Proyecto	**Entidad de Certificación**
Título	**Declaración de Prácticas y Política de Certificación de LLEIDANET PKI SUCURSAL DE PERÚ**

Realizado por	**LLEIDANET PKI SUCURSAL DE PERÚ**		
Dirigido a	**INDECOPI**		
Documento	**DOC-160909.1690912**		
Fecha aprobación	**18/09/2025**	Revisión	**8**

Firmado por: EVA PANE VIDAL
Fecha firma: 18/09/2025 12:19:39 CEST

Firmado por: Raul Gisbert Rodas
Fecha firma: 18/09/2025 13:25:57 CEST

ER-1140/2011 NMS-0009/2012 SI-0024/2013 ES-1140/2011

Avda. de Toribio Nº 143 Of. 38
San Isidro, Lima
Tel. (34) 96 381 99 47
Fax (34) 96 381 99 48
info@lleida.net
www.lleida.net

1 DATOS DEL DOCUMENTO

Proyecto	Entidad de Certificación
Título	Declaración de Prácticas y Política de Certificación de LLEIDANET PKI SUCURSAL DE PERÚ
Código	DOC-160909.1690912
Tipo de documento	DOC - Documento
Clasificación del documento	Público
Realizado por	LLEIDANET PKI SUCURSAL DE PERÚ
Dirigido a	INDECOPI
Fecha aprobación	18/09/2025
Revisión	8

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	14/06/2016	Creación del documento	RA
2	17/01/2018	Actualización del documento	JS
3	31/03/2020	Modificaciones EC	NG
4	28/09/2020	Añadir nuevos apartados	NG
5	26/04/2023	Actualizar enlace de donde se encuentran los documentos	CJ
6	02/06/2023	Actualizar RFC 3280 por RFC 5280 y RFC 2560 por RFC 6960	CJ

7	02/04/2025	Actualizar denominación de Indenova Sucursal del Perú a Lleidanet PKI Sucursal de Perú Actualizar en el apartado 10 la dirección de la Entidad de Certificación, de Registro y la Oficina Administrativa de la ER	Compliance (CJ)
8	18/09/2025	Se incluyen condiciones de uso para firma remota y se actualiza el repositorio donde se encuentran las declaraciones de practicas, políticas, etc.	Compliance (CJ)

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de Calidad Fecha: 18/09/2025
Revisado por:	Nombre: Lleidanet PKI (SB) Cargo: Administrador del Servicio Fecha: 18/09/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información Cargo: Comisión de Seguridad de la Información Fecha: 18/09/2025

4 INTRODUCCIÓN

LLEIDANET PKI SUCURSAL DE PERÚ es una empresa trasnacional que nació con vocación de desarrollar, innovar y generar soluciones tecnológicas TIC en el ámbito empresarial e institucional. Está especializada en soluciones de firma electrónica, securización de archivos y comunicaciones y cifrado de datos, criptografía, movilidad, certificados digitales y procedimientos electrónico, invirtiendo en el desarrollo e implantación de las mismas el 95% de su actividad.

Como Entidad Certificación (EC), LLEIDANET PKI SUCURSAL DE PERÚ provee los servicios de emisión, re-emisión, distribución y revocación de certificados digitales, provistos por la EC de LLEIDANET PKI SUCURSAL DE PERÚ.

Junto a los servicios de certificación digital, LLEIDANET PKI SUCURSAL DE PERÚ brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales.

El planteamiento es ofrecer una oferta diferenciada, generadora de soluciones y servicios innovadores, con el objetivo de crear valor. Para ello combinamos un alto grado de conocimiento de los directivos y profesionales, con su amplia experiencia en certificados digitales y firma electrónica para eCommerce y eAdministración y el uso de tecnología avanzada.

Nuestros SERVICIOS están dirigidos a la Administración Electrónica y Comercio electrónico y, en general, para proyectos de "oficina sin papeles", tiene como componente central la Plataforma eSigna®, a partir del cual se apoyan el resto de nuestros productos y soluciones, entendidos como módulos independientes y a su vez interconectados, según las necesidades del proyecto a implantar.

5 VISION GENERAL

El alcance de la acreditación cubre la infraestructura y sistemas de certificación que utiliza LLEIDANET PKI SUCURSAL DE PERÚ en la entrega de sus servicios, y que son proporcionados por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ.

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por LLEIDANET PKI SUCURSAL DE PERÚ

6 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza LLEIDANET PKI SUCURSAL DE PERÚ para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual).

7 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación - EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Titular	Entidad que requiere los servicios provistos por la EC de LLEIDANET PKI SUCURSAL DE PERÚ y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

7.1 PKI PARTICIPANTES

7.1.1 ENTIDAD DE CERTIFICACIÓN LLEIDANET PKI SUCURSAL DE PERÚ (EC LLEIDANET PKI SUCURSAL DE PERÚ)

LLEIDANET PKI SUCURSAL DE PERÚ, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

7.1.2 AUTORIDAD DE REGISTRO LLEIDANET PKI SUCURSAL DE PERÚ (EC LLEIDANET PKI SUCURSAL DE PERÚ)

LLEIDANET PKI SUCURSAL DE PERÚ, brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

7.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (EC LLEIDANET PKI SUCURSAL DE PERÚ)

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, cuando la entidad de certificación así lo requiere y garantizan la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece LLEIDANET PKI SUCURSAL DE PERÚ son provistos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ.

7.1.4 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos publicados en la CPS de LLEIDANET PKI SUCURSAL DE PERÚ.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por LLEIDANET PKI SUCURSAL DE PERÚ conforme lo establecido en la Política de Certificación.

7.1.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

7.1.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo esta la CPS de LLEIDANET PKI SUCURSAL DE PERÚ.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

7.1.7 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ a un titular. El Tercero que confía, a su vez puede ser o no titular.

7.1.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

7.1.9 OTROS PARTICIPANTES

7.1.9.1 EL COMITÉ DE SEGURIDAD

El comité de seguridad es un organismo interno de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, conformado por el Gerente, el Administrador del Sistema, Jefe de Operaciones y el Auditor del Ciclo de Certificación y tiene entre otras funciones la aprobación de la CPS como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la CPS aprobada y autorizar su publicación. El comité de Seguridad es el responsable de integrar la CPS, a la CPS de terceros prestadores de servicios de certificación.

8 SERVICIOS DE CERTIFICACIÓN DIGITAL

LLEIDANET PKI SUCURSAL DE PERÚ establece la Política de Seguridad que los proveedores de servicios de certificación digital deben cumplir.

En caso de incidentes que puedan afectar la seguridad de los servicios contratados a LLEIDANET PKI SUCURSAL DE PERÚ, las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por LLEIDANET PKI SUCURSAL DE PERÚ, de acuerdo con su documento Declaración de Prácticas de Certificación y Política de Certificación, publicado en:

https://www.lleida.net/es/politicas-y-practicas?tab=peru

LLEIDANET PKI SUCURSAL DE PERÚ brinda los servicios de certificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos sobre los servicios prestados por LLEIDANET PKI SUCURSAL DE PERÚ a través de la Entidad de Certificación son recibidas directamente por LLEIDANET PKI SUCURSAL DE PERÚ como prestador de Servicios Digitales o a través de nuestra Entidad de Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone LLEIDANET PKI SUCURSAL DE PERÚ es permanente.

9 USO DEL CERTIFICADO

9.1 USOS ADECUADOS DEL CERTIFICADO

Los usos adecuados de los Certificados emitidos son especificados en Políticas de Certificación de LLEIDANET PKI SUCURSAL DE PERÚ.

Los Certificados emitidos bajo esta CPS pueden ser utilizados con los siguientes propósitos:

- **Identificación del Titular:** El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.
- **Integridad del documento firmado:** La utilización del Certificado garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.
- **No repudio de origen:** Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

9.2 USOS PROHIBIDOS DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta CPS y concretamente en las Políticas de Certificación.

Se consideran indebidos aquellos usos que no están definidos en esta CPS y en consecuencia para efectos legales, LLEIDANET PKI SUCURSAL DE PERÚ queda eximida de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según esta CPS.

10 PERSONA DE CONTACTO

Datos de la Entidad de Certificación Digital:

Nombre: LLEIDANET PKI SUCURSAL DE PERÚ

Dirección: Avenida Santo Toribio N° 143 Piso 2 Oficina 38

Domicilio: San Isidro, Lima

Correo electrónico: consultas@indenova.com

Página Web: https://www.lleida.net/es

Datos de la Entidad de Registro o Verificación:

Nombre: LLEIDANET PKI SUCURSAL DE PERÚ

Dirección: Avenida Santo Toribio N° 143 Piso 2 Oficina 38

Domicilio: San Isidro, Lima

Correo electrónico: consultas@indenova.com

Página Web: https://www.lleida.net/es

Datos de la Oficina Administrativa ER:

Nombre: LLEIDANET PKI SUCURSAL DE PERÚ

Dirección: Avenida Santo Toribio N° 143 Piso 2 Oficina 38

Domicilio: San Isidro, Lima

Correo electrónico: consultas@indenova.com

Página Web: https://www.lleida.net/es

11 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por LLEIDANET PKI SUCURSAL DE PERÚ, son responsables de revisar la presente CPS y las Políticas de Certificación, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

12 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP Y CPS

LLEIDANET PKI SUCURSAL DE PERÚ administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la EC de LLEIDANET PKI SUCURSAL DE PERÚ.

Para cualquier consulta contactar:

- Dirección de correo electrónico: consultas@indenova.com
- Cargo: Responsable de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ

13 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Certificación Digital - CPS de Cargo: Responsable de la SVA de LLEIDANET PKI SUCURSAL DE PERÚ, la Política y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección: https://www.lleida.net/es/politicas-y-practicas?tab=peru

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el Responsable de la EC de LLEIDANET PKI SUCURSAL DE PERÚ antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Los documentos referidos a la Declaración de Prácticas y Políticas de Certificación de los proveedores de LLEIDANET PKI SUCURSAL DE PERÚ, así como la Declaración de Prácticas de las ER con las que tiene filiación serán publicados en la siguiente dirección:

https://www.lleida.net/es/politicas-y-practicas?tab=peru

14 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Certificado Raíz de servicios de LLEIDANET PKI SUCURSAL DE PERÚ

http://certs.esigna.es/root/indenova_global_root_ca.crt

Certificados Subordinadas LLEIDANET PKI SUCURSAL DE PERÚ

http://certs.esigna.es/ca/indenova_pki_001_pe.crt

Lista de Certificados Revocados (CRL)

http://crl.esigna.es/root/indenova_pki_001_pe.crl

http://crl1.esigna.es/root/indenova_pki_001_pe.crl

Declaración de Prácticas de Certificación (CPS)

http://cps.esigna.es/sub/cps_sub001pe_ca.pdf

Validación de Certificados

https://ocsp2.esigna.es

14.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de LLEIDANET PKI SUCURSAL DE PERÚ es el encargado de la autorización de la publicación de la CPS y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web: www.lleida.net

La Lista de Certificados Revocados es publicada en la página web www.lleida.net y está firmada digitalmente por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ.

La información del estado de los certificados digitales vigentes está disponible para consulta mediante protocolo OCSP.

14.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en el numeral Frecuencia de emisión de las CRLs.

Declaración de Prácticas de Certificación (CPS)

Con autorización del Responsable de la Entidad de Certificación de LLEIDANET PKI SUCURSAL DE PERÚ y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ junto con la nueva versión. La Auditoria anual validará estos cambios y emitirá el informe de cumplimiento.

Validación de Certificados

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ publicará los certificados emitidos en un repositorio en formato X.509 V3 los cuales podrán ser consultados en la dirección:

14.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página Web de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de la Entidad de Certificación, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a la misma.

15 IDENTIFICACION Y AUTENTICACION

15.1 NOMBRES

15.1.1 TIPOS DE NOMBRES

El documento guía que LLEIDANET PKI SUCURSAL DE PERÚ utiliza para la identificación única de los titulares de certificados emitidos está definido en la estructura del Nombre Distintivo "Distinguished Name (DN)" de la norma ISO/IEC 9595 (X.500).

Los certificados emitidos por LLEIDANET PKI SUCURSAL DE PERÚ contienen el nombre distintivo (distinguished name o DN) X.500 del emisor y el destinatario del certificado en los campos issuer name y subject name respectivamente.

15.1.1.1 CERTIFICADO RAÍZ DE LLEIDANET PKI SUCURSAL DE PERÚ

El DN del 'issuer name' del certificado raíz, tiene los siguientes campos y valores fijos:

C = ES

L = Valencia

STREET = https://www.indenova.com/aviso-legal/

OU = Internet Certification Authority https://www.indenova.com

SERIALNUMBER = B97458996

O = Indenova SL

CN = Global Certification Authority Root Indenova

E = ca@indenova.com

En el DN del 'subject name' se incluyen los siguientes campos:

C = ES

L = Valencia

STREET = https://www.indenova.com/aviso-legal/

OU = Internet Certification Authority https://www.indenova.com

SERIALNUMBER = B97458996

O = Indenova SL

CN = Global Certification Authority Root Indenova

E = ca@indenova.com

15.1.1.2 CERTIFICADOS DE LAS SUBORDINADAS LLEIDANET PKI SUCURSAL DE PERÚ

El DN del 'issuer name' de los certificados de las subordinadas de LLEIDANET PKI SUCURSAL DE PERÚ, tiene las siguientes características:

C = ES

L = Valencia

STREET = https://www.indenova.com/aviso-legal/

OU = Internet Certification Authority https://www.indenova.com

SERIALNUMBER = B97458996

O = Indenova SL

CN = Global Certification Authority Root Indenova

E = ca@indenova.com

En el DN del 'subject name' se incluyen los siguientes campos:

C = PE

L = LIMA

STREET = http://www.indenova.com

OU = Internet Certification Authority http://www.indenova.com

T = Subordinate Certificate Perú

O = inDenova Sucursal del Perú

E = sub_ca_pe@indenova.com

SERIALNUMBER = 20549615709

CN = inDenova SUB001_PE

Description = inDenova Subordinate Certificate 001 Perú HW-KUSU

15.1.1.3 CERTIFICADOS DE TITULAR DE LLEIDANET PKI SUCURSAL DE PERÚ

El DN del 'issuer name' de los certificados de titular de LLEIDANET PKI SUCURSAL DE PERÚ, tiene las siguientes características generales:

C = PE

L = LIMA

STREET = http://www.indenova.com

OU = Internet Certification Authority http://www.indenova.com

T = Subordinate Certificate Perú

O = inDenova Sucursal del Perú

E = sub_ca_pe@indenova.com

SERIALNUMBER = 20549615709

CN = inDenova SUB001_PE

Description = inDenova Subordinate Certificate 001 Perú HW-KUSU

En el DN del 'subject name' se incluyen los siguientes campos:

CN=<APELLIDO1> <APELLIDO2> <NOMBRE1> <NOMBRE2>

GN=<NOMBRE1> <NOMBRE2>

SN=<APELLIDO1> <APELLIDO2>

NUMERO DE SERIE=<Número del documento de Identificación>

La descripción de los DN para cada tipo de certificado cubiertos por esta CPS, están detallados en la Política de Certificación.

15.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los nombres distintivos (DN) de los certificados emitidos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ son únicos y permiten establecer un vínculo entre la clave pública y el número de identificación del titular.

Debido a que una misma persona o entidad puede solicitar varios certificados a su nombre, estos se diferenciarán por el uso de un valor único en el campo DN. Si se llegase a presentar conflicto sobre la asignación y empleo de un nombre, este será resuelto previo conocimiento por parte del Comité de Seguridad.

15.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES

No se podrán utilizar alias en los campos de Titular ya que dentro del certificado debe figurar el verdadero nombre, razón social sigla y/o denominación del solicitante del certificado.

15.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

La regla utilizada para interpretar los nombres distintivos del emisor y de los titulares de certificados que emite LLEIDANET PKI SUCURSAL DE PERÚ es el estándar ISO/IEC 9595 (X.500) Distinguished Name (DN).

15.1.5 SINGULARIDAD DE LOS NOMBRES

El DN de los certificados digitales emitidos es único.

15.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ no está obligada a recopilar o solicitar evidencia en relación con la posesión o titularidad de marcas registradas u otros signos distintivos antes de la emisión de los certificados. Esta política se extiende al uso y empleo de nombres de dominio.

16 VALIDACIÓN INICIAL DE LA IDENTIDAD

16.1 MÉTODO PARA DEMOSTRAR LA POSESIÓN DE LA CLAVE PRIVADA

Para garantizar la emisión, posesión y control de la clave privada por parte del suscriptor, ésta es directamente generada por él, utilizando un dispositivo criptográfico seguro “Hardware Security Module (HSM)”, de generación segura de claves y transmitida mediante un canal seguro; o mediante archivo protegido utilizando el estándar PKCS#12.

No se realizan servicios de almacenamiento de originales, copias o back-ups de la clave privada de firma digital del suscritor en la ER ni en la EC.

16.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN (PERSONA JURÍDICA)

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

No obstante lo anterior, LLEIDANET PKI SUCURSAL DE PERÚ se reserva el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

16.3 AUTENTICACIÓN DE UNA IDENTIDAD INDIVIDUAL (PERSONA NATURAL)

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

No obstante lo anterior, LLEIDANET PKI SUCURSAL DE PERÚ se reserva el derecho de no expedir certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial y/o idoneidad legal o moral de todo el sistema de certificación.

16.4 INFORMACIÓN DE TITULAR NO VERIFICADA

Bajo ninguna circunstancia LLEIDANET PKI SUCURSAL DE PERÚ omitirá las labores de verificación que conduzcan a la identificación del Titular y que se traduce en la solicitud de exhibición de los documentos mencionados para organizaciones y personas naturales.

16.5 VALIDACIÓN DE LA AUTORIDAD

La validación de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ respecto a la propiedad de un dominio se realiza a través de la comprobación de la existencia de un correo que contiene la dirección del dominio en cuestión y/o verificación de datos de registro de dominio respectivo.

Los procedimientos de autenticación de validación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

16.6 CRITERIOS PARA LA INTEROPERABILIDAD

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ únicamente emitirá certificados a EC Subordinadas, que estén directamente vinculadas y/o operadas por LLEIDANET PKI SUCURSAL DE PERÚ.

17 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

17.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE-EMISIÓN DE RUTINA

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ realiza en todos los eventos el proceso de autenticación del solicitante incluso en los de renovación y con base en ello emite los certificados digitales.

Los procedimientos de autenticación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

17.2 IDENTIFICACIÓN Y AUTENTICACIÓN TRAS UNA REVOCACIÓN

Debido a que una revocación implica la expedición de un nuevo certificado, La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, realiza un nuevo proceso de autenticación del solicitante.

Los procedimientos de autenticación son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

18 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

LLEIDANET PKI SUCURSAL DE PERÚ, atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el numeral Circunstancias para la revocación de un certificado en esta CPS y autentica la identidad de quien solicita la revocación de certificado.

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

19 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

19.1 SOLICITUD DEL CERTIFICADO

Cualquier persona que requiera la prestación del servicio de certificación debe diligenciar el formulario de solicitud de certificado digital publicado en la página Web o el enviado al correo electrónico del solicitante, aceptar el Acuerdo del Titular cuyo modelo aparece al final de esta CPS y aportarlos junto con la documentación requerida para autenticar la información suministrada. Una vez completada y confirmada la información por parte del solicitante, el formulario de solicitud es enviado a la Entidad de Registro o Verificación, quien se encargará de validar la información suministrada y aprobarla de conformidad con el cumplimiento de los requisitos exigidos para cada tipo de certificado.

La solicitud de un servicio de certificación digital puede radicarse a través de los canales electrónicos o físicos que para el efecto disponga LLEIDANET PKI SUCURSAL DE PERÚ.

Los usuarios que solicitan nuestros productos y servicios aceptan los términos de uso y condiciones del servicio especificadas en la presente CPS y en el acuerdo del titular.

El solicitante aporta los documentos necesarios y se surten los procedimientos establecidos por LLEIDANET PKI SUCURSAL DE PERÚ, para la obtención de su certificado digital.

LLEIDANET PKI SUCURSAL DE PERÚ, se reserva el derecho de solicitar documentos adicionales a los exigidos en el formulario de solicitud, en original o copia; con el fin de verificar la identidad del solicitante, también puede eximir de la presentación de cualquier documento cuando la identidad del solicitante haya sido suficientemente verificada por LLEIDANET PKI SUCURSAL DE PERÚ a través de otros medios.

El solicitante acepta que LLEIDANET PKI SUCURSAL DE PERÚ tiene el derecho discrecional de rechazar una solicitud de certificado digital cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial, buen nombre de LLEIDANET PKI SUCURSAL DE PERÚ y/o idoneidad legal o moral de todo el sistema de certificación, notificando la no aprobación sin necesidad de indicar las causas.

Los procedimientos de autenticación de la identidad de los titulares y suscriptores son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

19.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud de emisión de un certificado digital.

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder. En este caso, el titular del certificado será el poderdante y corresponderá al

apoderado la condición de suscriptor. El ámbito de utilización del certificado digital en este supuesto se encontrará circunscrito y limitado a las facultades expresamente conferidas en el poder.

En el caso de personas jurídicas, se pueden solicitar certificados de atributo para ser usados por funcionarios y personal específico, incluso por el Representante legal. En este caso, se considera como aspirante a titular del certificado a la persona jurídica y dichas personas naturales vienen a ser los aspirantes a ser suscriptores.

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por un representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Los procedimientos de solicitud según el tipo de titular son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

19.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

LLEIDANET PKI SUCURSAL DE PERÚ en calidad de Entidad de Registro previamente cumplidos los requisitos de autenticación y verificación de los datos del solicitante, aprobará y firmará digitalmente la solicitud de emisión de certificados digitales. Toda la información relacionada quedará registrada en el sistema de la ER LLEIDANET PKI SUCURSAL DE PERÚ.

Las responsabilidades y limitaciones aplicables al certificado, así como las implicancias legales respectivas, son descritas en los contratos del titular.

20 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

20.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por la LLEIDANET PKI SUCURSAL DE PERÚ en calidad de Entidad de Registro, encargada de autorizar la emisión del certificado, quien comprueba si la información suministrada es auténtica y si la documentación anexa cumple con los requisitos definidos para cada tipo de certificado de acuerdo con su documento RPS.

La documentación que LLEIDANET PKI SUCURSAL DE PERÚ deberá comprobar para la correcta emisión de cada tipo de certificado se define en las Políticas de Certificación.

20.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Si una vez verificada la identidad del solicitante, la información suministrada cumple con los requisitos establecidos por esta CPS, se aprueba la solicitud. Si no es posible la identificación plena de la identidad del solicitante o no existe autenticidad plena de la información suministrada, se niega la solicitud y no se emite el certificado. LLEIDANET PKI SUCURSAL DE PERÚ no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación de la emisión de un certificado digital y así lo acepta y reconoce el solicitante al que le haya sido negada la expedición del respectivo certificado.

Igualmente, LLEIDANET PKI SUCURSAL DE PERÚ se reserva el derecho de no emitir certificados a pesar de que la identificación del solicitante y/o la información suministrada por este haya sido plenamente autenticada, cuando la emisión de un certificado en particular por razones de orden legal y/o de conveniencia comercial, buen nombre o reputación de EC de LLEIDANET PKI SUCURSAL DE PERÚ pueda poner en peligro el sistema de certificación digital.

En caso de que una solicitud sea aprobada por la ER, se realizará lo siguiente:

- Se comunicará a la EC su aprobación para la emisión del certificado. Para ello se deben implementar los mecanismos de seguridad necesarios para establecer una comunicación segura entre la EC y la ER durante el proceso de emisión del certificado y generación del par de claves.
- La ER de LLEIDANET PKI SUCURSAL DE PERÚ requerirá al suscriptor la firma de un contrato de conformidad personal de dichas responsabilidades, así como de conformidad por parte de los titulares en cuyo nombre actúa el suscriptor.

20.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

El plazo para la aprobación de una solicitud por parte de la ER de LLEIDANET PKI SUCURSAL DE PERÚ, es de tres (3) días hábiles desde el momento de recibir la documentación e información completa. El tiempo de entrega del certificado digital una vez recibida la solicitud completa es de cinco (5) días hábiles.

21 EMISIÓN DE CERTIFICADOS

21.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

El paso final del proceso de expedición de certificados digitales es la emisión del certificado y su entrega de manera segura al titular.

El proceso de emisión de certificados digitales vincula de una manera segura la información de registro y la clave pública generada.

El certificado emitido se encuentra firmado digitalmente por el proveedor de servicios de certificación digital que lo emitió.

21.2 NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO

Mediante correo electrónico se informa al titular la emisión de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá entregado el certificado. Se entenderá que se ha recibido el correo electrónico donde se notifica la emisión de un certificado, cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección de correo electrónico que consta en el formulario de solicitud.

La publicación de un certificado en el repositorio de certificados constituye la prueba y una notificación pública de su emisión.

22 ACEPTACIÓN DEL CERTIFICADO

22.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

No se requiere confirmación de parte del titular como aceptación del certificado recibido. Se considera que un certificado es aceptado por el titular desde el momento que solicita su expedición, por ello, si la información contenida en el certificado expedido no corresponde al estado actual de la misma o no fue suministrada correctamente, se debe solicitar su revocación por parte del solicitante y éste así lo acepta, según procedimiento descrito en el apartado Procedimiento de solicitud de revocación.

22.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

LLEIDANET PKI SUCURSAL DE PERÚ publica los certificados emitidos en un repositorio en formato X.509 V3 y puede ser consultado en la página Web www.lleida.net donde podemos acceder al repositorio de certificados.

22.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

No aplica.

23 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

23.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

El titular del certificado emitido y de la clave privada asociada acepta las condiciones de uso establecidas en esta CPS por el solo hecho de haber solicitado la emisión del certificado y solo podrá emplearlos para los usos explícitamente mencionados y autorizados en la presente CPS y de acuerdo con lo establecido en los campos "Extended Key Usage" de los certificados. Por consiguiente, los certificados emitidos y la clave privada no deberán ser usados en otras actividades que estén por fuera de los usos mencionados. Una vez perdida la vigencia del certificado, el titular está obligado a no seguir usando la clave privada asociada al mismo. Con base en lo anterior, desde ya acepta y reconoce el titular, que en tal sentido será el único responsable por cualquier perjuicio pérdida o daño que cause a terceros por el uso de la clave privada una vez expirada la vigencia del certificado. LLEIDANET PKI SUCURSAL DE PERÚ no asume ningún tipo de responsabilidad por los usos no autorizados.

El titular o suscriptor deberá notificar a la EC o ER de LLEIDANET PKI SUCURSAL DE PERÚ los siguientes casos:

1. La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, token criptográfico o tarjeta inteligente).
2. El compromiso potencial de su clave privada.
3. La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
4. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

Asimismo, el titular y suscriptor deberán dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado.

En el caso de los certificados de firma remota, el titular debe conservar las herramientas y/o dispositivos de autenticación de la firma remota de forma segura. Asimismo, debe mantener el PIN de activación de la clave privada del certificado de firma remota bajo su control exclusivo y de forma separada a las contraseñas de autenticación o dispositivos de autenticación.

23.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

El titular al que se le haya expedido un certificado se obliga a que cada vez que haga uso del certificado con destino a terceras personas deberá informarles que es necesario que consulten el estado del certificado en el repositorio de certificados revocados, así como en el de emitidos a fin de verificar su vigencia y que se esté aplicando dentro de sus usos permitidos establecidos en esta CPS.

En este sentido deberá comprobar que:

- Comprobar que el certificado asociado no incumple las fechas de inicio y final de validez.
- Comprobar que el certificado asociado a la clave privada no está revocado.

El tercero que confía deberá cumplir lo siguiente:

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la IOFE, sin permiso previo por escrito de la EC.
- No comprometer intencionadamente la seguridad de la Jerarquía de la IOFE.
- Aplicar los criterios de verificación adecuados para la validación de un certificado durante su uso en las transacciones electrónicas.
- Denunciar cualquier situación en la que la EC deba revocar el certificado de un titular, siempre y cuando se tengan pruebas fehacientes del compromiso de la clave privada o de un uso ilegal del manejo de la misma. Por ejemplo, debe denunciar la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena una clave privada que no le pertenece (computador, token criptográfico o tarjeta inteligente).

24 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, no atiende requerimientos de renovación de un certificado sin cambio de claves.

24.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

No aplica por cuanto no se expiden certificados sin cambio de claves.

24.2 QUIÉN PUEDE SOLICITAR UNA RENOVACIÓN SIN CAMBIO DE CLAVES

No aplica por cuanto no se expiden certificados sin cambio de claves.

24.3 TRÁMITES PARA LA SOLICITUD DE RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

No aplica por cuanto no se expiden certificados sin cambio de claves.

24.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO SIN CAMBIO DE CLAVES

No aplica por cuanto no se expiden certificados sin cambio de claves.

24.5 FORMA EN LA QUE SE ACEPTA LA RENOVACIÓN DE UN CERTIFICADO SIN CAMBIO DE CLAVES

No aplica por cuanto no se expiden certificados sin cambio de claves.

24.6 PUBLICACIÓN DEL CERTIFICADO RENOVADO POR LA EC SIN CAMBIO DE CLAVES

No aplica por cuanto no se expiden certificados sin cambio de claves.

24.7 NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RENOVADO POR LA EC A OTRAS ENTIDADES

No aplica por cuanto no se expiden certificados sin cambio de claves.

25 RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Para la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, un requerimiento de re-emisión de un certificado con cambio de claves es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante.

La EC de LLEIDANET PKI SUCURSAL DE PERÚ comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Si el suscriptor no solicita la re-emisión de certificado, el certificado expirará. Luego de ello, el suscriptor deberá realizar el proceso de validación de identidad desde la etapa inicial.

25.1 CIRCUNSTANCIAS PARA LA RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Las circunstancias son definidas en la Declaración de Prácticas de Registro de LLEIDANET PKI SUCURSAL DE PERÚ como Entidad de Registro.

25.2 QUIÉN PUEDE SOLICITAR UNA RE-EMISIÓN CON CAMBIO DE CLAVES

Las precisiones sobre quien puede solicitar una re-emisión son definidas en la Declaración de Prácticas de Registro de LLEIDANET PKI SUCURSAL DE PERÚ como Entidad de Registro.

25.3 TRÁMITES PARA LA SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

El procedimiento para re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de LLEIDANET PKI SUCURSAL DE PERÚ como Entidad de Registro.

25.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO CON CAMBIO DE CLAVES

Mediante correo electrónico se informa al titular la emisión de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico se entenderá entregado el certificado. Se entenderá que se ha recibido el correo electrónico donde se notifica la emisión

de un certificado cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección correo electrónico que consta en el formulario de solicitud.

La publicación de un certificado en el repositorio de certificados constituye la prueba y una notificación pública de su emisión.

25.5 FORMA EN LA QUE SE ACEPTA LA RE-EMISIÓN DE UN CERTIFICADO

No se requiere confirmación de parte del titular como aceptación del certificado recibido. Se considera que un certificado es aceptado por el titular desde el momento que solicita su expedición, por ello, si la información contenida en el certificado expedido no corresponde al estado actual de la misma o no fue suministrada correctamente se debe solicitar su revocación por parte del solicitante y éste así lo acepta.

El procedimiento para aceptar la re-emisión de certificados digitales es definido en la Declaración de Prácticas de Registro de LLEIDANET PKI SUCURSAL DE PERÚ como Entidad de Registro.

25.6 PUBLICACIÓN DEL CERTIFICADO RE-EMITIDO POR LA EC

Al igual que los certificados nuevos, la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ publica los certificados renovados en un repositorio en formato X.509 V3 y pueden ser consultados en la dirección www.lleida.net.

25.7 NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RE-EMITIDO POR LA EC A OTRAS ENTIDADES

No existen entidades externas a las que se requiera ser notificada la emisión de un certificado renovado.

26 MODIFICACIÓN DE CERTIFICADOS

Los certificados digitales emitidos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, no puede ser modificados. A cambio el titular debe solicitar la emisión de uno nuevo. En este evento y por una única vez se expedirá nuevo certificado al titular sin costo adicional de la emisión, por el tiempo faltante para el vencimiento original, cobrando solamente el valor del dispositivo criptográfico si a ello hubiere lugar.

26.1 CIRCUNSTANCIAS PARA LA MODIFICACIÓN DE UN CERTIFICADO

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

26.2 QUIÉN PUEDE SOLICITAR UNA MODIFICACIÓN

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

26.3 TRÁMITES PARA LA SOLICITUD DE MODIFICACIÓN DE UN CERTIFICADO

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

26.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

26.5 FORMA EN LA QUE SE ACEPTA LA MODIFICACIÓN DE UN CERTIFICADO

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

26.6 PUBLICACIÓN DEL CERTIFICADO MODIFICADO POR LA EC

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

26.7 NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO POR LA EC A OTRAS ENTIDADES

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ no pueden ser modificados.

27 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

27.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

El titular reconoce y acepta que los certificados deben ser revocados cuando ocurra cualquiera de las siguientes circunstancias:

- Solicitud voluntaria del Titular.
- Divulgación voluntaria o involuntaria de la clave privada.
- Compromiso de la clave privada del Titular por pérdida, hurto o daño.
- Pérdida, hurto o daño del dispositivo físico del Certificado.
- Fallecimiento del titular, incapacidad sobreviniente, total o parcial.
- Conocimiento de eventos que modifiquen el estado inicial de los datos suministrados, entre otros: terminación de la Representación Legal, terminación del vínculo laboral, liquidación y/o extinción de la personería jurídica, cesación en la función pública o cambio a una distinta.
- En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante.
- Terminación de actividades del prestador de servicios de certificación salvo que los certificados emitidos sean transferidos a otro prestador de servicios
- Compromiso de la clave privada de la Entidad de Certificación por pérdida, robo, hurto o daño.
- Pérdida, hurto o daño del dispositivo físico del Certificado de la Entidad de Certificación.
- Por incumplimiento por parte de la Entidad de Certificación o el Titular de las obligaciones establecidas en la Declaración de Prácticas de Certificación.
- Uso indebido de la clave privada del titular de conformidad con lo expuesto en la CPS.
- Por orden judicial o de entidad administrativa competente.
- Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante e LLEIDANET PKI SUCURSAL DE PERÚ.
- Por revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por decisión de la legislación respectiva.

Además, el certificado de un titular debe ser revocado por la EC cuando:

- Se produce la renovación del certificado.
- Se produce la re-emisión del certificado.

No obstante, las causales anteriores, LLEIDANET PKI SUCURSAL DE PERÚ, también podrá revocar certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial, buen nombre de EC de LLEIDANET PKI SUCURSAL DE PERÚ y/o idoneidad legal o moral de todo el sistema de certificación.

27.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

El titular, un Tercero que confía o cualquier persona interesada cuando tenga constancia demostrable de conocimiento de hechos y causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta CPS y que comprometan la clave privada:

- El titular o suscriptor del certificado.
- La EC que emitió el certificado.
- Un juez que de acuerdo a la Ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento

El comité de Seguridad como máximo ente de control que tiene atribuida la administración de la seguridad de la infraestructura tecnológica de la Entidad de Certificación, está en capacidad de solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la clave privada del subscriptor o cualquier otro hecho que tienda al uso indebido de clave privada del titular o de la Entidad de Certificación.

27.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

Las personas interesadas en solicitar la revocación de un certificado digital cuyas causas están especificadas en esta CPS lo pueden hacer bajo los siguientes procedimientos:

- Servicio de Revocación en línea. A través de la página Web de LLEIDANET PKI SUCURSAL DE PERÚ, ingresando al servicio de revocación de certificados digitales y mediante la autenticación del PIN de revocación (CRIN), asignado durante el proceso de solicitud del certificado digital.
- En las oficinas de LLEIDANET PKI SUCURSAL DE PERÚ. En horario de atención al público se reciben las solicitudes escritas de revocación de certificados digitales firmadas por los titulares.
- Servicio de Revocación telefónica. A través de la línea de atención telefónica permanente los titulares y terceros pueden solicitar la revocación de certificados digitales conforme a las causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta CPS.
- Servicio de Revocación vía correo electrónico. Por medio de nuestro correo electrónico, los titulares y terceros pueden solicitar la revocación de certificados digitales conforme a las

causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta CPS.

Los procedimientos de solicitud de revocación según el tipo de solicitante son descritos en el documento de Declaración de Prácticas de Registro o Verificación de LLEIDANET PKI SUCURSAL DE PERÚ – RPS.

27.4 PERIODO DE GRACIA DE SOLICITUD DE REVOCACIÓN

Previa validación de la autenticidad de una solicitud de revocación, LLEIDANET PKI SUCURSAL DE PERÚ procederá en forma inmediata con la revocación solicitada, dentro de los horarios de oficina de éste. En consecuencia, no existe un periodo de gracia que permita al solicitante cancelar la solicitud. Si se trató de una falsa alarma, el titular debe solicitar un nuevo, pues el certificado revocado perdió su validez inmediatamente fue validada la solicitud de revocación.

El procedimiento utilizado por LLEIDANET PKI SUCURSAL DE PERÚ para verificar la autenticidad de una solicitud de revocación formulada por una persona determinada, es verificar la solicitud y validarla directamente con el titular realizando el contacto con él mismo y confrontando los datos suministrados en la solicitud original.

Una vez solicitada la revocación del certificado, si se evidencia que dicho certificado es utilizado vinculado con la clave privada, el titular releva de toda responsabilidad legal a LLEIDANET PKI SUCURSAL DE PERÚ, toda vez que reconoce y acepta que el control, custodia y confidencialidad de la clave privada es responsabilidad exclusiva de este.

27.5 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

La solicitud de revocación de un certificado digital debe ser atendida con la máxima urgencia, sin que su revocación tome más de 24 horas una vez validada la solicitud.

Una vez cumplidas las formalidades previstas para la revocación y si por alguna razón, no se hace efectiva la revocación de un certificado en los términos establecidos por esta CPS, LLEIDANET PKI SUCURSAL DE PERÚ como prestador de servicios de certificación responderá por los perjuicios que se causen a los titulares o Terceros que confían derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de la Entidad de Certificación y para ello cuenta con un seguro de responsabilidad civil de conformidad con el Artículo 8°. Garantías, del Decreto 1747 de 2000. LLEIDANET PKI SUCURSAL DE PERÚ no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente CPS.

27.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Es responsabilidad del titular de un certificado digital y éste así lo acepta y reconoce, informar a los Terceros que confían de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado. Informará igualmente el titular al Tercero que confía que, para realizar dicha consulta, dispone de la lista de certificados revocados CRL, publicada de manera de periódica por LLEIDANET PKI SUCURSAL DE PERÚ.

27.7 FRECUENCIA DE EMISIÓN DE LAS CRLS

Cada vez que se produzca una revocación de un certificado, LLEIDANET PKI SUCURSAL DE PERÚ generará y publicará una nueva CRL de manera inmediata en su repositorio y a pesar de que no se produzca ninguna revocación cada veinticuatro (24) horas se generará y publicará una nueva CRL.

27.8 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática, menor a una hora como lo establece el INDECOPI.

27.9 REVOCACIÓN ON-LINE/DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

LLEIDANET PKI SUCURSAL DE PERÚ publicará tanto la CRL como el estado de los certificados revocados en repositorios de libre acceso y fácil consulta, con disponibilidad 7X24 durante todos los días del año. LLEIDANET PKI SUCURSAL DE PERÚ ofrece un servicio de consulta en línea basada en el protocolo OCSP en la dirección https://ocsp2.esigna.es.

27.10 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE

Para obtener la información del estado de revocación de un certificado en un momento dado, se puede hacer la consulta en línea en la dirección https://ocsp2.esigna.es para lo cual se debe contar con un software que sea capaz de operar con el protocolo RFC 6960. La mayoría de los navegadores ofrecen este servicio.

27.11 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

LLEIDANET PKI SUCURSAL DE PERÚ mantendrá un archivo histórico hasta de cinco (5) años de las CRL´s generadas y que estarán a disposición de los titulares mediante solicitud escrita dirigida a LLEIDANET PKI SUCURSAL DE PERÚ.

27.12 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

Si se solicitó la revocación de un certificado digital por compromiso (pérdida, destrucción, robo, divulgación) de la clave privada, el titular puede solicitar un nuevo certificado digital por un periodo igual o mayor al inicialmente solicitado presentando una solicitud de renovación en relación con el certificado digital comprometido. La responsabilidad de la custodia de la clave es del titular y éste así lo acepta y reconoce, por tanto, es él quien asume el costo de la renovación de conformidad con las tarifas vigentes fijadas para la renovación de certificados digitales.

27.13 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

LLEIDANET PKI SUCURSAL DE PERÚ no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

27.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

No aplica por cuanto LLEIDANET PKI SUCURSAL DE PERÚ no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

27.15 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

No aplica por cuanto LLEIDANET PKI SUCURSAL DE PERÚ no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

27.16 LÍMITES DEL PERIODO DE SUSPENSIÓN

No aplica por cuanto LLEIDANET PKI SUCURSAL DE PERÚ no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

27.17 NOTIFICACIÓN DE LA REVOCACIÓN DE UN CERTIFICADO

Dentro de las 24 horas siguientes a la revocación de un certificado, LLEIDANET PKI SUCURSAL DE PERÚ informa al titular, mediante correo electrónico, la revocación de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico se entenderá que su solicitud fue atendida. Se entenderá que se ha recibo el correo electrónico donde se notifica la revocación de un certificado cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección correo electrónico que consta en el formulario de solicitud.

La publicación de un certificado revocado en la CRL constituye la prueba y una notificación pública de su revocación.

28 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

28.1 CARACTERÍSTICAS OPERACIONALES

Para la consulta del estado de los certificados emitidos por LLEIDANET PKI SUCURSAL DE PERÚ, se dispone de un servicio de consulta en línea basada en el protocolo OCSP (Online Certificate Status Protocol: Protocolo que permite revisar en línea el estado de un certificado digital) en la dirección https://ocsp2.esigna.es. El titular envía una petición de consulta sobre el estado del certificado a través del protocolo OCSP, que una vez consultada la base de datos, es atendida mediante una respuesta vía http.

28.2 DISPONIBILIDAD DEL SERVICIO

El servicio de consulta del estado de certificados digitales está disponible en la página Web de forma permanente las 24 horas durante todos los días del año.

LLEIDANET PKI SUCURSAL DE PERÚ realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre inaccesible de forma continua más de 24 horas, siendo este un servicio crítico en las actividades de LLEIDANET PKI SUCURSAL DE PERÚ y por lo tanto tratado de forma adecuada en el Plan de contingencias y de continuidad de negocio.

28.3 CARACTERÍSTICAS OPCIONALES

Para obtener la información del estado de certificado en un momento dado, se puede hacer la consulta en línea en la dirección https://ocsp2.esigna.es, para lo cual se debe contar con un software que sea capaz de operar con el protocolo OCSP. La mayoría de navegadores ofrecen este servicio.

28.4 FINALIZACIÓN DE LA VIGENCIA DE UN CERTIFICADO

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ da por finalizada la vigencia de un certificado digital emitido ante las siguientes circunstancias:

- Pérdida de validez por revocación del certificado digital.
- Vencimiento del periodo para el cual un titular contrato la vigencia del certificado.

29 CUSTODIA Y RECUPERACIÓN DE CLAVES

29.1 ALMACENAMIENTO DE LA CLAVE PRIVADA DEL TITULAR

La clave privada del titular se puede almacenar en un dispositivo software o hardware. El dispositivo criptográfico en hardware utilizado por LLEIDANET PKI SUCURSAL DE PERÚ es una tarjeta criptográfica o token USB que cumple los requerimientos mínimos de la normatividad vigente y las garantías de la certificación europea Common Criteria como "dispositivo seguro de creación de firma".

Estos dispositivos criptográficos seguros de creación de firma, cumplen con las certificaciones como chip criptográfico: nivel de seguridad CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 NIVEL 3 y las certificaciones SO del chip criptográfico: nivel de seguridad CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) – BSI –DSZ-CC-0422-2008 y soportan los estándares PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE.

LLEIDANET PKI SUCURSAL DE PERÚ publica en su portal www.lleida.net las características de los dispositivos criptográficos que ofrece a los titulares que así lo solicitan para creación y almacenamiento de sus claves privadas.

29.2 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

La generación de la clave privada es responsabilidad del titular y es generada directamente sobre un dispositivo seguro (hardware), del cual no se puede exportar. En consecuencia, no es posible la recuperación de la clave privada del titular debido a que no existe copia alguna. La responsabilidad de la custodia de la clave privada es del titular y éste así lo acepta y reconoce.

29.3 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE LA CLAVE DE SESIÓN

La recuperación de la clave de sesión del titular o PIN, no es posible ya que no existe copia alguna por cuanto es él, el único que puede generarlo y este así lo declara y acepta. La responsabilidad de la custodia de la clave de sesión o PIN es del titular quien acepta no mantener registros digitales, escritos o en cualquier otro formato y quien se obliga a memorizarlo, por lo que su olvido requiere la solicitud de revocación del certificado y la solicitud de uno nuevo por cuenta del titular.

30 CONTROLES FÍSICOS DE LA INSTALACION, GESTIÓN Y OPERACIONALES

30.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA A TRAVÉS DE LA CUAL LLEIDANET PKI SUCURSAL DE PERÚ PRESTA SUS SERVICIOS.

30.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

LLEIDANET PKI SUCURSAL DE PERÚ dispone de medidas de seguridad para el control de acceso al edificio donde se encuentra su infraestructura, ya que los servicios de certificación digitales regulados y prestados a través de esta CPS se realizan a través de un proveedor de servicio debidamente avalado con ISO 27001 e ISO 20000. Solo se permite el ingreso al edificio de personas previamente identificadas y autorizadas que porten en un lugar visible el carné de visitantes.

Dicho proveedor cuenta con un área restringida, separada físicamente de las demás áreas, con perímetros identificados, donde se realizan las operaciones más sensibles de LLEIDANET PKI SUCURSAL DE PERÚ y a donde únicamente tiene acceso el personal autorizado.

Esta área restringida cumple con los siguientes requisitos:

- Está completamente aislado de las demás áreas.
- Ingresan únicamente personas autorizadas.
- Los equipos de misión crítica están debidamente protegidos en racks.
- No posee ventanas hacia el exterior del edificio.
- Cuenta con un circuito cerrado de televisión las 24 horas, con cámaras tanto al interior como al exterior del centro de cómputo.
- Cuenta con control de acceso basado en tarjeta y lector biométrico.
- Sistemas de protección y prevención de incendios: detectores de humo, sistema de extinción de incendios.
- Cuenta con personal capacitado para actuar ante eventos catastróficos

- Cuenta con un sistema detector de intrusos
- El cableado está debidamente protegido contra daños, intentos de sabotaje o interceptación por medio de canaletas.
- Está separado de áreas de carga y descarga.
- No existe tránsito frecuente de personas por los alrededores.

30.1.2 ACCESO FÍSICO

Existen varios niveles de seguridad que restringen el acceso a la infraestructura tecnológica a través de la cual LLEIDANET PKI SUCURSAL DE PERÚ presta sus servicios y cada uno ellos disponen de sistemas de control de acceso físico. Las instalaciones cuentan con un servicio de circuito cerrado de televisión y con personal de vigilancia. Existen dentro de las instalaciones zonas restringidas que por el tipo de equipos considerados críticos y operaciones sensibles que se manejan tienen acceso permitido solo a ciertas personas de acuerdo a su rol.

30.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

El centro de cómputo cuenta con un sistema de aire acondicionado y dispone de un adecuado suministro de electricidad con protección contra caídas de tensión y otras fluctuaciones eléctricas que podrían eventualmente afectar sensiblemente a los equipos y producir daños graves. Adicionalmente, se cuenta con un sistema de respaldo que garantiza que no haya interrupción en el servicio con una autonomía suficiente para garantizar la continuidad en el servicio. En caso de una falla en el sistema de respaldo, se cuenta con el tiempo suficiente para hacer un apagado controlado.

30.1.4 EXPOSICIÓN AL AGUA

El centro de cómputo se encuentra aislado de posibles fuentes de agua y cuenta con sensores de detección de inundaciones conectados al sistema general de alarma.

30.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

El centro de cómputo cuenta de un sistema de detección de incendios y un sistema de extinción de incendios. Se cuenta con un sistema de cableado que protege las redes internas.

30.1.6 SISTEMA DE ALMACENAMIENTO

Se cuenta con procedimientos de toma de back ups, restauración y pruebas de los mismos. Los medios magnéticos son almacenados en sitios seguros de acceso restringido. Una copia reposa dentro de las instalaciones y otra en un sitio externo, protegidas con controles ambientales.

30.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

Todo documento en papel que contenga información sensible de la entidad y que ha cumplido su vida útil deberá ser destruido físicamente para garantizar la imposibilidad de recuperación de información. Si el documento o información está almacenado en un medio magnético se debe formatear, borrar permanentemente o destruir físicamente el dispositivo en casos extremos como daños de dispositivos de almacenamiento o dispositivos no reutilizables, siempre garantizando que no sea posible la recuperación de la información por cualquier medio conocido o no conocido por el momento.

30.1.8 BACKUP FUERA DE LA INSTALACIÓN

LLEIDANET PKI SUCURSAL DE PERÚ mantendrá una copia de respaldo de las bases de datos en custodia fuera de las instalaciones.

30.2 CONTROLES DE PROCEDIMIENTO

30.2.1 ROLES DE CONFIANZA

Para la operación del sistema se han definido los siguientes roles dentro del sistema de emisión de certificados digitales:

- Administrador del Sistema: responsable de actividades relacionadas con la instalación, configuración y mantenimiento de la infraestructura de hardware, software.
- Auditor del ciclo de certificación: Encargado de auditar los procesos del ciclo de emisión de certificados digitales y garantizar el cumplimiento de los procedimientos y políticas de seguridad de la información. Entre sus funciones está la revisión periódica de los logs de auditoria.
- Oficial de Registro (Entidad de Registro de LLEIDANET PKI SUCURSAL DE PERÚ): Es el responsable de verificar que la información suministrada por los solicitantes de certificados digitales sea auténtica e integra. Es el responsable de solicitar en nombre de los titulares la emisión o revocación de certificados digitales.

30.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Para cada uno de los roles mencionados se requiere una persona.

La EC garantiza al menos la colaboración de dos personas para realizar las tareas que afectan a la gestión de claves criptográficas de la propia EC.

30.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

El Administrador de Sistema, el Auditor del ciclo de certificación y el oficial de registro se autentican mediante certificados digitales emitidos por LLEIDANET PKI SUCURSAL DE PERÚ.

Las personas asignadas para cada rol son identificadas por el auditor que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y claves.

30.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

El rol de Auditor del ciclo de certificación es incompatible con cualquier otro rol. El rol de Administrador del Sistema y el rol de Oficial de Registro son incompatibles.

30.3 CONTROLES DE PERSONAL

30.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Se tiene definido un proceso de selección de personal que tiene como base el perfil de cada uno de los cargos involucrados en el proceso de emisión de certificados digitales. El candidato a un cargo debe tener la formación, experiencia, conocimientos y habilidades definidas en el perfil para el cargo requerido.

30.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

Los candidatos a ocupar cargos del ciclo de certificación deben presentar su certificado de antecedentes vigente.

30.3.3 REQUISITOS DE FORMACIÓN

Los requisitos de formación para cada uno de los cargos mencionados se encuentran en el manual de funciones que es dado a conocer a la persona seleccionada para ocupar el cargo como parte de su inducción. Los aspectos más destacados que son parte de la formación son:

- Conocimiento de la Declaración de Prácticas de Certificación.
- Conocimiento de la normatividad vigente y relacionada con las entidades de certificación abierta y los servicios que presta.
- Conocimiento de las Políticas de Seguridad y la aceptación de un acuerdo de confidencialidad sobre la información que se maneja en virtud del cargo.

- Conocimiento de la operación del software y hardware para cada papel específico.
- Conocimiento de los procedimientos de seguridad para cada rol específico.
- Conocimiento de los procedimientos de operación y administración para cada rol específico.
- Conocimiento de los Procedimientos de Contingencia.
- Conocimiento del Documento de Segregación de Funciones.

30.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Dentro de la programación anual de capacitación se incluye una actualización en Seguridad de la Información para los integrantes del ciclo de emisión de certificados digitales.

30.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No existe rotación de tareas en los cargos mencionados.

30.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Es calificada como falta grave ejecutar acciones no autorizadas y las personas serán sancionadas de conformidad con el manual interno de trabajo. Las acciones no autorizadas son las que no están especificadas dentro de la Declaración de Prácticas de certificación o en la normatividad vigente.

30.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Entre los requisitos de contratación de terceros está el conocimiento de las Políticas de Seguridad y la firma de un Acuerdo de Confidencialidad sobre la información que sea suministrada o conocida.

30.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

La documentación mencionada en el numeral Requisitos de Formación, está publicada en la intranet para fácil consulta y forma parte de la inducción de personal.

30.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

30.4.1 TIPOS DE EVENTOS REGISTRADOS

Las actividades más sensibles del ciclo de certificación requieren el control y seguimiento de eventos que se pueden presentar durante su operación. De conformidad con su nivel de criticidad los eventos se clasifican en:

- Informativo: una acción terminó de manera exitosa.
- Tipo marca: inicio y finalización de una sesión
- Advertencia: presencia de un hecho anormal pero no de una falla.
- Error: una operación generó una falla predecible.
- Error fatal: una operación generó una falla impredecible.

Se registran los siguientes eventos:

- Encendido y apagado de los sistemas.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema de certificación.
- Intentos de entrada y salida del sistema de certificación.
- Intentos no autorizados de acceso a los registros o bases de datos del sistema de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos no autorizados de entrada a la red de la EC.
- Generación de claves de la EC.
- Intentos nulos de lectura y escritura en un certificado y en el repositorio.
- Eventos relacionados con el ciclo de vida del certificado: emisión, revocación, re emisión, suspensión y modificación
- Mantenimientos y cambios de configuración del sistema.
- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos incluye la hora, fecha e identificadores software/hardware.

30.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

Los registros de auditoria son revisados utilizando procedimientos manuales y automáticos con una frecuencia semanal.

La revisión de los log se realiza cuando se detecte una alerta de seguridad o existan indicios de un funcionamiento no usual de los sistemas.

30.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría se mantienen durante seis (6) meses en el sistema y son almacenadas durante 10 años en medios magnéticos seguros. Transcurrido los 10 años y con autorización del comité de seguridad y del INDECOPI se puede proceder a destruirlos.

30.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los logs de auditoria forman parte del respaldo diario del sistema de información y se conservan de igual manera manteniendo una copia en el sitio y otra copia fuera de las instalaciones.

30.4.5 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Los respaldos de los registros de auditoria siguen los mismos procedimientos para la de respaldo de los sistemas de información.

30.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de recopilación de información de auditoría se basa en los registros automáticos de las aplicaciones que soportan el ciclo de certificación incluyendo los logs de aplicación, logs de seguridad y logs del sistema.

Las auditorías internas se llevan a cabo una vez al año.

Las auditorías externas se llevan a cabo una vez al año (auditoría periódica).

30.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

A juicio del Comité de seguridad se hará la notificación al sujeto causa de un incidente de seguridad detectado a través de los logs de auditoria a fin de tener respuesta formal sobre lo sucedido.

30.4.8 ANÁLISIS DE VULNERABILIDADES

Además de las revisiones periódicas de logs, LLEIDANET PKI SUCURSAL DE PERÚ realiza de manera esporádica o ante actividades sospechosas la revisión de los mismos de conformidad con los procedimientos internos establecidos.

30.5 ARCHIVO DE REGISTROS

30.5.1 TIPOS DE EVENTOS ARCHIVADOS

Se mantiene un archivo de registros de los eventos más relevantes sobre las operaciones realizadas durante el proceso de emisión de los certificados digitales.

30.5.2 PERIODO DE CONSERVACIÓN

El periodo de conservación de este tipo de documentación es de 10 años.

30.5.3 PROTECCIÓN DE ARCHIVOS

Los archivos generados se conservan bajo custodia con estrictas medidas de seguridad para conservar su estado e integridad.

30.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Las copias de respaldo de los Archivos de registros se realizan según los procedimientos establecidos para copias de respaldo y recuperación de respaldo del resto de sistemas de información.

30.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los servidores se mantienen actualizados con la hora UTC Time (tiempo universal coordinado). Están sincronizados mediante el protocolo NTP (Network Time Protocol).

30.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

La información de auditoría tanto externa como interna es almacenada y custodiada en un sitio externo a las instalaciones de LLEIDANET PKI SUCURSAL DE PERÚ una vez haya sido digitalizada. Los archivos de auditoría digitalizados son accedidos únicamente por el personal autorizado mediante herramientas de visualización.

30.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.

Los archivos de registros son accedidos únicamente por el personal autorizado mediante herramientas de visualización y gestión de eventos con el propósito de verificar integridad de los mismos o para auditorias ante incidentes de seguridad.

30.6 CAMBIO DE CLAVES DE UNA EC

30.6.1 CAMBIO DE CLAVES DE LA RAÍZ

El procedimiento de cambio de claves de la Raíz es el equivalente a generar un nuevo certificado digital. Los certificados emitidos por las EC subordinadas con la clave anterior deben ser revocados o se debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el titular.

Antes de que el uso de la clave privada de la EC caduque se realizará un cambio de claves. La vieja EC y su clave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por las subordinadas de la EC vieja. Se generará una nueva EC con una clave privada nueva y un nuevo DN. La clave pública se publicará en el mismo repositorio con un nombre nuevo que la diferencia de la anterior.

30.6.2 CAMBIO DE CLAVES DE UNA EC SUBORDINADA

El procedimiento de cambio de claves de una EC subordinada es el equivalente a generar un nuevo certificado digital. Los certificados emitidos con la clave anterior de la subordinada deben ser revocados o se debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el titular.

Antes de que el uso de la clave privada de la EC subordinada caduque se realizará un cambio de claves. La vieja subordinada de EC y su clave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por la subordinada EC vieja. Se generará una nueva EC subordinada con una clave privada nueva y un nuevo DN. La clave pública se publicará en el mismo repositorio con un nombre nuevo que la diferencia de la anterior.

30.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

30.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

La Entidad de Certificación tiene establecido un Plan de Contingencia que establece las acciones a seguir en caso de producirse una vulnerabilidad o un incidente de seguridad. Una vez ejecutados de manera satisfactoria los procedimientos de restablecimiento de los sistemas, se dará servicio al público.

30.7.2 ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

Ante una sospecha de alteración de los recursos hardware, software, y/o datos se detendrá el funcionamiento de la EC hasta que se restablezca la seguridad del entorno. Para evitar que se repita el incidente se debe identificar la causa de la alteración. Ante una ocurrencia de este hecho LLEIDANET PKI SUCURSAL DE PERÚ informará al INDECOPI o dando explicación y justificación.

30.7.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ tiene establecido un Plan de Contingencia que define las acciones a seguir en caso de producirse una vulnerabilidad de la clave privada de la raíz de LLEIDANET PKI SUCURSAL DE PERÚ o de una de sus EC subordinadas. En estos casos se deben revocar de manera inmediata las claves privadas comprometidas de LLEIDANET PKI SUCURSAL DE PERÚ y los certificados firmados bajo su jerarquía. Se debe generar una nueva clave privada y a solicitud de los titulares se deben emitir nuevos certificados.

En caso de compromiso de la EC el proveedor de servicio de Certificación:

- Informará a todos los Titulares, Tercero que confía y otras EC's con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.
- LLEIDANET PKI SUCURSAL DE PERÚ informará al INDECOPI.

30.7.4 CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

LLEIDANET PKI SUCURSAL DE PERÚ ante un desastre natural u otro tipo de catástrofe, está en capacidad de recuperar los servicios más críticos del negocio, descritos en el documento Plan de Contingencia, dentro de las cuarenta y ocho (48) horas posteriores a la ocurrencia del evento. El restablecimiento de otros servicios como la emisión de certificados digitales se hará entre los cinco (5) días después de la ocurrencia del evento.

30.8 PREPARACIÓN ANTES DEL CESE DE EC Y ER

30.8.1 ENTIDAD DE CERTIFICACIÓN

LLEIDANET PKI SUCURSAL DE PERÚ informará a todos los titulares, con una anticipación de (30) días, sobre la terminación de su actividad o actividades, la fecha precisa de cesación y las consecuencias jurídicas de ésta respecto de los certificados expedidos. Si por causas de fuerza mayor el servicio es suspendido

temporalmente, LLEIDANET PKI SUCURSAL DE PERÚ informará al titular dentro de las veinticuatro (24) horas siguientes de ocurrido el incidente.

Los registros competentes de los certificados emitidos a los ciudadanos y empresas privadas serán mantenidos hasta ser cumplido el plazo de 10 años.

30.8.2 ENTIDAD DE REGISTRO O VERIFICACIÓN

En el caso de cese de actividades de la Entidad de Registro o Verificación, se debe informar con un (1) mes de anticipación tanto al INDECOPI como a los titulares, suscriptores y terceros que confían.

31 CONTROLES TÉCNICOS DE SEGURIDAD

31.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

31.1.1 GENERACIÓN DEL PAR DE CLAVES

31.1.1.1 GENERACIÓN DEL PAR DE CLAVES DE LA EC RAÍZ

La generación del par de claves de la EC Raíz, se realizó dentro de la sala criptográfica del proveedor de servicios de plataforma de la EC/ER con las más estrictas medidas de seguridad y bajo el protocolo de ceremonia de generación de claves establecido para este tipo de eventos y en presencia del representante legal de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ. Para el almacenamiento de la clave privada se utilizó un dispositivo criptográfico homologado FIPS 140-2 nivel 3 con control dual.

31.1.1.2 GENERACIÓN DEL PAR DE CLAVES DE LAS EC SUBORDINADAS DE LLEIDANET PKI SUCURSAL DE PERÚ

La generación del par de claves de las EC subordinadas de LLEIDANET PKI SUCURSAL DE PERÚ, se realiza dentro de la sala criptográfica del proveedor de servicios de LLEIDANET PKI SUCURSAL DE PERÚ bajo el protocolo de ceremonia de generación de claves. Para el almacenamiento de la clave privada subordinada se utiliza un dispositivo criptográfico homologado FIPS 140-2 nivel 3 con control dual.

31.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

La clave privada es generada por el titular en su dispositivo criptográfico y no es posible la extracción de la misma. No existe por tanto ninguna copia de clave privada del titular.

31.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública es enviada a la EC LLEIDANET PKI SUCURSAL DE PERÚ como parte de la petición de solicitud del certificado digital en formato PKIX-CMP.

31.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS ACEPTANTES

La clave pública de la EC Raíz y de la EC Subordinada está incluida en su certificado digital.

El certificado de la EC Raíz puede ser consultado por los terceros de confianza en la dirección http://certs.esigna.es/root/indenova_global_root_ca.crt

El certificado de la EC Subordinada puede ser consultado por los terceros de confianza en la dirección http://certs.esigna.es/ca/indenova_pki_001_pe.crt

31.1.5 TAMAÑO DE LAS CLAVES

El tamaño de las claves de la EC Raíz de LLEIDANET PKI SUCURSAL DE PERÚ es de 4096 bits.

El tamaño de las claves de las Subordinadas de LLEIDANET PKI SUCURSAL DE PERÚ es de 4096 bits.

El tamaño de las claves de los certificados emitidos por LLEIDANET PKI SUCURSAL DE PERÚ a usuarios finales es de 2048 bits.

Al intentar derivar la clave privada, a partir de la clave pública de 2048 bits contenida en los certificados de usuarios finales, el problema radica, en encontrar los factores primos de dos números grandes, ya que se tendrían 22047 posibilidades por cada número. En la actualidad resulta computacionalmente imposible factorizar estos números en un tiempo razonable. Se estima que descifrar una clave pública de 2048 bits requeriría un trabajo de procesamiento del orden de 3 x1020 MIPS-año*.

*MIPS-año: unidad utilizada para medir la capacidad de procesamiento de un computador funcionando durante un año. Equivale al número de millones de instrucciones que es capaz de procesar un computador por segundo durante un año.

31.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

La clave pública de la EC Raíz está codificada de acuerdo con el estándar RFC 5280 y PKCS#1. El algoritmo de firma utilizado en la generación de las claves es el RSA.

La clave pública de las subordinadas de LLEIDANET PKI SUCURSAL DE PERÚ está codificada de acuerdo con el estándar RFC 5280 y PKCS#1. El algoritmo de firma utilizado en la generación de las claves es el RSA.

La clave pública de los certificados de usuario final está codificada de acuerdo con el estándar RFC 5280 y PKCS#1. El algoritmo de firma utilizado en la generación de las claves es el RSA.

31.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

Los usos permitidos de la clave para cada tipo de certificado vienen establecidos por la Política de Certificación definida para cada tipo de certificado emitido por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ.

Todos los certificados digitales emitidos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ contienen la extensión 'Key Usage' definida por el estándar X.509 v3, la cual es calificada como crítica.

TIPO DE CERTIFICADO	KEY USAGE
Certificado de Firma	Digital Signature
Certificado de Autenticación	Non Repudiation

31.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

31.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos utilizados en la creación de claves utilizadas por EC Raíz de Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

31.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

Las claves privadas, de LLEIDANET PKI SUCURSAL DE PERÚ Raíz y las claves privadas de las subordinadas de, se encuentran bajo control multipersona. El método de activación de las claves privadas es mediante la inicialización del software de LLEIDANET PKI SUCURSAL DE PERÚ por medio de una combinación de claves en poder de varios operadores.

31.2.3 CUSTODIA DE LA CLAVE PRIVADA

Las claves privadas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

La clave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del titular. Bajo ninguna circunstancia LLEIDANET PKI SUCURSAL DE PERÚ guarda copia de la clave privada

del titular ya que esta es generada por el mismo titular y no es posible tener acceso a ella por LLEIDANET PKI SUCURSAL DE PERÚ.

31.2.4 BACKUP DE LA CLAVE PRIVADA

Las claves privadas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver Custodia de la clave privada).

Las copias de backup de las claves privadas de LLEIDANET PKI SUCURSAL DE PERÚ, están almacenadas en dispositivos externos protegidas criptográficamente por un control dual y solo son recuperables dentro de un dispositivo igual al que se generaron.

31.2.5 ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver Custodia de la clave privada).

El archivo de las copias de backup de las claves privadas está archivado en la caja de seguridad de un centro externo.

No deberán ser archivadas las claves privadas empleadas para la firma y autenticación de los usuarios finales, ni de los archivos electrónicos que los contengan (por ejemplo, los archivos con extensión PFX).

31.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA A/DESDE EL MÓDULO CRIPTOGRÁFICO

Las claves privadas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (Ver Custodia de la clave privada).

El proceso de descarga de las claves privadas se realiza según procedimiento del dispositivo criptográfico y se almacenan de forma segura protegidas por claves criptográficas con control dual.

31.2.7 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ son generadas y almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (Ver Custodia de la clave privada).

Las claves criptográficas pueden cargarse en un dispositivo criptográfico de igual prestación a partir de las copias de backup mediante un proceso que exige la participación de al menos dos operadores.

31.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves privadas, de LLEIDANET PKI SUCURSAL DE PERÚ Raíz y de las EC Subordinadas, se encuentran bajo control multipersona. El método de activación de la clave privada es mediante la inicialización del software de LLEIDANET PKI SUCURSAL DE PERÚ por medio de una combinación de claves en poder de varios operadores.

Se requiere un control multi-persona para la activación de la clave privada de la EC. Se necesitan al menos 2 de 4 personas para la activación de las claves.

31.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La desactivación de la clave privada se realiza mediante desactivación del software y/o el apagado del servidor EC. Se activa nuevamente mediante el uso de control multipersona, siguiendo los procedimientos marcados por el fabricante del módulo criptográfico.

31.2.10 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

El método utilizado en caso de requerirse la destrucción de la clave privada es mediante el borrado de las claves almacenadas en los dispositivos criptográficos tal y como se describe en el manual del fabricante del dispositivo y la destrucción física de las tarjetas de acceso en poder de los operadores.

31.2.11 EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO

El dispositivo criptográfico es monitoreado mediante el software propio del mismo para prever posibles fallas.

31.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

31.3.1 ARCHIVO DE LA CLAVE PÚBLICA

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ mantendrá controles para el archivo de su propia clave pública.

31.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

El periodo de uso del par de claves está determinado por la vigencia del certificado.

El periodo de validez del certificado digital y el par de claves de EC Raíz de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ es de treinta (30) años.

El periodo de validez del certificado digital y el par de claves de las EC Subordinadas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ es de veinticinco (25) años.

31.4 DATOS DE ACTIVACIÓN

31.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para el funcionamiento de la Entidad de Certificación se crean tarjetas criptográficas para los operadores del dispositivo criptográfico y que servirán junto con un PIN para la activación de las claves privadas.

Los datos de activación de la clave privada se encuentran divididos en tarjetas criptográficas custodiadas por un sistema multipersona donde 4 personas comparten el código de acceso de dichas tarjetas.

31.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

El conocimiento de los datos de activación es personal e intransferible. Cada uno de los intervinientes es responsable por su custodia y debe manejarlo como información confidencial.

31.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

La clave de activación es confidencial, personal e intransferible y por tanto se deben tener en cuenta las normas de seguridad para su custodia y uso.

31.5 CONTROLES DE SEGURIDAD INFORMÁTICA

La EC emplea sistemas fiables para ofrecer sus servicios de certificación. La EC ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se sigue el esquema ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de r y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

31.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

LLEIDANET PKI SUCURSAL DE PERÚ cuenta con una infraestructura tecnológica debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar una alta disponibilidad y confianza en los servicios ofrecidos a sus titulares y terceros de confianza.

La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes acreditados que requieran de su conocimiento.

31.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

El sistema de gestión de la seguridad de la Información evalúa los procesos relacionados con la infraestructura tecnológica con el fin de identificar posibles debilidades y definir los planes de mejoramiento continuo con el apoyo de las auditorias permanentes y periódicas.

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

Este análisis se realiza de forma continua de forma que se localicen nuevas vulnerabilidades de los sistemas.

31.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

31.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ cumple con los procedimientos de control de cambios establecidos para los nuevos desarrollos y actualizaciones de software.

31.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ mantiene un control sobre los inventarios de los activos utilizados en su proceso de certificación. Existe una clasificación de los mismos de conformidad con su nivel de riesgo.

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ monitorea de manera periódica su capacidad técnica con el fin de garantizar una infraestructura de alta disponibilidad.

31.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

LLEIDANET PKI SUCURSAL DE PERÚ cuenta con los debidos controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan algún impacto en la seguridad de los certificados digitales emitidos.

31.7 CONTROLES DE SEGURIDAD DE LA RED

LLEIDANET PKI SUCURSAL DE PERÚ cuenta con una infraestructura de red debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar una alta disponibilidad y confianza en los servicios ofrecidos a sus titulares y Terceros que confían.

La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes acreditados que requieran de su conocimiento.

31.8 SELLADO DE TIEMPO

Los servidores se mantienen actualizados con la hora UTC. Están sincronizados mediante el protocolo NTP (Network Time Protocol).

32 PERFILES DE CERTIFICADOS, CRL Y OCSP

32.1 PERFIL DE CERTIFICADO

Los certificados cumplen con el estándar X.509 versión 3 y para la infraestructura de autenticación se basa en el RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Contenido de los certificados. Un certificado emitido por LLEIDANET PKI SUCURSAL DE PERÚ, además de estar firmado digitalmente por ésta, contendrá como mínimo lo siguiente:

1. Nombre, dirección y domicilio del titular.
2. Identificación del titular nombrado en el certificado.
3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
4. La clave pública del usuario.
5. La metodología para verificar la firma digital del titular, impuesta en el mensaje de datos.
6. El número de serie del certificado.
7. Fecha de emisión y expiración del certificado.

<u>Para el caso de personas naturales</u>

La identificación del titular implica el número de documento de identidad y el tipo de documento.

<u>Para el caso de personas jurídicas</u>

El nombre y la identificación del titular implica lo siguiente:

Razón social:

- Número del Registro Único de Contribuyentes (RUC)

- Nombres Completos del suscriptor
- Número de documento oficial de identidad del suscriptor
- Tipo de documento del suscriptor

Descripción del contenido de los certificados

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por LLEIDANET PKI SUCURSAL DE PERÚ
Algoritmo de Firma	SHA1RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para LLEIDANET PKI SUCURSAL DE PERÚ como emisor se especifica: C = PE L = LIMA STREET = http://www.indenova.com OU = Internet Certification Authority http://www.indenova.com T = Subordinate Certificate Perú O = inDenova Sucursal del Perú E = sub_ca_pe@indenova.com SERIALNUMBER = 20549615709 CN = inDenova SUB001_PE Description = inDenova Subordinate Certificate 001 Perú HW-KUSU
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido. Se encuentra sincronizado con el servicio de tiempo UTC-5.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Se encuentra sincronizado con el servicio de tiempo UTC-5.
Sujeto	Ver sección "Reglas para la interpretación de varias formas de nombre".
Clave pública del Sujeto	Codificado de acuerdo con el RFC 5280. La longitud mínima de la clave es de 1024 bits y algoritmo RSA. Los certificados emitidos por LLEIDANET PKI SUCURSAL DE PERÚ tienen una longitud de 2048 bits y algoritmo RSA.

Identificador de clave de la autoridad	Es utilizado para identificar el certificado raíz en la jerarquía de certificación. Normalmente referencia el campo "Subject Key Identifier" de LLEIDANET PKI SUCURSAL DE PERÚ como entidad emisora de certificación digital.
Identificador de la clave del sujeto	Es usado para identificar un certificado que contiene una determinada clave pública.
Política de certificado	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible las políticas de certificación.
Uso de la clave	Especifica los usos permitidos de la clave. Es un CAMPO CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de LLEIDANET PKI SUCURSAL DE PERÚ. En el certificado de la EC Raíz, este atributo no se especifica.
Acceso a la información de la Autoridad	Es usado para indicar las direcciones donde se encuentra el certificado raíz de LLEIDANET PKI SUCURSAL DE PERÚ. Además, para indicar la dirección para acceder al servicio de OCSP. En el certificado raíz de LLEIDANET PKI SUCURSAL DE PERÚ, este atributo no se especifica.
Usos extendidos de la clave	Se especifican otros propósitos adicionales al uso de la clave.
Restricciones básicas	La extensión "PathLenConstraint" indica el número de sub-niveles que se admiten en la ruta del certificado. No existe restricción para LLEIDANET PKI SUCURSAL DE PERÚ por tanto, es cero.

32.1.1 NÚMERO DE VERSIÓN

Los certificados emitidos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ cumplen con el estándar X.509 Versión 3.

32.1.2 EXTENSIONES DEL CERTIFICADO

En el Anexo 2 de esta CPS se describe de forma detallada los certificados emitidos bajo esta CPS

32.1.3 KEY USAGE

El "key usage" es una extensión crítica que indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

32.1.4 EXTENSIÓN DE POLÍTICA DE CERTIFICADOS

La extensión de "certificatepolicies" del X.509 versión 3 es el identificador del objeto de esta CPS de acuerdo con la sección Identificador de objeto de la Política de Certificación de esta CPS. La extensión no es considerada como crítica.

32.1.5 NOMBRE ALTERNATIVO DEL SUJETO

La extensión "sujectAltName" es opcional y el uso de esta extensión es "NO crítico".

32.1.6 RESTRICCIONES BÁSICAS

Para el caso de LLEIDANET PKI SUCURSAL DE PERÚ en el campo "PathLenghtConstraint" de certificado de las subordinadas tiene un valor de 0, para indicar que LLEIDANET PKI SUCURSAL DE PERÚ no permite más sub-niveles en la ruta del certificado. Es un campo crítico.

32.1.7 USO EXTENDIDO DE LA CLAVE

Esta extensión permite definir otros propósitos adicionales de la clave. Es considerada No crítica. Los propósitos más comunes son:

OID	Descripción	Tipos de Certificados
1.3.6.1.5.5.7.3.1	Autenticación de Servidor	Autenticación Agente Electrónico
1.3.6.1.5.5.7.3.2	Autenticación del Cliente	Autenticación persona Natural. Firma digital. Agente electrónico.
1.3.6.1.5.5.7.3.4	Protección de correo.	Firma Digital de persona natural y Agente Electrónico
1.3.6.1.5.5.7.3.8	Sellado de tiempo	Sellado de tiempo
1.3.6.1.4.1.311.20.2.2	Smart Card Logon	Autenticación Persona Natural.

32.1.8 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

El identificador de objeto del algoritmo de firma es

1.2.840.113549.1.1.5 SHA-1 with RSA Encryption

El identificador de objeto del algoritmo de la clave pública es

1.2.840.113549.1.1.1 rsaEncryption

32.1.9 FORMATOS DE NOMBRES

De conformidad con lo especificado en el numeral Tipos de nombres de esta CPS.

32.1.10 RESTRICCIONES DE LOS NOMBRES

Los nombres se deben escribir en mayúsculas y sin tildes, la letra Ñ solo se permite para los nombres de personas naturales o jurídicas.

El código del país se asigna de acuerdo al estándar ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países". Para el caso de Perú es "PE".

32.1.11 IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN

El identificador de objeto de la Política de certificado correspondiente a cada tipo de certificado, conforme se establece en las Políticas de Certificación de los certificados LLEIDANET PKI SUCURSAL DE PERÚ, cualquier cambio será comunicado al INDECOPI.

32.1.12 USO DE LA EXTENSIÓN POLICY CONSTRAINS

No se estipula.

32.1.13 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

El calificador de la política está definido en la extensión de "Certificate Policies" y contiene una referencia al URL donde esta publicada la CPS del proveedor de servicios de certificación.

32.1.14 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES

No se estipula.

32.2 PERFIL DE CRL

Las CRL´s emitidas por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ cumplen con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" y contienen los siguientes elementos básicos:

32.2.1 NÚMERO DE VERSIÓN

Las CRL´s emitidas por LLEIDANET PKI SUCURSAL DE PERÚ cumplen con el estándar X.509 versión 2.

32.2.2 CRL Y EXTENSIONES CRL

La información sobre el motivo de la revocación de un certificado estará incluida en la CRL, utilizando las extensiones de la CRL y más específicamente en el campo de motivos de revocación (reasonCode).

32.3 PERFIL OCSP

El servicio OCSP cumple con lo estipulado en el RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

32.3.1 NÚMERO DE VERSIÓN

Cumple con la OCSP Versión 1 del RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

32.3.2 EXTENSIONES OCSP

No aplica.

33 AUDITORIA DE CONFORMIDAD Y OTROS CONTROLES

33.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

La infraestructura y procedimientos de LLEIDANET PKI SUCURSAL DE PERÚ será evaluado al menos anualmente por el INDECOPI, en el marco de los requerimientos de la Guía de Acreditación de Entidades de Certificación.

33.2 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

LLEIDANET PKI SUCURSAL DE PERÚ, somete su infraestructura y sistemas de gestión a evaluadores autorizados por el INDECOPI.

33.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

La única relación establecida entre el Auditor y la Entidad auditada es la de Auditor y Auditado. La firma de Auditoría ejerce su absoluta independencia en el cumplimiento de sus actividades de auditoria y no existe conflicto de intereses pues la relación es netamente de tipo contractual.

33.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

Los elementos cubiertos por la auditoría son la implementación de las prácticas de certificación, personal, procedimientos y técnicas, descritos en el anexo 2 de la presente Guía de Acreditación.

33.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

Las deficiencias detectadas durante el proceso de Auditoria deben ser subsanadas a través de un Plan de Mejoramiento que contenga las acciones, procedimientos o implementación de los controles requeridos para minimizar riesgos.

33.6 COMUNICACIÓN DE RESULTADOS

Una vez terminada la Auditoria, la firma Auditora debe presentar el Informe de Auditoria a LLEIDANET PKI SUCURSAL DE PERÚ y si se requiere LLEIDANET PKI SUCURSAL DE PERÚ debe establecer un Plan de Mejoramiento.

34 OTROS ASUNTOS LEGALES Y COMERCIALES

34.1 TARIFAS

34.1.1 TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

Las tarifas serán definidas por LLEIDANET PKI SUCURSAL DE PERÚ de acuerdo a los contratos celebrados con sus clientes.

34.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a la consulta del estado de los certificados emitidos es libre y gratuito y por tanto no aplica una tarifa.

34.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

La solicitud de revocación de un certificado no tiene costo. El acceso a la información de estado de los certificados emitidos, es libre y gratuito y por tanto no aplica una tarifa.

34.1.4 TARIFAS DE OTROS SERVICIOS

Una vez se ofrezcan otros servicios por parte de LLEIDANET PKI SUCURSAL DE PERÚ, se publicarán en la dirección http://www.lleida.net

34.1.5 POLÍTICA DE REEMBOLSO

Una vez solicitado un certificado, esta solicitud se convierte en un contrato de prestación de servicios y no está sujeto a reembolso alguno.

34.2 RESPONSABILIDAD

La EC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente en Perú.

La EC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los Firmante/Titulares y de los terceros que confíen en los certificados.

Las responsabilidades de la EC incluyen las establecidas por la presente CPS, así como las que resulten de aplicación como consecuencia de la normativa peruana e internacional.

La EC será responsable del daño causado ante el Titular o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Titular, la clave privada correspondiente a la clave pública dada o identificada en el certificado.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

34.3 EXONERACIÓN DE RESPONSABILIDAD

La EC no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.

- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente CPS y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Entidad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Titular o Terceros que confían en la normativa vigente, la presente CPS y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Titular.
- Fraude en la documentación presentada por el solicitante.

34.4 RESPONSABILIDADES FINANCIERAS

34.4.1 COBERTURA DEL SEGURO

El seguro cubre todos los perjuicios contractuales y extracontractuales de los titulares clientes de LLEIDANET PKI SUCURSAL DE PERÚ, que confían exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ en el desarrollo de las actividades para las cuales cuenta con autorización.

34.4.2 PROVISIONES Y GARANTÍAS

Las garantías por los servicios de registro y certificación digital serán definidas en los contratos de titulares, en relación con errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

34.4.3 EXCEPCIONES DE GARANTÍAS

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ no se responsabiliza en casos de compromiso de la clave en manos del suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento así como en la Declaración de Prácticas de la ER.

34.4.4 INDEMNIZACIÓN

Los casos de indemnización son definidos en los contratos de los titulares.

34.4.5 OTROS BIENES

LLEIDANET PKI SUCURSAL DE PERÚ cuenta con la capacidad económica y financiera suficiente para prestar los servicios autorizados y responder por sus deberes como entidad de certificación. LLEIDANET PKI SUCURSAL DE PERÚ como prestador de servicios de certificación responderá por los perjuicios que se causen a los titulares o Terceros que confían derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ en el desarrollo de las actividades para las cuales cuenta con autorización y para ello cuenta con un seguro de responsabilidad civil de conformidad con el del Artículo 8°. Garantías, del Decreto 1747 del 2000. LLEIDANET PKI SUCURSAL DE PERÚ no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente CPS.

34.4.6 SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ ha adquirido un seguro expedido por una entidad aseguradora autorizada para operar en Perú, que cubre todos los perjuicios contractuales y extracontractuales de los titulares y Terceros que confían exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ en el desarrollo de las actividades para las cuales cuenta con autorización.

Actualización anual de información de estados financieros y garantías: La entidad de certificación abierta deberá remitir a esta Superintendencia los estados financieros de fin de ejercicio certificados y dictaminados, copia de las garantías y el informe de auditoría contemplado en el numeral 8.2.1 literal c) de este capítulo, dentro de los primeros quince (15) días del mes de abril de cada año calendario.

34.5 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

34.5.1 ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

Toda información no pública es considerada confidencial y por tanto de acceso restringida:

- Confidencialidad de la clave privada de la Entidad de Certificación.
- Confidencialidad de la clave privada del titular.
- Confidencialidad de la información suministrada por el titular.
- Registros de las transacciones
- Registros de pistas de Auditoría
- Políticas de seguridad
- Plan de Contingencia.
- Planes de continuidad del negocio.

34.5.2 INFORMACIÓN NO CONFIDENCIAL

Toda información no confidencial es considerada pública y por tanto de libre acceso para terceros:

- La contenida en la presente Declaración de Prácticas de Certificación.
- La contenida en el repositorio sobre el estado de los certificados.
- La lista de certificados revocados.

34.5.3 DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

LLEIDANET PKI SUCURSAL DE PERÚ mantiene medidas de seguridad para proteger toda la información confidencial suministrada a ella directamente o a través de los canales establecidos para ello desde su recibo hasta su almacenamiento y custodia en el archivo central donde reposarán por 10 años de conformidad con la normatividad vigente peruana. LLEIDANET PKI SUCURSAL DE PERÚ cuenta con un procedimiento de Seguridad para el manejo y custodia de la información. En él se destaca que una vez recibida la información suministrada por el solicitante o titular, con ésta se arma una carpeta identificada con el nombre, número de identificación y se le asigna un número de radicación. Estos datos son relacionados y registrados para su control y seguimiento. Esta carpeta es asignada al Aprobador, quien siempre la mantiene bajo clave. Una vez verificados los datos y su autenticidad por parte de la Entidad de Registro o Verificación, la carpeta es entrega al Archivo de Gestión que se encargará de almacenarlos bajo clave antes de ser enviados al archivo central junto con la relación de los documentos entregados. El archivo central cuenta con controles ambientales, lógicos y físicos para custodia y conservación de este tipo de documentos. LLEIDANET PKI SUCURSAL DE PERÚ tiene definidos los cargos y perfiles que tendrán acceso a dicha información y la oficina de la Entidad de Registro o Verificación cuenta con puerta de seguridad y sistema de Alarma y monitoreo 7X24 horas durante todo el año. El acceso a la información una vez archivada debe estar soportado por un requerimiento autorizado por la Gerencia de LLEIDANET PKI SUCURSAL DE PERÚ. Esto nos permite asegurar que la información de nuestros titulares no será comprometida, ni divulgada a terceras personas salvo que medie solicitud formal de una Autoridad competente que así la requiera.

Las personas que por razón de su trabajo tengan acceso a información confidencial deben tener conocimiento de las políticas de seguridad y deben firmar un Acuerdo de Confidencialidad. Así mismo, el personal contratado directamente o indirectamente y que participe en actividades que por sus funciones requieran el conocimiento de información confidencial debe firmar el Acuerdo de Confidencialidad.

34.6 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

34.6.1 POLÍTICA DE PRIVACIDAD

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ tiene como política de privacidad lo establecido en el derecho de habeas data: “La información privada, será aquella que por versar sobre información personal o no, y que por encontrase en un ámbito privado, solo puede ser obtenida u ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.”

34.6.2 INFORMACIÓN TRATADA COMO PRIVADA

La información personal suministrada por el titular y que es requerida para la aprobación del certificado digital es considerada información de carácter privado.

34.6.3 INFORMACIÓN NO CALIFICADA COMO PRIVADA

La información personal suministrada por el titular y que es contenida en el certificado digital no es considerada información de carácter privado.

34.6.4 RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ es responsable y cuenta con los adecuados mecanismos de seguridad y control para garantizar la protección, confidencialidad y debido uso de la información suministrada por el titular.

34.6.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL

Los datos de carácter personal no podrán ser comunicados a terceros, sin la debida notificación y consentimiento de su dueño.

34.6.6 REVELACIÓN EN EL MARCO DE UN PROCESO ADMINISTRATIVO O JUDICIAL

Los datos de carácter personal podrán ser comunicados cuando se requieran por parte de una autoridad competente en el marco de un proceso administrativo o judicial sin la debida notificación y consentimiento de su dueño, de conformidad con la legislación peruana.

34.6.7 OTRAS CIRCUNSTANCIAS DE REVELACIÓN DE INFORMACIÓN

La Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ tiene como política de privacidad a lo estrictamente establecido en el derecho de habeas data: “La información privada, será aquella que por versar sobre información personal o no, y que por encontrase en un ámbito privado, solo puede ser obtenida u ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.”

34.6.8 NOTIFICACIONES Y COMUNICACIONES INDIVIDUALES DE LOS PARTICIPANTES

Para cualquier comunicación con la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ se utilizará el correo electrónico: consultas@indenova.com.

En el caso de ser necesario los medios de notificación individual con los participantes serán definidos en los contratos de titulares y suscriptores.

34.7 DERECHOS DE PROPIEDAD INTELECTUAL

Se prohíbe la reproducción, divulgación, comunicación pública y transformación de cualquiera de los elementos contenidos en la presente CPS, que son propiedad exclusiva de LLEIDANET PKI SUCURSAL DE PERÚ, sin su autorización expresa.

34.8 OBLIGACIONES

34.8.1 OBLIGACIONES DE LA EC

LLEIDANET PKI SUCURSAL DE PERÚ está obligada según normativa vigente y en lo dispuesto en las Políticas de Certificación y en esta CPS a:

1. Respetar lo dispuesto en la normatividad vigente, en esta CPS y en las Políticas de Certificación PC.
2. Publicar esta CPS y cada una de las Políticas de Certificación en la página Web de LLEIDANET PKI SUCURSAL DE PERÚ.
3. Informar al INDECOPI sobre las modificaciones de la CPS y de las Políticas de Certificación.
4. Mantener publicada en la página Web la última versión de la CPS y las Políticas de Certificación de LLEIDANET PKI SUCURSAL DE PERÚ
5. Proteger y custodiar de manera segura y responsable su clave privada.
6. Emitir certificados conforme a las Políticas de Certificación y a los estándares definidos en la presente CPS.
7. Generar certificados consistentes con la información suministrada por el solicitante o titular.
8. Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.
9. Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
10. Publicar el estado de los certificados emitidos en un repositorio de acceso libre.
11. No mantener copia de la clave privada del solicitante o titular.
12. Revocar los certificados según lo dispuesto en la Política de revocación de certificados digitales.
13. Actualizar y publicar la lista de certificados revocados CRL con los últimos certificados revocados.
14. Notificar al Solicitante o Titular la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con la política de revocación de certificados digitales.

34.8.2 OBLIGACIONES DE LA ER

Las ER son las entidades delegadas por la EC para realizar la labor de identificación y registro, por lo tanto, la ER está obligada en los términos definidos en esta Declaración de Prácticas de Certificación a:

1. Conocer y dar cumplimiento a lo dispuesto en la presente CPS y en la Política de Certificación correspondiente a cada tipo de certificado.

2. Custodiar y proteger su clave privada.
3. Comprobar la identidad de los Solicitantes y Titulares de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
5. Archivar y custodiar la documentación suministrada por el solicitante o titular, durante el tiempo establecido por la legislación vigente.
6. Respetar lo dispuesto en los contratos firmados entre LLEIDANET PKI SUCURSAL DE PERÚ y el titular.
7. Identificar e informar a la EC las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

34.8.3 OBLIGACIONES DEL TITULAR

El Titular como titular de un certificado digital está obligado a cumplir con lo dispuesto por la normativa vigente y lo dispuesto en la presente CPS como es:

1. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados digitales para facilitar su oportuna y plena identificación.
2. Cumplir con lo aceptado y firmado en el Formulario de Solicitud de certificado digital.
3. Proporcionar con exactitud y veracidad la información requerida.
4. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
5. Custodiar y proteger de manera responsable su clave privada.
6. Dar uso al certificado de conformidad con las Políticas de Certificación establecidos en la presente CPS para cada uno de los tipos de certificado.
7. Solicitar como titular de manera inmediata la revocación de su certificado digital cuando tenga conocimiento que existe una causal definida en numeral Circunstancias para la revocación de un certificado de la presente CPS.
8. No hacer uso de la clave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
9. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
10. Informar al Tercero que confía para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera de periódica por LLEIDANET PKI SUCURSAL DE PERÚ.

34.8.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los Terceros que confían en su calidad de parte que confía en los certificados digitales emitidos por la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ está en la obligación de:

1. Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
2. Conocer lo dispuesto en la Declaración de Prácticas de Certificación.
3. Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
4. Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
5. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.

34.8.5 OBLIGACIONES DE LA ENTIDAD

Conforme lo establecido en las Políticas de Certificación anexadas a este documento, en el caso de los certificados donde se acredite la vinculación del Titular con la misma será obligación de la Entidad solicitar a la ER la suspensión/revocación del certificado cuando cese o se modifique dicha vinculación.

34.8.6 OBLIGACIONES DE OTROS PARTICIPANTES

El Comité de Seguridad como organismo interno de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ está en la obligación de:

1. Revisar la consistencia de CPS con la normatividad vigente.
2. Autorizar los cambios o modificaciones requeridas sobre la CPS.
3. Autorizar la publicación de la CPS en la página Web de LLEIDANET PKI SUCURSAL DE PERÚ.
4. Integrar la CPS, a la CPS de terceros proveedores de servicios de certificación.
5. Aprobar los cambios o modificaciones a las Políticas de Seguridad de LLEIDANET PKI SUCURSAL DE PERÚ.
6. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ.
7. Asegurar la existencia de controles sobre la infraestructura tecnológica de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ.
8. Solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la clave privada del subscriptor o cualquier otro hecho que tienda al uso indebido de clave privada del titular o de la Entidad de Certificación
9. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.

34.9 ENMENDADURAS Y CAMBIOS

Las enmendaduras y cambios serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

34.10 RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas será definido en los contratos de los titulares.

34.11 CONFORMIDAD

Puesto que el documento Declaración de Prácticas de la Entidad de Certificación es un documento normativo, que implica una obligación frente a los clientes de la EC, este documento debe ser adecuadamente gestionado a fin de mantener su autenticidad, vigencia, actualización y publicación.

35 VIGENCIA Y CONCLUSIÓN

35.1 VIGENCIA

Este documento de Declaración de Prácticas y Política de Certificación y cualquier enmienda a este entrarán en vigencia tras su publicación en la web de LLEIDANET PKI SUCURSAL DE PERÚ y permanecerán vigentes hasta que sea reemplazado por una versión más nueva.

35.2 TERMINACIÓN

Este documento de Declaración de Prácticas y Política de Certificación y cualquier enmienda permanecerán en vigor hasta que se modifique o reemplace por una versión más nueva.

35.3 EFECTO DE LA TERMINACIÓN Y LA SUPERVIVENCIA

Al finalizar esta Declaración de Prácticas y Política de Certificación, los participantes de LLEIDANET PKI SUCURSAL DE PERÚ están sujetos a sus términos para todos los certificados emitidos por el resto de los períodos de validez de dichos certificados. Como mínimo, todas las responsabilidades relacionadas con la protección de la información confidencial sobrevivirán a la terminación.

36 PROVISIONES MISCELÁNEAS

36.1 ACUERDO COMPLETO

Sin estipulación.

36.2 ASIGNACIÓN

Las CA emisoras, los suscriptores, las partes confiantes, las Entidades de registro o cualquier otra entidad que opere bajo esta Declaración de Prácticas y Política de Certificación no tienen derecho a asignar ninguno de sus derechos u obligaciones bajo esta Declaración de Prácticas y Política de Certificación sin el consentimiento previo por escrito de LLEIDANET PKI SUCURSAL DE PERÚ.

36.3 DIVISIBILIDAD

Si alguna de las disposiciones de esta Declaración de Prácticas y Política de Certificación se considera inválida por una autoridad competente en la jurisdicción aplicable, el resto de la Declaración de Prácticas y Política de Certificación seguirá siendo válido y exigible.

36.4 FUERZA MAYOR

LLEIDANET PKI SUCURSAL DE PERÚ no acepta ninguna responsabilidad por cualquier retraso o incumplimiento de una obligación en virtud de su Declaración de Prácticas y Política de Certificación en la medida en que dicho retraso o incumplimiento sea causado por eventos que escapen a su control razonable.

37 OTRAS PROVISIONES

Sin estipulación.

38 CONFORMIDAD CON LA LEY APLICABLE

LLEIDANET PKI SUCURSAL DE PERÚ es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales -Ley27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

39 BIBLIOGRAFÍA

a) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
b) Ley de Firmas y Certificados Digitales –Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012