Proyecto	**Entidad de Registro o Verificación**
Título	**Declaración de Prácticas y Política de Registro de Lleidanet PKI Sucursal de Perú**

Realizado por	**LLEIDANET PKI SUCURSAL DE PERÚ**		
Dirigido a	**INDECOPI**		
Documento	**DOC-160912.1691208**		
Fecha aprobación	**09/06/2025**	Revisión	**10**

Firmado por: Raul Gisbert Rodas
Fecha firma: 26/06/2025 8:43:46 CEST

Firmado por: EVA PANE VIDAL
Fecha firma: 26/06/2025 9:54:16 CEST

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

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 26/06/2025 9:44:24 CEST

Av. Pascual 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 5
2 HISTORIA DEL DOCUMENTO 5
3 ELABORACIÓN, REVISIÓN Y APROBACIÓN 6
4 INTRODUCCIÓN 7
5 VISIÓN GENERAL 7
6 OBJETIVO 7
7 DEFINICIONES Y ABREVIACIONES 8
7.1 PKI PARTICIPANTES 8
8 ENTIDAD DE CERTIFICACIÓN ASOCIADA A ER DE LLEIDANET PKI SUCURSAL DE PERÚ 10
9 USO DEL CERTIFICADO 11
9.1 USOS ADECUADOS DEL CERTIFICADO 11
9.2 USOS PROHIBIDOS DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD 11
10 PERSONA DE CONTACTO 11
11 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES 12
12 RESPONSABILIDADES DE LOS TERCEROS QUE CONFÍAN 12
13 RESPONSABILIDADES DE LOS TERCEROS CONTRATISTAS 13
14 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS RPS 13
15 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS 14
15.1 PROTECCIÓN DE INTEGRIDAD DEL DOCUMENTO 14
16 IDENTIFICACIÓN Y AUTENTICACIÓN 14
16.1 NOMBRES 14
17 CERTIFICADOS DIGITALES 17
18 CERTIFICADOS DIGITALES DE PERSONA NATURAL 17
18.1 SERVICIOS BRINDADOS 17
18.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD 18
18.3 MODALIDADES DE ATENCIÓN 18
18.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADO 18
18.5 REGISTRO DE DOCUMENTOS 22
18.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS 23

19 CERTIFICADOS DIGITALES DE PERSONA JURÍDICA REPRESENTANTE LEGAL O PERTENECIENTE A EMPRESA 23

19.1 SERVICIOS BRINDADOS 23
19.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD 23
19.3 MODALIDADES DE ATENCIÓN 24
19.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADO 24
19.5 REGISTRO DE DOCUMENTOS 29
19.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS 30

20 CERTIFICADOS DIGITALES DE AGENTE AUTOMATIZADO 30

20.1 SERVICIOS BRINDADOS 30
20.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD 31
20.3 MODALIDADES DE ATENCIÓN 31
20.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADO 31
20.5 REGISTRO DE DOCUMENTOS 35
20.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS 36

21 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES 36

21.1 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA NATURAL 36
21.2 SOLICITUD DE RE-EMISIÓN CERTIFICADOS DE PERSONA JURÍDICA 38
21.3 PROCESAMIENTO DE LA SOLICITUD DE RE-EMISIÓN 40

22 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS 41

22.1 CIRCUNSTANCIAS PARA REALIZAR LA SOLICITUD 41
22.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS 42
22.3 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN 44

23 GESTIÓN DE LA SEGURIDAD 46

24 GESTIÓN DE OPERACIONES 46

24.1 MÓDULO CRIPTOGRÁFICO 46
24.2 RESTRICCIONES DE LA GENERACIÓN DE CLAVES 46
24.3 ENTREGA DE LA CLAVE PÚBLICA 46
24.4 DEPÓSITO DE CLAVE PRIVADA 47
24.5 DATOS DE ACTIVACIÓN 47

25 CONTROLES DE SEGURIDAD COMPUTACIONAL 47

26 PROTECCIÓN DE REGISTROS 47

26.1 TIPOS DE EVENTOS REGISTROS 47
26.2 PROTECCIÓN DE LOS REGISTROS 48
26.3 ARCHIVO DE LOS REGISTROS 48
26.4 TIEMPO DE ALMACENAMIENTO DEL ARCHIVO 48

27 SEGURIDAD EN LAS COMUNICACIONES CON LA EC 48
27.1 USO DE CANALES SEGUROS 48
27.2 AUTENTICACIÓN DE OPERADORES DE REGISTRO 49
27.3 REGISTROS DE AUDITORÍA 49
28 AUDITORÍAS 49
28.1 FRECUENCIAS DE AUDITORÍAS 49
28.2 CALIFICACIONES DE LOS AUDITORES 49
28.3 RELACIÓN DEL AUDITOR CON LA ER 49
29 ASPECTOS LEGALES DE LA OPERACIÓN DE LA ER 50
29.1 PREPARACIÓN Y PERSONALIZACIÓN 50
29.2 ALMACENAMIENTO Y DISTRIBUCIÓN DEL MÓDULO CRIPTOGRÁFICO 50
29.3 USO DEL MÓDULO CRIPTOGRÁFICO 50
29.4 DESACTIVACIÓN Y REACTIVACIÓN 51
29.5 REEMPLAZO DEL MÓDULO CRIPTOGRÁFICO 51
29.6 TERMINACIÓN DEL MÓDULO CRIPTOGRÁFICO 51
30 MATERIAS DE NEGOCIO Y LEGALES 52
30.1 TARIFAS 52
30.2 POLÍTICAS DE REEMBOLSO 52
30.3 COBERTURA DE SEGURO 52
30.4 PROVISIONES Y GARANTÍAS 52
30.5 EXCEPCIONES DE GARANTÍAS 52
30.6 OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES 52
30.7 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN 53
30.8 INDEMNIZACIÓN 53
30.9 NOTIFICACIONES 53
30.10 ENMENDADURAS Y CAMBIOS 53
30.11 RESOLUCIÓN DE DISPUTAS 53
30.12 CONFORMIDAD CON LA LEY APLICABLE 53
30.13 SUBROGACIÓN 53
30.14 FUERZA MAYOR 54
30.15 DERECHOS DE PROPIEDAD INTELECTUAL 54
30.16 APERTURA NUEVAS ER DE LLEIDANET PKI SUCURSAL DE PERÚ 54
30.17 TERCERIZACIÓN 54
31 FINALIZACIÓN DE LA ER DE LLEIDANET PKI SUCURSAL DE PERÚ 55
32 CONFORMIDAD 55
33 BIBLIOGRAFÍA 55

1 DATOS DEL DOCUMENTO

Proyecto	Entidad de Registro o Verificación
Título	Declaración de Prácticas y Política de Registro de Lleidanet PKI Sucursal de Perú
Código	DOC-160912.1691208
Tipo de documento	DOC - Documento genérico
Clasificación del documento	Público
Realizado por	LLEIDANET PKI SUCURSAL DE PERÚ
Dirigido a	INDECOPI
Fecha aprobación	09/06/2025
Revisión	10

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	12/09/2016	Creación del documento	CO
2	17/10/2018	Revisión documento	NG
3	26/02/2019	Ajustes de documento de acuerdo con la nueva versión de Guía de Acreditación del INDECOPI	NG
4	01/03/2019	Actualización de requisitos de certificados	NG
5	04/03/2019	Modificaciones menores	NG
6	27/01/2020	Modificaciones menores, certificados sw	NG

7	31/03/2020	Adición medidas especiales en la verificación de identidad	NG
8	26/04/2023	Actualizar enlace de donde se encuentran los documentos	CJ
9	20/06/2023	Actualización del apartado 26 Aspectos legales de la operación de la ER	CJ
10	25/06/2025	Actualización en la denominación a Lleidanet PKI Sucursal de Perú, de los participantes del comité de seguridad, del contenido para la emisión de certificados remota y del enlace de donde se encuentran los documentos asociados a la Entidad de Registro	Compliance (CJ)

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de Calidad Fecha: 25/06/2025
Revisado por:	Nombre: Lleidanet PKI SB Cargo: Administrador del Servicio Fecha: 25/06/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información Cargo: Comisión de Seguridad de la Información Fecha: 25/06/2025

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 VISIÓN GENERAL

El alcance de la acreditación cubre la infraestructura y sistemas de registro 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.

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 Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registros o Verificación (ER)" 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, reemisión, 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 firmada 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 Entidad de Registro LLEIDANET PKI SUCURSAL DE PERÚ (ER 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 (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 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 el, con conocimiento y plena aceptación de los derechos y deberes establecidos y 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 CPS.

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 La Comisión de Seguridad de la Información

La Comisión de Seguridad de la Información es un organismo interno de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ, conformado por el Director técnico, el Administrador del Sistema y la Responsable de Seguridad 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. La Comisión de Seguridad de la Información es el responsable de integrar la CPS, a la CPS de terceros prestadores de servicios de certificación.

8 ENTIDAD DE CERTIFICACIÓN ASOCIADA A ER DE LLEIDANET PKI SUCURSAL DE PERÚ

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, publicado en:

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

LLEIDANET PKI SUCURSAL DE PERÚ brinda los servicios de registro o verificación 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 titulares y suscriptores de los certificados digitales provistos por LLEIDANET PKI SUCURSAL DE PERÚ, son responsables de revisar y cumplir la presente Declaración de Prácticas, la CPS y las Políticas de Certificación de la EC, 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.

Todas las responsabilidades y obligaciones que debe cumplir los titulares y suscriptores están establecidas en los respectivos contratos.

12 RESPONSABILIDADES DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían deben actuar de acuerdo con las obligaciones y responsabilidades establecidas en la CPS de la EC y en los documentos normativos de la Entidad de Registro.

Los terceros que confían pueden verificar el estado de los certificados de acuerdo con los establecido en el marco de la IOFE.

La documentación normativa de la ER se encuentra publicada en https://www.lleida.net/es/politicas-y-practicas?tab=peru

13 RESPONSABILIDADES DE LOS TERCEROS CONTRATISTAS

Los terceros contratistas deben actuar de acuerdo con las obligaciones y responsabilidades establecidas en la CPS de la EC y en los documentos normativos de la Entidad de Registro.

La documentación normativa de la ER se encuentra publicada en https://www.lleida.net/es/politicas-y-practicas?tab=peru

La Entidad de Registro de LLEIDANET PKI SUCURSAL DE PERÚ garantiza la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión, durante la ejecución de las actividades de tercerización, los cuales están sujetos al cumplimiento de los contratos con los que se vincula a la ER de Lleidanet PKI.

En este sentido, la ER tiene previsto tercerizar las funciones de los operadores de registro en terceras entidades, con el fin de que éstas puedan realizar los procesos de validación y emisión de los certificados digitales. Para lo cual, se firmará un contrato con dichos terceros en el cual se indicarán las obligaciones de los mismos y los controles de seguridad que éstos deben cumplir, así como indicarse que deben de actuar de acuerdo con las obligaciones y responsabilidades establecidas en la CPS de la EC y en los documentos normativos de la Entidad de Registro.

14 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS RPS

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

Para cualquier consulta contactar:

- Nombre: Comisión de Seguridad de la Información
- Dirección de correo electrónico: consultas@indenova.com

15 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Registro - RPS de LLEIDANET PKI SUCURSAL DE PERÚ, la Política y Plan de Privacidad, así como la Declaración de Prácticas y Política de Certificación de LLEIDANET PKI SUCURSAL DE PERÚ y otra documentación relevante son publicados y difundidos 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.

15.1 PROTECCIÓN DE INTEGRIDAD DEL DOCUMENTO

El presente documento es firmado digitalmente por el Responsable de la ER 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.

16 IDENTIFICACIÓN Y AUTENTICACIÓN

16.1 NOMBRES

16.1.1 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.

16.1.2 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

16.1.3 Certificados de las Subordinadas de LLEIDANET PKI SUCURSAL DE PERÚ

El DN del 'issuer name' de los certificados de las subordinadas de LLEIDANET PKI SUCURSAL DE PERÚ, tienen 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

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

16.1.4 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 de la Comisión de Seguridad de la Información.

16.1.5 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.

16.1.6 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).

16.1.7 Singularidad de los nombres

El DN de los certificados digitales emitidos es único.

16.1.8 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.

17 CERTIFICADOS DIGITALES

La ER de Lleidanet PKI emite los certificados para los siguientes perfiles:

- Persona Natural.
- Persona Jurídica Representante Legal.
- Perteneciente a empresa.
- Agente automatizado.

Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden tener variación de acuerdo con lo establecido en la Política de Certificación y Declaración de Prácticas de la Entidad de Certificación LLEIDANET PKI SUCURSAL DE PERÚ a la que la ER de LLEIDANET PKI SUCURSAL DE PERÚ se encuentra vinculada, para cada tipo de certificado, tales documentos de la EC son publicados son publicados en la siguiente dirección web: https://www.lleida.net/es/politicas-y-practicas?tab=peru

Los certificados brindados por la ER de LLEIDANET PKI SUCURSAL DE PERÚ corresponden a las Entidades de Certificación acreditadas ante el INDECOPI, publicadas en su web.

El ciclo de vida de un certificado personal no debe exceder el periodo establecido por la IOFE, el mismo que será de máximo tres (3) años de acuerdo con la legislación vigente.

18 CERTIFICADOS DIGITALES DE PERSONA NATURAL

18.1 SERVICIOS BRINDADOS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de emisión, revocación, suspensión, re-emisión y modificación[1] de certificados para personas naturales de nacionalidad peruana.
b) Atención de solicitudes de emisión, revocación, suspensión, re-emisión y modificación[2] de certificados de atributos para personas naturales de nacionalidad extranjera.

[1] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de la EC LLEIDANET PKI SUCURSAL DE PERÚ.

[2] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de la EC LLEIDANET PKI SUCURSAL DE PERÚ.

18.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado.

18.3 MODALIDADES DE ATENCIÓN

La solicitud se podrá realizar en cualquiera de las modalidades de atención siguientes:

- De manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ.
- De manera presencial en las instalaciones del cliente, o un lugar asignado por este en presencia de un representante de la ER.
- En caso el aspirante a titular se encuentre en lugares remotos, la verificación presencial de identidad de aspirante se realizará mediante una video identificación autorizado por la EC, bajo la consulta a la base de datos de RENIEC para peruanos y a la base de datos de Migraciones para aspirantes extranjeros.
- En casos excepcionales, cuando la IOFE así lo indique se procederá a atender de forma remota únicamente.

18.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADO

La Entidad de Registro de LLEIDANET PKI SUCURSAL DE PERÚ puede emitir los siguientes certificados:

- Certificado de Persona Natural en Hardware: Cuando la ER proporciona el módulo criptográfico.
- Certificado de Persona Natural en Mobile: Cuando el certificado digital se emite en dispositivo móvil.

Para la emisión de certificados presencial:

- Se informa presencialmente o envía requisitos por correo a Titular de acuerdo con tipo de certificado solicitado.
- Se verifica pago de servicio o documento que evidencie el mismo.
- Se realiza verificación presencial y cumplimiento de requisitos.
- Se accede a Plataforma y selecciona tipo de certificado a emitir.

- De no ser parte del servicio el módulo criptográfico, este se evalúa para verificar la compatibilidad con la Plataforma de Registro[3] y que tenga la certificación FIPS 140-2 nivel 2[4].
- Se realiza la solicitud en Plataforma de registro, adjuntando evidencia de información.
- Se firma contrato de emisión de certificado.
- Se genera certificado en PKI.
- Se inserta en modulo criptográfico y generan claves.
- Se recibe clave de activación y revocación a través de correo electrónico declarado.

Para la emisión de certificados remota:

- Se realiza la solicitud del certificado en la web de solicitud de certificados según el tipo de certificado requerido por el usuario
- Se realiza el pago del certificado solicitado
- Se realiza la videoidentificación y firma del contrato de emisión de certificado
- El operador accede a la Plataforma para validar que los documentos y la información ingresada por el suscriptor sea verídica.
- Si el operador verifica que los documentos y la información es verídica genera certificado en PKI.
- Se inserta en modulo criptográfico y se generan las claves.
- Se recibe certificado digital, clave de activación y revocación a través de correo electrónico declarado.

18.4.1 Solicitud de certificados

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento, portando los siguientes documentos dependiendo de la nacionalidad del solicitante:

Para nacionales peruanos: debe aportar el original del documento nacional de identidad

Para extranjeros: debe aportar el original de la cedula de extranjería o el original del pasaporte, en caso de aportar pasaporte y de encontrarse en territorio peruano además deberá aportar pasaporte

[3] La plataforma de Registro solo reconoce los módulos con FIPS 140-2 nivel 2 mínimo homologados, de no ser así se detiene el proceso se informa al titular.

[4] Si la administración del módulo criptográfico lo realiza el Titular, la responsabilidad recae en él.

legalizado por un notario público, en caso aportar pasaporte y de encontrarse fuera de territorio peruano el pasaporte debe estar legalizado por un notario y apostillado ante la Haya.

La solicitud se realiza por medios no repudiables que establece la EC vinculada a ER de LLEIDANET PKI SUCURSAL DE PERÚ, garantizando su autenticidad y no repudio y es realizada en la Plataforma por el Operador de Registro.

18.4.2 Verificación de titulares

Tras la solicitud debe validarse la identidad a los aspirantes a titulares, estos pueden ser validados en cualquiera de las siguientes modalidades:

- De manera presencial.
- En el caso remoto, será necesario enviar la verificación de identidad realizada ante Notario Público (DNI y contrato legalizado) a la ER mediante correo o validado por la misma.
- En casos excepcionales y previo acuerdo con la IOFE, la verificación de los titulares se realizará mediante sistemas de video identificación o verificación biométrica facial. Estas pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenada para su posterior verificación en el caso de ser necesario.

La verificación del titular es un proceso que se realiza directamente con RENIEC.

La recopilación y validación del titular normalmente se realizará por la misma persona, con perfil de Operador de Registro (OR) que emitirá el certificado posteriormente.

El proceso de recopilación y validación del titular es un proceso que puede ser tercerizado por la ER.

18.4.3 Aprobación de la Solicitud de emisión de un CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, en caso de que una solicitud sea aprobada por la ER de LLEIDANET PKI SUCURSAL DE PERÚ, el operador de registro iniciará el siguiente proceso de forma inmediata:

a) Acceder a un sistema web (Plataforma de ahora en adelante) con control de acceso y la protección de un canal SSL para poder realizar la emisión del certificado.

b) Autenticarse en la Plataforma.

c) Validar que los datos, documentos e identidad del solicitante sea la correcta.

d) Emitir el certificado.

El perfil que inicia este proceso lo finaliza con la emisión del certificado.

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de LLEIDANET PKI SUCURSAL DE PERÚ enviará a la respectiva EC la autorización de la emisión del certificado de manera inmediata.

En el caso de que ocurra algún problema de conexión con la EC, el máximo tiempo de respuesta para la emisión del certificado será de cinco (5) días, luego de haber sido aprobada la validación de identidad.

18.4.4 Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE. Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles. O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC LLEIDANET PKI SUCURSAL DE PERÚ puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de esta.

18.4.5 Contrato del Titular

El solicitante deberá firmar un contrato, que en adelante llamaremos “contrato del Titular”, el cual contiene las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por la ER de LLEIDANET PKI SUCURSAL DE PERÚ en coordinación con la EC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera digital utilizando la Plataforma Click & Sign, por el titular, el cual será archivado en la Plataforma por la ER de LLEIDANET PKI SUCURSAL DE PERÚ. Esta firma se realizará por medios digitales mediante una clave que será enviada al móvil o al correo electrónico indicado por el solicitante

A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

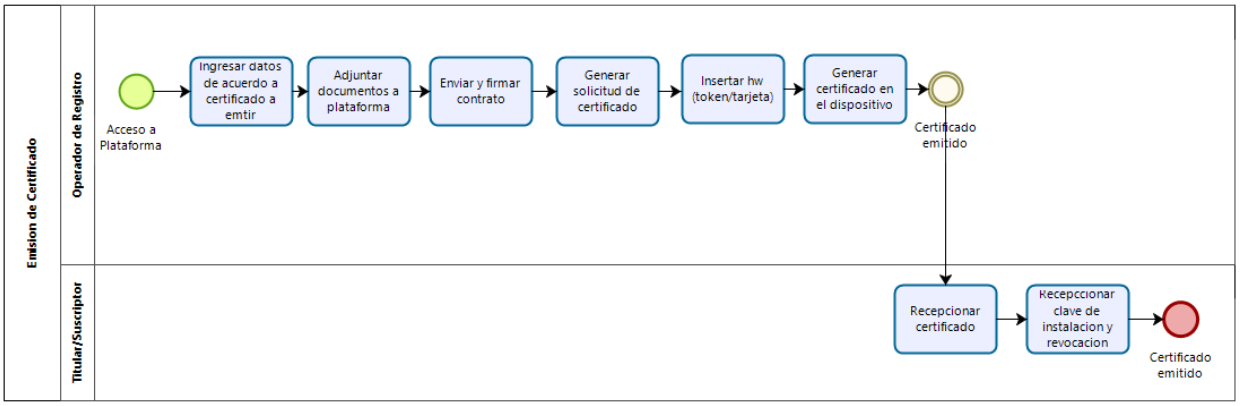
La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados, de no firmarse el contrato en un lapso de 24 horas este puede ser revocado por la ER.

18.4.6 Emisión del certificado

La emisión del certificado será realizada según el medio seleccionado: hardware o mediante Lleidanet Wallet.

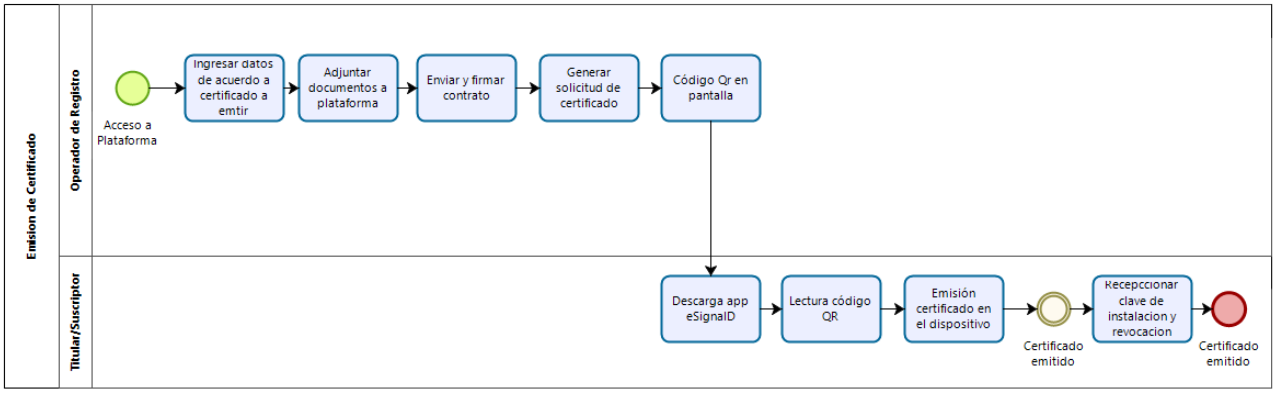
La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor. La petición segura del certificado a la EC LLEIDANET PKI SUCURSAL DE PERÚ se realizará en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

A. En el caso de que la emisión del certificado se haga mediante hardware el proceso es el siguiente:



En este caso la ER administra los módulos criptográficos por lo que los dispositivos que se entreguen ya sean tokens, tarjetas u otros, cumplirán como mínimo con los estándares FIPS 140-2 nivel 2.

B. En el caso de que la emisión del certificado se haga usando la aplicación Lleidanet Wallet el proceso es el siguiente:



En el caso de Lleidanet Wallet, se generará un código QR el cual será enviado en el correo indicado por el suscriptor. En este caso, el solicitante se instala el aplicativo Lleidanet Wallet en su smartphone con el que leerá el código QR. En este momento se generará el certificado en el smartphone.

En este caso la ER no administra ningún módulo criptográfico ya que el certificado es generado en el smartphone del usuario.

18.5 REGISTRO DE DOCUMENTOS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ revisará y registrará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante de forma electrónica en su Plataforma. Al

tratarse de documentos electrónicos su custodia se realizará en la propia Plataforma. Únicamente en el caso de que la verificación se haya realizado de forma remota, será necesario custodiar la información física enviada por el Notario Público (DNI y contrato legalizado) en una caja fuerte.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

18.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS

En el caso de los certificados de personas naturales, el periodo de vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo con la legislación vigente.

19 CERTIFICADOS DIGITALES DE PERSONA JURÍDICA REPRESENTANTE LEGAL O PERTENECIENTE A EMPRESA

19.1 SERVICIOS BRINDADOS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de emisión, revocación, suspensión y re-emisión[5] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
b) Atención de solicitudes de emisión, revocación, suspensión y re-emisión[6] de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.

19.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

La solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER un documento que acredite sus facultades como representante.

[5] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

[6] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

19.3 MODALIDADES DE ATENCIÓN

La solicitud se podrá realizar en cualquiera de las modalidades de atención siguientes:

- De manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ
- De manera presencial en las instalaciones del cliente, o un lugar asignado por el en presencia de un representante de la ER
- En caso el aspirante a titular se encuentre en lugares remotos, la verificación presencial de identidad de aspirante se realiza por medio de un Notario Público autorizado por la EC.
- En casos excepcionales, cuando la IOFE así lo indique se procederá a atender de forma remota únicamente.

19.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADO

La Entidad de Registro de LLEIDANET PKI SUCURSAL DE PERÚ puede emitir los siguientes certificados:

- Certificado de Persona Jurídica en Hardware: Cuando la ER proporciona el módulo criptográfico.
- Certificado de Persona Jurídica en Mobile: Cuando el certificado digital se emite en dispositivo móvil.

Para la emisión de certificados presencial

- Se informa presencialmente o envía requisitos por correo a Titular de acuerdo con tipo de certificado solicitado.
- Se verifica pago de servicio o documento que evidencie el mismo.
- Se realiza verificación presencial y cumplimiento de requisitos.
- Se accede a Plataforma y selecciona tipo de certificado a emitir.
- De no ser parte del servicio el módulo criptográfico, este se evalúa para verificar la compatibilidad con la Plataforma de Registro[7] y que tenga la certificación FIPS 140-2 nivel 2[8].

[7] La plataforma de Registro solo reconoce los módulos con FIPS 140-2 nivel 2 mínimo homologados, de no ser así se detiene el proceso se informa al titular.

[8] Si la administración del módulo criptográfico lo realiza el Titular, la responsabilidad recae en él.

- Se realiza la solicitud en Plataforma de registro, adjuntando evidencia de información.
- Se firma contrato de emisión de certificado.
- Se genera certificado en PKI.
- Se inserta en modulo criptográfico y generan claves.
- Se recibe clave de activación y revocación a través de correo electrónico declarado.

Para la emisión de certificados remota:

- Se realiza la solicitud del certificado en la web de solicitud de certificados según el tipo de certificado requerido por el usuario
- Se realiza el pago del certificado solicitado
- Se realiza la videoidentificación y firma del contrato de emisión de certificado
- El operador accede a la Plataforma para validar que los documentos y la información ingresada por el suscriptor se encuentre verídica.
- Si el operador verifica que los documentos y la información es verídica genera certificado en PKI.
- Se inserta en modulo criptográfico y se generan las claves.
- Se recibe certificado digital, clave de activación y revocación a través de correo electrónico declarado.

19.4.1 Solicitud de certificados

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.

La ER debe validar que los datos de la solicitud del certificado emitida a la EC correspondan a los datos de la identidad validada.

De manera general, no debe incluirse en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se debe comprobar que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. Pero, la ER no tiene que comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, todo es responsabilidad del solicitante.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

La solicitud se realiza por medios no repudiables que establece la EC vinculada a ER de LLEIDANET PKI SUCURSAL DE PERÚ, garantizando su autenticidad y no repudio y es realizada en la Plataforma por el Operador de Registro.

19.4.2 Verificación de titulares

La ER debe solicitar la documentación o información necesaria para garantizar que un nombre o marca pertenece al solicitante o representado de un certificado digital.

En el caso de validación de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.[9]

Se acredita al Representante Legal acreditando la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva. La identidad de la persona jurídica debe ser verificada:

- En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento[10] o consulta electrónica de vigencia emitidos por los Registros Públicos, SUNARP, o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido.
- Solicitud firmada por representante legal, apoderado o persona que cuente con los poderes suficientes solicitando la emisión del certificado digital
- En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.
- La verificación de identidad del representante se realiza directamente en la página web de RENIEC.
- En casos excepcionales y previo acuerdo con la IOFE, la verificación de los titulares se realizará mediante el sistema de video identificación o verificación biométrica facial. Estas pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenada para su posterior verificación en el caso de ser necesario.
- Resolución de designación del funcionario competente de la persona a la que se emitirá el certificado (para entidades públicas)

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, se solicita evidencia del cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo mediante un documento legal respectivo.

[9] No le corresponde a la ER resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

[10] La vigencia poder presentada no debe ser menor de 30 días.

19.4.3 Verificación de suscriptores

Tras la solicitud debe validarse la identidad a los aspirantes a suscriptores, estos pueden ser validados en cualquiera de las siguientes modalidades:

- De manera presencial, mediante la página web de RENIEC.
- En el caso remoto, será necesario enviar la verificación de identidad realizada ante Notario Público a la ER mediante correo validado por la misma.
- En casos excepcionales y previo acuerdo con la IOFE, la verificación de los titulares se realizará mediante un sistema de video identificación o verificación biométrica facial. Estas pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenada para su posterior verificación en el caso de ser necesario.

La identidad de los aspirantes a suscriptores debe ser verificada por la ER o un Notario Público autorizado por la AAC, u otra entidad autorizada o reconocida por la AAC, en convenio con la ER, en cuya presencia se debe firmar el contrato del suscriptor, garantizando que el suscriptor acepta las responsabilidades que conlleva el uso del certificado digital de persona jurídica, a través de la firma del Contrato del suscriptor o un documento de aceptación de dichas responsabilidades.

A fin de impedir la suplantación de identidad de suscriptores, o la asignación de responsabilidades sin contar con la autorización del empleado que adoptará el rol del suscriptor. De manera general, no debe incluirse en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se debe comprobar que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. Pero, la ER no tiene que comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, todo es responsabilidad del solicitante.

19.4.4 Aprobación de la Solicitud de emisión de un CERTIFICADO

Una vez validada la información proporcionada por el suscriptor, en caso de que una solicitud sea aprobada por la ER de LLEIDANET PKI SUCURSAL DE PERÚ, el operador de registro iniciará el siguiente proceso de forma inmediata:

a) Acceder a un sistema web (Plataforma de ahora en adelante) con control de acceso y la protección de un canal SSL para poder realizar la emisión del certificado.

b) Autenticarse en la Plataforma.

c) Validar que los datos, documentos e identidad del solicitante sean verídicos.

d) Emitir el certificado.

El perfil que inicia este proceso lo finaliza con la emisión del certificado.

En el procedimiento normal el tiempo de respuesta será inmediato. En el caso de que ocurra algún problema de conexión con la EC, el máximo tiempo de respuesta para la emisión del certificado será de cinco (5) días, luego de haber sido aprobada la validación de identidad.

19.4.5 Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE. Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

La EC LLEIDANET PKI SUCURSAL DE PERÚ puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de esta.

19.4.6 Contrato del Titular/Suscriptor

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato, que en adelante llamaremos “contrato del titular”, el cual contiene las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por la ER de LLEIDANET PKI SUCURSAL DE PERÚ en coordinación con la EC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera digital utilizando la Plataforma Click & Sign, por el titular, el cual será archivado en la Plataforma de la ER de LLEIDANET PKI SUCURSAL DE PERÚ. Esta firma se realizará por medios digitales mediante una clave que será enviada al móvil o al correo electrónico indicado por el solicitante

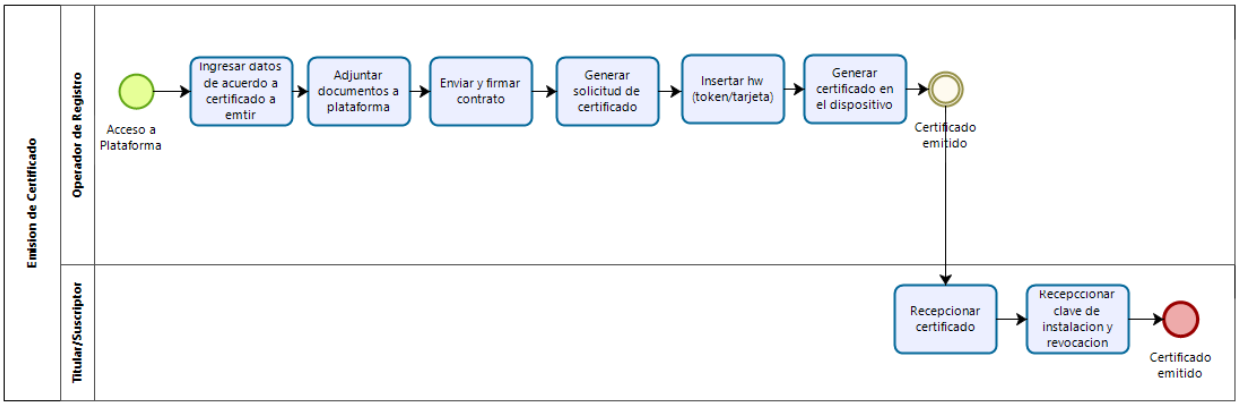
A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

19.4.7 Emisión del certificado

La emisión del certificado será realizada según el medio seleccionado: hardware o mediante Lleidanet Wallet.

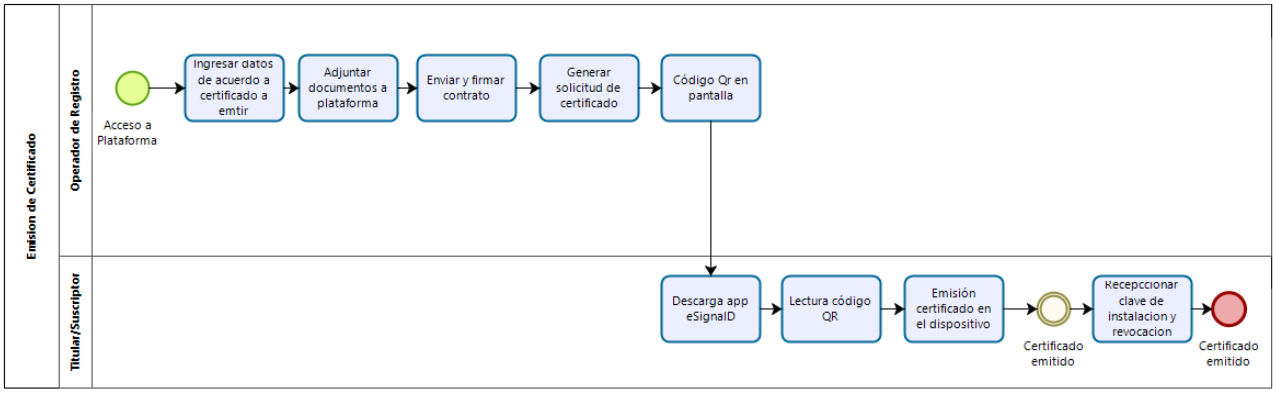
La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor. La petición segura del certificado a la EC LLEIDANET PKI SUCURSAL DE PERÚ se realizará en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

A. En el caso de que la emisión del certificado se haga mediante hardware el proceso es el siguiente:



En este caso la ER administra los módulos criptográficos por lo que los dispositivos que se entreguen, ya sean tokens, tarjetas u otros, cumplirán como mínimo con los estándares FIPS 140-2 nivel 2.

B. En el caso de que la emisión del certificado se haga usando la aplicación Lleidanet Wallet el proceso es el siguiente:



En el caso de Lleidanet Wallet, se generará un código QR en la pantalla del Operador de Registro. En este caso, el solicitante se instala el aplicativo Lleidanet Wallet en su smartphone con el que leerá el código QR. En este momento se generará el certificado en el smartphone.

En este caso la ER no administra ningún módulo criptográfico ya que certificado es generado en el smartphone del usuario.

19.5 REGISTRO DE DOCUMENTOS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ revisará y registrará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante de forma electrónica en su Plataforma. Al

tratarse de documentos electrónicos su custodia se realizará en la propia Plataforma, de contar con documentos físicos la custodia se realiza en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

19.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS

En el caso de los certificados de atributos, el periodo de vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo con la legislación vigente.

20 CERTIFICADOS DIGITALES DE AGENTE AUTOMATIZADO

La Entidad de Registro de LLEIDANET PKI SUCURSAL DE PERÚ puede emitir los siguientes certificados:

- Certificado de Persona Jurídica de agente automatizado en Hardware: Cuando la ER proporciona el módulo criptográfico.
- Certificado de Persona Jurídica en Software: Se emite un p12, utilizado exclusivamente para la facturación electrónica.

20.1 SERVICIOS BRINDADOS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ brinda los siguientes servicios de agentes automatizados a personas jurídicas:

a) Atención de solicitudes de emisión, revocación, suspensión, re-emisión[11] de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
b) Atención de solicitudes de emisión, revocación, suspensión y re-emisión[12] de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad

[11] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

[12] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

extranjera, como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

20.2 AUTORIZADOS PARA REALIZAR LA SOLICITUD

La solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER un documento que acredite sus facultades como representante.

20.3 MODALIDADES DE ATENCIÓN

La solicitud se podrá realizar en cualquiera de las modalidades de atención siguientes:

- De manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ
- De manera presencial en las instalaciones del cliente, o un lugar asignado por el en presencia de un representante de la ER
- En caso el aspirante a titular se encuentre en lugares remotos, la verificación presencial de identidad de aspirante se realiza por medio de un Notario Público autorizado por la EC.
- En casos excepcionales y previo acuerdo con la IOFE, la verificación de los titulares se realizará mediante un sistemas de video identificación o verificación biométrica facial. Estas pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenada para su posterior verificación en el caso de ser necesario.

20.4 PROCEDIMIENTO DE EMISIÓN DE CERTIFICADO

Para la emisión de certificados presencial:

- Se informa presencialmente o envía requisitos por correo a Titular de acuerdo con tipo de certificado solicitado.
- Se verifica pago de servicio o documento que evidencie el mismo.
- Se realiza verificación presencial y cumplimiento de requisitos.
- Se accede a Plataforma y selecciona tipo de certificado a emitir.

- De no ser parte del servicio el módulo criptográfico, este se evalúa para verificar la compatibilidad con la Plataforma de Registro [13]y que tenga la certificación FIPS 140-2 nivel 2.[14]
- Se realiza las solicitudes en Plataforma de registro, adjuntando evidencia de información.
- Se firma contrato de emisión de certificado.
- Se genera certificado en PKI.
- Se inserta en modulo criptográfico y generan claves.
- Se recibe clave de activación y revocación a través de correo electrónico declarado.

Para la emisión de certificados remota:

- Se envía requisitos por correo a Titular de acuerdo con tipo de certificado solicitado, indicando la legalización de verificación presencial y legalización de contrato.
- Se verifica pago de servicio y él envió de documentos que sustenten los requisitos para emisión.
- Se accede a Plataforma y selecciona tipo de certificado a emitir.
- De no ser parte del servicio el módulo criptográfico, este se evalúa para verificar la compatibilidad con la Plataforma de Registro [15]y que tenga la certificación FIPS 140-2 nivel 2.[16]
- Se realiza las solicitudes en Plataforma de registro, adjuntando evidencia de información.
- Se firma contrato de emisión de certificado.
- Se genera certificado en PKI.
- Se inserta en modulo criptográfico y generan claves.
- Se recibe clave de activación y revocación a través de correo electrónico declarado.
- Se envía certificado digital por transporte seguro o Courier, si es parte de servicio.

20.4.1 Solicitud de certificados para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo. En este caso,

[13] La plataforma de Registro solo reconoce los módulos con FIPS 140-2 nivel 2 mínimo homologados, de no ser así se detiene el proceso se informa al titular.

[14] Si la administración del módulo criptográfico lo realiza el Titular, la responsabilidad recae en él.

[15] La plataforma de Registro solo reconoce los módulos con FIPS 140-2 nivel 2 mínimo homologados, de no ser así se detiene el proceso se informa al titular.

[16] Si la administración del módulo criptográfico lo realiza el Titular, la responsabilidad recae en él.

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.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

La solicitud se realiza por medios no repudiables que establece la EC vinculada a ER de LLEIDANET PKI SUCURSAL DE PERÚ, garantizando su autenticidad y no repudio y es realizada en la Plataforma por el Operador de Registro.

20.4.2 Verificación de titulares

La ER debe solicitar la documentación o información necesaria para garantizar que un nombre o marca pertenece al solicitante o representado de un certificado digital.

En el caso de validación de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.[17]

Se acredita al Representante Legal acreditando la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva

La identidad de la persona jurídica debe ser verificada:

- En el caso de empresas con domicilio en Perú, la existencia y vigencia de la persona jurídica deberá acreditarse con el documento [18] o consulta electrónica de vigencia emitidos por los Registros Públicos, SUNARP, o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente, se debe verificar también mediante la base de datos de SUNAT que el RUC se encuentre activo y habido.
- En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.
- La verificación de identidad del representante se realiza directamente en la página web de RENIEC, de ser remota se realiza ante Notario Público.
- En casos excepcionales y previo acuerdo con la IOFE, la verificación de los titulares se realizará mediante una videoconferencia o sistemas de video identificación o verificación biométrica facial. Esta videoconferencia o las pericias del proceso de video identificación o verificación biométrica facial, serán grabadas y almacenada para su posterior verificación en el caso de ser necesario.

[17] No le corresponde a la ER resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

[18] La vigencia poder presentada no debe ser menor de 30 días.

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER se solicita la evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo mediante un documento legal respectivo o consulta a la base de datos respectiva.

20.4.3 Aprobación de la solicitud de emisión de un certificado

Una vez validada la información proporcionada por el suscriptor, en caso de que una solicitud sea aprobada por la ER de LLEIDANET PKI SUCURSAL DE PERÚ, el operador de registro iniciará el siguiente proceso de forma inmediata:

a) Acceder a un sistema web (Plataforma de ahora en adelante) con control de acceso y la protección de un canal SSL para poder realizar la emisión del certificado.

b) Autenticarse en la Plataforma.

c) Iniciar la solicitud de emisión de certificado.

d) Adjuntar electrónicamente al expediente los documentos que evidencien la verificación del titular del paso anterior.

e) Requerir la firma del contrato del titular.

f) Emitir el certificado.

El perfil que inicia este proceso lo finaliza con la emisión del certificado.

En el procedimiento normal el tiempo de respuesta será inmediato. En el caso de que ocurra algún problema de conexión con la EC, el máximo tiempo de respuesta para la emisión del certificado será de cinco (5) días, luego de haber sido aprobada la validación de identidad.

20.4.4 Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE. Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

La EC LLEIDANET PKI SUCURSAL DE PERÚ puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de esta.

20.4.5 Contrato del titular

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato, que en adelante llamaremos “contrato del titular”, el cual contiene las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por la ER de LLEIDANET

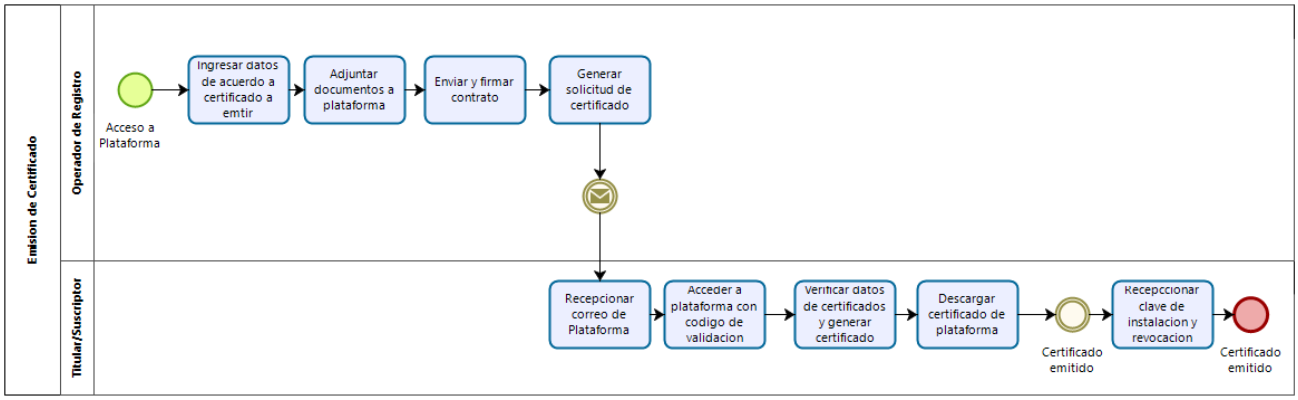
PKI SUCURSAL DE PERÚ en coordinación con la EC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera digital utilizando la Plataforma eSignaBox, por el representante legal de la persona jurídica o persona designada por él, para luego ser archivado en la Plataforma por la ER de LLEIDANET PKI SUCURSAL DE PERÚ. Esta firma se realizará por medios digitales: pantalla táctil con firma biométrica o huellero de firma con huella dactilar.

A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

20.4.6 Emisión del certificado

La emisión del certificado será realizada en software externo, tal y como se muestra en la imagen siguiente:



Se realizará el envío de un enlace al usuario por correo que incluye un código de validación. Una vez se acceda y se verifiquen los datos, se generará el certificado que se podrá descargar e instalar el certificado a través de un archivo el p12 de uso exclusivo para facturación electrónica.

20.5 REGISTRO DE DOCUMENTOS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ revisará y registrará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante de forma electrónica en su Plataforma. Al tratarse de documentos electrónicos su custodia se realizará en la propia Plataforma, de contar con documentos físicos la custodia se realiza en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

20.6 PERIODO DE VIGENCIA DE LOS CERTIFICADOS

En el caso de certificados para agentes automatizados, el periodo de vigencia puede variar de acuerdo con lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación a la que la ER de LLEIDANET PKI SUCURSAL DE PERÚ se encuentra vinculada.

21 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES

La re-emisión de un certificado es un proceso programado cada vez que un nuevo par de claves debe ser emitido debido a que la fecha de su expiración es cercana y su periodo de vigencia es menor a un plazo máximo de un año. En los casos que el certificado del titular hubiera expirado o hubiera sido revocado, deberá seguirse el proceso de solicitud para la emisión de un nuevo certificado descrito en el presente documento.

Sólo se podrá realizar una única re-emisión de certificado.

El proceso de re-emisión es opcional para las EC, por ello la habilitación del proceso dependerá de si dicha habilitación se encuentra establecida en la CPS de la EC que emitió el certificado.

Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden tener variación de acuerdo con lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación a la que la ER de LLEIDANET PKI SUCURSAL DE PERÚ se encuentra vinculada, para cada tipo de certificado, tales documentos de la EC son publicados son publicados en la siguiente dirección web: https://www.lleida.net/es/politicas-y-practicas?tab=peru

Sin embargo, conforme a lo establecido en la normatividad peruana, la ER de LLEIDANET PKI SUCURSAL DE PERÚ realizará como mínimo, los siguientes procedimientos de verificación para la validación de la identidad de una persona jurídica o natural.

21.1 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA NATURAL

21.1.1 Servicios brindados

La ER de LLEIDANET PKI SUCURSAL DE PERÚ brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de re-emisión[19] de certificados para personas naturales de nacionalidad peruana.
b) Atención de solicitudes de re-emisión[20] de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados brindados por la ER de LLEIDANET PKI SUCURSAL DE PERÚ corresponden a las Entidades de Certificación acreditadas ante el INDECOPI, publicadas en su web.

21.1.2 Autorizados para realizar la solicitud

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado.

21.1.3 Modalidades de atención

La solicitud se podrá realizar en cualquiera de las modalidades de atención siguientes:

- De manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ.
- De manera presencial en las instalaciones del cliente, o un lugar asignado por este en presencia de un representante de la ER.
- En caso el aspirante a titular se encuentre en lugares remotos, la verificación presencial de identidad de aspirante se realiza por medio de un Notario Público autorizado por la AC.
- En casos excepcionales, cuando la IOFE así lo indique se procederá a atender de forma remota únicamente.

21.1.4 Solicitud de re-emisión de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

21.1.5 Identificación y autenticación de solicitantes de certificados de persona natural

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de LLEIDANET PKI SUCURSAL DE PERÚ a través de un mecanismo de consulta a las bases de datos del RENIEC.

[19] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

[20] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de LLEIDANET PKI SUCURSAL DE PERÚ no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

En casos excepcionales y previo acuerdo con la IOFE, la verificación del titular o del suscriptor se realizará mediante una videconferencia. Esta videoconferencia será grabada y almacenada para su posterior verificacióne en el caso de ser necesario.

21.2 SOLICITUD DE RE-EMISIÓN CERTIFICADOS DE PERSONA JURÍDICA

21.2.1 Servicios brindados

La ER de LLEIDANET PKI SUCURSAL DE PERÚ brinda los siguientes servicios a personas jurídicas:

a) Atención de solicitudes de re-emisión[21] de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
b) Atención de solicitudes de re-emisión de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
c) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
d) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

[21] La suspensión, re-emisión y modificación dependerá de lo establecido en las Políticas de Certificación de las EC vinculadas.

21.2.2 Autorizados para realizar la solicitud

Sólo los titulares de certificados pueden solicitar la re-emisión de certificados, por lo que en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de LLEIDANET PKI SUCURSAL DE PERÚ, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

21.2.3 Modalidades de atención

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ
- De manera presencial en las instalaciones del cliente, o un lugar asignado por el en presencia de un representante de la ER, el Operador de Registro
- De realizarse de manera remota, deberá realizarse mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica.
- En casos excepcionales, cuando la IOFE así lo indique se procederá a atender de forma remota únicamente.

21.2.4 Solicitud de re-emisión de certificados de atributos

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

21.2.5 Solicitud de re-emisión de certificados para agente automatizado

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

21.2.6 Identificación y autenticación de solicitantes de re-emisión de certificados de persona jurídica

La ER de LLEIDANET PKI SUCURSAL DE PERÚ comprobará que la información del titular y del suscriptor contenida en la solicitud continúa siendo válida, respecto de la existencia de la persona jurídica en los Registros Públicos y de los suscriptores en la base de datos del RENIEC.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

En el caso de empresas constituidas en el extranjero, el solicitante deberá acreditar la continuidad de su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

En el caso de suscriptores extranjeros, estos tendrán que presentar al Operador de Registro, su documento oficial de identidad, pasaporte o carnet de extranjería.

En casos excepcionales y previo acuerdo con la IOFE, la verificación del titular y del suscriptor se realizará mediante una videconferencia. Esta videoconferencia será grabada y almacenada para su posterior verificación en el caso de ser necesario.

21.3 PROCESAMIENTO DE LA SOLICITUD DE RE-EMISIÓN

21.3.1 Aprobación de la solicitud de re-emisión de un certificado

En caso de que una solicitud sea aprobada por la ER de LLEIDANET PKI SUCURSAL DE PERÚ realizará lo siguiente:

a) Acceder a un sistema web (Plataforma de ahora en adelante) con control de acceso y la protección de un canal SSL para poder realizar la emisión del certificado.

b) Autenticarse en la Plataforma.

c) Iniciar la solicitud de re-emisión de certificado.

d) Adjuntar electrónicamente al expediente los documentos que evidencien la verificación del titular del paso anterior.

e) Requerir la firma del contrato del suscriptor.

f) Re-emitir el certificado.

El perfil que inicia este proceso lo finaliza con la emisión del certificado.

En el procedimiento normal el tiempo de respuesta será inmediato. En el caso de que ocurra algún problema de conexión con la EC, el máximo tiempo de respuesta para la emisión del certificado será de cinco (5) días, luego de haber sido aprobada la validación de identidad.

La re-emisión de los certificados se realiza del mismo modo explicado para su emisión en apartados anteriores.

21.3.2 Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC LLEIDANET PKI SUCURSAL DE PERÚ puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de LLEIDANET PKI SUCURSAL DE PERÚ.

21.3.3 Registro de documentos

La ER de LLEIDANET PKI SUCURSAL DE PERÚ revisará y registrará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante de forma electrónica en su Plataforma. Al tratarse de documentos electrónicos su custodia se realizará en la propia Plataforma. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

22 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

22.1 CIRCUNSTANCIAS PARA REALIZAR LA SOLICITUD

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica
- 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.
- Por decisión de la legislación respectiva.
- Pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada.

- Compromiso potencial de la clave privada.
- Pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.

22.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

22.2.1 Servicios brindados

La ER de LLEIDANET PKI SUCURSAL DE PERÚ brinda los siguientes servicios a personas jurídicas y naturales:

a) Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.
b) Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.
c) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
d) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
e) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
f) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: https://www.lleida.net/es/politicas-y-practicas?tab=peru

22.2.2 Autorizados para realizar la solicitud

De acuerdo con lo estipulado por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son:

- El titular del certificado
- El suscriptor del certificado.
- La EC o ER que emitió el certificado.
- Un juez que de acuerdo con 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.

En el caso de personas jurídicas, los titulares de certificados pueden solicitar la revocación de certificados, por lo que en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de LLEIDANET PKI SUCURSAL DE PERÚ, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

22.2.3 Identificación y autenticación de los solicitantes

En los casos de que la solicitud sea presencial:

- Los suscriptores deben presentar en la ER como mínimo su documento oficial de identidad.
- El representante asignado por la persona jurídica debe presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.
- Los terceros (diferentes de la EC, el suscriptor y el titular) deberán presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo con la ley vigente, junto a la orden judicial respectiva.
- En casos excepcionales y previo acuerdo con la IOFE, la verificación de los suscriptores, representantes y terceros se realizará mediante una videconferencia. Esta videoconferencia será grabada y almacenada para su posterior verificación en el caso de ser necesario.

22.2.4 Modalidades de atención

La solicitud puede ser realizada por los titulares y suscriptores mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ
- De manera presencial en las instalaciones del cliente, o un lugar asignado por el en presencia de un representante de la ER, el Operador de Registro, en el caso de tercerización de las ER que son en el mismo cliente.
- De manera remota, mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica o por el suscriptor. El certificado digital a emplear no debe ser el que se desea revocar.

- De manera remota en una comunicación directa con la EC, mediante un control de acceso o contraseña brindados al suscriptor en el momento de la solicitud de emisión de los certificados. En esta modalidad se contará con un registro de las revocaciones realizadas.
- En casos excepcionales, cuando la IOFE así lo indique se procederá a atender de forma remota únicamente.

Para todos los demás actores, diferentes a los suscriptores y titulares, la solicitud deberá ser de manera presencial en las instalaciones de la ER de LLEIDANET PKI SUCURSAL DE PERÚ.

La EC no requerirá realizar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato o en caso sea necesario por revocación del certificado de la EC. Una EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su CPS y se encuentren de acuerdo con la legislación vigente.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER de LLEIDANET PKI SUCURSAL DE PERÚ, utilizando un certificado digital reconocido por el INDECOPI.

22.2.5 Solicitud de revocación de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

22.2.6 Solicitud de revocación de certificados para agente automatizado

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

22.3 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

22.3.1 Aprobación de la solicitud de revocación de un certificado

En caso de que, una solicitud sea aprobada por la ER de LLEIDANET PKI SUCURSAL DE PERÚ realizará lo siguiente:

a) Acceder a un sistema web (Plataforma de ahora en adelante) con control de acceso y la protección de un canal SSL para poder realizar la emisión del certificado.

b) Autenticarse en la Plataforma.

c) Iniciar la solicitud de revocación de certificado.

d) Adjuntar electrónicamente al expediente los documentos que evidencien la verificación del titular del paso anterior.

e) Requerir la firma del contrato del suscriptor.

f) Revocación el certificado.

22.3.2 Rechazo de la solicitud de revocación emisión de un certificado

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER de LLEIDANET PKI SUCURSAL DE PERÚ.

22.3.3 Registro de documentos

La ER de LLEIDANET PKI SUCURSAL DE PERÚ registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de esta a la EC, sus suscriptores y los terceros que confían.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

En caso de que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

22.3.4 Tiempo para el procesamiento de la solicitud de revocación

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de LLEIDANET PKI SUCURSAL DE PERÚ enviará a la respectiva EC la autorización de la revocación del certificado de manera inmediata.

El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la CP y CPS de la EC.

22.3.5 Revocación del certificado

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

23 GESTIÓN DE LA SEGURIDAD

Las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los servicios de registro son señaladas en la Política de Seguridad de la ER de LLEIDANET PKI SUCURSAL DE PERÚ.

24 GESTIÓN DE OPERACIONES

24.1 MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores debe ser realizada en módulos criptográficos FIPS 140-2.

Los módulos criptográficos usados por los Operadores de Registro deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

24.2 RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

24.3 ENTREGA DE LA CLAVE PÚBLICA

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ERs acepten las claves públicas en representación de los emisores de los certificados, éstas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

24.4 DEPÓSITO DE CLAVE PRIVADA

La ER de LLEIDANET PKI SUCURSAL DE PERÚ no genera copias de las claves privada de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

24.5 DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de LLEIDANET PKI SUCURSAL DE PERÚ, se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

25 CONTROLES DE SEGURIDAD COMPUTACIONAL

Los sistemas de registro utilizados por v son provistos y administrados por la propia LLEIDANET PKI SUCURSAL DE PERÚ. La ER sólo accede a estos sistemas vía web con acceso vía certificados digitales de los Operadores de Registro.

26 PROTECCIÓN DE REGISTROS

Los registros de las solicitudes de emisión, re-emisión, revocación, modificación o suspensión de certificados deben ser protegidas y almacenadas para servir como evidencia en caso de procesos judiciales.

26.1 TIPOS DE EVENTOS REGISTROS

Se debe custodiar información de los siguientes registros:

- Información de contacto de los solicitantes de los servicios de la ER, incluyendo a suscriptores y titulares.
- Solicitudes de emisión, re-emisión, revocación, suspensión o modificación de certificados digitales, realizadas mediante un medio no repudiable por parte del titular y/o suscriptor de los certificados.
- Resultados y evidencias de cada proceso de validación de identidad de persona jurídica o natural, incluyendo procesos con resultados positivos como procesos fallidos en los que se denegó el servicio a un cliente.
- Contratos del suscriptor y titular.
- Registros o evidencias de las solicitudes de emisión, re-emisión, revocación, suspensión o modificación de certificados digitales realizadas por parte de los operadores de

registro a la Entidad de Certificación, indicando el operador de registro que realizó la transacción.

- Registro de contratación de operadores de registro.

26.2 PROTECCIÓN DE LOS REGISTROS

La ER de LLEIDANET PKI SUCURSAL DE PERÚ debe restringir el acceso físico y lógico a la modificación y traslado, borrado de registros a personal responsable de la seguridad de la información de la ER, el cual debe ser distinto a los operadores de registro.

26.3 ARCHIVO DE LOS REGISTROS

Los registros deben ser archivados para ser conservados íntegros en un lugar seguro, que posea los controles ambientales y físicos necesarios para garantizar su duración en el tiempo, incluyendo controles antiincendios, acceso físico y aniego.

Ningún personal no autorizado debe tener acceso al archivo de los registros.

26.4 TIEMPO DE ALMACENAMIENTO DEL ARCHIVO

La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 15 años.

27 SEGURIDAD EN LAS COMUNICACIONES CON LA EC

27.1 USO DE CANALES SEGUROS

La comunicación entre los sistemas de registro y los sistemas de certificación de la EC se comunican por un canal cifrado SSL, mediante un certificado digital emitido por un EC con una certificación ISO 27001.

Las comunicaciones entre la ER y la EC se realizan a través de mecanismos que permitan una comunicación ininterrumpida para garantizar la atención oportuna de las solicitudes de emisión del certificado, así como la actualización de la relación de certificados emitidos y revocados. Las comunicaciones referidas a la aprobación o revocación de certificados deben ser llevadas a cabo mediante un mecanismo que garantice el no repudio.

27.2 AUTENTICACIÓN DE OPERADORES DE REGISTRO

Los operadores de registro pueden autenticarse en los sistemas de registro mediante un certificado digital, mecanismos de biometría o mediante mecanismos de autenticación en doble factor, antes de tener acceso a solicitar la emisión, re-emisión, revocación, modificación o suspensión de certificados.

27.3 REGISTROS DE AUDITORÍA

Los sistemas de registro deben generar registros de auditoría sobre las solicitudes de misión, re-emisión, revocación, modificación o suspensión de certificados, indicando el personal que hizo la solicitud, y el resultado positivo o fallido de la misma.

28 AUDITORÍAS

El INDECOPI como Autoridad Administrativa Competente velarán porque los controles implementados por la Entidad para el cumplimiento de la Guía de Acreditación de Entidad de Registro, por lo que realizara evaluaciones una vez al año.

28.1 FRECUENCIAS DE AUDITORÍAS

Las auditorías internas se llevarán a cabo al menos una vez al año en la ER de LLEIDANET PKI SUCURSAL DE PERÚ.

Las evaluaciones técnicas del INDECOPI se llevarán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.

28.2 CALIFICACIONES DE LOS AUDITORES

La selección de los auditores se realizará de entre el listado proporcionado por el INDECOPI.

28.3 RELACIÓN DEL AUDITOR CON LA ER

Los auditores o asesores deben ser independientes de la ER de LLEIDANET PKI SUCURSAL DE PERÚ.

29 ASPECTOS LEGALES DE LA OPERACIÓN DE LA ER

29.1 PREPARACIÓN Y PERSONALIZACIÓN

a) Cuando la personalización y generación de las claves sea gestionada por la ER se garantiza la seguridad y autenticidad de los procesos de personalización del módulo, para ello se incluye lo siguiente:

i. La carga de la información de identificación se realiza dentro del módulo.
ii. La generación de las claves del suscriptor
iii. La carga del certificado del suscriptor en el módulo donde se garantiza que no existe la generación de copias ni el uso no autorizado de la clave, debido a que solamente el suscriptor tiene acceso y control sobre la misma
iv. La protección lógica del módulo de acceso no autorizado.

b) La ER genera registros de auditoría de los procesos de preparación y personalización.

c) El módulo no será emitido sino ha sido personalizado por la ER o el tercero asignado.

d) Un módulo no será utilizado sino se encuentra en estado de activación o reactivación.

29.2 ALMACENAMIENTO Y DISTRIBUCIÓN DEL MÓDULO CRIPTOGRÁFICO

a) Se han implementado procedimientos para la distribución y registro seguro de la recepción segura del módulo por parte del suscriptor.

b) Los datos de activación del módulo son comunicados de manera segura al suscriptor garantizando que sólo él suscriptor tiene acceso a los mismos, y en el caso de usar contraseña, se le requerirá al suscriptor realizar la modificación. La contraseña de acceso será entregada por un canal seguro el cual es diferente a la entrega de las claves o el módulo criptográfico.

c) La distribución y activación del módulo será registrado para efectos de auditoría por la ER o un tercero asignado.

29.3 USO DEL MÓDULO CRIPTOGRÁFICO

a) El suscriptor será provisto de un mecanismo que protege el acceso a los datos del módulo incluyendo el almacenamiento de las claves privadas.

b) Las claves del suscriptor no podrán ser exportadas por una aplicación para realizar funciones criptográficas.

c) El suscriptor será requerido para usar mecanismos de autenticación para aplicaciones criptográficas y funciones del módulo.

d) La aplicación del módulo del suscriptor generará registros de auditoría, incluyendo los casos de intentos de acceso en el proceso de verificación del titular del módulo.

29.4 DESACTIVACIÓN Y REACTIVACIÓN

a) La activación y desactivación del módulo criptográfico, que contiene la clave privada del suscriptor será controlada solamente por el suscriptor, y no podrá ser manipulada por los empleados o contratistas de la ER.

No se admitirá el depósito, almacenamiento o copia de claves privadas de firma y autenticación de los usuarios finales, ni de los módulos hardware que los contienen, estando estos en modo activado.

29.5 REEMPLAZO DEL MÓDULO CRIPTOGRÁFICO

a) Se han establecido procedimientos para reemplazar módulos perdidos o dañados.

b) En caso de pérdida o daño del módulo, las claves y certificados del suscriptor serán revocados y reemitidos.

c) El reemplazo del módulo será registrado para efectos de auditoría de la ER o el tercero asignado.

29.6 TERMINACIÓN DEL MÓDULO CRIPTOGRÁFICO

a) Todos los módulos que hayan sido retornados a la ER serán desactivados o destruidos de manera segura con el contenido no recuperable o reutilizable para prevenir el uso no autorizado, esta desactivación o destrucción será realizada al momento en el que el módulo ha sido retornado a la ER, de modo que se garantiza que sólo el suscriptor ha tenido control sobre su clave privada.

b) La terminación del módulo será controlado por el emisor del módulo.

c) Se generarán registros de auditoría de la terminación de un módulo.

No serán 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).

30 MATERIAS DE NEGOCIO Y LEGALES

30.1 TARIFAS

Las tarifas por los servicios de registro y certificación digital serán definidas en los contratos de titulares.

30.2 POLÍTICAS DE REEMBOLSO

Las políticas de reembolso por los servicios los servicios de registro serán definidas en los contratos de titulares.

30.3 COBERTURA DE SEGURO

LLEIDANET PKI SUCURSAL DE PERÚ proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil de la Entidad de Certificación.

30.4 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.

30.5 EXCEPCIONES DE GARANTÍAS

La ER de 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.

30.6 OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.

En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación de sus certificados en casos de compromiso de su clave privada.

30.7 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

30.8 INDEMNIZACIÓN

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

30.9 NOTIFICACIONES

Los medios de notificación serán definidos en los contratos de titulares y suscriptores.

30.10 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.

30.11 RESOLUCIÓN DE DISPUTAS

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

30.12 CONFORMIDAD CON LA LEY APLICABLE

La ER de LLEIDANET PKI SUCURSAL DE PERÚ se compromete a cumplir la ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

30.13 SUBROGACIÓN

La ER de LLEIDANET PKI SUCURSAL DE PERÚ no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes como las EC son especificados en este documento.

30.14 FUERZA MAYOR

Las cláusulas de fuerza mayor serán definidas en los contratos de los titulares.

30.15 DERECHOS DE PROPIEDAD INTELECTUAL

La ER de LLEIDANET PKI SUCURSAL DE PERÚ tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

30.16 APERTURA NUEVAS ER DE LLEIDANET PKI SUCURSAL DE PERÚ

La apertura de nuevas oficinas ER requerirá de evaluación de su viabilidad por parte de LLEIDANET PKI SUCURSAL DE PERÚ y de una posterior comunicación al INDECOPI de la apertura.

30.17 TERCERIZACIÓN

Las funciones de ER podrán ser tercerizadas. En este caso la ER de LLEIDANET PKI SUCURSAL DE PERÚ evaluará el cumplimiento de sus políticas realizando evaluaciones internas que determinen su cumplimiento.

La tercerización no corresponde a la apertura de nuevas oficinas de ER.

Tal y como recoge la guía, la ER puede tercerizar las funciones de verificación y registro sin ningún límite ni restricción, siempre dejando claro que el responsable final es la ER, siempre que se asegure la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión (lo cual se realiza a través de nuestra plataforma de PKI), tal y como recoge el punto 14, del numeral 1.2.1. “En caso de tercerizar las funciones de registro, las responsabilidades de los terceros deberán ser claramente definidas en la RPS. Sin embargo, la responsabilidad legal frente a la IOFE, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro. La Entidad de Registro debe garantizar la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión, durante la ejecución de las actividades de tercerización, quedando claro que ante la IOFE el responsable ante terceros es la ER.”

Cabe indicar que LLEIDANET PKI SUCURSAL DE PERÚ suministra al tercero la Plataforma de ER para la creación de la solicitud y la emisión de los certificados, asegurando la integridad en todo el proceso, accediendo a la plataforma pki.esigna.es/PortaEmpleado con el certificado digital del operador. La verificación de la identidad se hace en un portal proporcionado por terceros, véase RENIEC, SUNAT o SUNARP, con lo que es responsabilidad de los terceros que hacen el proceso de verificación acceder a dichos entornos, ya que además no es LLEIDANET PKI SUCURSAL DE PERÚ la que los suministros. Si dichos

accesos implican la firma de un convenio con esas entidades, será el tercero el responsable de disponer y mantener dicho convenio.

31 FINALIZACIÓN DE LA ER DE LLEIDANET PKI SUCURSAL DE PERÚ

Antes de su finalización, la ER de LLEIDANET PKI SUCURSAL DE PERÚ informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al INDECOPI o a otro PSC designado por éste.

En caso de una operación de transferencia de titularidad, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los requisitos de acreditación.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una EC que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección: https://www.lleida.net/es/politicas-y-practicas?tab=peru

32 CONFORMIDAD

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

33 BIBLIOGRAFÍA

(1) Guía de Acreditación de Entidades de Registro o Verificación, INDECOPI
(2) Ley de Firmas y Certificados Digitales –Ley 27269
(3) Decreto Supremo 052-2008
(4) Decreto Supremo 070-2011