable	8
8.2. Procedimientos de Resolución de Conflictos.....	8
9. CESIÓN DE DERECHOS	8
10. CONTACTOS.....	8
11. VIGENCIA.....	8
12. MODIFICACIONES DE ESTE ACUERDO	8

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 3 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

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

USTED DEBE LEER EL PRESENTE ACUERDO CON SUSCRIPTORES DE UN CERTIFICADO DIGITAL ANTES DE SOLICITAR, ACEPTAR O UTILIZAR UN CERTIFICADO DIGITAL EN EL MARCO DE LA “POLÍTICA DE CERTIFICACIÓN PARA FIRMA DIGITAL DE PERSONAS VINCULADAS”. SI USTED NO ESTÁ DE ACUERDO CON LOS TÉRMINOS Y CONDICIONES DE ÉSTE ACUERDO, NO SOLICITE, ACEPTE NI UTILICE EL CERTIFICADO DIGITAL.

Asimismo, 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 Firma Digital de Personas Vinculadas”, Política de Privacidad, Política de Seguridad, 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 éste Documento.

1. DESCRIPCIÓN DE LOS CERTIFICADOS

1.1. Alcance

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 alcances estipulados a continuación:

a) Suscribir digitalmente todo tipo de documentos, comunicaciones, archivos, registros, trámites, bases y bancos de datos, que el Suscriptor en función de su rol o vínculo con la Persona Jurídica a la cual pertenece o se halla vinculada se encuentre facultado a firmar, en concordancia con lo dispuesto por la normativa legal vigente. Siempre teniendo en cuenta los límites previstos en el artículo 4º de la Ley Nacional Nº 25.506 y demás límites que pudieran existir. Ello, toda vez que los certificados de clave pública emitidos en virtud de la Política de Certificación de referencia, identificarán al firmante en su rol o vínculo con la Persona Jurídica a la que pertenece o se halla vinculada.

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

- Autenticidad: Permitirá atribuir el documento digital o la comunicación suscripta digitalmente a su autor de manera fehaciente;
- Integridad del documento, permitirá identificar si el contenido del documento digital o de la comunicación firmada digitalmente fue alterado con posterioridad a su suscripción;
- No repudio.

b) Suscribir todo tipo de comunicación realizada a través de la dirección de correo electrónico (siempre que el servidor del Correo lo permita) y la dirección sea la que se encuentra incorporada en el texto del certificado digital del Suscriptor.

c) Cifrar con su clave pública documentos digitales a los que sólo se podrá acceder con la correspondiente clave privada.

1.2. Vigencia

Los certificados emitidos en el marco de la Política de Certificación para Firma Digital de Personas Vinculadas antes del 11 de abril de 2016 tienen un período de vigencia de DOS (2) años, mientras que los emitidos con posterioridad a dicha fecha tienen un período de vigencia de CUATRO (4) años, contados a partir de la fecha de emisión. Transcurrido el plazo mencionado, el certificado expirará automáticamente, perdiendo toda validez.

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 4 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

En tal caso, el Suscriptor debe gestionar uno nuevo, para lo cual iniciará el correspondiente proceso de solicitud de emisión.

1.3. Contenido

El certificado de clave pública contiene los siguientes datos:

- a) Número de versión X.509 del certificado.
- b) Nombre y Apellido del Suscriptor del certificado.
- c) Nombre de la Persona Jurídica a la cual se encuentra vinculada.
- d) Numero de CUIT de la Persona Jurídica a la cual se encuentra vinculada.
- e) Rol o vínculo del Suscriptor con la Persona Jurídica, y número de matrícula, si correspondiera.
- f) País de Residencia Habitual del Suscriptor.
- g) Dirección de correo electrónico del Suscriptor.
- 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).
- n) URL donde se encuentra disponible la Política de Certificación asociada al presente Acuerdo.

2. SOLICITUD DE CERTIFICADO Y PROCESAMIENTO DE LA SOLICITUD

2.1. Solicitud de Certificado

La tarea de validación de la identidad del Solicitante de un certificado de clave pública podrá ser llevada a cabo por Firma Digital de San Luis, en adelante FDSL, o por Autoridades de Registro Remotas constituidas 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 que el Solicitante dice pertenecer y la verificación del vínculo con aquella, además de la guarda de la documentación probatoria, ya sea en soporte digital o papel.

A los efectos de la constitución de una Autoridad de Registro, será indispensable la celebración de un “Convenio de Constitución de Autoridad de Registro Remota” entre FDSL y quien pretenda constituirse como tal, individualizando expresamente la Política de Certificación; designando a los Responsables - Titular y Suplente - de la Autoridad de Registro Remota y detallando qué documentación requerirá a los efectos de la acreditación de la identidad del Solicitante, de la existencia de la persona jurídica con la que pretende acreditar su vínculo y su relación o vínculo con ella.

Es necesario tener presente que dichos Convenios deberán ser refrendados por la Autoridad de Aplicación.

Asimismo, en los casos que no proceda la constitución de una Autoridad de Registro, FDSL podrá solicitar la suscripción de un Acta de Emisión de Certificados Digitales con aquellas Personas Jurídicas que pretendan introducir la utilización de certificados de clave pública entre sus dependientes, colaboradores, clientes, proveedores, matriculados u otros, a cuyo efecto deberá acreditar previamente su existencia y denunciar el tipo de vínculo con los futuros suscriptores y detallar la documentación con la que acreditará ese vínculo, asumiendo la responsabilidad de solicitar inmediatamente la revocación de los certificados de los suscriptores vinculados a aquella, cuando cese o se encuentre suspendido el vínculo probado.

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 5 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

La celebración de cualquiera de los Convenios o Actas enunciados precedentemente, determinará el modo y procedimiento a realizar para cumplir con la validación de la identidad de los Solicitantes de certificados.

Así, a los fines de adquirir un certificado digital de clave pública el Solicitante deberá concurrir personalmente ante FDSL o a la Autoridad de Registro Remota constituida a tales efectos, con un Dispositivo Criptográfico técnicamente confiable y con la documentación que a continuación se detalla según se deba presentar ante FDSL o una Autoridad de Registro Remota:

- **Ante FDSL:**

- a) Documento Nacional de Identidad (vigente al momento de la solicitud) o Cédula de Identidad Provincial Electrónica (CIPE).
- b) Una Nota de Solicitud de certificado que, en carácter de declaración jurada, debe ser suscripta digitalmente o en su defecto ológrafamente por el Representante de Firma Digital designado por la Persona Jurídica a la que cual se encuentra vinculado el solicitante, requiriendo se extienda un certificado de clave pública, en la que deberá especificarse:
 - Nombre y Apellido del Solicitante,
 - Documento de Nacional de Identidad (DNI u otro de validez nacional);
 - Rol, cargo o tipo de vínculo que lo une con la Persona Jurídica a la que pertenece;
 - Correo electrónico de la Persona o Área responsable de la suscripción de la Nota de Solicitud.
- c) Documentación que acredita la existencia de la Persona Jurídica a la que se halla vinculado, debidamente certificada y/o legalizada por escribano público, en el caso que la Persona Jurídica haya sido constituida en extraña jurisdicción;
- d) Constancia de pago del arancel establecido por FDSL;
- e) Constancia de Inscripción en la Administración Federal de Ingresos Públicos;

De ser necesario, el Responsable de Normativa Jurídica contará con un plazo de entre siete (7) y diez (10) días hábiles, a los fines de analizar la documentación presentada y acordará con el Solicitante la fecha en la que deberá presentarse nuevamente para concretar la emisión.

- **Ante Autoridad de Registro Remota o ante FDSL cuando se hubiera suscripto un Acta de Emisión de Certificado con la Persona Jurídica a la que se halla vinculada:**

- a) Documento Nacional de Identidad o Cédula de Identidad Provincial Electrónica (CIPE).
- b) Una Nota de Solicitud de certificado que, en carácter de declaración jurada debe ser suscripta digitalmente o en su defecto ológrafamente por el Responsable de Firma Digital designado en el Convenio de Constitución de ARR o en el Acta de Emisión de Certificado, requiriendo se extienda a su favor un certificado de clave pública, en la que deberá especificarse:
 - Nombre y Apellido del Solicitante;
 - Documento Nacional de Identidad (DNI u otro de validez nacional);
 - Rol, cargo o tipo de vínculo que lo une con la Persona Jurídica a la que pertenece;
 - Correo electrónico de la Persona o Área responsable de la suscripción de la Nota de Solicitud. -
- c) Constancia de pago del arancel establecido por FDSL.

Una vez que el Responsable de Normativa Jurídica, verifique que el Suscriptor acompañó la documentación obligatoria y su veracidad, el Responsable de la Autoridad de Registro procederá a completar el "Formulario de Solicitud de Certificado Digital". En esta instancia el Suscriptor deberá aceptar el Acuerdo con Suscriptores.

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 6 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

Una vez aceptado, el Responsable de la Autoridad de Registro o FDSL imprimirá el “Formulario de Solicitud de Emisión de Certificados Digitales”, el cual deberá ser suscrito ológrafamente tanto por el Suscriptor como por el Responsable de la Autoridad de Registro. Dicho formulario debe conservarse junto a la documentación de respaldo acompañada.

El Responsable de la ARR o FDSL, deberá aprobar la Solicitud de Emisión mediante el sistema de gestión de expedientes a efectos de evidenciar el cumplimiento de todos los extremos para la emisión del certificado solicitado. Concluido ello, se podrá descargar el certificado en el dispositivo correspondiente del Solicitante, a cuyo efecto le será requerido que ingrese su pin/contraseña o huella biométrica, según sean las características del mismo.

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.

2.2. Aceptación del Certificado

La descarga del certificado en el Dispositivo Criptográfico del Solicitante, importará la aceptación del mismo, 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.

2.3. 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 esta Política de emisión, disponibles en www.firmadigital.sanluis.gov.ar.

3. OBLIGACIONES DEL SUSCRIPTOR

El Suscriptor asume dar cumplimiento a todas y cada una de las obligaciones enumeradas en la “Política de Certificación para Firma Digital de Personas Vinculadas”, en lo que respecta al ciclo de vida y revocación del certificado digital emitido por la AC-FDSL.

3.1. Pedido de Revocación

El Suscriptor está OBLIGADO a 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 (ej. Modificación en el vínculo con la persona jurídica, modificación en el nombre de la persona jurídica, etc.);
- 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 y/o vínculo con la Persona Jurídica, a la cual se encuentra vinculada sin perjuicio de la obligación que le corresponde a la Persona Jurídica en relación a las notificaciones relativas a la actualización de los datos de su propia estructura organizativa.

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 la FDSL por cualquiera de los medios previstos en la Política de Certificación asociada al presente Acuerdo.

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 7 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

3.2. Medios para solicitar la Revocación

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

- 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 Firma Digital de Personas Vinculadas, y conectar su dispositivo criptográfico.
- En forma presencial, ante la Autoridad de Registro donde tramito la emisión del Certificado o en su defecto ante FDSL.

3.3. Obligaciones tras la revocación o expiración

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

3.4. Información disponible sobre certificados Emitidos y Revocados

FDSL pone a disposición de los Suscriptores y Terceros, 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 presente Política de Certificación. -

Este servicio mantiene una disponibilidad de 24 horas x 7 días, 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 presente Política.

4. RESPONSABILIDAD DEL SUSCRIPTOR

Queda bajo la exclusiva responsabilidad del Suscriptor el mantenimiento de la contraseña/pin que le haya asignado a su Dispositivo Criptográfico, a esos efectos recomendamos reproducirla en algún lugar seguro ya que al ser desconocida por terceros (privada), no existe proceso de recupero, debiendo en tal caso blanquearse el dispositivo criptográfico y solicitar nuevamente la emisión de un certificado, con todo los gastos y condiciones que ello requiere.

5. OBLIGACIONES DE FDSL

FDSL asume dar cumplimiento a todas y cada una de las obligaciones enumeradas en la “Política de Certificación para Firma Digital de Personas Vinculadas” en lo que respecta al ciclo de vida y revocación del certificado digital.

6. POLÍTICA DE PRIVACIDAD

FDSL ha confeccionado su Política de Privacidad la cual debe ser cumplida y respetada por FDSL y el Suscriptor, siendo incorporada al presente Acuerdo por referencia y que forma parte integrante de éste documento.

7. LIMITACIONES DE LA RESPONSABILIDAD

No cabe responsabilidad alguna para FDSL, en caso de utilización no autorizada de un certificado, 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 siempre que pueda demostrar que ha tomado todas las medidas razonables.

La responsabilidad de FDSL no compromete, en ningún caso, la responsabilidad pecuniaria del Estado Provincial.

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital

ACS-005	ACUERDO CON SUSCRIPTORES – FIRMA DIGITAL DE PERSONAS VINCULADAS			FDSL 3.0 FIRMA DIGITAL DE SAN LUIS
Pág. 8 de 8	12/01/2017	3	1	
	Fecha Emisión	Versión	Revisión	

Tampoco cabe responsabilidad alguna para FDSL por hechos fortuitos o de fuerza mayor, que éste no pudiera prever, o habiendo sido previsto no pudo evitarlo.

8. LEGISLACIÓN APLICABLE Y PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

8.1. 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, la Ley Provincial N° II-0947-2016, el Decreto N° 8630-MCyT-2016, la Ley Nacional N° 25.506, el Decreto N° 2628/2002, la Resolución Rectoral N° 1150007-ULP-2010 y demás normas complementarias aplicables dictadas por autoridad competente.

8.2. 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 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.

9. CESIÓN DE DERECHOS

Ninguno de los derechos del Suscriptor de un Certificado digital de FDSL, bajo los términos del presente Acuerdo pueden ser cedidos o transferidos.

10. CONTACTOS

FDSL funciona en el ámbito de la Agencia San Luis Ciencia, Tecnología y Sociedad.

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>

11. VIGENCIA

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

12. MODIFICACIONES DE 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.

Aprobación Calidad	Aprobación Área Legal	Aprobación Dueño
Responsable de Calidad	Jefe Área Legal	Director de Instituto Firma Digital