ANEXO I

Resolución Rectoral Nº 11150004-ULP-2010

POLITICA DE CERTIFICACION

DEL INSTITUTO DE FIRMA DIGITAL DE LA PROVINCIA DE SAN LUIS

"Política de Certificación del Instituto

de Firma Digital de la Provincia de San Luis

para Firma Digital de Habitantes"

INFRAESTRUCTURA DE FIRMA DIGITAL

DE LA PROVINCIA DE SAN LUIS

Contenido

1. INTRODUCCION

1.1. DESCRIPCION GENERAL

El presente documento establece la Política de Certificación para la emisión de certificados digitales a Habitantes de la Provincia de San Luis por lo cual regula la relación entre el Instituto de Firma Digital de la Provincia de San Luis, en su calidad de Certificador Licenciado, las Autoridades de Registro, los Suscriptores de certificados digitales emitidos en el ámbito de la presente Política y los Terceros Usuarios que reciban información firmada digitalmente por dichos Suscriptores. Ello, de conformidad con lo establecido en la Ley Nº V-0591-2007, el Decreto Reglamentario Nº 0428-MP-2008 y demás normas aplicables, por cuanto los certificados emitidos por el Instituto en el ámbito del presente documento son certificados digitales reconocidos por dicha normativa, y pueden ser utilizados para firmar digitalmente conforme la aplicabilidad prevista en esta Política de Certificación.

Asimismo, a los efectos de optimizar los recursos con los que cuenta la Provincia de San Luis, esta Política de Certificación contempla y facilita el procedimiento de emisión de certificados cuando el Solicitante o Suscriptor posea una Cédula de Identificación Electrónica Provincial (CIPE) conforme las previsiones de la Ley Nº V-0698-2009 y sus normas reglamentarias.

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

- El Instituto de Firma Digital de la Provincia de San Luis, quien actuará como Certificador Licenciado;

- Las Autoridades de Registros;

- 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.

Esta Política de Certificación será identificada como “Política de Certificación para Firma Digital de Habitantes de la Provincia de San Luis”, encontrándose su ámbito de aplicación definido en el Punto 1.3.4.

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

a) El Manual de Procedimientos de Certificación;

b) El Acuerdo con Suscriptores de Certificados;

c) Los Términos y Condiciones con Terceros Usuarios;

d) La Política de Privacidad del Certificador Licenciado;

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) El Tarifario.

1.2. IDENTIFICACIÓN

Título del Documento:

"Política de Certificación del Instituto de Firma Digital de la Provincia de San Luis para Firma Digital de Habitantes de la Provincia de San Luis".

Versión: 1

O.I.D.: 2.16.32.1.3.2.1.1.2.

Fecha: 15/11/2010

URL: http://www.pki.sanluis.gov.ar

Lugar: Provincia de San Luis, República Argentina.

1.3. PARTICIPANTES Y APLICABILIDAD

Los participantes de esta Política de Certificación son:

a) El Instituto de Firma Digital de la Provincia de San Luis, en adelante EL INSTITUTO, quien actuará como Certificador Licenciado;

b) Las Autoridades de Registro:

c) Los Suscriptores de Certificados;

d) Los Terceros Usuarios.

1.3.1. Certificador

Para esta Política de Certificación, la función de Certificador la cumple el Instituto de Firma Digital de la Provincia de San Luis, en virtud de lo dispuesto en el artículo 24 del Decreto Nº 0428-MP-2008, reglamentario de la Ley Provincial Nº V-0591-2007.

1.3.2. Autoridad de Registro

La presente Política de Certificación admite la posibilidad que la tarea de validación de la identidad del Solicitante de un certificado de clave pública sea realizada por una Autoridad de Registro Remota a cuyo efecto deberá celebrarse el correspondiente Convenio de Constitución de Autoridad de Registro Remota para la Política de Certificación del Instituto de Firma Digital de la Provincia de San Luis para Firma Digital de Habitantes de la Provincia de San Luis (O.I.D. 2.16.32.1.3.2.1.1.2.). Dicho Convenio deberá ser suscripto entre el máximo Responsable del Organismo en quien se delegue la referida tarea y el Director del Instituto, individualizando expresamente la presente Política de Certificación; designando a los Responsables de la ARR, por lo menos un Titular y un Suplente. Ese Convenio deberá ser refrendado por la Autoridad de Aplicación Provincial del Régimen de Firma Digital.

Específicamente, todas las Oficinas de Expedición de la CIPE serán constituidas en Autoridades de Registro de la presente Política, y tienen por misión realizar las funciones de asistencia a la Autoridad de Certificación en los procedimiento y trámites relacionados con los habitantes para su identificación, registro y autenticación, y la verificación y guarda de la documentación de respaldo. La ubicación geográfica de las mencionadas Autoridades de Registro Remotas serán las oficinas y las instalaciones habilitadas para los equipos móviles, así como otros lugares que a tal efecto determine la Autoridad de Aplicación encargada de la

expedición y gestión de la CIPE.

En concordancia con lo expuesto, la presente Política admite la posibilidad de constituir otras Autoridades de Registro Remotas distintas a las constituídas en las Oficinas de Expedición de CIPE.

1.3.3. Suscriptores de Certificados

Podrán ser Suscriptores de certificados digitales emitidos en el marco de la presente Política de Certificación todos los habitantes de la Provincia de San Luis.

1.3.4. Aplicabilidad

Los certificados emitidos en el marco de la presente Política de Certificación podrán ser utilizados exclusivamente para firmar trámites o documentos siempre que ello no contradiga lo establecido en el Código Civil y demás normativa nacional vigente en materia de capacidad. Este certificado permite sustituir la firma manuscrita por la digital en las relaciones del habitante con terceros.

Asimismo, permite suscribir todo tipo de comunicación realizada a través de la dirección de correo electrónico incorporado en el texto del certificado digital del Suscriptor.

Además, los certificados digitales emitidos en el marco de la presente Política podrán ser utilizados por el suscriptor para cifrar con su clave pública documentos digitales a lo que sólo se podrá acceder con la correspondiente clave privada.

Los certificados de firma son certificados reconocidos de acuerdo con lo establecido en la Ley Nº V-0591-2007, su Decreto Reglamentario Nº 0428-MP-2008 y demás normas aplicables.

El uso de los certificados de clave pública emitidos en el marco de la presente Política proporcionan las siguientes garantías:

No repudio de origen

Asegura que el documento proviene del habitante titular del certificado digital.

Dado que la CIPE cuenta con un dispositivo seguro de creación de firma y que las claves de firma permanecen desde el momento de su emisión bajo el control del habitante titular, se garantiza el compromiso del mismo con la firma realizada (garantía de “no repudio”).

En el caso de utilizar un dispositivo criptográfico diferente al de la CIPE, éste deberá cumplir con las normas de seguridad exigidas por el Instituto de Firma Digital de la Provincia de San Luis.

Integridad

Con el empleo del Certificado de Firma Digital se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación con posterioridad a su suscripción. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma digital. El uso de este sistema permite comprobar si un mensaje firmado ha sido alterado luego de haber sido suscripto. Para ello se firma con la clave privada un resumen único (digesto) del documento de forma que cualquier alteración del mensaje revierte en una

alteración de su resumen.

1.4. CONTACTOS

El INSTITUTO funciona en el ámbito de la Universidad de La Punta.

Para efectuar consultas, reclamos y/o sugerencias dirigirse a:

Universidad de La Punta

Dirección: Av. Universitaria S/N,

Ciudad de La Punta (5710) – Provincia de San Luis. República Argentina.

Teléfono: (02652) 452000 int. 6098

consultaspki@ulp.edu.ar

O http://www.pki.sanluis.gov.ar

Allí estarán disponibles los datos de contacto de todas las Autoridades de Registro Remotas que se encontraran constituidas.

2. ASPECTOS GENERALES DE LA POLITICA DE CERTIFICACION

2.1. - OBLIGACIONES

2.1.1. – Obligaciones del Certificador

Son obligaciones del INSTITUTO, en su carácter de Certificador Licenciado, cumplir con las previsiones establecidas en:

2.5.1.1. Los artículos 28, 32, 33 y 34 del Decreto Provincial Nº 0428- MP-2008.

a) Verificar fehacientemente la información identificatoria del solicitante de un certificado de clave pública, la cual deberá estar siempre incluida en el certificado y toda otra información que según lo dispuesto en el Manual de Procedimientos deba ser objeto de verificación, lo cual deberá realizarse de acuerdo a lo dispuesto en el citado Manual;

b) Numerar correlativamente los certificados emitidos;

c) Mantener copia de todos los certificados emitidos, consignando su fecha de emisión;

d) Abstenerse de generar, exigir, o por cualquier otro medio, tomar conocimiento o acceder, bajo ninguna circunstancia, a la Clave Privada de los Suscriptores de Certificados;

e) Mantener el control de su Clave Privada e impedir su divulgación;

f) Solicitar inmediatamente la revocación de su Certificado, cuando tuviera sospechas fundadas de que su Clave Privada ha sido comprometida;

g) Proceder a la revocación de su Certificado previo aviso a la Autoridad de Aplicación cuando la Clave Pública, en él contenida, deje de ser técnicamente confiable o cuando la información contenida en su certificado sufriera algún cambio significativo;

h) Operar utilizando un sistema técnicamente confiable;

i) Notificar al Solicitante de un certificado sobre las medidas necesarias que deberá obligatoriamente adoptar, para crear firmas digitales seguras y para su verificación confiable y de las obligaciones que aquel asume, por el sólo hecho de ser Suscriptor de un certificado de clave pública;

j) Recabar únicamente aquellos datos personales del Suscriptor del certificado, que sean

necesarios y de utilidad para la emisión del mismo, quedando el solicitante en libertad de proveer información adicional. Toda información así recabada, pero que no figure en el Certificado, será de trato confidencial por parte del INSTITUTO;

k) Poner a disposición del Suscriptor de un certificado emitido por el INSTITUTO, toda la información relativa a la tramitación del certificado;

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

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

n) Publicar su dirección y sus números telefónicos;

ñ) Permitir el ingreso de los auditores acreditados a su local operativo, poner a su disposición toda la información necesaria, y proveer la asistencia del caso;

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

p) En caso de cese de actividades, los certificados emitidos se revocarán a partir del día y la hora en que cesa su actividad, a menos que sean transferidos a otro Certificador Licenciado de acuerdo lo establezca la normativa vigente;

q) Notificar, mediante la publicación por tres (3) días consecutivos en el Boletín Oficial y Judicial, la fecha y hora de cese de sus actividades, que no podrá ser anterior a los noventa (90) días corridos contados desde la fecha de la última publicación;

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

s) Incluir inmediatamente en el Listado de Certificados Revocados aquellos certificados que hubiera revocado,

t) Hacer público en forma permanente el Listado de Certificados Revocados por medio de conexiones de telecomunicaciones públicamente accesibles;

u) Emitir a favor una constancia de la revocación para el Suscriptor del certificado

v) Publicación su propio certificado de clave pública en el Boletín Oficial y en dos diarios de difusión nacional, durante tres (3) días consecutivos a partir del día de su emisión.

2.5.1.2. - Asimismo, la Ley Nacional Nº 25.506 y su Decreto reglamentario Nº 2628/02, a la cual adhiere la Ley Provincial Nº V-0591-2007, requieren adicionalmente en sus artículos 21 y 34 y 36, respectivamente:

a) Incorporar en su Política de Certificación los efectos de la revocación de su propio certificado digital;

b) Publicar en internet o en la red de acceso público de transmisión o difusión de datos que la

sustituya en el futuro en forma permanente e ininterrumpida las Políticas de Certificación, la información relevante de la última auditoría de que hubiera sido objeto, su Manual de Procedimientos (de corresponder) y toda información que determine la Autoridad de Aplicación;

c) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

d) Someter a aprobación de la Autoridad de Aplicación el Manual de Procedimientos, el Plan de Seguridad y el de Cese de Actividades, así como el detalle de los componentes técnicos a utilizar;

e) Constituir domicilio legal en la República Argentina;

f) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a la normativa vigente;

g) Disponer de un servicio de atención a titulares y terceros que permita evacuar consultas y la pronta solicitud de revocación de certificados;

h) Informar a la Autoridad de Aplicación de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio;

i) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio salvo consentimiento expreso de éste;

j) Cumplir las normas y recaudos establecidos para la protección de datos personales;

k) En los casos de revocación de certificados, ya sea a solicitud de su titular o si se determinara que fue emitido en base a una información falsa que hubiera sido objeto de verificación al momento de su emisión o si los procedimientos de emisión y/o verificación hubieran dejado de ser seguros o por condiciones especiales definidas en la presente Política o en el caso de resolución judicial o de la autoridad de aplicación, deberá sustituir en forma gratuita aquel certificado salvo que el certificado hubiera dejado de ser seguro por razones atribuibles a su titular;

l) Enviar periódicamente a la Autoridad de Aplicación informes de estado de operaciones con carácter de declaración jurada;

m) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido.

2.1.2. - Obligaciones de la Autoridad de Registro

Son obligaciones de la Autoridad de Registro, cumplir con las previsiones previstas en:

2.5.2.1. - El artículo 40 del Decreto Nº 0428-MP-2008:

a) La recepción de solicitudes de emisión de certificados;

b) La validación de la identidad y autenticación de los datos de los titulares de certificados;

c) La validación de otros datos de los titulares de certificados que presenten ante ella cuya verificación delegue el INSTITUTO;

d) La remisión de las solicitudes aprobadas al INSTITUTO;

e) La recepción y validación de las solicitudes de revocación de certificados realizadas personalmente y su direccionamiento al INSTITUTO;

f) La identificación y autenticación de los solicitantes de revocación de certificados, cuando la revocación fuera realizada personalmente;

g) El archivo y la conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos en el Manual de Procedimientos de Certificación;

h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales;

i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos, en la parte que resulte aplicable, y demás normativa regulatoria;

2.5.2.2. - Asimismo, la Autoridad de Registro deberá:

a) Proteger sus claves privadas

b) Cumplir con todas las medidas previstas en los documentos asociados a la presente Política de Certificación tales como Plan de Seguridad, Manual de Procedimientos Operativos, Política de Privacidad, Acuerdo con Suscriptores, Términos y Condiciones con Terceros Usuarios así como las pautas previstas en el Convenio de Constitución de Autoridad de Registro Remota.

2.1.3. - Obligaciones de los Suscriptores de los Certificados

Son obligaciones de los Suscriptores de certificados de clave pública dar cumplimiento a lo previsto en:

2.5.3.1. - El artículo 36 del Decreto Nº 0428-MP-2008:

a) Proveer todos los datos requeridos por el Certificador Licenciado, bajo declaración jurada;

b) Mantener el control de su clave privada e impedir su divulgación;

c) Informar inmediatamente al Certificador Licenciado sobre cualquier circunstancia que pueda haber comprometido su clave privada;

d) Informar inmediatamente al Certificador Licenciado cuando cambie alguno de los datos contenidos en el certificado que hubieran sido objeto de certificación.

2.5.3.2. - Asimismo, la Ley Nacional Nº 25.506 requiere adicionalmente en su artículo 25:

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

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

2.5.3.3. - Adicionalmente, es obligación del Suscriptor:

a) Utilizar sus certificados de forma adecuada, conforme lo previsto en la Política de Certificación;

b) Tomar conocimiento de los derechos y obligaciones que se establezcan en la presente Política de Certificación, en el Acuerdo con Suscriptor y en todo documento que le sea aplicable;

c) Solicitar la revocación de su certificado en caso de ocurrir algún hecho que lo excluya de la aplicación de la presente Política.

2.1.4. - Obligaciones de los Terceros Usuarios

Son obligaciones de los Terceros Usuarios de certificados de clave pública, dar cumplimiento a lo previsto en:

2.1.4.1. La Resolución Rectoral Nº 2120004-ULP-2009:

a) Conocer los alcances de la Política de Certificación conforme los Términos y Condiciones con Terceros Usuarios;

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 del Suscriptor.

2.1.5. OBLIGACIONES DEL SERVICIO DE REPOSITORIO

El INSTITUTO tiene la obligación de mantener cierta información disponible en forma permanente y gratuita permitiendo el acceso público a la misma, conforme lo prevé la siguiente normativa:

2.5.5.1. - El Decreto Nº 0428-MP-2008, dispone en sus artículos 28, inc. 4 y 34, inc. 11 y 12:

a) Permitir el acceso público permanente a los certificados de clave pública que ha emitido a favor de los Suscriptores, a la Lista de Certificados Revocados;

b) Permitir el acceso a la información sobre direcciones y números telefónicos por medio de conexiones de telecomunicaciones públicamente accesibles;

c) Publicar su dirección y números telefónicos.

2.5.5.2. - Asimismo, la Ley Nº 25.506 (artículo 21, inciso k), y el Decreto Reglamentario Nº 2628/02, art. 34, incisos g, h, m, y la Resolución Rectoral Nº 2120004-ULP-2009 disponen:

a) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, la política de certificación, la información relevante de los informes de la ultima auditoria de que hubiera sido objeto, su manual de procedimientos (de corresponder) y toda información que determine la Autoridad de Aplicación;

b) Cumplir las normas y recaudos establecidos para la protección de datos personales;

c) Disponer y dedicar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y legal.

2.5.5.3. - De conformidad con lo enunciado precedentemente, el INSTITUTO debe publicar la siguiente información:

a) Esta Política de Certificación (última versión y anteriores);

b) El Acuerdo con Suscriptores de Certificados;

c) Los Términos y Condiciones con Terceros Usuarios de Certificados;

d) La Política de Privacidad;

e) La Lista de Certificados emitidos;

f) La Lista de Certificados Revocados debidamente actualizada;

g) Información relevante de los informes de auditoría de que fuera objeto el Certificador Licenciado;

h) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto del INSTITUTO;

i) El Tarifario.

2.2. - RESPONSABILIDADES

El INSTITUTO 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, 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.

No cabe responsabilidad alguna para el INSTITUTO, en caso de utilización no autorizada de un certificado, cuya descripción se encuentra establecida en esta Política de Certificación, como tampoco responde por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y procedimientos establecidos, deba ser objeto de verificación.

Asimismo, conforme lo previsto por el artículo 41 del Decreto Nº 0428-MP-2008, el INSTITUTO es responsable aun en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del INSTITUTO 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.-

2.3. - RESPONSABILIDAD FINANCIERA

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

2.4. - INTERPRETACION Y APLICACION DE LAS NORMAS

2.4.1. - Legislación 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, la Ley Nacional Nº 25.506, el Decreto Nº 2628/2002, la Resolución Rectoral Nº 2120004-ULP-2009y demás normas complementarias aplicables, dictadas por autoridad competente.

2.4.2. - Forma de interpretación y aplicación

La interpretación y/o aplicación de las disposiciones de esta Política de Certificación y demás documentación asociada, será resuelta según lo previsto en la normativa citada en el Punto 2.4.1., siguiendo el procedimiento previsto en el Punto 2.4.3..

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.

2.4.3. - Procedimientos de Resolución de Conflictos

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

Previo agotamiento del procedimiento administrativo ante el Instituto de Firma Digital de la Provincia de San Luis, la controversia o conflicto será resuelta por la Autoridad de Aplicación conforme el régimen recursivo de la Universidad de La Punta.

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

2.5. - ARANCELES

La solicitud, emisión, renovación y revocación de los certificados de clave pública emitidos bajo la presente Política de Certificación se regirá conforme lo dispuesto en el Tarifario vigente.

2.6. - PUBLICACION Y REPOSITORIOS DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRL)

2.6.1. - Publicación de información del Certificador

El INSTITUTO opera un sitio de publicación, el que se encuentra disponible en:

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

En este sitio se puede encontrar la siguiente información:

- El certificado digital de clave pública de la Autoridad Certificante Raíz de la Provincia de San Luis y el certificado digital de la Autoridad Certificante Intermedia de la Provincia;
- El certificado digital de clave pública de la Autoridad Certificante del INSTITUTO para la emisión de los certificados generados en virtud de la presente Política;
- Los datos de contacto del INSTITUTO;
- Esta Política de Certificación, el Acuerdo con Suscriptores de certificados digitales de clave pública, los Términos y Condiciones con Terceros Usuarios de certificados de clave pública, la Política de Privacidad y toda otra documentación técnica de carácter público que se emita, en sus versiones actuales y anteriores;
- El Tarifario vigente;
- La Lista de Certificados Emitidos;
- La Lista de Certificados Revocados (CRL);
- La información relevante de los datos de la última auditoría de que hubiera sido objeto el INSTITUTO;
- Los datos de las Autoridades de Registro Remotas.

El INSTITUTO también, pone a disposición de los Suscriptores 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 bajo la presente política de

certificación.

Dicho servicio de verificación:

1. Cumple con lo señalado en el RFC 2560 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 Instituto 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.

2.6.2. - Frecuencia de publicación

La información alojada en el sitio de publicación será actualizada inmediatamente después que la información a incluir en ellos haya sido verificada y autorizada por el INSTITUTO.

La Lista de Certificados Revocados (CRL) será actualizada según lo previsto en el Punto 4.4.9 de la presente Política de Certificación.

2.6.3. - Controles de acceso a la información

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

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

2.6.4. - Repositorios de Certificados y Listas de Revocación

Los sitios de publicación se encontrarán disponibles para uso público durante veinticuatro (24) horas diarias, siete (7) días a la semana, sujeto a un calendario de mantenimiento.

Tales repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por el INSTITUTO.-

2.7. - AUDITORÍAS

El INSTITUTO se encuentra sujeto a auditorías de la Autoridad de Aplicación conforme lo dispuesto en la Ley Provincial Nº V-0591-2007, el Decreto Nº 0428-MP-2008, la Resolución Rectoral Nº 2120003-ULP-2009 y la Resolución Rectoral Nº 2120004-ULP-2009.

La información relevante de los informes de la última auditoría, será publicada en el sitio de publicación del INSTITUTO.

Entre los principales temas a auditar se encontrarán: 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 de la Autoridad Certificante; Ciclo de vida de los certificados de Suscriptores; Estructura y contenido de los certificados y Listas de Certificados Revocados; Mecanismos de acceso a la documentación publicada, certificados y CRLs; Pautas para la Autoridad de Registro.

En caso de dictámenes no favorables, el Director del INSTITUTO implementará las medidas correctivas necesarias.

Las Autoridades de Registro, además, se encuentran sujetas a las auditorías del INSTITUTO.

2.8. - CONFIDENCIALIDAD

2.8.1. - Información Confidencial

Toda información referida a los Suscriptores de Certificados, que haya sido recibida por el INSTITUTO 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 el INSTITUTO tenga acceso durante el ciclo de vida de los certificados emitidos, así como cualquier otra información vinculada a la operatoria del INSTITUTO.

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

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

2.8.2. - INFORMACIÓN NO CONFIDENCIAL

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 el INSTITUTO;

e) La información legítimamente obtenida de terceros;

f) La información publicada por el Suscriptor con posterioridad al momento de su difusión.

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

a) Esta Política de Certificación;

b) El Acuerdo con los Suscriptores de Certificados;

c) Los Términos y Condiciones con Terceros Usuarios;

d) La Política de Privacidad del Instituto de Firma Digital de San Luis.

2.8.3. - PUBLICACION DE INFORMACION SOBRE LA REVOCACION DE UN CERTIFICADO

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

http://fdhabitantes.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

Y, alternativamente, en:

http://fdhabitantes1.pki.sanluis.gov.ar/cer/firmadigitalparahabitantes.crt

2.8.4. - DIVULGACION DE INFORMACION A AUTORIDADES JUDICIALES

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

2.8.5. - DIVULGACION DE INFORMACION COMO PARTE DE UN PROCESO JUDICIAL O ADMINISTRATIVO

La información confidencial en poder del INSTITUTO podrá ser revelada ante requerimiento de autoridad competente como parte de un proceso administrativo o judicial.

2.8.6. - DIVULGACION DE INFORMACION POR SOLICITUD DEL SUSCRIPTOR

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del Suscriptor o de cualquier otra información generada o recibida durante el ciclo de vida del certificado, solo podrá efectuarse previa autorización de ese Suscriptor.

No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público irrestricto.

2.8.7. - OTRAS CIRCUNSTANCIAS DE DIVULGACION DE INFORMACION

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

2.9. - DERECHOS DE PROPIEDAD INTELECTUAL

La Universidad de La Punta mantiene, en forma exclusiva, todos los derechos de propiedad intelectual con respecto a la documentación y aplicaciones pertenecientes al INSTITUTO. Asimismo, mantiene, en forma exclusiva, todos los derechos de propiedad intelectual relacionados con sus nombres y claves criptográficas.

Ninguna parte de este documento se puede reproducir o distribuir sin que la previa notificación de derechos de propiedad intelectual aparezca en forma precisa, completa y sin modificaciones, atribuyendo su autoría a la Universidad de La Punta.

3. - IDENTIFICACION Y AUTENTICACION

3.1. - REGISTRO INICIAL

El proceso de solicitud debe ser iniciado exclusivamente por el Solicitante quien deberá cumplir cada uno de los pasos y procedimiento de validación previsto en el Punto 3.1.9 de la presente Política de Certificación.

3.1.1. - TIPOS DE NOMBRES

Sólo se admitirá el nombre y apellido que figure en la documentación identificatoria de la persona solicitante de certificado digital.

3.1.2. - NECESIDAD DE NOMBRES DISTINTIVOS

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

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

"commonName" (OID 2.5.4.3: Nombre común):

Se corresponde exactamente con el nombre que figura en el documento de identidad del Suscriptor.

"serialNumber" (OID 2.5.4.5: Numero de serie):

Contiene el número de Documento de Identidad del titular que utilizó para identificarse frente a quien validó su identidad. El campo se representa bajo el formato: "DU", "LE", "LC", "CI" según corresponda Documento Nacional de Identidad, Libreta de Enrolamiento, Libreta Cívica, Cédula de Identidad.

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.

"emailAddress" (OID 1.2.840.113549.1.9.1: Correo electrónico):

Esta presente en todos los certificados y contiene la dirección de correo electrónico del Suscriptor.

"stateOrProvinceName" (OID 2.5.4.8: Provincia):

Identifica la provincia donde el Suscriptor denuncia estar domiciliado.

"countryName" (OID 2.5.4.6: Código de país):

Debe representar la nacionalidad del Suscriptor del certificado de clave pública.

Asimismo, los certificados emitidos en el marco de la presente Política de Certificación incluirán la extensión *"SubjectDirectoryAttributes"* (Atributos de Directorio del Suscriptor) el que contendrá los siguientes atributos adicionales asociados con el campo *"Subject"*, como complemento a la información presente en el mismo y en la extensión *"SubjectAlternativeName":*

"dateOfBirth" (OID 1.3.6.1.5.5.7.9.1Fecha de nacimiento):

Debe expresar la fecha de nacimiento del Suscriptor del certificado de clave pública.

3.1.3. – REGLAS PARA LA INTERPRETACION DE NOMBRES

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con los del correspondiente Documento Personal. En caso de coincidencia de nombres, el método de resolución será la combinación del "Nombre común" con el atributo "Número de serie".

3.1.4. - UNICIDAD DE NOMBRES

El nombre distintivo de cada certificado es único para cada Suscriptor.

Si dos o más Suscriptores tuvieran el mismo nombre y apellido, la unicidad queda resuelta por medio de los atributos citados en el Punto 3.1.3.

3.1.5. - PROCEDIMIENTO DE RESOLUCION DE DISPUTAS SOBRE NOMBRES

El INSTITUTO resolverá los conflictos que pudieran generarse respecto de la utilización de nombres distintivos.

3.1.6. RECONOCIMIENTO, AUTENTICACION Y ROL DE LAS MARCAS REGISTRADAS.

No aplicable.

3.1.7. - METODOS PARA COMPROBAR LA POSESION DE LA CLAVE PRIVADA

Para la comprobación de la posesión de la clave privada se utiliza el siguiente procedimiento:

a) El solicitante es participe directo y necesario para la generación de su par de claves criptográficas asimétricas.

b) Durante el proceso de solicitud, el solicitante es requerido para la generación de un par de claves criptográficas asimétricas.

c) Las claves son generadas y almacenadas en su Cédula de Identidad Provincial Electrónica o el dispositivo criptográfico aprobado por el Instituto de Firma Digital.

Si el Solicitante utiliza su Cédula de Identidad Provincial Electrónica, la generación de claves sólo puede ser realizada en Oficinas de Expedición de CIPE o en sus terminales autorizados, ambos dotados de un dispositivo identificador de terminal mediante el que se establece un canal seguro (autenticado y cifrado) con la tarjeta soporte de la CIPE. Las claves privadas se generan en la tarjeta soporte de la CIPE y no pueden ser exportadas en ningún formato.

d) 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 INSTITUTO.

e) La aplicación de la Autoridad Certificante valida el requerimiento PKCS#10.

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.

3.1.8. AUTENTICACION DE LA IDENTIDAD DE PERSONAS JURIDICAS PUBLICAS O PRIVADAS.

No aplicable.

3.1.9. - AUTENTICACION DE LA IDENTIDAD DE PERSONAS FISICAS

3.1.9.1. Autenticación de la Identidad de Personas Físicas con utilización de CIPE.

La identificación y autenticación del habitante para la solicitud de los certificados de firma digital seguirá un proceso integrado con el registro para la expedición de la CIPE.

Por lo tanto si se trata de una **primera solicitud,** el ciudadano deberá **comparecer** en una Oficina de Expedición de CIPE con la documentación que se indica en su sitio web la cual incluye su Documento Nacional de Identidad, Libreta Cívica o Libreta de Enrolamiento.

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 firma digital de personas el poseer aprobada la solicitud de emisión de la Cédula de Identidad Provincial Electrónica.

Si el Solicitante requiere la emisión de un nuevo certificado de firma digital de habitante en el dispositivo contenido en su CIPE, podrá hacerlo vía web utilizando sus certificados de autenticación y firma digital siempre que se encontraran vigentes, de lo contrario deberá presentarse ante la Oficina de Expedición de CIPE con su Documento Nacional de Identidad, Libreta Cívica, Libreta de Enrolamiento o su CIPE vigente.

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.

3.1.9.2. Autenticación de la Identidad de Personas Físicas con utilización de otros Dispositivos Criptográficos

Todo habitante de la Provincia de San Luis podrá solicitar la emisión de un certificado de clave pública en el marco de la presente Política utilizando un dispositivo criptográfico aprobado por el Instituto de Firma Digital ante las Autoridades de Registro que se constituyan a tal efecto.

Si el Solicitante posee certificado de autenticación y de firma digital de habitantes vigentes, podrá hacerlo utilizando ambos certificados a través de la página web del Instituto de Firma Digital de la Provincia de San Luis.

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

Se requiere el cumplimiento de los pasos descriptos en el punto 3.1.9 de la presente Política de Certificación.

3.3. - PROCEDIMIENTOS DE GENERACION DE UN NUEVO PAR DE CLAVES DESPUES DE UNA REVOCACION - SIN COMPROMISO DE CLAVE – Y PREVIO A LA REVOCACION O CADUCIDAD DEL PAR DE CLAVES.

3.3.1. PROCEDIMIENTO DE GENERACIÓN DE UN NUEVO PAR DE CLAVES DESPUÉS DE UNA REVOCACIÓN

Se requiere el cumplimiento de los pasos descriptos en el punto 3.1.9 de la presente Política de Certificación.

3.3.2. PROCEDIMIENTOS DE GENERACIÓN DE UN NUEVO PAR DE CLAVES PREVIO A UNA REVOCACIÓN O CADUCIDAD DE LA VIGENCIA DEL CERTIFICADO

No Aplicable

3.4. - REQUERIMIENTO DE REVOCACION

El procedimiento de revocación de un Certificado se inicia con la recepción de la solicitud de revocación por el INSTITUTO 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://fdhabitantes.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

y alternativamente en:

http://fdhabitantes1.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

Una vez validada la información contenida en la solicitud de revocación, el INSTITUTO 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 el INSTITUTO.

El servicio de consulta basado en el protocolo de comunicación OSCP, brindado por el INSTITUTO, consulta en forma *on line* la información de estado de revocación de los certificados incluidos en esta Lista de Certificados Revocados (CRL)

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - SOLICITUD DE CERTIFICADO

En el caso que el Solicitante desee utilizar como soporte de su certificado digital la Cédula de Identidad Provincial Electrónica deberá hallarse en la Autoridad de Registro instalada en cualquiera de las Oficinas de Expedición de CIPE.

Para el supuesto que desee utilizar un dispositivo criptográfico distinto a la CIPE deberá ser alguno de los aprobados por el Instituto de Firma Digital

4.2. - EMISION DEL CERTIFICADO

Una vez finalizado exitosamente el proceso de validación de la identidad del Suscriptor según los procedimientos indicados en el Punto 3.1.9 de esta Política de Certificación, la AC INSTITUTO emitirá el certificado digital correspondiente. Seguidamente, el solicitante o Suscriptor tendrá disponible su certificado para ser descargado en el dispositivo criptográfico utilizado.

Los certificados digitales tendrán una validez de DIEZ (10) años.

4.3. - ACEPTACION DEL 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. - SUSPENSION Y REVOCACION DE CERTIFICADOS

4.4.1. - CAUSAS DE LA REVOCACION

4.4.1.1. - REVOCACION VOLUNTARIA:

El Suscriptor de un certificado puede solicitar su revocación por cualquier motivo y en cualquier momento, para lo cual debe comunicarlo a la AC-INSTITUTO siguiendo el procedimiento que establece esta Política.

4.4.1.2. - REVOCACION OBLIGATORIA:

4.4.1.2.1. Por el Suscriptor:

Un Suscriptor debe obligatoriamente pedir la revocación de su certificado 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) En el caso de extravío, sustracción, destrucción, deterioro o renovación de la CIPE siempre que el certificado digital estuviera allí almacenado.

d) En caso que el suscriptor olvide su clave (PIN) o no pueda identificarse biométricamente y deba procederse al formateo de su chip CIPE

4.4.1.2.2. Por el INSTITUTO y las Autoridades de Registro:

El INSTITUTO y las Autoridades de Registro deben obligatoriamente revocar el certificado de un Suscriptor en las siguientes situaciones:

a) Ante incumplimiento por parte del Suscriptor de las obligaciones establecidas por la normativa provincial vigente, por esta Política de Certificación de la AC-INSTITUTO, por el Manual de Procedimientos o cualquier otro acuerdo, regulación o ley aplicable al certificado.

b) Si toma conocimiento que existe sospecha que la clave privada del Suscriptor se encuentra comprometida.

c) Si la AC-INSTITUTO determina que el certificado no fue emitido de acuerdo a los lineamientos de la normativa provincial vigente, de esta Política de Certificación, del Manual de Procedimientos o de los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional.

d) Si toma conocimiento del fallecimiento del Suscriptor.

4.4.1.2.3. Por la Autoridad de Aplicación:

La Autoridad de Aplicación de la Ley Nº V-0591-2007 se encuentra facultada a solicitar la revocación del certificado de clave pública de un Suscriptor en los mismos supuestos que la AC-INSTITUTO.

4.4.1.2.4. Por Organismos Públicos

Se hallan facultados a pedir la revocación de los certificados digitales los organismos públicos que tomen conocimiento fehaciente de una causal de revocación.

4.4.2. - AUTORIZADOS A PEDIR REVOCACION

Sólo pueden pedir la revocación de un certificado:

a) El Suscriptor;

b) El INSTITUTO;

c) La Autoridad de Registro;

d) La Autoridad de Aplicación;

e) La Autoridad Judicial competente;

f) Otros Organismos Públicos con autoridad para solicitarlo.

4.4.3. - PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACION

Producida una causa de revocación del certificado, el Suscriptor o bien alguno de los Terceros Autorizados indicados en la Presente Política de Certificación, deben comunicarlo a la Autoridad de Registro ante quien se hubiera realizado la validación de la identidad del Suscriptor o ante el Director de la AC-INSTITUTO, según corresponda.

Son aceptados los pedidos de revocación que se efectúen por los siguientes medios:

4.4.3.1. A través del sitio web del Instituto de Firma Digital y del sitio web del organismo emisor de la CIPE

Esta vía de revocación estará disponible las 24 horas del día, los 7 días de la semana.

Sólo podrá ser utilizada por el Suscriptor de un certificado de clave pública.

4.4.3.2. A través de un correo electrónico firmado digitalmente.

Esta vía de revocación podrá ser utilizada por los terceros autorizados conforme lo dispuesto en el Punto 4.4.2. de la Presente Política (Autorizados a Solicitar la Revocación).

El texto del mensaje debe incluir los datos de identificación del Suscriptor, Número de Serie del certificado a revocar y la causa que origina el pedido de revocación. El mail deberá ser dirigido al Responsable de la Autoridad de Registro Remota, quien deberá cumplir el trámite de revocación del certificado indicando claramente en el Asunto “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 primer hora hábil del primer día hábil siguiente al de realizado el pedido vía correo electrónico.

4.4.3.3. Personalmente.

Esta vía de revocación podrá ser utilizada por el Suscriptor o por los terceros autorizados conforme lo dispuesto en el Punto 4.4.2. – Autorizados a Solicitar la Revocación - ante alguna de las Autoridades de Registro constituídas en el marco de la presente Política de Certificación.

Si quien concurre es el Suscriptor, se dará curso al pedido de revocación en forma inmediata, previa verificación de su documento de identidad. Si quien concurre es alguno de los terceros autorizados conforme lo dispuesto en el Punto 4.4.2., aquel debe acreditar su identidad mediante presentación de su documento de identidad y la documentación que acredite que se encuentra autorizado a solicitar la revocación.

En ambos casos, deberá labrarse un Acta en la que se dejará constancia de los datos del Suscriptor del certificado, el Número de Serie del Certificado a Revocar, los datos de quien requiere la revocación del certificado y la causa de la solicitud. La misma deberá ser suscripta por el requirente y el responsable de la Autoridad de Registro que interviene, debiendo cada uno de ellos conservar un ejemplar de la misma.

Este requerimiento podrá realizarse únicamente en días y horarios hábiles de la Administración Pública Provincial.

4.4.3.4. Procedimiento de Excepción.

Dada la urgencia del caso y siempre que existan causas suficientes que lo justifiquen, el Responsable de la Autoridad de Registro o Director de la AC-INSTITUTO puede autorizar la revocación de un certificado de clave pública obviando la presentación del pedido de revocación y efectuando una confirmación telefónica de la solicitud.

4.4.4. PLAZO PARA LA SOLICITUD DE REVOCACIÓN

La recepción de la solicitud de revocación está disponible los siete días de la semana, durante las veinticuatro horas del día a través de la página web.

La solicitud recibida será procesada de inmediato, conforme lo exigido por la normativa vigente.

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado digital en los sitios de publicación será de 24 horas para la Lista de Certificados Revocados.

4.4.5. CAUSAS DE SUSPENSION

No aplicable.

4.4.6. AUTORIZADOS A SOLICITAR SUSPENSION

No aplicable.

4.4.7. PROCEDIMIENTOS PARA LA SOLICITUD DE SUSPENSION.

No aplicable.

4.4.8. LIMITES DEL PERIODO DE SUSPENSION DEL CERTIFICADO

No aplicable.

4.4.9. FRECUENCIA DE EMISION DE LISTAS DE CERTIFICADOS REVOCADOS

El INSTITUTO mantiene publicada una Lista de Certificados Revocados en forma permanente, efectuando su actualización semanalmente.

Sin perjuicio de ello, toda vez que se produce una revocación, el INSTITUTO 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 deberá ser suscripta por la AC INSTITUTO.

El acceso a las Listas de Certificados Revocados es público, no pudiendo establecerse ninguna clase de restricción. Se encuentra disponible en el sitio web del INSTITUTO en el siguiente URL:

http://fdhabitantes.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

Y, alternativamente, en:

http://fdhabitantes1.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

4.4.10. REQUISITOS PARA LA VERIFICACION DE LA LISTA DE CERTIFICADOS REVOCADOS

Los Terceros Usuarios deben verificar la validez de los certificados digitales emitidos por el INSTITUTO utilizados para firmar documentos por él recibidos, a través de las siguientes acciones:

I) Utilizando la Lista de Certificados Revocados

a) Verificar que el certificado digital correspondiente al documento firmado, no se encuentre incluido en la Lista de Certificados Revocados publicada en el sitio

http://fdhabitantes.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

Y, alternativamente, en:

http://fdhabitantes1.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

b) Verificar la autenticidad de la Lista de Certificados Digitales, mediante la verificación de la firma digital de la AC INSTITUTO 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.

II) Utilizando el servicio de consulta basado en el protocolo de comunicación OSCP,

disponible en

http://ocsp.pki.sanluis.gov.ar/ocsp

4.4.11. DISPONIBILIDAD DEL SERVICIO DE CONSULTA SOBRE REVOCACION Y DE ESTADO DEL CERTIFICADO

La verificación del estado de los certificados puede realizarse indistintamente a través del servicio de consulta basado en el protocolo de comunicación OCSP, o de la consulta de las Listas de Certificados Revocados, disponibles de manera permanente y gratuita en el sitio web:

http://fdhabitantes.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

Y, alternativamente, en:

http://fdhabitantes1.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl

4.4.12. REQUISITOS PARA LA VERIFICACION EN LINEA DEL ESTADO DE REVOCACION

Para utilizar el servicio de consulta basado en el protocolo de comunicación OSCP es necesario poseer conexión a internet.

4.4.13. OTRAS FORMAS DISPONIBLES PARA LA DIVULGACION DE LA REVOCACION.

No aplicable.

4.4.14. REQUISITOS PARA LA VERIFICACION DE OTRAS FORMAS DE DIVULGACION DE REVOCACION

No aplicable.

4.4.15. REQUISITOS ESPECIFICOS PARA CASOS DE COMPROMISO DE CLAVES

El Suscriptor debe informar al INSTITUTO 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 4.4.3. de la presente Política “Procedimiento para la solicitud de revocación”.

4.5. PROCEDIMIENTOS DE AUDITORIA DE SEGURIDAD

La AC del INSTITUTO mantiene registros de auditoría de todas las operaciones que realiza, protegiendo su integridad, en medios de almacenamiento encriptados y conservándolos por diez (10) años.

Los referidos registros son utilizados para tareas de monitoreo habitual, del funcionamiento de los sistemas y procesos, para posibles auditorías internas y externas.

Asimismo, se mantienen registros no informatizados de toda aquella información que no ha sido registrada en el sistema.

4.6. ARCHIVOS DE REGISTRO DE EVENTOS REGISTRADOS

La AC del INSTITUTO conserva el registro de eventos sobre cada una de las siguientes actividades:

4.6.1. ADMINISTRACION DEL CICLO DE VIDA DE LAS CLAVES CRIPTOGRAFICAS

a) Generación y almacenamiento de las claves criptográficas del certificador.

b) Resguardo y recuperación de las claves criptográficas del certificador

c) Utilización de las claves criptográficas del certificador

d) Archivo de las claves criptográficas del certificador

e) Retiro de servicio de datos relacionados con las claves criptográficas

f) Destrucción de claves criptográficas del certificador

g) Identificación de la entidad que autoriza una operación de administración de claves criptográficas

h) Identificación de la entidad que administra los datos relativos a las claves criptográficas

i) Compromiso de la clave privada

4.6.2. ADMINISTRACION DEL CICLO DE VIDA DE LOS CERTIFICADOS

a) Recepción de solicitudes de certificados

b) Transferencia de claves públicas para la emisión del certificado

c) Cambios en los datos de la solicitud del certificado

d) Generación de certificados

e) Distribución de la clave pública del certificador

f) Solicitudes de revocación de certificados

g) Generación y emisión de listas de certificados revocados

h) Acciones tomados en relación con la expiración de un certificado

4.6.3. ADMINISTRACION DEL CICLO DE VIDA DE LOS DISPOSITIVOS CRIPTORGRAFICOS

Recepción del dispositivo

Ingreso o retiro del dispositivo del lugar de almacenamiento

Instalación del dispositivo

Uso del dispositivo

Desinstalación del dispositivo

Envío de un dispositivo para servicio técnico o reparación

Retiro, baja o borrado de información del dispositivo

4.6.4. INFORMACION RELACIONADA CON LA SOLICITUD DE CERTIFICADOS

Tipos de documentos de identificación presentados por el solicitante

Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación

Identificación de la entidad que recibe y acepta la solicitud

Método utilizado para validar los documentos de identificación

Identificación de la Autoridad de Registro

4.6.5. EVENTOS DE SEGURIDAD

Lecturas y/o escrituras en archivos sensibles de seguridad

Borrado de datos sensibles de seguridad

Cambios en los perfiles de seguridad

Registro de intentos exitosos y fallidos de accesos al sistema, los datos y recursos.

Caídas del sistema, fallas en el hardware y software, u otras anomalías

Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad

Cambios en la relación entre la Autoridad Certificante y su Autoridad de Registro o personal relacionado con el proceso de certificación

Accesos a los componentes del sistema de la Autoridad Certificante

Eventos o situaciones no previstas

4.7. - CAMBIO DE CLAVES CRIPTOGRAFICAS DEL INSTITUTO

El par de claves criptográficas de la AC INSTITUTO para esta Política tendrán una duración 60 años.

El cambio de par de claves criptográficas de la Autoridad Certificante del INSTITUTO dará origen a la emisión de un nuevo certificado por parte de la Autoridad Certificante Raíz de la Provincia de San Luis.

4.8. - PLAN DE CONTINGENCIA Y RECUPERACION ANTE DESASTRES

El INSTITUTO cuenta con un Plan de Contingencia que permite garantizar el mantenimiento mínimo de la operatoria y la recuperación de los recursos comprometidos dentro de las 24 horas de producida una emergencia.

El Plan de Contingencia comprende el conjunto de procedimientos que debe llevar a cabo su personal ante eventos que impidan la continuidad de sus operaciones. El Plan es conocido por todo el personal del INSTITUTO e incluye pruebas periódicas para garantizar su implementación efectiva en caso necesario.

El INSTITUTO dispone controles que aseguran:

a) La continuidad de las operaciones en caso de desastre.

b) La continuidad de las operaciones en caso de la vulneración de su clave privada.

Para ello el INSTITUTO establece procedimientos para minimizar las interrupciones de sus actividades y para proteger los procesos críticos de los efectos de fallas significativas o desastres. La administración de la continuidad de las operaciones incluirá controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Los procedimientos se encuentras descriptos detalladamente en el referido Plan de Contingencia.

4.8.1. - COMPROMISO DE RECURSOS INFORMATICOS, APLICACIONES Y DATOS

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

4.8.2. - CONTINUIDAD DE LAS OPERACIONES DE LA AUTORIDAD CERTIFICANTE DEL INSTITUTO

El INSTITUTO dispone de procedimientos para asegurar la continuidad de sus operaciones en instalaciones alternativas. El INSTITUTO comunicará a los Suscriptores de Certificados si el evento afecta actividades previstas.

4.8.3. - COMPROMISO DE LA CLAVE PRIVADA DE LA AUTORIDAD CERTIFICANTE DEL INSTITUTO

Ante sospecha de compromiso de la Clave Privada del INSTITUTO, el mismo dispone de Procedimientos para la Revocación de su Certificado y el Restablecimiento de su Infraestructura, contemplándose las siguientes actividades:

a) Ceremonia de generación de un nuevo Par de Claves,

b) Publicación del Nuevo Certificado,

c) Emisión de nuevos Certificados para los Suscriptores.

El INSTITUTO tomará las siguientes acciones:

a) Informar a los Suscriptores que sus Certificados serán revocados y que las Claves Privadas asociadas a esos Certificados no deben ser utilizadas;

b) Revocar los Certificados Digitales de los Suscriptores;

c) Publicar en su sitio de publicación que se ha revocado el Certificado de la AC INSTITUTO, notificando a los Terceros Usuarios que no deben considerarlo como un certificado confiable.

4.9. - PLAN DE CESE DE ACTIVIDADES

El eventual cese de actividades de la Autoridad Certificante queda reservado a una decisión del INSTITUTO, que deberá ser comunicada a la Autoridad de Aplicación.

En caso de producirse el Cese de Actividades, el INSTITUTO cumplirá con los siguientes procedimientos:

a) Publicará en el Boletín Oficial durante tres (3) días consecutivos la fecha y hora del Cese de sus actividades, que no podrá ser anterior a los NOVENTA (90) días corridos contados desde la fecha de la última publicación, en un diario de difusión provincial y en el sitio web del INSTITUTO;

b) Notificará a los Suscriptores vía correo electrónico con una antelación no menor a los NOVENTA (90) días de la fecha prevista de cese;

c) Revocará la totalidad de los Certificados que hubiere emitido y que se encontraren vigentes a la fecha de Cese de sus Actividades;

d) Una vez revocados los Certificados, destruirá la Clave Privada de la AC INSTITUTO mediante un procedimiento que garantice su destrucción total de acuerdo al último estado del arte.

Toda información digital será resguardada por el INSTITUTO por un plazo de diez (10) años, así como toda la documentación de respaldo de las solicitudes. Si el cese se debiera a la disolución del INSTITUTO, los registros pasarán a manos del organismo que se instituya para realizar funciones similares o, en su defecto, a la Autoridad de Aplicación.

5. - CONTROLES DE SEGURIDAD FISICA, FUNCIONALES Y PERSONALES

5.1. - CONTROLES DE SEGURIDAD FISICA

El INSTITUTO ha implementado controles apropiados que restringen el acceso a los equipos, programas y datos utilizados por la AC INSTITUTO para la provisión del servicio de Certificación, limitándolo a personas debidamente autorizadas.

La AC INSTITUTO opera en instalaciones construidas bajo estrictas normas internacionales de seguridad física y ambiental que le brindan una protección adecuada.

5.1.1. - CONSTRUCCION Y UBICACION DE LAS INSTALACIONES

Para realizar las operaciones de la Autoridad Certificante, el INSTITUTO cuenta con instalaciones apropiadas que disponen de controles físicos para evitar, prevenir y detectar el acceso indebido a los equipos, programas y datos utilizados. Las instalaciones poseen perímetros de seguridad expresamente definidos.

5.1.2. - NIVELES DE ACCESO FISICO

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

5.1.3. - ENERGIA ELECTRICA Y AIRE ACONDICIONADO

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

5.1.4. - EXPOSICION AL AGUA E INUNDACIONES

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

5.1.5. - PREVENCION Y PROTECCION CONTRA INCENDIO

Los equipos de la AC INSTITUTO están alojados en instalaciones que cuentan con alarmas de detección y sistemas de extinción de incendios.

5.1.6. - MEDIOS DE ALMACENAMIENTO DE INFORMACION

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

El INSTITUTO almacena copias completas de respaldo en instalaciones externas. Además

cuenta con procedimientos de recuperación escritos que son verificados periódicamente.

5.1.7. DESCARTE DE MEDIOS DE ALMACENAMIENTO DE INFORMACION

- Disposición Final o Reutilización segura de los equipos y medios de almacenamiento-

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

5.2. - CONTROLES FUNCIONALES

El INSTITUTO ha establecido una estructura de personal estable con roles específicos, definidos para realizar las actividades de emisión de certificados y operación de la AC INSTITUTO que contempla una adecuada separación de funciones.

5.2.1. - DEFINICION DE ROLES AFECTADOS AL PROCESO DE CERTIFICACION

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

5.2.2. - SEPARACION DE FUNCIONES

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

5.2.3. - NUMERO DE PERSONAS REQUERIDO POR FUNCION

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

5.2.4. - IDENTIFICACION Y AUTENTIFICACION PARA CADA ROL

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

5.3. - CONTROLES DE SEGURIDAD DEL PERSONAL

El INSTITUTO sigue la Política de administración de personal establecida para la Universidad de La Punta y las específicamente previstas en el Plan de Seguridad.

5.3.1. - ANTECEDENTES LABORALES, CALIFICACIONES, EXPERIENCIA E IDONEIDAD DEL PERSONAL

El personal del INSTITUTO posee experiencia y calificaciones adecuadas para las funciones que desempeñan. Dicho personal tiene pleno conocimiento de las Políticas de Seguridad y Certificación que permiten mantener un ambiente seguro y confiable así como del resto de la documentación asociada a la presente Política.

El personal del INSTITUTO ha sido cuidadosamente seleccionado y calificado antes de

iniciar sus actividades.

5.3.2. - ENTRENAMIENTO Y CAPACITACIÓN INICIAL

El personal del INSTITUTO ha sido entrenado adecuadamente antes de iniciar sus actividades.

5.3.3. - FRECUENCIAS DEL PROCESO DE ACTUALIZACION TECNICA

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

5.3.4. - SANCIONES A APLICAR POR ACTIVIDADES NO AUTORIZADAS

El personal del INSTITUTO que incumpliere sus funciones y responsabilidades, será sancionado de acuerdo al régimen de sanciones establecido por la Universidad de La Punta

5.3.5. - REQUISITOS PARA CONTRATACION DE PERSONAL

El personal del INSTITUTO es contratado de acuerdo al régimen de la Universidad de La Punta.

5.3.6. - DOCUMENTACION Y MATERIALES PROVISTOS AL PERSONAL

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

Asimismo, el personal cuenta con tarjetas de aproximación personal y enrolamiento en censores biométricos, según los diferentes niveles de seguridad física a los cuales puede tener acceso y dispositivos criptográficos, conforme el rol asignado.

6. - CONTROLES DE SEGURIDAD TECNICA

6.1. . - GENERACION E INSTALACION DEL PAR DE CLAVES CRIPTOGRAFICAS

6.1.1. - GENERACION DEL PAR DE CLAVES CRIPTOGRAFICAS

A) El Par de Claves Criptográficas de la Autoridad Certificante es generado en hardware criptográfico seguro que cumple con las características definidas en FIPS 140 Versión 2 para el nivel 3.

El Par de Claves criptográficas utilizadas por el INSTITUTO 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 utilizando un dispositivo criptográfico seguro que cumple con las características definidas en FIPS 140 Versión 2 para el nivel 3

La Autoridad de Registro genera su clave mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

C) El par de claves criptográficas de los Suscriptores son generadas y almacenadas en dispositivos criptográficos que cumplen con las disposiciones previstas en FIPS 140 Versión 2 Nivel 2.

Los Suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

6.1.2. - ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Las claves privadas de los Suscriptores son generadas por ellos mismos durante el proceso de solicitud, absteniéndose el INSTITUTO de generar, exigir o por cualquier otro medio tomar conocimiento o acceder, a sus datos de creación de firma.

Para la generación y almacenamiento de las claves, los Suscriptores cuentan con dispositivos criptográficos externos que las protegen por medio de dos factores de seguridad:

a) Mediante la posesión del dispositivo,

b) Mediante un PIN o contraseña definida por el propio Suscriptor, o mediante huella biométrica.

6.1.3. - ENTREGA DE LA CLAVE PUBLICA AL INSTITUTO

Durante el proceso de solicitud del certificado, la clave pública del Solicitante es entregada al INSTITUTO 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.

Los solicitantes deben probar su identidad y demostrar que la solicitud les pertenece presentándose frente a la Autoridad de Registro.

6.1.4. - DISPONIBILIDAD DE LA CLAVE PUBLICA

El INSTITUTO publica los certificados de clave pública de la Autoridad Certificante Raíz de la Provincia de San Luis, de la Autoridad Certificante Intermedia de la Provincia de San Luis, de la Autoridad Certificante emitido a los efectos de la generación de los certificados de firma digital de habitantes de la Provincia de San Luis y los que hubiere emitido a los Suscriptores en:

http://pki.sanluis.gov.ar

6.1.5. - TAMAÑO DE CLAVES

A) La Autoridad Certificante utiliza un par de claves criptográficas RSA de 4096 bits de longitud para emitir los certificados.

B) La Autoridad de Registro utiliza claves RSA con un tamaño mínimo de 1024 bits.

C) Los Suscriptores de certificados utilizan claves RSA con un tamaño mínimo de 1024 bits.

6.1.6. - GENERACION DE PARAMETROS DE CLAVES ASIMETRICAS

Los parámetros son:

Algoritmo: RSA

Exponente: 65537

Longitud: según se indica en el Punto 6.1.5.

6.1.7. - VERIFICACION DE CALIDAD DE LOS PARAMETROS

No se requieren verificaciones particulares de la calidad de los parámetros de generación de claves toda vez que no podrá ser solicitado certificado digital sin utilizar alguno de los modelos homologados por el INSTITUTO.

6.1.8. .- GENERACION DE CLAVES POR HARDWARE O SOFTWARE

El Par de Claves criptográficas se generan en dispositivos criptográficos que cumplan con lo definido en el punto 6.2.1 de la presente Política de Certificación, es decir:

a) Las claves de la Autoridad Certificante son generadas por hardware sobre dispositivos criptográficos FIPS 140-2 nivel 3.

b) Las claves de la Autoridad de Registro son generadas por hardware sobre dispositivos criptográficos FIPS 140-2 nivel 2.

c) Las claves de los Suscriptores son generadas por hardware sobre dispositivos criptográficos FIPS 140-2 nivel 2.

6.1.9. - PROPÓSITOS DE UTILIZACION DE CLAVES (campo “Key Usage” en certificados X.509 v.3)

Las claves criptográficas del INSTITUTO tienen como exclusivo propósito la firma de los Certificados de sus Suscriptores y su Lista de Certificados Revocados (CRL).

Las claves criptográficas de los Suscriptores podrán ser utilizadas exclusivamente para los fines definidos por la Política de Certificación que le sea de aplicación.

Los valores a utilizar son: “Firma Digital, Sin Repudio” “Cifrado de Clave” “Cifrado de Datos”.

6.2. - PROTECCION DE LA CLAVE PRIVADA

6.2.1. - ESTANDARES PARA DISPOSITIVOS CRIPTOGRAFICOS

a) La Autoridad Certificante del INSTITUTO dispone de un dispositivo criptográfico que cumple con las características definidas en FIPS 140 versión 2, nivel 3, para la generación y almacenamiento de su Par de Claves criptográficas;

b) Para el personal de sus Autoridades de Registro, serán de Nivel 2;

c) Para los Suscriptores de certificados digitales, el estándar correspondiente es de Nivel 2.

6.2.2. - CONTROL ”M DE N” DE LA CLAVE PRIVADA

La clave privada de la Autoridad Certificante es activada exclusivamente en las instalaciones del INSTITUTO 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 cuatro funcionarios de la Autoridad Certificante Raíz de la Provincia de San Luis y dos del INSTITUTO.

Lo dicho no se hace necesariamente extensivo a las Autoridades de Registro.

6.2.3. - RECUPERACION DE LA CLAVE PRIVADA

En caso de necesidad, el INSTITUTO posee procedimientos para la recuperación de su Clave Privada a partir de sus copias de respaldo, detallados en su Manual de Procedimientos de Certificación.

Esta recuperación solo puede ser realizada por personal autorizado, sobre uno de los dispositivos criptográficos seguros de los que dispone el INSTITUTO y exclusivamente en los niveles de seguridad de la Autoridad Certificante en su sitio principal o de contingencia.-

No se implementan mecanismo 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

El INSTITUTO mantiene una copia de seguridad (es realizada inmediatamente después de su generación por personal autorizado) de su Clave Privada.

6.2.5. - ARCHIVO DE CLAVE PRIVADA

La copia de seguridad de la clave privada es almacenada y protegida con un nivel de seguridad no inferior al establecido para la versión original de la Clave y mantenida por el plazo de validez del Certificado correspondiente.

6.2.6. - INCORPORACION DE CLAVES PRIVADAS EN DISPOSITIVOS CRIPTOGRAFICOS

A) Las Claves Privadas se generan en dispositivos criptográficos conforme lo establecido en la presente Política y nunca se extraen de los mismos.

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

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

B) La clave privada de la Autoridad de Registro y la de los Suscriptores es almacenada en el mismo dispositivo criptográfico donde es generada y no permite su exportación.

6.2.7. - METODO DE ACTIVACION DE CLAVES PRIVADAS

A) La activación de la Clave Privada de la AC INSTITUTO 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 cuatro funcionarios de la Autoridad Certificante Raíz de la Provincia de San Luis y dos, de la AC INSTITUTO.

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 y los Suscriptores tienen acceso a su clave privada y a su certificado contenidos en el dispositivo criptográfico a través de PIN/ contraseña o huella biométrica.

6.2.8. - METODO DE DESACTIVACION DE CLAVES PRIVADAS

La desactivación de las claves privadas de la AC INSTITUTO 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 deberá ser realizado por personal técnico, de seguridad y funcionarios testigos que garanticen la operación.

6.2.9. - METODO DE DESTRUCCION DE CLAVES PRIVADAS

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

6.3. - OTROS ASPECTOS DE ADMINISTRACION DE CLAVES

6.3.1. - ARCHIVO PERMANENTE DE LA CLAVE PUBLICA

Los certificados digitales, con sus claves públicas, se almacenan en repositorios de certificados digitales, permitiendo de este modo la verificación de su integridad y de su vigencia por medio del servicio asociado en el sitio web de la Autoridad Certificante.

Los repositorios de certificados digitales se encuentran en el sitio web:

https://www.pki.sanluis.gov.ar

6.3.2. - PERIODO DE USO DE CLAVE PUBLICA Y PRIVADA

El período de validez del Par de Claves se corresponde con el período de validez de los Certificados emitidos.

Todos los certificados emitidos por el INSTITUTO bajo la presente Política a favor de los Suscriptores tienen un período de vigencia de DIEZ (10) años, contados a partir de la fecha de emisión. Esta información consta expresamente en el certificado.

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.

6.4. - DATOS DE ACTIVACION

6.4.1. - GENERACION E INSTALACION DE DATOS DE ACTIVACION

A) Los datos de activación de las Claves Privadas de la AC INSTITUTO 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 huella biométrica. Esta clave de seguridad, conocida solo por el Suscriptor, protege su clave privada e impide el acceso a la misma por parte de terceros, incluida la AC INSTITUTO

6.4.2. - PROTECCION DE LOS DATOS DE ACTIVACION

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.

6.4.3. - OTROS ASPECTOS REFERIDOS A LOS DATOS DE ACTIVACION

No es Aplicable

6.5. - CONTROLES DE SEGURIDAD INFORMATICA

6.5.1. - REQUISITOS TECNICOS ESPECIFICOS

Sólo personal debidamente autorizado puede acceder a las instalaciones y sistemas que intervienen en las operaciones de Certificación. Acorde a la Política de Seguridad del INSTITUTO se garantiza:

a) Una efectiva administración de los accesos para aquellos usuarios involucrados en el ciclo de vida de los Certificados,

b) La segregación de funciones según lo especificado en la Política de Seguridad,

c) La correcta identificación y autenticación del personal en las actividades críticas relacionadas con el ciclo de vida de los certificados,

d) El registro de eventos relacionados con el ciclo de vida de los certificados,

e) La protección, integridad y confidencialidad de datos críticos.

6.5.2. CALIFICACIONES DE SEGURIDAD COMPUTACIONAL

a) LUNA SA 4.3

Certificaciones Regulatorias Estándar

• *U/L 1950 (EN60950) & CSA*

C22.2 y en conformidad con CSA

C22.2

• *FIPS 140-2, Nivel 3 validado*

• *RoHS en conformidad*

• *BAC y EAC Certificación ePassport*

Protocolos SSL Soportados

• SSL v2.0, SSL v3.0, TLS

• Cryptographic APIs

• PKCS#11 v2.01, Microsoft CAPI v2.0

Características del Cryptographic Acceleration Hardware

• FIPS 140-2 Nivel 3 validado

• True hardware accSelerated para la generación acelerada de número aleatorio (Anexo C of ANSI X9.17)

• Generación de par de llaves simétricas y asimétricas

• Encriptación y desencriptación RSA (RSA 512-BIT TO 4096-bit longitud de llave)

Algoritmos Criptográficos

• Llave asimétrica

• Diffie-Hellman (1024-4096 bit)

• RSA (512-4096 bit) (PKCS#1#1 v1.5, OAEP PKCS#1 V2.0)

Firma Digital

Rsa (1024-4096 bit), DSA (512-1024-bit), (PKCS#1 v1.5)

Llaves simétricas

3DES, (doble y triple longitud de llave), AES, RC2, RC4, RC5,

CAST-128

Hash Digest

SHA-1, SHA-2 (160, 256, 512), MD-5

Claves de Autenticación de Mensaje (MAC)

HMAC-MD5, HMAC-SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC

Características Físicas

Conectividad

• *2x10/100 Ethernet, CAT5, UTP*

• *Hasta 800 NTLS*

• *Puerto de autenticación Luna PED*

• *Consola de puerto local en serie*

• *Ranura para token Luna PC-Card*

Almacenamiento Extraíble

• *Ranura para PC-Card Tipo II, 5V*

Hardware con Aceleración SSL de Alto Desempeño

Luna SA proporciona hasta 4000 sesiones SSL por segundo (RSA 1024-bit desencriptaciones).

b) <u>Certificaciones y descripción de Célula de Sala Cofre</u>

- Material refractario resistente al fuego y gases corrosivos
- Estructura auto-portante para paredes, techo y piso
- Puertas herméticas de cerramiento automático y blindaje de cables y ductos
- Carga de losa reducida, desmontable, reubicable y expansible
- Estanqueidad comprobada contra gases corrosivos y polvo, de acuerdo con la norma DIN 18095.

- Estanqueidad en relación al agua de basamentos o de combate a incendio, de acuerdo con el laudo bw 8995.01 del LGA.

- Testeada y aprobada como conjunto, simulando la situación real de incendio, según la norma europea EN 1047-2:2000 y la VDMA Alemana 24991/2.

- Certificado EN1047-2 por ECBS (Consejo Europeo de Certificación).

- Certificación -Seguridad: Certificado ABNT 15247

La tecnología de Sala Cofre IT Modular, está certificada bajo norma EN 1047/2 es producida exclusivamente en Alemania o Brasil, bajo el control y procesos de calidad de Lampertz AG, lo que permite garantizar la producción ininterrumpida de células Lampertz aún en caso de desastres en alguna de estas fábricas.

c) TRAMIX PKI

El software de administración TRAMIX PKI, se basa en todos los servicios de certificados nativos del Windows 2003 Server, permitiendo a su vez darle soporte documental a todos los circuitos diseñados para implementar la infraestructura de clave pública.

Se trata de un software totalmente escalable, modular e integrable, e incluye todas las llamadas a las funciones de Windows 2003 Server que cuenta con un completo sistema de seguridad diseñado según las normativas de seguridad ITU: X.509v3, RSA: PKCS 1,7,9,10,12 y IETF: RFC2459, CMC, concordante con las de la provincia de San Luis y de la Nación, en especial la DA 06/2007.

6.6. - 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 del INSTITUTO y de su Autoridad Certificante utilizan sistemas debidamente protegidos, garantizando su integridad.

6.7. .- CONTROLES DE INGENIERIA DE DISPOSITIVOS CRIPTOGRAFICOS

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

6.8. - CONTROLES TECNICOS DEL CICLO DE VIDA DE LOS SISTEMAS

6.8.1. - CONTROLES DE DESARROLLO DE SISTEMAS

No aplica.

6.8.2. - ADMINISTRACION DE CONTROLES DE SEGURIDAD

No aplica.

6.8.3. . CALIFICACIONES DE SEGURIDAD DEL CICLO DE VIDA DEL SOFTWARE

No aplica.

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

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

7.1. - PERFIL DEL CERTIFICADO

Se usarán los siguientes campos del formato X.509 versión 3 en el Certificado de la Autoridad Certificante del INSTITUTO para la presente Política de Certificación:

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	Sha1RSA
Nombre distintivo del emisor	CN= CA del Instituto de Firma Digital de la Provincia de San Luis OU= Universidad de La Punta O= Gobierno de la Provincia de San Luis C= AR
Validez	60 años Se especifica desde/hasta
Nombre Distintivo del Suscriptor	CN= CA IFDPSL de Firma Digital para Habitantes OU= Universidad de La Punta OU= http://www.pki.sanluis.gov.ar/firmadigitalparahabitantes/cps.pdf O= Gobierno de la Provincia de San Luis C= AR
Clave Pública del Suscriptor	La Clave Pública RSA es de 4096 bits
Extensiones	
Identificador de la Clave del Suscriptor	Contiene un hash de 20 bytes del atributo Clave Pública del Suscriptor
Uso de Claves	Firma digital, Firma de certificados, Firma CRL sin conexión, Firma CRL
Políticas de Certificación	Constará el OID correspondiente a la Política de Certificación asignado al Ente Licenciante Provincial 2.16.32.1.3.2.1.1.0

Restricciones Básicas	cA=TRUE
Punto de distribución de la Lista de Certificados Revocados	URL = http://acraiz.sanluis.gov.ar/crl/entelicenciante.crl URL = http://acraiz1.sanluis.gov.ar/crl/entelicenciante.crl
Información de acceso de la Autoridad Certificante	URL = http://acraiz.sanluis.gov.ar/cer/entelicenciante.crt URL = http://acraiz1.sanluis.gov.ar/cer/entelicenciante.crt

Se usarán los siguientes campos del formato X.509 versión 3 en el Certificado de Firma Digital de los Suscriptores de Certificados:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Numero de Serie	Número asignado por la CA Firma Digital para Habitantes
Algorítmo de firma	sha1RSA
Nombre distintivo del emisor	CN= CA IFDPSL de Firma Digital para Habitantes OU= Universidad de La Punta OU=http://www.pki.sanluis.gov.ar/firmadigitalparahabitantes/cps.pdf O= Gobierno de la Provincia de San Luis C= AR
Validez	10 años Se especifica desde/hasta
Nombre distintivo del Suscriptor	CN= <Nombre del Suscriptor> Serial Number = <Número Documento> E = <Email> S = <Provincia> C= <Nacionalidad del Suscriptor>
Clave pública del Suscriptor	La Clave Pública RSA no debe ser menor a 1024 bits
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la CA Firma Digital para Habitantes
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, Cifrado de clave, Cifrado de datos
Políticas de Certificación	OID de la Política de Certificación en virtud de la cual se emite el certificado al suscriptor. Es otorgado por el Ente Licenciante Provincial. “2.16.32.1.3.2.1.1.2”

Atributos de Directorio del Suscriptor	2.5.29.9.= <Fecha de nacimiento del Suscriptor>
Restricciones básicas	cA=FALSE pathlen=0
Puntos de distribución de la lista de certificados revocados	http://fdhabitantes.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl Y, alternativamente, en: http://fdhabitantes1.pki.sanluis.gov.ar/crl/firmadigitalparahabitantes.crl http://ocsp.pki.sanluis.gov.ar/ocsp
Información de Acceso de la Autoridad Certificante	http://fdhabitantes.pki.sanluis.gov.ar/cer/firmadigitalparahabitantes.crt http://fdhabitantes1.pki.sanluis.gov.ar/cer/firmadigitalparahabitantes.crt

7.2. - PERFIL DE LA LISTA DE CERTIFICADOS REVOCADOS

Se usarán los siguientes campos del formato X.509 versión 2 en la Lista de Certificados Revocados (CRL) de la Autoridad Certificante Raíz:

X.509 v2 Certificado Atributos / Extensiones	Contenido
ibutos	
Versión	V2
Algoritmo de Firma	sha1RSA
Nombre Distintivo del Emisor	CN= CA IFDPSL de Firma Digital para Habitantes OU= Universidad de La Punta OU= http://www.pki.sanluis.gov.ar/firmadigitalparahabitantes/ cps.pdf O= Gobierno de la Provincia de San Luis C = AR
Día y Hora de Vigencia	Día y hora de emisión de esta CRL
Próxima actualización	Día y hora de la próxima emisión de 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 cambia una CRL

8. .- ADMINISTRACION DE ESPECIFICACIONES

8.1. .- PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIONES

El INSTITUTO 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 Universidad de La Punta.

Toda modificación será sometida a la aprobación de la Autoridad de Aplicación.

8.2. - PROCEDIMIENTOS DE PUBLICACION Y NOTIFICACION

El INSTITUTO publicará, en su sitio de publicación, las modificaciones aprobadas a la Política de Certificación, indicando en cada caso, el texto reemplazado. Asimismo, publicará el texto de la nueva versión del documento modificado.

Lo mismo se aplica al Acuerdo con Suscriptores de Certificados de la AC INSTITUTO y a los Términos y Condiciones con Terceros Usuarios de Certificados de la AC INSTITUTO.

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.

8.3. - PROCEDIMIENTOS DE APROBACION

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