

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 1 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

ANEXO I

Resolución Rectoral N° 2240005-ULP-2009

POLITICA DE CERTIFICACION

DEL ENTE LICENCIANTE DE LA PROVINCIA DE SAN LUIS

INFRAESTRUCTURA DE FIRMA DIGITAL

DE LA PROVINCIA DE SAN LUIS

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 2 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Contenido

1- INTRODUCCION	4
1.1.- DESCRIPCIÓN GENERAL.....	5
1.2. - IDENTIFICACIÓN	5
1.3 - PARTICIPANTES Y APLICABILIDAD	6
1.3.1. – Certificador	6
1.3.1.1. Autoridad de Aplicación de la Provincia de San Luis	6
1.3.1.2.- Ente Licenciante de la Provincia de San Luis.....	7
1.3.2.- Autoridad de Registro.....	7
1.3.3.- Suscriptores de Certificados	7
1.3.4.- Aplicabilidad.....	7
1.4.- CONTACTOS	8
2.- ASPECTOS GENERALES DE LA POLITICA DE CERTIFICACION	8
2.1. - OBLIGACIONES.....	8
2.1.1. – Obligaciones y atribuciones de la Autoridad de Aplicación de la Provincia de San Luis.....	8
2.1.1.2. Obligaciones del Ente Licenciante de la Provincia de San Luis	9
2.1.2.- Obligaciones de la Autoridad de Registro	10
2.1.3. - Obligaciones de los Certificadores Licenciados.....	10
2.1.5.- Obligaciones del Servicio de Repositorio.....	12
2.1.6.- Obligaciones de los Terceros Usuarios:.....	12
2.2.- RESPONSABILIDADES	13
2.3.- RESPONSABILIDAD FINANCIERA	13
2.3.1. - Responsabilidad Financiera del Ente Licenciante	13
2.4.- INTERPRETACIÓN Y APLICACIÓN DE LAS NORMAS	13
2.4.1.- Legislación Aplicable	13
2.4.2.- Forma de Interpretación y Aplicación	14
2.4.3.- Procedimientos de Resolución de Conflictos	14
2.5.- ARANCELES	15
2.6.- PUBLICACIÓN Y REPOSITORIOS DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRLs).....	16
2.6.1.- Publicación de Información del Ente Licenciante Provincial.....	16
2.6.2.- Frecuencia de Publicación	16
2.6.3.- Controles de Acceso a la Información.....	17
2.6.4.- Repositorios de Certificados y Listas de Revocación.....	17
2.7.- AUDITORÍAS	17
2.8.- CONFIDENCIALIDAD.....	18
2.8.1.- Información Confidencial	18
2.8.2.- Información No Confidencial	18
2.8.3.- Publicación de Información sobre la Revocación de un Certificado.....	19
2.8.4.- Divulgación de Información a Autoridades Judiciales	19
2.8.5.- Divulgación de Información como parte de un Proceso Judicial o Administrativo	19
2.8.6.- Divulgación de Información por Solicitud del Suscriptor	19
2.8.7.- Otras circunstancias de divulgación de información	19
2.9.- DERECHOS DE PROPIEDAD INTELECTUAL	20
3.- IDENTIFICACION Y AUTENTICACION.....	20
3.1.- Registro Inicial.....	20
3.1.1.- Tipos de Nombres.....	21
3.1.2.- Necesidad de Nombres Distintivos.....	21
3.1.3. - Unicidad de Nombres	21
3.1.4.- Procedimiento de Resolución de Disputas sobre Nombres	22
3.1.5.- Reconocimiento, Autenticación y Rol de las Marcas Registradas	22
3.1.6.- Métodos para comprobar la posesión de la Clave Privada	22
3.1.7.- Autenticación de la Identidad del Certificador.....	22
3.2.- GENERACIÓN DE UN NUEVO PAR DE CLAVES (RUTINA DE RE-KEY)...	23
3.3.- GENERACIÓN DE UN NUEVO PAR DE CLAVES DESPUÉS DE UNA REVOCACIÓN - SIN COMPROMISO DE CLAVE - REEMPLADO DE CERTIFICADO DIGITAL	23

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 3 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

3.4.- REQUERIMIENTO DE REVOCACIÓN	23
4.- CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS	24
4.1. - SOLICITUD DE CERTIFICADO	24
4.2.- EMISIÓN DEL CERTIFICADO.....	24
4.3.- ACEPTACIÓN DEL CERTIFICADO	25
4.4.- SUSPENSIÓN O REVOCACIÓN DE CERTIFICADOS	25
4.4.1.- CAUSAS DE REVOCACIÓN	26
4.4.2.- Autorizados a Solicitar la Revocación.....	26
4.4.3.- Procedimientos para la Solicitud de Revocación.....	26
4.4.4.- Plazo para la Solicitud de Revocación.....	27
4.4.5.- Frecuencia de Emisión de Listas de Certificados Revocados.....	27
4.4.6.- Requisitos para la Verificación de la Lista de Certificados Revocados	27
4.4.7.- Requisitos Específicos para Casos de Compromiso de Claves	28
4.5.- PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD.....	28
4.5.1.- Tipos de eventos registrados.....	28
4.5.2.- Frecuencia de Procesamiento del Registro de Eventos	30
4.5.3.- Período de Retención del Registro de Eventos.....	30
4.5.4.- Protección del Registro de Eventos	30
4.5.5.- Procedimientos de Respaldo del Registro de Eventos.....	30
4.5.6.- Sistema de recolección de información acerca de eventos	31
4.5.7.- Notificación al Causante del Evento.....	31
4.5.8.- Análisis de Vulnerabilidad.....	31
4.6.- ARCHIVO DE LA INFORMACIÓN	31
4.6.1.- Tipo de Información Archivada.....	31
4.6.2.- Período de Retención.....	32
4.6.3.- Protección de los Archivos de Información.....	32
4.6.4.- Procedimiento de Copia de Respaldo (Backup)	32
4.6.5.- Ubicación del Archivo de Información	32
4.6.6.- Procedimientos de Obtención y Verificación de la Información Archivada	32
4.7.- RENOVACIÓN DE CERTIFICADOS Y CAMBIO DE CLAVES CRIPTOGRÁFICAS.....	33
4.8.- PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE DESASTRES.....	33
4.8.1.- Compromiso de Recursos Informáticos, Aplicaciones y Datos	34
4.8.2.- Continuidad de las Operaciones de la Autoridad Certificante del Ente Licenciante Provincial y de la Autoridad Certificante Raíz de la Provincia de San Luis	34
4.8.3.- Compromiso de la Clave Privada de la Autoridad Certificante del Ente Licenciante Provincial y de la Autoridad Certificante Raíz de la Provincia de San Luis	34
4.9.- PLAN DE CESE DE ACTIVIDADES.....	35
5.- CONTROLES DE SEGURIDAD FISICA, FUNCIONALES Y PERSONALES.....	35
5.1.- CONTROLES DE SEGURIDAD FÍSICA.....	35
5.1.1.- Construcción y Ubicación de las Instalaciones.....	36
5.1.2.- Niveles de Acceso Físico.....	36
5.1.3.- Energía Eléctrica y Aire Acondicionado	36
5.1.4.- Exposición al agua e inundaciones	36
5.1.5.- Prevención y Protección contra Incendio	36
5.1.6.- Medios de Almacenamiento de Información.....	37
5.1.7.- Descarte de Medios de Almacenamiento de Información.....	37
5.1.8.- Instalaciones de Seguridad Externas.....	37
5.2.- CONTROLES FUNCIONALES	37
5.2.1.- Definición de Roles Afectados al Proceso de Certificación	37
5.2.2.- Separación de Funciones	38
5.2.3.- Número de Personas Requerido por Función	38
5.2.4.- Identificación y Autenticación para cada Rol	38
5.3.- Controles de Seguridad del Personal de La Autoridad Certificante del Ente Licenciante y de la Autoridad Certificante Raíz.....	38
5.3.1.- Antecedentes Laborales, Calificaciones, Experiencia e Idoneidad del Personal..	38
5.3.2.- Entrenamiento y Capacitación Inicial.....	39
5.3.3.- Frecuencias del Proceso de Actualización Técnica	39
5.3.4.- Sanciones a aplicar por Actividades No Autorizadas	39

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 4 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

5.3.5.- Requisitos para Contratación de Personal	39
5.3.6.- Documentación Provista al Personal	39
6.- CONTROLES DE SEGURIDAD TECNICA	39
6.1. - GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES CRIPTOGRÁFICAS	40
6.1.1.- Generación del Par de Claves Criptográficas	40
6.1.1.1.- Par de Claves de la Autoridad Certificante Raíz y Par de Claves de la Autoridad Certificante del Ente Licenciante Provincial.....	40
6.1.1.2.- Par de Claves de Autoridad Certificante de Certificador Licenciado.....	40
6.1.2.- Entrega de la Clave Privada al Certificador Licenciado.....	40
6.1.3.- Entrega de la Clave Pública al Ente Licenciante	41
6.1.4.- Disponibilidad de la Clave Pública.....	41
6.1.5.- Tamaño de Claves.....	42
6.1.6.- Generación de Claves por Hardware o Software.....	42
6.1.7.- Propósitos de Utilización de Claves (Key Usage)	42
6.2.- PROTECCIÓN DE LA CLAVE PRIVADA.....	42
6.2.1.- Estándares para dispositivos criptográficos	43
6.2.2.- Control "M de N" de la Clave Privada	43
6.2.3.- Recuperación de la clave privada	43
6.2.4.- Copia de seguridad de la clave privada	44
6.2.5.- Archivo de Clave Privada	44
6.2.6.- Incorporación de Claves Privadas en Módulos Criptográficos	44
6.2.7.- Método de Activación de Claves Privadas	44
6.2.8.- Método de Desactivación de Claves Privadas	45
6.2.9.- Método de Destrucción de Claves Privadas	45
6.3.- OTROS ASPECTOS DE ADMINISTRACIÓN DE CLAVES	45
6.3.1.- Archivo de la Clave Pública	45
6.3.2.- Período de Uso de Clave Pública y Privada	45
6.4.- DATOS DE ACTIVACIÓN.....	46
6.4.1.- Generación e Instalación de Datos de Activación	46
6.4.2.- Protección de los Datos de Activación	46
6.5.- CONTROLES DE SEGURIDAD INFORMÁTICA.....	46
6.5.1.- Requisitos Técnicos Específicos.....	46
6.6.- CONTROLES TÉCNICOS DEL CICLO DE VIDA DE LOS SISTEMAS	46
6.6.1.- Controles de Desarrollo de Sistemas	46
6.6.2.- Administración de Controles de Seguridad	47
6.7.- CONTROLES DE SEGURIDAD DE RED	47
6.8.- CONTROLES DE INGENIERÍA DE DISPOSITIVOS CRIPTOGRÁFICOS	47
7.- PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS	47
7.1.- PERFIL DEL CERTIFICADO	48
7.2. - Perfil de la Lista de Certificados Revocados	51
8.- ADMINISTRACION DE ESPECIFICACIONES	52
8.1.- PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIONES	52
8.2.- PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN	52
8.3.- PROCEDIMIENTOS DE APROBACIÓN	52

1- INTRODUCCION

FD-025	Resolución Rectoral N° 2240005-UPL-2009. ANEXO I.			
Pág. 5 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

1.1.- DESCRIPCIÓN GENERAL

El Decreto N° 0428-MP-2008, reglamentario de la Ley Provincial N° V-0591-2007 que adhiere a la Ley Nacional N° 25.506 de Firma Digital, establece que en el ámbito de la Administración Pública de la Provincia de San Luis, funciona la Infraestructura de Firma Digital de la Provincia de San Luis, cuya Autoridad de Aplicación es la Universidad de La Punta.

En ejercicio de las facultades otorgadas por el artículo 11 del mencionado Decreto la Autoridad de Aplicación de la Provincia de San Luis dicta la presente Política de Certificación, la cual indica la aplicabilidad de los Certificados emitidos por el Ente Licenciantes a través de su Autoridad Certificante.

Con relación a ello, corresponde aclarar que a los efectos de fortalecer la seguridad de la Cadena de Confianza característica en la operatoria de la tecnología de Firma Digital la Provincia de San Luis ha optado por utilizar una jerarquía de dos niveles motivo por el cual su infraestructura de firma digital además de contar con una Autoridad Certificante Raíz Provincial posee una Autoridad Certificante Intermedia o Autoridad Certificante del Ente Licenciantes de la Provincia de San Luis, cuya función será emitir certificados a las futuras Autoridades Certificantes de los Certificadores Licenciados correspondientes a sus Políticas de Certificación aprobadas, es decir, a las Autoridades Certificantes Subordinadas.

Las relaciones entre el Ente Licenciantes con los Certificadores que soliciten licencias para sus Políticas de Certificación, se rigen por la Ley Provincial N° V-0591-2007, su Decreto Reglamentario N° 0428-MP-2008, la Resolución Rectoral N° 2120004-UPL-2009 y demás normas complementarias.-

Esta Política de Certificación se complementa con los siguientes documentos:

- a) Los Procedimientos de Licenciamiento;
- b) El Manual de Procedimientos de Certificación;
- c) La Política de Privacidad del Ente Licenciantes;
- d) El Plan de Cese de Actividades;
- e) El Plan de Seguridad: Política de Seguridad y Manual de Procedimientos de Seguridad;
- f) El Plan de Contingencia.
- g) La Normativa Jurídica Interna de la Sala Cofre del Instituto de Firma Digital de la Provincia de San Luis, aprobada por Resolución Rectoral N° 2120006-UPL-2009.

1.2. - IDENTIFICACIÓN

Título del Documento:

“Política de Certificación del Ente Licenciantes de la Provincia de San Luis”

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 6 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Versión: 2.0.

Fecha: 26/10/10.

OID: 2.16.32.1.3.2.1.1.0

URL: <http://www.acraiz.sanluis.gov.ar>

Lugar: Provincia de San Luis. República Argentina.

1.3 - PARTICIPANTES Y APLICABILIDAD

Son las partes esenciales de la Infraestructura de Firma Digital de la Provincia de San Luis:

- a) La Autoridad de Aplicación de la Provincia de San Luis (Universidad de La Punta)
- b) El Ente Licenciante de la Provincia de San Luis (Instituto de Firma Digital de la Provincia de San Luis)
- c) Los Suscriptores de Certificados (Certificadores Licenciados).

1.3.1. – Certificador

Para esta Política de Certificación, la función de Certificador la cumple el Ente Licenciante de la Provincia de San Luis, es decir, el Instituto de Firma Digital de la Provincia de San Luis quien administra la Autoridad Certificante Raíz de la Provincia de San Luis y la Autoridad Certificante Intermedia o Autoridad Certificante del Ente Licenciante Provincial.

1.3.1.1. Autoridad de Aplicación de la Provincia de San Luis

Según lo dispuesto por la Ley N° V-0591-2007 y su Decreto Reglamentario N° 0428-MP-2008, y en concordancia con lo ordenado por la Ley Nacional de Firma Digital N° 25.506, la Universidad de La Punta es la Autoridad de Aplicación de la Provincia de San Luis.

Conforme lo previsto en el artículo 11 del referido Decreto la Autoridad de Aplicación se encuentra facultada para adquirir, administrar y mantener la Infraestructura de Firma Digital de la Provincia.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 7 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

1.3.1.2.- Ente Licenciante de la Provincia de San Luis

El Ente Licenciante de la Provincia de San Luis es el órgano administrativo encargado de otorgar las licencias a los Certificadores Licenciados y de supervisar su actividad.

En tal carácter, administra la Autoridad Certificante Raíz de la Provincia de San Luis y la Autoridad Certificante Intermedia también denominada Autoridad Certificante del Ente Licenciante Provincial, emitiendo certificados digitales a las Autoridades Certificantes de los Certificadores Licenciados correspondientes a sus Políticas de Certificación aprobadas.

1.3.2.- Autoridad de Registro

En el marco de la presente Política, la función de Autoridad de Registro será cumplida por el Ente Licenciante de la Provincia de San Luis.

1.3.3.- Suscriptores de Certificados

Serán Suscriptores de los certificados emitidos por la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis el ente público, ente privado u organismo de derecho público no estatal que se constituya como Certificador Licenciado conforme lo dispuesto en la legislación vigente. En tal carácter, podrá emitir Certificados de Clave Pública, entendiendo por tal, al que asocia una Clave Pública con el suscriptor durante el período de vigencia del Certificado, haciendo plena prueba dentro de la Administración del Sector Público Provincial, los Poderes del Estado Provincial y el Sector Privado, de la veracidad de su contenido.

El Certificador Licenciado podrá proveer el servicio de sellado digital de fecha y hora.

1.3.4.- Aplicabilidad

Los certificados a emitirse por el Ente Licenciante a través de su Autoridad Certificante podrán ser utilizados exclusivamente para los fines especificados en la presente Política de Certificación, a saber:

a) Validación de la facultad otorgada a los entes u organismos que oportunamente sean constituidos en Certificadores Licenciados de la Provincia de San Luis, de conformidad con

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 8 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

la Resolución que al efecto dictará en cada caso la Autoridad de Aplicación de la Ley N° V-0591-2007.

Es decir, el Ente Licenciante de la Provincia de San Luis utiliza su Clave Privada, mantenida en dispositivos criptográficos seguros, para firmar los Certificados de las Autoridades Certificantes de los Certificadores Licenciados, posibilitando que estos últimos emitan Certificados Digitales a sus suscriptores, en el marco de la Ley de Firma Digital de la Provincia N° V-0591-2007.

1.4.- CONTACTOS

La Autoridad de Aplicación de la Provincia de San Luis funciona en el ámbito de la Universidad de La Punta; así como el Ente Licenciante funciona en el ámbito del Instituto de Firma Digital de la Provincia de San Luis situado también en la órbita de la Universidad de La Punta.

Para consultas y sugerencias acerca de este documento se puede obtener información personalmente o por correo en:

Universidad de La Punta
 Av. Universitaria s/n,
 Ciudad de la Punta (5710) – San Luis. República Argentina.
 Teléfono mesa de entrada: 0266 4452000 int. 6095
consultaspki@ulp.edu.ar
<http://www.acraiz.sanluis.gov.ar>

2.- ASPECTOS GENERALES DE LA POLITICA DE CERTIFICACION

2.1. - OBLIGACIONES

2.1.1. - Obligaciones y atribuciones de la Autoridad de Aplicación de la Provincia de San Luis

La Autoridad de Aplicación Provincial se encuentra facultada para dictar el Manual de Procedimientos del Ente Licenciante, fijando las pautas a que deben adecuarse los Certificadores Licenciados para confeccionar sus propios Manuales, o a dictar los Manuales de Procedimientos de los Certificadores Licenciados, las Normas de Auditoría y la creación

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 9 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

de esta Política de Certificación.

Determinará los estándares tecnológicos aplicables a las claves conteniendo el último estado del arte.

Llevará a cabo las auditorías de acuerdo a lo dispuesto en el Capítulo V del Decreto Reglamentario N° 0428-MP-2008 y sus normas complementarias, y resolverá todas aquellas contingencias que puedan presentarse respecto a la Infraestructura de Firma Digital de la Provincia de San Luis.

La Universidad de La Punta, en su condición de Autoridad de Aplicación, deberá presentar el diseño de la estructura operativa que le permita cumplir con el mandato incorporado en la Ley N° V-0591-2007 y su Decreto Reglamentario N° 0428-MP-2008.-

2.1.1.2. Obligaciones del Ente Licenciente de la Provincia de San Luis

Son obligaciones del Ente Licenciente:

- a) Administrar el par de claves criptográficas de la Autoridad Certificante Raíz y de su Autoridad Certificante.
- b) Otorgar las licencias habilitantes para acreditar a los Certificadores que soliciten la licencia y emitir los correspondientes “Certificados de Clave Pública”, que permiten verificar las firmas digitales de los Certificados que éstos emitan.
- c) Denegar las solicitudes de licencias a los Certificadores que no cumplan con los requisitos establecidos para su aprobación.
- d) Revocar las licencias otorgadas a los Certificadores Licenciados que dejen de cumplir con los requisitos establecidos para su ejercicio.
- e) Verificar que los Certificadores Licenciados utilicen sistemas técnicamente confiables, entendiéndose por tales a los que cumplan con los estándares tecnológicos que al efecto dicte la Autoridad de Aplicación de la Provincia de San Luis.
- f) Considerar para su aprobación el Manual de Procedimientos, los Planes de Seguridad y los de Cese de Actividades presentados por los Certificadores.
- g) Generar un Plan de Auditoría para los Certificadores Licenciados.
- h) Disponer la realización de auditorías de oficio.
- i) Resolver los conflictos individuales que se susciten entre el suscriptor de un Certificado y un Certificador Licenciado emisor del mismo.

El Ente Licenciente cumplirá para con los Certificadores Licenciados en la Provincia de San Luis, las obligaciones que el Art. 21 de la Ley N° 25.506 asigna al Certificador Licenciado.

En su calidad de suscriptor de certificado y de Certificador Licenciado, el Ente Licenciente, tiene idénticas obligaciones que los Certificadores Licenciados, y además debe:

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 10 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

- a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a la Clave Privada de cualquier suscriptor de los certificados que emita.
- b) Mantener el control de su propia clave privada e impedir su divulgación.
- c) Revocar su propio certificado de clave pública frente al compromiso de su clave privada.
- d) Permitir el acceso público permanente a los certificados de clave pública que ha emitido en favor de los Certificadores Licenciados, a la Lista de Certificados Revocados, a la información sobre direcciones y números telefónicos de los Certificadores Licenciados, por medio de conexiones de telecomunicaciones públicamente accesibles;
- e) Permitir el ingreso de los auditores, debidamente acreditados, a su local operativo. Poner a disposición de aquellos toda la información necesaria y proveer la asistencia del caso.
- f) Publicar su propio certificado de clave pública en el Boletín Oficial y en dos (2) diarios de difusión nacional durante tres (3) días consecutivos a partir del día de su emisión.
- g) Revocar los certificados emitidos en favor de los Certificadores Licenciados incursos en causales de revocación de licencia, o que han cesado sus actividades.
- h) Revocar los certificados emitidos en favor de los Certificadores Licenciados, cuando las claves públicas que en ellos figuran dejan de ser técnicamente confiables.
- i) Supervisar la ejecución del Plan de Cese de Actividades de los Certificadores Licenciados que discontinúan sus funciones.
- j) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.-

2.1.2.- Obligaciones de la Autoridad de Registro

Las obligaciones de Autoridad de Registro son asumidas por el Ente Licenciantes de la Provincia de San Luis.

2.1.3. - Obligaciones de los Certificadores Licenciados

Son obligaciones de los Certificadores Licenciados:

- a) Proveer toda la información necesaria en forma completa y precisa para su identificación y autenticación contenida en su Solicitud de Licencia al iniciar el proceso de licenciamiento.
- b) Al aceptar un certificado emitido por la Autoridad Certificante del Ente Licenciantes Provincial para su Autoridad Certificante, será responsable por toda la información por él provista y contenida en el mismo.
- c) Operar conforme con su propio Manual de Procedimientos de Certificación y su Política de Certificación, implementados de acuerdo a lo establecido en la normativa vigente y

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 11 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

aprobada por el Ente Licenciante de la Provincia de San Luis.

- d) Abstenerse de generar, exigir, o por cualquier otro medio, tomar conocimiento o acceder, bajo ninguna circunstancia, a la Clave Privada del suscriptor;
- 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) Solicitar al Ente Licenciante la revocación de su Certificado cuando la Clave Pública, en él contenida, deje de ser técnicamente confiable;
- h) Informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos contenidos en su Certificado o sobre cualquier hecho significativo que pueda afectar la información contenida en el mismo;
- i) Operar utilizando un sistema técnicamente confiable;
- j) 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;
- k) 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 Certificador Licenciado;
- l) Poner a disposición del suscriptor de un Certificado emitido por éste Certificador Licenciado, toda la información relativa a la tramitación del Certificado;
- m) Mantener la documentación de respaldo de los Certificados emitidos durante diez (10) años, contados a partir de su fecha de vencimiento o revocación;
- n) 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;
- ñ) Publicar su dirección y sus números telefónicos;
- o) 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;
- p) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
- q) En caso de Cese de Actividades, los Certificados emitidos por un Certificador Licenciado 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;
- r) 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. La notificación, también, deberá hacerse individualmente al Ente Licenciante.

Cuando se hayan emitido Certificados a entes, entidades o personas ajenas al Sector Público Provincial, el Certificador Licenciado publicará durante tres (3) días consecutivos, en uno o más diarios de difusión nacional, el cese de sus actividades.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 12 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

El Certificador Licenciado podrá disponer de medios adicionales de comunicación del cese de sus actividades, para notificar a los suscriptores de Certificados que son ajenos al Sector Público Provincial. Si los certificados son transferidos a otro Certificador Licenciado, toda la documentación pertinente también deberá ser transferida a aquel.

s) 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.

2.1.5.- Obligaciones del Servicio de Repositorio

Para esta Política de Certificación son obligaciones del Ente Licenciente la publicación en los sitios desarrollados a tal fin, de la siguiente información:

- a) Esta Política de Certificación (última versión y anteriores);
- b) La Política de Privacidad;
- c) La Política de Seguridad;
- d) Los Certificados emitidos por la Autoridad Certificante del Ente Licenciente de la Provincia de San Luis;
- e) Su Lista de Certificados Revocados;
- f) Información relevante de los informes de auditoría a que fue objeto el Ente Licenciente;
- g) Información relevante de los informes de las auditorías realizadas por el Ente Licenciente a los Certificadores Licenciados;
- h) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de los contactos del Ente Licenciente;
- i) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos de los Certificadores Licenciados;
- j) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos de los Certificadores Licenciados cuyas licencias han sido revocadas.

2.1.6.- Obligaciones de los Terceros Usuarios:

Son obligaciones de los Terceros Usuarios de Certificados de Clave Pública:

- a) Conocer los alcances de la Política de Certificación;
- b) Rechazar la utilización del certificado para fines distintos a los previstos en la Política de

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 13 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Certificación que lo respalda;

c) Verificar la validez del certificado.

2.2.- RESPONSABILIDADES

El Ente Licenciante será responsable, en caso de corresponder, ante terceros por el incumplimiento de las previsiones de la Ley Provincial N° V-0591-2007, Decreto Reglamentario N° 0428-MP-2008, y toda otra normativa aplicable, respecto a los procedimientos que respaldan la emisión de Certificados por su Autoridad Certificante, por los errores u omisiones en los certificados por ella emitidos y por su falta de revocación en la forma y plazos previstos.

No cabe responsabilidad alguna para el Ente Licenciante, 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 siempre que pueda demostrar que ha tomado todas las medidas razonables.

2.3.- RESPONSABILIDAD FINANCIERA

2.3.1. - Responsabilidad Financiera del Ente Licenciante

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

2.4.- INTERPRETACIÓN Y APLICACIÓN DE LAS NORMAS

2.4.1.- Legislación Aplicable

La interpretación, obligatoriedad, diseño y validez de esta Política de Certificación se encuentran sometidos a lo establecido por la Ley Provincial N° V-0591-2007, el Decreto Reglamentario N° 0428-MP-2008, la Resolución Rectoral N° 2120004-ULP-2009, la Ley

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 14 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Nacional N° 25.506, el Decreto N° 2628/2002 y demás normas complementarias aplicables.

2.4.2.- Forma de Interpretación y Aplicación

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

Las disposiciones que surgen de la presente Política de Certificación son de cumplimiento obligatorio.

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 Ente Licenciante, 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.

La Autoridad de Aplicación de la Provincia de San Luis evaluará el accionar de todos los partícipes de la Infraestructura de Firma Digital y recibirá las denuncias que contra cualquiera de ellos se presentasen.

En su carácter de Órgano de Control aplicará sanciones de apercibimiento, suspensión, multa, clausura o cancelación para funcionar como tal, a los Certificadores Licenciados o a las Autoridades de Registro.

Las multas aplicables por la Autoridad de Aplicación van de un mínimo de una (1) Unidad de Multa y hasta un máximo de un mil (1000) Unidades de Multa.

La Unidad de Multa, será un importe equivalente a un (1) salario mínimo vital y móvil vigente a la fecha de comisión del hecho.

La cuantía de las sanciones se graduará atendiendo a:

- a) la naturaleza de los derechos afectados,
- b) los beneficios obtenidos,
- c) el grado de intencionalidad,
- d) la reincidencia,

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 15 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

- e) los daños y perjuicios causados a las personas interesadas y a terceros,
f) y cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

Se considerará reincidente a quien habiendo sido sancionado por una infracción incurriera en otra de similar naturaleza dentro del término de Tres (3) años, a contar desde la aplicación de la sanción.

El procedimiento se ajustará a las siguientes disposiciones:

- a) La Autoridad de Aplicación de la Provincia de San Luis iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Provincial de Firma Digital, a su Decreto Reglamentario y/o a las demás normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, o asociaciones de consumidores o usuarios.
- b) Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida. En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de cinco (5) días hábiles, presente su descargo por escrito o por vía telemática con firma digital. En su primera presentación, el presunto infractor deberá constituir domicilio y acreditar personería.
- c) La constancia del acta labrada conforme a lo previsto en este artículo, así como las comprobaciones técnicas que se dispusieran, constituirán prueba suficiente de los hechos así comprobados, salvo en los casos en que resultaren desvirtuados por otras pruebas.
- d) Las pruebas se admitirán solamente en caso de existir hechos controvertidos y siempre que no resulten manifiestamente inconducentes. Contra la resolución que deniegue medidas de prueba sólo se concederá recurso de reconsideración. La prueba deberá producirse dentro del término de diez (10) días hábiles, prorrogables cuando haya causas justificadas, teniéndose por desistidas aquellas no producidas dentro de dicho plazo por causa imputable al infractor.
- e) Concluidas las diligencias sumariales, se dictará la resolución definitiva dentro del término de veinte (20) días hábiles.

2.5.- ARANCELES

A los fines del cumplimiento de lo establecido en la Ley Provincial N° V-0591-2007, su Decreto Reglamentario, y en las Resoluciones complementarias específicas, la Autoridad de Aplicación de la Provincia de San Luis se encuentra facultada para fijar en la oportunidad que lo considere pertinente, el monto de los aranceles a abonarse por los diferentes servicios a prestar a fin de efectivizar la operatoria de la Firma Digital en el ámbito público y privado.-

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 16 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Asimismo el Ente Licenciante podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos.

2.6.- PUBLICACIÓN Y REPOSITARIOS DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRLs)

2.6.1.- Publicación de Información del Ente Licenciante Provincial

El Ente Licenciante Provincial opera en su sitio de publicación la Lista de Certificados Revocados (CRL), esta información está disponible en:

URL=<http://acraiz.sanluis.gov.ar/crl/entelicenciante.crl>

y, alternativamente en:

<http://acraiz1.sanluis.gov.ar/crl/entelicenciante.crl>

Asimismo, la publicación de la información del Ente Licenciante está disponible en:

[http:// www.acraiz.sanluis.gov.ar](http://www.acraiz.sanluis.gov.ar)

En este sitio se puede encontrar la siguiente información:

- a) El Certificado vigente de la Autoridad Certificante Raíz, el Certificado digital de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis y los Certificados de las Autoridades Certificantes de Certificadores Licenciados;
- b) Los datos de los contactos del Ente Licenciante como de los Certificadores Licenciados;
- c) El Registro de Certificadores Licenciados conteniendo el número de la Resolución que concede, renueva o revoca las licencias de Políticas de Certificación que fueron aprobadas, así como el número de la Resolución que rechaza la aprobación de las Políticas de Certificación durante el proceso de licenciamiento;
- d) Esta Política de Certificación, la Política de Privacidad, la Política de Seguridad y toda otra documentación técnica de carácter público que se emita, en sus versiones actuales y anteriores;
- e) La Lista de Certificados Revocados.

2.6.2.- Frecuencia de Publicación

La información alojada en los sitios de publicación será actualizada inmediatamente después de que la información a incluir en ellos haya sido verificada y

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 17 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

autorizada por el Ente Licenciante.

La información respecto a emisiones y revocaciones de Certificados será incluida tan pronto como se hayan cumplido los procedimientos de validación de identidad de los solicitantes establecidos en esta Política de Certificación para cada caso en particular.

La Lista de Certificados Revocados (CRL) será actualizada y la nueva versión será publicada cuando se produzca la revocación de un certificado o bien a los seis (6) meses de la última emisión de la Lista de Certificados Revocados, si ninguna de las dos condiciones anteriores ocurre antes.

2.6.3.- Controles de Acceso a la Información

El Ente Licenciante brinda acceso irrestricto a sus sitios de publicación, para consultar, a través de Internet, documentación de carácter público, incluyendo la clave pública del certificado de la Autoridad Certificante Raíz, la clave pública del certificado de la Autoridad Certificante Intermedia de la Provincia de San Luis, la Lista de Certificados Revocados y esta Política de Certificación.

El Ente Licenciante establecerá controles para restringir la posibilidad de escritura y modificación.

2.6.4.- Repositorios de Certificados y Listas de Revocación

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

2.7.- AUDITORÍAS

El Ente Licenciante se encuentra sujeto a auditorias de la Autoridad de Aplicación de la Provincial de San Luis conforme lo dispuesto en el Capítulo V del Decreto Provincial N° 0428-MP-2008 y las resoluciones específicas que se dictaren al respecto. La información relevante de los informes de las auditorias, es publicada en el sitio de publicación del Ente Licenciante.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 18 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

2.8.- CONFIDENCIALIDAD

2.8.1.- Información Confidencial

Toda información referida a los Certificadores Licenciados, que haya sido recibida por el Ente Licenciante durante el proceso de licenciamiento o renovación, 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. La exigencia se extiende a toda otra información, referida a los Certificadores Licenciados, a la que el Ente Licenciante tenga acceso durante el ciclo de vida de los certificados emitidos.

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

Ni la Autoridad de Aplicación, ni el Ente Licenciante generarán ni accederán a las claves privadas de las Autoridades Certificantes de los Certificadores Licenciados. La generación y administración del par de claves criptográficas queda bajo exclusiva responsabilidad de los Certificadores Licenciados.

En los casos relativos a información personal, resulta de aplicación lo dispuesto en la Ley N° 25.326 de Protección de Datos Personales.

2.8.2.- Información No Confidencial

No se considerada confidencial lo siguiente:

- 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.

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

- a) Esta Política de Certificación;
- b) El Acuerdo con los Certificadores Licenciados;
- c) Los Términos y Condiciones con Terceros Usuarios de certificados de la Autoridad Certificante del Ente Licenciante Provincial;
- d) La Política de Privacidad del Ente Licenciante de la Provincia de San Luis;
- e) La Política de Seguridad del Ente Licenciante de la Provincia de San Luis.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 19 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

2.8.3.- Publicación de Información sobre la Revocación 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:

URL=<http://acraiz.sanluis.gov.ar/crl/entelicenciante.crl>

Y, alternativamente en: <http://acraiz1.sanluis.gov.ar/crl/entelicenciante.crl>

2.8.4.- Divulgación de Información 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.- Divulgación de Información como parte de un Proceso Judicial o Administrativo

La información confidencial en poder del Ente Licenciante podrá ser revelada ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

2.8.6.- Divulgación de Información por Solicitud del Suscriptor

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del Certificador Licenciado o de cualquier otra información generada o recibida durante el ciclo de vida del certificado, solo podrá efectuarse previa autorización de ese Certificador. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público irrestricto.

2.8.7.- Otras circunstancias de divulgación de información

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

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 20 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

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 Ente Licenciante y a la Autoridad de Aplicación de la Provincia de San Luis. 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

De acuerdo a la normativa vigente, en el proceso de registración de un Certificador Licenciado interviene el Ente Licenciante, otorgando o denegando licencias a las Políticas de Certificación presentadas y asociadas a sus Autoridades Certificantes.

La entidad que desee obtener una Licencia como Certificador Licenciado deberá:

- a) Presentar una solicitud;
- b) Contar con un dictamen favorable emitido por el Organismo Auditante;
- c) Someter a aprobación del Ente Licenciante la Política de Certificación, el Manual de Procedimientos, el Plan de Seguridad y el de Cese de Actividades, así como el detalle de los componentes técnicos a utilizar;
- d) Emplear para el ejercicio de las actividades de certificación, personal técnicamente idóneo y que no se encuentre incurso en los supuestos de inhabilitación para desempeñar funciones dentro del Sector Público Provincial;
- e) Presentar toda otra información relevante al proceso de otorgamiento de licencias, que sea exigida por el Ente Licenciante.

La presentación de solicitud de licencia para una Política de Certificación por parte del Certificador, inicia el proceso de licenciamiento que culmina con el otorgamiento o denegación de licencia por parte del Ente Licenciante, y la publicación en el Boletín Oficial de la Resolución que la otorga o deniega.

Con el otorgamiento de licencia, el Ente Licenciante a través de su Autoridad Certificante, emite un certificado digital para la Autoridad Certificante vinculada a la Política de Certificación licenciada.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 21 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

En el acto de emisión del Certificado por la Autoridad Certificante del Ente Licenciante Provincial, el Certificador Licenciado debe confirmar que la información contenida en el Certificado sea correcta. Además en ese acto, el Certificador Licenciado firma el Acuerdo con Suscriptores de Certificados de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis.

3.1.1.- Tipos de Nombres

Las Autoridades Certificantes vinculadas a las Políticas de Certificación licenciadas son subordinadas de la Autoridad Certificante del Ente Licenciante Provincial, y en consecuencia, a la Autoridad Certificante Raíz y tendrán un nombre definido por el Certificador Licenciado de acuerdo a la normativa vigente, que será controlado por el Ente Licenciante para permitir su identificación unívoca en el ámbito de la Infraestructura de Firma Digital de la Provincia de San Luis.

Cada Certificado tiene un nombre distintivo único (ver punto 3.1.4) en formato X.500 en el campo "Subject" del Certificado.

3.1.2.- Necesidad de Nombres Distintivos

Todos los nombres distintivos son semánticamente significativos dentro del ámbito de la Infraestructura de Firma Digital de la Provincia de San Luis. Son de fácil comprensión y asociación con el Certificador Licenciado y la Autoridad Certificante que representa.

3.1.3. - Unicidad de Nombres

Los nombres distintivos (Distinguished Name o DN) son únicos dentro del ámbito de la Infraestructura de Firma Digital de la Provincia de San Luis. El Ente Licenciante es el encargado de controlar la unicidad de los nombres distintivos.

Se podrán emitir varios certificados a favor de un mismo Certificador Licenciado utilizando el mismo DN cuando así se estime conveniente, ya que la utilización de un mismo DN en varios certificados, no afecta la unicidad de dicho nombre dentro de la Infraestructura de Firma Digital de la Provincia de San Luis.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 22 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

3.1.4.- Procedimiento de Resolución de Disputas sobre Nombres

El Ente Licenciante resolverá los conflictos que pudieran generarse respecto de la utilización de nombres distintivos que como suscriptores puedan adoptar los Certificadores Licenciados.

En tales casos, corresponde al solicitante del Certificado demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.1.5.- Reconocimiento, Autenticación y Rol de las Marcas Registradas

No se permite el uso de marcas comerciales, marcas de servicio o nombres de fantasía como Nombres Distintivos de las Autoridades Certificantes de Certificadores Licenciados dependientes de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis.

3.1.6.- Métodos para comprobar la posesión de la Clave Privada

Para formalizar la solicitud de Certificado se utiliza el requerimiento de firma de certificado (CSR o "Certificate Signing Request") en formato PKCS#10.

La Autoridad Certificante del Ente Licenciante de la Provincia de San Luis verifica que la Clave Pública asociada al requerimiento de firma de certificado (CSR) de la Autoridad Certificante del Certificador Licenciado, se corresponda con la Clave Privada que el Certificador Licenciado utilizó para firmarlo.

3.1.7.- Autenticación de la Identidad del Certificador

Durante el proceso de licenciamiento el Ente Licenciante procede a identificar fehacientemente la identidad de la persona de existencia ideal, registros públicos de contratos u organismo público solicitante.

Para el caso de organismos públicos, se verifica la identidad de la máxima autoridad del organismo. Para las personas de existencia ideal, se solicita la documentación constitutiva de la entidad y de acreditación del apoderado o representante legal y si se tratara de registros públicos de contratos, la documentación que acredite su condición.

Asimismo, deberán presentar adicionalmente la documentación indicada en la sección 1.4 del Anexo I de la Resolución Rectoral N° 2120004-ULP-2009.

Toda la documentación relativa a este proceso mencionado es mantenida y resguardada por el Ente Licenciante.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 23 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

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

Se requiere el cumplimiento de los pasos descriptos en el punto 3.1 - Registro Inicial.

3.3.- GENERACIÓN DE UN NUEVO PAR DE CLAVES DESPUÉS DE UNA REVOCACIÓN - SIN COMPROMISO DE CLAVE - REEMPLADO DE CERTIFICADO DIGITAL.

Se requiere el cumplimiento de los pasos descriptos en el punto 3.1 - Registro Inicial.

No se admite la utilización del mismo par de claves criptográficas para la renovación de un Certificado.

Sin embargo, se admite el reemplazo del certificado digital, el cual no supone el cambio del par de claves. El procedimiento sólo podrá llevarse a cabo, previa autorización de la Autoridad de Aplicación y en presencia de personal autorizado del Ente Licenciente.

3.4.- REQUERIMIENTO DE REVOCACIÓN

El procedimiento de revocación de un Certificado correspondiente a una Autoridad Certificante de Certificador Licenciado se inicia con la recepción de la solicitud de revocación por el Ente Licenciente y termina cuando una nueva Lista de Certificados Revocados (CRL) conteniendo el número de serie del Certificado en cuestión se publica en

URL=<http://acraiz.sanluis.gov.ar/crl/entelicenciente.crl>

Y, alternativamente en: <http://acraiz1.sanluis.gov.ar/crl/entelicenciente.crl>

Las solicitudes de revocación deberán comunicarse por escrito mediante el formulario diseñado al efecto y disponible en el sitio del Ente Licenciente.

El Ente Licenciente realiza la identificación y validación de la identidad del solicitante de la revocación.

Una vez validada la información contenida en la solicitud de revocación, el Ente Licenciente procederá a la revocación del Certificado en un plazo no mayor a las veinticuatro (24) horas de recibida y validada. Toda la documentación generada en este

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 24 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

proceso es mantenida y resguardada por el Ente Licenciente.

4.- CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - SOLICITUD DE CERTIFICADO

Una vez otorgada la licencia de la Política de Certificación por parte del Ente Licenciente y publicada la Resolución de otorgamiento en el Boletín Oficial, el Certificador Licenciado está en condiciones de solicitar el Certificado.

El Certificador Licenciado genera en sus instalaciones, el par de claves para la Autoridad Certificante para la Política de Certificación Licenciada, en presencia de personal autorizado del Ente Licenciente a quien entrega en ese acto el Formulario de Solicitud de Emisión del Certificado debidamente completado junto con el requerimiento de firma de Certificado (CSR) en formato PKCS#10.

El Certificador Licenciado debe seguir los siguientes pasos:

- a) Generar el par de claves para la Autoridad Certificante vinculada a la Política de Certificación Licenciada, en presencia de personal del Ente Licenciente;
- b) Generar el requerimiento de firma de Certificado (CSR), en presencia de personal del Ente Licenciente;
- c) Demostrar que la Clave Pública presentada al Ente Licenciente se corresponda con la Clave Privada utilizada para la firma del requerimiento de firma de Certificado (CSR);
- d) Presentar la solicitud de emisión de Certificado al Ente Licenciente debidamente firmada por la máxima autoridad en caso de organismo público o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos.

Una vez cumplidos los pasos mencionados, el personal del Ente Licenciente procederá a verificar la autenticidad del requerimiento de firma de Certificado (CSR).

4.2.- EMISIÓN DEL CERTIFICADO

Las Autoridades Certificantes de Certificador Licenciado integran la Infraestructura de Firma Digital de la Provincia de San Luis y dependen de la Autoridad Certificante del Ente Licenciente Provincial, y en consecuencia, de la Autoridad Certificante Raíz. Por lo tanto, la emisión de sus Certificados se efectúa en instalaciones de la Autoridad Certificante del Ente Licenciente Provincial con la participación del Certificador Licenciado, representado por su máxima autoridad o quien él designe, en caso de organismo público, o

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 25 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

por su apoderado o representante legal, para el caso de personas de existencia ideal o registros públicos de contratos. Por parte del Ente Licenciante, participará el personal debidamente autorizado a dicho efecto.

Los certificados emitidos por la Autoridad Certificante del Ente Licenciante Provincial a favor de una Autoridad Certificante de Certificador Licenciado tienen un período de validez de sesenta (60) años desde su fecha de emisión, siempre que dicho plazo no exceda el período de uso del certificado de la Autoridad Certificante del Ente Licenciante Provincial, o hasta su revocación (lo que ocurra primero).

Con la recepción de la Solicitud de Emisión de Certificado remitida por el Certificador Licenciado, la Autoridad Certificante del Ente Licenciante se encuentra en condiciones de generar el Certificado Digital para la Autoridad Certificante correspondiente.

4.3.- ACEPTACIÓN DEL CERTIFICADO

Un Certificado emitido por la Autoridad Certificante del Ente Licenciante se considera aceptado por el Certificador Licenciado después que su apoderado o representante legal, si se trata de una persona de existencia ideal o un registro público de contratos, o la máxima autoridad o quien él designe, si se trata de un organismo público, haya recibido formalmente el Certificado Digital generado en la ceremonia de emisión y haya firmado el Acuerdo con los Suscriptores de Certificados de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis.

La Autoridad Certificante del Ente Licenciante entrega el Certificado emitido al personal del Certificador Licenciado referido en el párrafo precedente, según corresponda.

Una vez recibido el Certificado Digital emitido por la Autoridad Certificante del Ente Licenciante Provincial, el Certificador Licenciado debe instalarlo en su Autoridad Certificante, encontrándose en condiciones de emitir Certificados a sus suscriptores.

El Ente Licenciante publicará ese Certificado Digital en su sitio de publicación
www.acraiz.sanluis.gov.ar

Por otra parte, el Certificador Licenciado procederá a publicar en el Boletín Oficial de la Provincia de San Luis y en dos (2) diarios de difusión nacional durante tres (3) días consecutivos el Certificado de Clave Pública correspondiente a la Política de Certificación Licenciada.

4.4.- SUSPENSIÓN O REVOCACIÓN DE CERTIFICADOS

De acuerdo con lo dispuesto por la Ley N° V-0591-2007, que adhiere a la Ley N° 25.506, no existe el estado de suspensión de Certificados.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 26 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

La solicitud de revocación de un Certificado de Autoridad Certificante de Certificador Licenciado debe ser presentada ante el Ente Licenciante.

4.4.1.- CAUSAS DE REVOCACIÓN

El Ente Licenciante revocará el Certificado Digital de la Autoridad Certificante de Certificador Licenciado que hubiera emitido su Autoridad Certificante en los siguientes casos:

- a) A solicitud del Certificador Licenciado, cuando la clave privada o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo;
- b) Si se determina que el certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación;
- c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros;
- d) Por resolución judicial o del mismo Ente Licenciante debidamente fundada;
- e) Por cancelación de la licencia de la Política de Certificación;
- f) En caso de cese de actividades del Certificador Licenciado;
- g) Por condiciones especiales definidas en las Políticas de Certificación;
- h) Si se determina que la información contenida en el Certificado ha dejado de ser válida.

4.4.2.- Autorizados a Solicitar la Revocación

Se encuentran autorizados a solicitar la revocación de un Certificado emitido por la Autoridad Certificante del Ente Licenciante Provincial:

- a) El Certificador Licenciado, titular del Certificado en cuestión, a través de su máxima autoridad en caso de organismo público o por su apoderado o representante legal para el caso de personas de existencia ideal o registros públicos de contratos;
- b) Aquellas personas previa y debidamente autorizadas por el Certificador Licenciado para efectuar tal solicitud;
- c) El Ente Licenciante;
- d) La Autoridad de Aplicación del presente régimen;
- e) La autoridad judicial competente.

4.4.3.- Procedimientos para la Solicitud de Revocación

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 27 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

El procedimiento de revocación de un Certificado correspondiente a una Autoridad Certificante de Certificador Licenciado, se inicia con la recepción de la solicitud de revocación por ante el Ente Licenciante y termina cuando una nueva Lista de Certificados Revocados (CRL) conteniendo el número de serie del certificado en cuestión se publica en

URL=<http://acraiz.sanluis.gov.ar/crl/entelicenciante.crl>

Y, alternativamente en:

<http://acraiz1.sanluis.gov.ar/crl/entelicenciante.crl>

La solicitud de revocación debe ser completada en papel, firmada y entregada por el solicitante al Ente Licenciante. El formulario de solicitud se encuentra disponible en el sitio de publicación del Ente Licenciante <http://www.acraiz.sanluis.gov.ar>

El Ente Licenciante verificará la autenticidad de los datos de la solicitud de revocación.

En los casos que la solicitud de revocación surgiera de una decisión judicial o del Ente Licenciante, se efectuará la notificación al Certificador Licenciado antes de comenzar el proceso de revocación.

La solicitud de revocación se archiva, junto con la documentación recabada en el proceso de licenciamiento de la Política de Certificación asociada al Certificado que se revoca.

Un Certificado revocado será válido, únicamente, para la verificación de firmas generadas durante el período en que el referido Certificado era válido.

4.4.4.- Plazo para la Solicitud de Revocación

El plazo máximo entre la recepción de la solicitud de revocación y la actualización de la Lista de Certificados Revocados, indicando los motivos de la revocación, es de veinticuatro (24) horas.

4.4.5.- Frecuencia de Emisión de Listas de Certificados Revocados

La Autoridad Certificante del Ente Licenciante Provincial emite y publica la Lista de Certificados Revocados (CRL) cuando se revoca un Certificado o a los seis (6) meses de la última emisión de CRL, si la condición anterior no ocurre antes.

4.4.6.- Requisitos para la Verificación de la Lista de Certificados Revocados

Los Certificadores Licenciados están obligados a verificar la autenticidad y validez

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 28 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

de los certificados en la Lista de Certificados Revocados (CRL) mediante la verificación de la Firma Digital de la Autoridad Certificante del Ente Licenciante Provincial y de su período de validez.

Los Terceros Usuarios, además de ello, están obligados a verificar la utenticidad y validez de los certificados en la Lista de Certificados Revocados (CRL) mediante la verificación de la Firma Digital de las Autoridades Certificantes de los Certificadores Licenciados.

El Ente Licenciante garantizará el acceso permanente, eficiente y gratuito a su Lista de Certificados Revocados.

4.4.7.- Requisitos Específicos para Casos de Compromiso de Claves

El Ente Licenciante en su carácter de responsable de la Clave Privada de la Autoridad Certificante Raíz de la Provincia de San Luis y de la Clave Privada de su Autoridad Certificante, se compromete a comunicar a los Certificadores Licenciados en caso de compromiso de dichas claves.

4.5.- PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

4.5.1.- Tipos de eventos registrados

Con el fin de mantener un ambiente seguro y controlado, se registrará la ocurrencia de los siguientes eventos; registrándose para cada uno, la información relativa al tipo de evento y el tiempo en que el evento ocurrió.

1.- Relacionados con el Ente Licenciante:

- a) Cambios en la Política de Certificación,
- b) Cambios en los Procedimientos de Certificación,
- c) Cambios en el Acuerdo con los Certificadores Licenciados (suscriptores de certificados de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis),
- d) Cambios en los términos y condiciones con Terceros Usuarios de Certificados de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis,
- e) Cambios en la Política de Seguridad,
- f) Cambios en el Plan de Contingencia,
- g) Pruebas del Plan de Contingencia,
- h) Cambios en la Política de Privacidad,

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 29 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

- i) Cambios en el personal vinculado al Ente Licenciante de la Provincia de San Luis,
- j) Revisiones de auditoría,
- k) Cambios en los Procedimientos de Licenciamiento,
- l) Cambios en la Normativa Jurídica Interna de la Sala Cofre del Instituto de Firma Digital de la Provincia de San Luis, aprobada por Resolución Rectoral N° 2120006-ULP-2009.

2.- Relacionados con la Autoridad Certificante Raíz y con la Autoridad Certificante del Ente Licenciante Provincial:

- a) Ceremonia de generación de claves,
- b) Encendido y apagado de los equipos y de publicación,
- c) Operaciones de mantenimiento, accesos a los sistemas, y cambios y actualizaciones de software y hardware,
- d) Entrada en servicio y finalización de las aplicaciones de la Autoridad Certificante y del servicio de publicación,
- e) Operaciones de lectura y escritura de las aplicaciones de la Autoridad Certificante y del servicio publicación,
- f) Intentos satisfactorios y fallidos de crear, borrar, acceder, establecer y cambiar contraseñas, permisos y roles del personal afectado a los servicios de Certificación,
- g) Generación de copias de seguridad,
- h) Ciclo de vida de los dispositivos criptográficos incluyendo recepción, instalación, puesta en servicio, uso y finalización del servicio,
- i) Generación, almacenamiento, recuperación, activación, desactivación, archivo y destrucción de las claves de la Autoridad Certificante Raíz,
- j) Registro de acceso físico a los diferentes niveles de seguridad,
- k) Registros producidos por los elementos de seguridad de las instalaciones (por ej. registro de alarmas, grabaciones de cámaras de vigilancia, etc.),
- l) Registro de poseedores de credenciales de activación de los dispositivos criptográficos que contienen las claves privadas de la Autoridad Certificante.

3.- Relacionados con el ciclo de vida de los Certificados y las Listas de Revocación de Certificados:

- a) Solicitud de emisión de Certificado por el Certificador Licenciado,
- b) Aprobación o denegación de solicitud de emisión de Certificado,
- c) Emisión de Certificado por la Autoridad Certificante del Ente Licenciante Provincial,
- d) Aceptación del Certificado por el Certificador Licenciado y firma del Acuerdo con Suscriptores de la Autoridad Certificante del Ente Licenciante Provincial por el Certificador Licenciado,
- e) Asignación del dispositivo criptográfico al responsable poseedor de claves del Certificador Licenciado,

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 30 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

- f) Publicación del Certificado en el sitio del Ente Licenciante,
- g) Recepción de solicitud de revocación de Certificado,
- h) Revocación del Certificado,
- i) Emisión de la Lista de Certificados Revocados,
- j) Publicación de la Lista de Certificados Revocados,
- k) Registro de destrucción de material conteniendo información de claves y datos de su activación,
- l) Renovación de Certificados.

4.5.2.- Frecuencia de Procesamiento del Registro de Eventos

Los registros de eventos de la Autoridad Certificante Raíz y de la Autoridad Certificante del Ente Licenciante son analizados periódicamente en relación a su criticidad. Ese análisis es realizado por personal autorizado del Ente Licenciante.

4.5.3.- Período de Retención del Registro de Eventos

Los registros de eventos correspondientes al sistema de la Autoridad Certificante Raíz y de la Autoridad Certificante del Ente Licenciante Provincial se mantienen por un período de diez (10) años a partir de su generación. Los registros de eventos correspondientes al sistema de publicación del Ente Licenciante se conservan por diez (10) años.

4.5.4.- Protección del Registro de Eventos

Toda la información pertinente al Registro de Eventos se mantiene de manera segura y accedida por personal estrictamente autorizado.

4.5.5.- Procedimientos de Respaldo del Registro de Eventos

Las Copias de Respaldo del Registro de Eventos se realizan acorde a un detallado cronograma que será confeccionado por el Ente Licenciante.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 31 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

4.5.6.- Sistema de recolección de información acerca de eventos

La información recogida automáticamente es registrada por el sistema operativo y el software de aplicación. La información sobre eventos manuales es registrada por personal autorizado del Ente Licenciante.

4.5.7.- Notificación al Causante del Evento

Los sistemas de recolección de eventos no efectúan ninguna notificación al causante del evento sobre el hecho de que sus acciones han sido registradas.

4.5.8.- Análisis de Vulnerabilidad

Los eventos registrados son utilizados para analizar posibles vulnerabilidades sobre los sistemas y los procedimientos vigentes.

4.6.- ARCHIVO DE LA INFORMACIÓN

El Ente Licenciante mantendrá toda la información relativa a los Certificados Digitales emitidos por su Autoridad Certificante y por la Autoridad Certificante Raíz, de acuerdo a lo establecido en el marco legal vigente.

4.6.1.- Tipo de Información Archivada

El Ente Licenciante almacenará toda la información asociada a los Certificados a lo largo de su ciclo de vida incluyendo su renovación. Se registrará:

- a) La información obtenida en las diferentes etapas del ciclo de vida del Certificado (solicitud, revocación, renovación, etc.);
- b) Los documentos asociados a dichas etapas, incluyendo el licenciamiento;
- c) Las diferentes versiones de Políticas de Certificación, Manuales de Procedimientos y sus documentos asociados.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 32 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

4.6.2.- Período de Retención

El Ente Licenciante almacenará la información asociada a los Certificados Digitales emitidos bajo la presente Política, por un período de diez (10) años contados a partir de la fecha de su vencimiento o revocación.

4.6.3.- Protección de los Archivos de Información

El Ente Licenciante garantiza:

- a) La integridad y confidencialidad de la información referente a los Certificados Digitales emitidos,
- b) El almacenamiento de la información en forma completa,
- c) La privacidad de los datos obtenidos durante el procedimiento de licenciamiento.

4.6.4.- Procedimiento de Copia de Respaldo (Backup)

El Ente Licenciante efectuará copias de respaldo de la información en soporte electrónico, que serán almacenadas en instalaciones externas. Las copias de respaldo serán:

- a) Efectuadas según la Política de Backup detallada en los documentos técnicos asociados,
- b) Almacenadas en instalaciones que cumplen al menos con los mismos niveles de protección física y ambiental que las instalaciones principales donde se encuentran instalados los equipos asociados a los Procesos de Certificación,
- c) Verificadas frecuentemente, según lo indica los documentos técnicos asociados, para asegurar la confiabilidad de los procedimientos de restauración.

4.6.5.- Ubicación del Archivo de Información

El Ente Licenciante mantiene un esquema distribuido de archivos entre sus instalaciones principales y de respaldo.

4.6.6.- Procedimientos de Obtención y Verificación de la Información Archivada

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 33 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Solo las personas autorizadas por el Ente Licenciante tienen acceso a la información archivada, ya sea en las instalaciones principales como en las de respaldo.

4.7.- RENOVACIÓN DE CERTIFICADOS Y CAMBIO DE CLAVES CRIPTOGRÁFICAS

La Renovación de Certificado de la Autoridad Certificante de Certificador Licenciado deberá seguir el procedimiento indicado en el punto 3.1 de la presente Política.

La renovación implica, en todos los casos, la generación de un nuevo Par de Claves. Transcurrido el periodo de validez del par de claves asociado al Certificado, deberán ser retiradas de servicio, de acuerdo a lo indicado en el punto 6.3.2 de esta Política.

Únicamente se podrá renovar el Certificado si se cumple alguna de las siguientes condiciones:

- a) Para sustituir las Claves que van a ser retiradas,
- b) Para modificar la información contenida en el Certificado, siempre que ello no fuera posible a través del procedimiento de reemplazo conforme lo contemplado en el punto 3.3. de la presente Política de Certificación, o
- c) Por modificaciones realizadas a la Política de Certificación licenciada que así lo ameriten.

El Ente Licenciante realizará una nueva ceremonia de emisión de Certificado asociado a la Autoridad Certificante, de acuerdo a su Manual de Procedimientos.

El trámite de renovación de un Certificado Digital emitido a favor de un Certificador Licenciado, debe ser iniciado sesenta (60) días hábiles antes del comienzo del mayor período de validez de los Certificados Digitales que emite.

Para solicitar un nuevo Certificado, se deberá seguir el procedimiento indicado en el punto 4.1 de la presente Política.

La Clave Privada que es objeto de renovación debe ser utilizada para continuar firmando las Listas de Revocación de Certificados (CRLs) hasta la fecha de expiración del último Certificado emitido por la Autoridad Certificante utilizando esa Clave. En ese momento se debe:

- a) Solicitar al Ente Licenciante la revocación de ese certificado, y
- b) Destruir la clave privada de acuerdo a lo indicado en el punto 6.2.9 de la presente política.

4.8.- PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE DESASTRES

Ante hechos que comprometan la continuidad de sus operaciones, el Ente Licenciante deberá implementar un Plan de Contingencia y Recuperación ante Desastres que garantice el mantenimiento de sus servicios mínimos (recepción de solicitudes de

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 34 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

revocación, revocación de certificados, emisión de CRL y consulta de Listas de Certificados Revocados actualizadas).

El plan deberá tener las siguientes características:

- a) Ser conocido por todo el personal que cumple funciones en el Ente Licenciante;
- b) Incluir pruebas completas de funcionamiento periódicamente.

4.8.1.- Compromiso de Recursos Informáticos, Aplicaciones y Datos

El Ente Licenciante 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 Ente Licenciante Provincial y de la Autoridad Certificante Raíz de la Provincia de San Luis

El Ente Licenciante dispone de procedimientos para asegurar la continuidad de sus operaciones en instalaciones alternativas. El Ente Licenciante comunicará a los Certificadores Licenciados si el evento afecta actividades previstas.

4.8.3.- Compromiso de la Clave Privada de la Autoridad Certificante del Ente Licenciante Provincial y de la Autoridad Certificante Raíz de la Provincia de San Luis

Ante sospecha de compromiso de la Clave Privada de la Autoridad Certificante del Ente Licenciante Provincial o de la Autoridad Certificante Raíz, el Ente Licenciante 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 Certificadores Licenciados.

El Ente Licenciante tomará las siguientes acciones:

- a) Informar a los Certificadores Licenciados que sus Certificados serán revocados, y que las

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 35 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Claves Privadas asociadas a esos Certificados no deben ser utilizadas,

b) Revocar los Certificados Digitales de las Autoridades Certificantes de los Certificadores Licenciados,

c) Publicar en su sitio de publicación que se ha revocado el Certificado de la Autoridad Certificante del Ente Licenciantes Provincial o de la Autoridad Certificante Raíz (según correspondiera), 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 del Ente Licenciantes Provincial o de la Autoridad Certificante Raíz queda reservado a una decisión de la Autoridad de Aplicación de la Provincia de San Luis.

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

- a) Publicará fecha y hora del Cese de Actividades en el Boletín Oficial durante tres (3) días consecutivos que no podrá ser anterior a los noventa (90) días corridos contados de la última publicación.
- b) Notificará a los Certificadores Licenciados 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 de los Certificadores Licenciados, destruirá la Clave Privada de la Autoridad Certificante correspondiente mediante un procedimiento que garantice su destrucción total.

5.- CONTROLES DE SEGURIDAD FISICA, FUNCIONALES Y PERSONALES

5.1.- CONTROLES DE SEGURIDAD FÍSICA

El Ente Licenciantes ha implementado controles apropiados que restringen el acceso a los equipos, programas y datos utilizados por su Autoridad Certificante y la Autoridad Certificante Raíz para la provisión del servicio de Certificación, limitándolo a personas debidamente autorizadas.

Tanto la Autoridad Certificante del Ente Licenciantes Provincial como la Autoridad Certificante Raíz operan en instalaciones construidas bajo estrictas normas de seguridad

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 36 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

física y ambiental internacionales que les brindan una protección adecuada.

5.1.1.- Construcción y Ubicación de las Instalaciones

Para realizar las operaciones de la Autoridad Certificante del Ente Licenciantes Provincial y de la Autoridad Certificante Raíz, el Ente Licenciantes 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 Físico

Para ingresar al recinto que contiene los equipos de la Autoridad Certificante Raíz y de la Autoridad Certificante del Ente Licenciantes Provincial, 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.- Energía Eléctrica y Aire Acondicionado

Los equipos de la Autoridad Certificante Raíz de la Provincia de San Luis y de la Autoridad Certificante del Ente Licenciantes Provincial 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.- Exposición al agua e inundaciones

Dentro de las instalaciones, los equipos de la Autoridad Certificante Raíz y de la Autoridad Certificante del Ente Licenciantes están alojados en compartimentos estancos a fin de prevenir el impacto producido por inundaciones o filtraciones de líquidos.

5.1.5.- Prevención y Protección contra Incendio

Los equipos de la Autoridad Certificante Raíz y de la Autoridad Certificante del

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 37 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Ente Licenciante Provincial están alojados en instalaciones que cuentan con alarmas de detección y sistemas de extinción de incendios.

5.1.6.- Medios de Almacenamiento de Información

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

El Ente Licenciante 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 Información

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

5.1.8.- Instalaciones de Seguridad Externas

El Ente Licenciante dispone de instalaciones externas que tienen niveles de protección física y ambiental similares al de las instalaciones principales.

5.2.- CONTROLES FUNCIONALES

El Ente Licenciante ha establecido una estructura de personal estable con roles específicos definidos para realizar las actividades de licenciamiento y operación de las Autoridades Certificantes que contempla una adecuada separación de funciones.

5.2.1.- Definición de Roles Afectados al Proceso de Certificación

El personal del Ente Licenciante que tenga acceso a los equipos involucrados en los procesos de emisión o revocación de Certificados, incluyendo la emisión de la Lista de

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 38 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

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.- Separación de Funciones

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

5.2.3.- Número de Personas Requerido por Función

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.- Identificación y Autenticación 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 de La Autoridad Certificante del Ente Licenciante y de la Autoridad Certificante Raíz

El Ente Licenciante sigue la Política de administración de personal establecida para la Universidad de La Punta.

5.3.1.- Antecedentes Laborales, Calificaciones, Experiencia e Idoneidad del Personal

El personal del Ente Licenciante 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.

El personal del Ente Licenciante ha sido cuidadosamente seleccionado y calificado

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 39 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

antes de iniciar sus actividades.

5.3.2.- Entrenamiento y Capacitación Inicial

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

5.3.3.- Frecuencias del Proceso de Actualización Técnica

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

5.3.5.- Requisitos para Contratación de Personal

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

5.3.6.- Documentación Provista al Personal

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

6.- CONTROLES DE SEGURIDAD TECNICA

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 40 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

6.1. - GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES CRIPTOGRÁFICAS

6.1.1.- Generación del Par de Claves Criptográficas

6.1.1.1.- Par de Claves de la Autoridad Certificante Raíz y Par de Claves de la Autoridad Certificante del Ente Licenciantes Provincial

El Par de Claves Criptográficas de la Autoridad Certificante Raíz de la Provincia de San Luis es generado por el Ente Licenciantes en instalaciones de la propia Autoridad Certificante Raíz, 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 Ente Licenciantes para emisión y revocación de Certificados y emisión de la Lista de Certificados Revocados es de 4096 bits generado con algoritmo RSA.

6.1.1.2.- Par de Claves de Autoridad Certificante de Certificador Licenciado

El Par de Claves criptográficas de una Autoridad Certificante se genera en las instalaciones del Certificador Licenciado, en presencia de personal del Ente Licenciantes, después de haberle sido otorgada la licencia.

El Certificador Licenciado, en su carácter de responsable de la Autoridad Certificante a la que la Autoridad Certificante del Ente Licenciantes Provincial le emite un Certificado, es el responsable del par de claves criptográficas y, como tal, está obligado a generarlo en un dispositivo criptográfico seguro conforme a la normativa, a no revelar su Clave Privada a terceros bajo ninguna circunstancia y a almacenarla en un medio que garantice su integridad y confidencialidad. En todo momento, la clave privada de la Autoridad Certificante se encuentra bajo el exclusivo y permanente control del Certificador Licenciado.

Durante la generación y almacenamiento de la Clave Privada de la Autoridad Certificante, por parte del Certificador Licenciado debe asegurarse que:

- a) La Clave Privada sea única y su seguridad se encuentre garantizada, y
- b) No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas.

6.1.2.- Entrega de la Clave Privada al Certificador Licenciado

De acuerdo al artículo 28, punto 1 del Decreto N° 0428-MP-2008, reglamentario de

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 41 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

la Ley N° V-0591-2007 que adhiere a la Ley Nacional N° 25.506, el Ente Licenciante no genera ni toma conocimiento o accede a los datos de generación de firma de las Autoridades Certificantes del Certificador Licenciado.

6.1.3.- Entrega de la Clave Pública al Ente Licenciante

El Certificador Licenciado, a través del personal designado para representarlo, entrega al Ente Licenciante copia de su Clave Pública contenida en un CSR (Certificate Signing Request), en formato PKCS#10, de manera que:

- a) No pueda ser alterada, y
- b) El Certificador Licenciado posea la Clave Privada que corresponde a dicha clave pública.

Todas las actividades que se llevan a cabo en el proceso de recepción de la clave pública son registradas para fines de auditoría.

6.1.4.- Disponibilidad de la Clave Pública

Se publica el Certificado de la Autoridad Certificante Raíz, en:

URL=http://caroot.sanluis.gov.ar/CertEnroll/caroot.certs1.gov.ar_Instituto%20de%20Firma%20Digital%20de%20la%20Provincia%20de%20San%20Luis.crt

Y, alternativamente en:

http://caroot1.sanluis.gov.ar/CertEnroll/caroot.certs1.gov.ar_Instituto%20de%20Firma%20Digital%20de%20la%20Provincia%20de%20San%20Luis.crt

El Ente Licenciante publica su propio Certificado, en:

URL=<http://acraiz.sanluis.gov.ar/cer/entelicenciante.crt>

Y, alternativamente en:

<http://acraiz1.sanluis.gov.ar/cer/entelicenciante.crt>

Asimismo, publica los Certificados de las Autoridades Certificantes de Certificadores Licenciados que su Autoridad Certificante hubiera emitido, en:

<http://www.acraiz.sanluis.gov.ar>

El Certificador Licenciado es responsable de publicar los Certificados de sus Autoridades Certificantes y de sus suscriptores para que Terceros Usuarios puedan acceder a ellos.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 42 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

6.1.5.- Tamaño de Claves

La Autoridad Certificante Raíz utiliza un par de claves criptográficas RSA de 4096 bits de longitud para emitir el certificado de la Autoridad Certificante del Ente Licenciente de la Provincia de San Luis.

La Autoridad Certificante del Ente Licenciente Provincial utiliza un par de claves criptográficas RSA de 4096 bits de longitud para emitir los certificados de las Autoridades Certificantes de los Certificadores Licenciados.

En caso de tomar conocimiento de técnicas de criptoanálisis que vulneren el algoritmo utilizado para la generación de firma con la longitud indicada, el Ente Licenciente revocará los Certificados emitidos, notificando previamente a los Certificadores Licenciados y anunciará la implementación de una nueva versión de la presente Política de Certificación.

6.1.6.- Generación 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.

6.1.7.- Propósitos de Utilización de Claves (Key Usage)

Las Claves criptográficas de la Autoridad Certificante Raíz tienen como exclusivo propósito la firma de su Certificado y del certificado de la Autoridad Certificante del Ente Licenciente Provincial.

Las Claves criptográficas de la Autoridad Certificante del Ente Licenciente Provincial tienen como exclusivo propósito la firma de su Lista de Certificados Revocados (CRL) y de los Certificados de las Autoridades Certificantes de Certificadores Licenciados.

Las claves criptográficas de las Autoridades Certificantes de Certificadores Licenciados tienen como exclusivo propósito su utilización para la firma de Certificados de sus Suscriptores y la firma de sus Listas de Certificados Revocados (CRLs).

6.2.- PROTECCIÓN DE LA CLAVE PRIVADA

Las claves privadas de la Autoridad Certificante Raíz de la Provincia de San Luis y de la Autoridad Certificante del Ente Licenciente Provincial están bajo responsabilidad del Ente Licenciente y protegidas mediante la utilización de sistemas y procedimientos que

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 43 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

incluyen la designación de funcionarios responsables de su control, custodia y activación segura y de su destrucción en caso de compromiso.

Las claves privadas de las Autoridades Certificantes de los Certificadores Licenciados están bajo su propia responsabilidad, y protegidas mediante la utilización de sistemas y procedimientos confiables que evitan el uso no autorizado o pérdida de las mismas.

6.2.1.- Estándares para dispositivos criptográficos

La Autoridad Certificante Raíz de la Provincia de San Luis y la Autoridad Certificante del Ente Licenciante Provincial disponen cada una de ellas 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.

Para la generación y almacenamiento de sus pares de Claves criptográficas, el Certificador Licenciado dispone de dispositivos criptográficos que cumplen con las características definidas en FIPS 140 versión 1 o 2, de por lo menos:

- a) Nivel 3, para sus Autoridades Certificantes, y
- b) Nivel 2, para sus Autoridades de Registro.

6.2.2.- Control "M de N" de la Clave Privada

El Ente Licenciante utiliza procedimientos que requieren la participación de varias personas para la activación de la Clave Privada de la Autoridad Certificante Raíz y de la Clave Privada de la Autoridad Certificante del Ente Licenciante Provincial.

Los Certificadores Licenciados deben adoptar procedimientos que requieran la participación de varias personas para la activación de las Claves Privadas de sus Autoridades Certificantes.

Lo indicado anteriormente en este punto no se hace necesariamente extensivo a las Autoridades de Registro de los Certificadores Licenciados.

6.2.3.- Recuperación de la clave privada

El Ente Licenciante posee procedimientos para la recuperación de la Clave Privada de su Autoridad Certificante y de la Autoridad Certificante Raíz, detallados en sus documentos técnicos asociados.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 44 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

6.2.4.- Copia de seguridad de la clave privada

El Ente Licenciante mantiene una copia de seguridad de su Clave Privada y de la Autoridad Certificante Raíz. Estas copias son almacenadas y protegidas con un nivel de seguridad no inferior al establecido para la versión original de las Claves y mantenidas por el plazo de validez del Certificado correspondiente.

El Ente Licenciante no mantiene copia de las Claves Privadas de las Autoridades Certificantes de los Certificadores Licenciados.

Las Claves Privadas de las Autoridades Certificantes de Certificadores Licenciados cuentan con al menos una copia de seguridad de manera tal de poder recuperarlas en caso de desastre o mal funcionamiento del sistema.

Estas copias están protegidas bajo las mismas condiciones de acceso físico que se implementan en el ambiente de producción. Están resguardadas en dispositivos criptográficos equivalentes a los que contienen las claves originales.

6.2.5.- Archivo de Clave Privada

Cuando las claves privadas de las Autoridades Certificantes están desactivadas, los dispositivos criptográficos que las contienen permanecen bajo los controles de seguridad física descritos en la presente Política y el acceso a los mismos es debidamente registrado y solo permitido a personal autorizado.

6.2.6.- Incorporación de Claves Privadas en Módulos Criptográficos

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 descritas en la presente Política y se realizan a través de los procedimientos de resguardo propios de los dispositivos criptográficos utilizados.

6.2.7.- Método de Activación de Claves Privadas

La activación de las Claves Privadas de las Autoridades Certificantes utiliza un esquema de control compartido ("M de N"), por lo que se necesita la intervención simultanea de varias personas autorizadas.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 45 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

6.2.8.- Método de Desactivación de Claves Privadas

La desactivación de las claves privadas se realiza a través de procedimientos que garantizan la inhabilitación de esas claves. Para volver a utilizarlas es necesario seguir el procedimiento de activación de claves descriptas en la presente Política.

6.2.9.- Método de Destrucción 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 ADMINISTRACIÓN DE CLAVES

6.3.1.- Archivo de la Clave Pública

La Clave Pública se archiva utilizando métodos que garantizan su integridad. El Ente Licenciantes posee procedimientos para el archivo de su Clave Privada, detallados en sus documentos técnicos asociados.

6.3.2.- Período de Uso de Clave Pública y Privada

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

El certificado de la Autoridad Certificante Raíz de la Provincia de San Luis y el certificado de la Autoridad Certificante del Ente Licenciantes Provincial expiran a los cien (100) años y ocho (8) meses desde su emisión. Los certificados de Autoridades Certificantes de Certificador Licenciado expiran a los noventa y ocho (98) años, once (11) meses, siete (7) días, siempre que dicho plazo no exceda el período de uso del certificado de la Autoridad Certificante del Ente Licenciantes Provincial, o cuando sean revocados.

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 46 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

6.4.- DATOS DE ACTIVACIÓN

6.4.1.- Generación e Instalación de Datos de Activación

Los datos de activación de las Claves Privadas utilizan un esquema de control compartido ("M de N").

6.4.2.- Protección de los Datos de Activación

Los datos de activación son tratados como información confidencial y no deben estar expuestos en medios accesibles por terceros. Asimismo las personas responsables de su custodia no deben divulgar su condición.

6.5.- CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1.- Requisitos Técnicos Específicos

Solo personal debidamente autorizado puede acceder a las instalaciones y sistemas que intervienen en las operaciones de Certificación. Acorde a la Política de Seguridad aprobada por el Ente Licenciente 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 del Ente Licenciente,
- 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.

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

6.6.1.- Controles de Desarrollo de Sistemas

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 47 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Para la implementación de los sistemas en el ambiente de producción se consideran los siguientes controles:

- a) Análisis de seguridad en todos sus componentes,
- b) Entornos separados de desarrollo, prueba y producción,
- c) Procedimiento formal de autorización y registro para la actualización de los sistemas,
- d) En caso de que el sistema fuera adquirido debe existir un acuerdo de nivel de servicio con el proveedor, que coincida con el ofrecido por el Certificador Licenciado a sus suscriptores.

6.6.2.- Administración de Controles de Seguridad

Según el análisis de riesgo efectuado, se clasificaron los activos informáticos de acuerdo a sus necesidades de protección y se mantiene su inventario. Los sistemas son auditados de forma periódica de acuerdo a lo que establezca el Plan de Auditoría.

6.7.- CONTROLES DE SEGURIDAD DE RED

Los Servicios de Certificación de la Autoridad Certificante Raíz y de la Autoridad Certificante del Ente Licenciente Provincial se realizan fuera de línea lo que asegura su protección de cualquier ataque a través de redes.

Los Servicios de Publicación del Ente Licenciente y de la Autoridad Certificante Raíz utilizan sistemas debidamente protegidos, garantizando integridad.

6.8.- CONTROLES DE INGENIERÍA DE DISPOSITIVOS CRIPTOGRÁFICOS

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

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).

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 48 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

7.1.- PERFIL DEL CERTIFICADO

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de la Autoridad Certificante Raíz de la Provincia de San Luis:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Versión	V3
Número de Serie	Número Asignado por la AC Raíz de la Provincia de San Luis 3e ce fc e4 46 01 fe a3 44 bd 91 b5 22 d9 04 2f
Algoritmo de firma	Sha 1 RSA
Nombre distintivo del emisor	CN = 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

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 49 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Validez	100 años, 8 meses Se especifica desde 26/02/09 hasta 26/10/2109
Nombre distintivo del suscriptor	CN = 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
Clave pública del suscriptor	<p>La clave pública RSA es de 4096 bits</p> <pre> 30 82 02 0a 02 82 02 01 00 b0 ed ac a6 95 92 e7 e7 23 99 9e 95 be 4c 1a 3d 66 6f 98 a4 a3 13 9c 6a a3 33 40 d6 92 bb e0 48 28 d7 01 3a 40 41 f1 fd 1e ea c4 70 1f 95 24 fb 4e 60 15 92 69 9f bd e6 3d bc 8e da c4 e0 d7 bb d5 e3 bb 85 25 fb e5 d6 63 2c 35 cc 2c 50 9c 5a 94 6d 4c c9 f2 b6 55 b7 7a 8a 81 4d 9f bc dd 1a e3 13 7a 24 3d 43 57 df 6f 5b e3 d3 f9 a3 d3 66 9f ec 7f 88 a7 12 e6 f8 95 48 34 55 07 f4 5b d9 8d 29 e2 63 76 35 57 16 08 6f 25 cc 6c b1 0a d4 1e f6 9f ee f5 50 f3 d7 72 9e 7d a4 cf 5e 66 ae 6d 20 06 91 09 32 8a 51 b7 41 aa 28 50 fb 01 4e d4 df 5f f1 85 6c 79 fb 3b 28 56 f3 98 18 e3 ec 27 4c 1f 38 0d d5 8b 98 ff 5d 86 6a c9 13 fe 6b cc 94 ef 0e a9 80 98 3e bf 52 f1 6b 1f 31 e7 16 2f e0 a8 cf a7 5a de 62 b6 6c 23 3e 5e a9 84 15 0b aa 78 3f c3 37 01 45 77 f2 c4 3e 8c 46 d4 46 64 a6 05 35 50 81 82 50 36 ba 78 4a 1f 2b 02 0c 0a 54 ea 41 d1 4a a9 a2 6d f6 e0 63 c7 f1 42 c7 33 9d ff d0 13 26 8c 44 b8 db 2b fe 34 4e df 0b 10 03 d2 08 99 10 f5 51 e7 91 d2 f5 cf 3b 58 e1 13 a3 ec 4f b4 22 f5 52 0e 56 3e ad f2 4e 0b 41 27 14 99 1f a3 11 71 73 fe 3a 31 8d 07 92 cb 9f 63 9b a1 32 44 89 cd d7 24 a0 84 e9 eb 34 77 bc 29 cd 4e e7 db fa 5f 21 4f 26 a6 6c b9 7c ab 4c 99 b4 b3 aa b6 1e 32 20 c9 c1 33 1b 75 0b 77 e8 dd 1e f8 e9 ca ac 63 08 54 40 cf c6 08 00 9e 9d 09 e1 ff 00 ed e6 ab 09 43 c7 64 ea 5d e0 09 b2 59 04 6c ce a6 ef ba 3e 71 df 1a b6 1a 6f c8 7a 83 1a ff c8 62 d3 e7 68 e5 05 01 c8 bb aa 08 b7 d0 41 c2 bb 20 ed eb 47 ad 5a 19 19 a6 95 f2 ea b7 c3 dc 0d 4a 33 ab 79 7d 70 1c 97 a2 62 75 6f 92 63 78 29 ea d6 13 5e 44 6d 02 9c 37 </pre>
Extensiones	
Identificador de la clave del suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves	<p>Los bits deben estar como se indican</p> <p>Digital Signature = 0 Non Repudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0</p>
Restricciones básicas	cA=TRUE

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de las Autoridades Certificantes del Ente Licenciantes Provincial:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Numero de Serie	Número asignado por la Autoridad Certificante Raíz de la Provincia de San Luis 13 e6 e9 68 00 00 00 00 03
Algoritmo de firma	sha1RSA
Nombre distintivo del emisor	CN = 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

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 50 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Validez	98 años, 11 meses, 7 días Se especifica desde 26/10/2010 hasta 02/10/2109
Nombre distintivo del suscriptor	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
Clave pública del suscriptor	<p>La clave pública RSA es de 4096 bits</p> <pre> 30 82 02 0a 02 82 02 01 00 a5 90 88 71 97 83 f3 bd 3a 09 9c df 91 cc aa b5 cf f8 07 1f 73 a8 26 91 55 e7 63 eb 1e 35 13 dc d0 74 24 c4 7f 12 3c 04 24 66 b8 ce f8 1f b7 46 55 1d de 75 44 7a 4a f3 db 62 96 c6 70 d5 2e b6 89 4b 7e 60 15 31 dd 51 cf cd 54 d7 09 6e 54 e8 66 21 4c 17 95 0f 63 da 01 2d 63 c7 f4 de 32 a5 24 c2 07 10 4c fc b6 f3 ba 40 de 19 e6 17 1a 7e 29 31 bd 65 a3 d5 1a 4c 9c 1e 2a d6 c5 89 9f c7 5c 46 b8 3c 1d f2 1f 92 d2 81 49 39 2d 62 33 e3 51 44 17 14 08 a5 1e 89 a3 98 30 5c 33 30 24 21 37 8d ed e6 fc 3b 0c 78 25 d6 96 24 5e c9 29 cb b8 39 17 97 7a 37 cd c7 5b d8 05 2c 5b f0 2f 6c 65 86 b9 3f c3 26 e6 15 d4 21 e6 6b 75 bc 29 44 f0 77 80 88 c8 87 2b a7 63 2e c4 e0 cc 76 46 57 e4 93 10 3d 22 3f b0 1b 96 4b cd 9a c3 d5 2c ba 7a 17 d0 40 c3 aa 0a 4d 49 0b 38 66 5b 08 9f 2c e6 cb c5 94 42 6e d4 81 9d fe 1e 56 6c fe 4a a9 3a a9 91 8f e2 81 32 58 58 64 2b 83 b8 f2 e6 7d 86 01 a9 ab 53 6e c4 92 0e 6d 45 ca 41 a3 82 cb 12 10 f1 9c 8a f6 b9 5c be 11 2b e5 35 69 3a 1f a2 da 4a 11 c8 6b f0 3d 82 a9 81 a8 61 12 f2 d3 8d 9d 36 d6 3e 2f 4a 8d 67 b3 67 ed 4a 42 7a fb 93 60 02 7f 57 18 a8 d7 09 1c 48 f4 79 47 05 49 b7 b2 97 69 7f 4a 61 fc 9b c5 86 c3 74 81 d5 89 32 7d 0e f8 4b 3a e9 69 b7 03 e2 70 62 25 29 19 c1 2d 14 5c a8 06 d8 97 6a 63 12 82 c9 76 87 f4 cd 9e 13 e4 f1 50 57 b0 ab a9 9f ec e4 34 46 11 71 fc 9f 48 85 a2 64 60 1f 8e 4e 1a f9 4a 28 f2 04 a2 ed 3f 1a db 32 fc 55 81 3e 27 f9 85 b0 7f a3 11 75 6a be d5 ad 05 55 12 34 f9 e7 28 5c f4 1b 9c 1b d9 6b d9 1f 20 00 91 09 62 1b c1 70 70 1a c9 5a ae 8b a3 2c 2f e8 06 41 85 a5 29 78 5b 02 03 01 00 01 </pre>
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la Autoridad Certificante Raíz de la Provincia de San Luis
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 de CRL sin conexión, Firma CRL
Políticas de Certificación	Debe incluir el OID de esta Política 2.16.32.1.3.2.1.1.0.
Restricciones básicas	cA=TRUE pathlen=0
Puntos de distribución de la Lista de Certificados Revocados	URL: http://caroot.sanluis.gov.ar/CertEnroll/Instituto%20de%20Firma%20Digital%20de%20la%20Provincia%20de%20San%20Luis.crl URL: http://caroot1.sanluis.gov.ar/CertEnroll/Instituto%20de%20Firma%20Digital%20de%20la%20Provincia%20de%20San%20Luis.crl
Información de Acceso de la Autoridad Certificante	URL: http://caroot.sanluis.gov.ar/CertEnroll/caroot.certs1.gov.ar_Instituto%20de%20Firma%20Digital%20de%20la%20Provincia%20de%20San%20Luis.crt URL: http://caroot1.sanluis.gov.ar/CertEnroll/caroot.certs1.gov.ar_Instituto%20de%20Firma%20Digital%20de%20la%20Provincia%20de%20San%20Luis.crt

Se usarán los siguientes campos del formato X.509 versión 3 en el certificado de las Autoridades Certificantes de los Certificadores Licenciados:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Atributos	
Versión	V3
Numero de Serie	Número asignado por la Autoridad Certificante del Ente

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 51 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

	Licenciante 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	9 años o menos Se especifica desde/hasta
Nombre distintivo del suscriptor	Según lo especificado en Anexo III de la Resolución Rectoral N° 212004-ULP-2009 en lo referente a certificados de certificadores. Si el certificado digital no incluyera la extensión Políticas de Certificación, deberá incluir en el presente la URL donde se encuentra publicada la correspondiente Política de Certificación.
Clave pública del suscriptor	Según lo especificado en Anexo III de la Resolución Rectoral N° 212004-ULP-2009 en lo referente a certificados de certificadores.
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un identificador de la clave pública de la Autoridad Certificante del Ente Licenciante de la Provincia de San Luis
Identificador de la clave del suscriptor	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Uso de claves	Los bits deben estar como se indican Digital Signature = 0 Non Repudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación	Según lo especificado en Anexo III de la Resolución Rectoral N° 212004-ULP-2009
Restricciones básicas	cA=TRUE pathlen=0
Puntos de distribución de la lista de certificados revocados	URL: http://acraiz.sanluis.gov.ar/crl/entelicenciante.crl http://acraiz1.sanluis.gov.ar/crl/entelicenciante.crl
Información de Acceso de la Autoridad Certificante	URL: https://acraiz.sanluis.gov.ar/cer/entelicenciante.crt https://acraiz1.sanluis.gov.ar/cer/entelicenciante.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 del Ente Licenciante de la Provincia de San Luis:

X.509 v2 Certificado Atributos / Extensiones	Contenido
--	-----------

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 52 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Atributos	
Versión	V2
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
Día y hora de vigencia	Día y hora de emisión de esta CRL Día y hora de la próxima emisión de
Próxima actualización	
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 Ente Licenciante cuenta con Procedimientos de Administración de Cambios para efectuar cualquier modificación a la presente Política de Certificación.

8.2.- PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN

El Ente Licenciante 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 a los demás documentos públicos asociados.

Todos los cambios producidos en los documentos antedichos serán notificados a los Certificadores Licenciados.

8.3.- PROCEDIMIENTOS DE APROBACIÓN

FD-025	Resolución Rectoral N° 2240005-ULP-2009. ANEXO I.			
Pág. 53 de 53	28/10/2010	2	0	
	Fecha Emisión	Versión	Revisión	

Esta Política de Certificación o cualquier documento vinculado, así como sus actualizaciones, serán aprobados por la Autoridad de Aplicación de la Provincia de San Luis.