Proyecto	**Prestador de Servicios de Confianza**
Título	**Declaración de Prácticas Certificación de Lleidanet PKI S.L.**

Realizado por	**LLEIDANET PKI S.L.**		
Dirigido a	**Público**		
Documento	**DOC-201112.20C1715**		
Fecha aprobación	**22/05/2025**	Revisión	**18**

Firmado por: Raul Gisbert Rodas
Fecha firma: 22/05/2025 16:25:14 CEST

Firmado por: PASCUAL FERRER PONCE
Fecha firma: 22/05/2025 21:07:32 CEST

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

Firmado por: JORDI GISBERT RODAS
Fecha firma: 23/05/2025 15:01:52 CEST

Els Traginers, 14 - 2°B
Pol. Ind. Vara de Quart
46014 Valencia
Tel. (34) 96 381 99 47
Fax (34) 96 381 99 48
info@lleida.net
www.lleida.net

1 DATOS DEL DOCUMENTO

Proyecto	Prestador de Servicios de Confianza
Título	Declaración de Prácticas Certificación de Lleidanet PKI S.L.
Código	DOC-201112.20C1715
Tipo de documento	DOC - Documento genérico
Clasificación del documento	Público
Realizado por	LLEIDANET PKI S.L.
Dirigido a	Público
Fecha aprobación	22/05/2025
Revisión	18

2 HISTORIA DEL DOCUMENTO

Revisión	Fecha	Motivo de la modificación	Responsable
1	17/12/2020	Creación del documento	Indenova S.L.
2	22/01/2021	Auditoria externa	Indenova S.L.
3	24/05/2021	Actualización del documento	Indenova S.L.
4	31/05/2021	Nueva ceremonia de claves de la PKI	Indenova S.L.
5	03/11/2021	Cambiar referencia a ley de firma por la referencia a la ley de servicios de confianza	Indenova S.L.
6	23/06/2022	Cambios relacionados con la adaptación de mecanismos de videoidentificacion adaptación ley 6/2020	Indenova S.L.

7	31/08/2022	Adaptar los mecanismos de video identificación adaptación ley 6/2020	Indenova S.L.U.
8	08/09/2022	Agregar nuevos perfiles	Indenova S.L.U.
9	24/10/2022	Debido al cambio en el control OVR-6.3.5-12 de la ETSI EN 319 411-2	Indenova S.L.U.
10	07/11/2022	Se modifica la redacción del párrafo que hace mención a "... procedimiento de video-conferencia autorizado por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias..." quedando como "InDenova SL dispone de un método de Video Identificación (videofirma de eSignaBox integrado con la solución eKYC de Lleida.net). Los certificados expedidos por esta vía no tendrán consideración de cualificados mientras no exista resolución favorable por parte del Organismo de Supervisión"	Indenova S.L.U.
11	09/06/2023	Se agrega el perfil de certificado Empleado Público con Seudónimo, también se cambia denominación de Indenova S.L.U. a Lleidanet PKI S.L. y se cambia eSigna ID por Lleida.net Wallet	Lleidanet PKI S.L.
12	04/08/2023	Se agrega apartado 4.9.3. Notificación al suscriptor. Agregar nota en el apartado 3.2.5 y 7.1 especificando lo que debe contener los perfiles de certificados que podrán ser utilizados para la identificación y firma de las personas interesadas ante las Administraciones Públicas.	Lleidanet PKI S.L.
13	03/10/2023	Actualizar los documentos requeridos al usuario al solicitar Certificado de Sello Electrónico	Lleidanet PKI S.L.
14	23/09/2024	Especificar la cantidad de días que es válida la videoidentificación que realiza el usuario	Lleidanet PKI S.L.
15	30/10/2024	Se agrega apartado acerca de los certificados de pruebas	Lleidanet PKI S.L.

16	10/12/2024	Especificar acerca de la vigencia del certificado en caso de existir dos certificados del mismo tipo para el mismo suscriptor	Lleidanet PKI S.L.
17	27/02/2025	Extraer a un documento externo, los documentos requeridos según el tipo de certificado solicitado por el suscriptor e indicar el enlace de donde se encuentran los documentos requeridos. Se actualizan los roles de confianza y los miembros de la comisión de seguridad de la información.	Lleidanet PKI S.L.
18	22/05/2025	Se actualiza el apartado de la custodia de la clave privada.	Lleidanet PKI S.L.

3 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Nombre: Compliance (CJ) Cargo: Responsable de calidad Fecha: 22/05/2025
Revisado por:	Nombre: SB Cargo: Administrador del Servicio Fecha: 22/05/2025
Aprobado por:	Nombre: Comisión de Seguridad de la Información (CSI) Cargo: Comisión de Seguridad de la Información Fecha: 22/05/2025

4 INTRODUCCIÓN

LLEIDANET PKI S.L. es una empresa trasnacional que nació con la 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 electrónicos, invirtiendo en el desarrollo e implantación de las mismas el 95% de su actividad.

Como Prestador de Servicios de Confianza, LLEIDANET PKI S.L. provee los servicios de emisión, re-emisión, distribución y revocación de certificados digitales, provistos por la EC de LLEIDANET PKI S.L., además, LLEIDANET PKI S.L. brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales, los cuales son provistos por la ER de LLEIDANET PKI S.L.

Como Autoridad de Sellado de Tiempo - TSA, LLEIDANET PKI S.L. provee los servicios de emisión de sellado de tiempo, utilizando una infraestructura periódicamente auditada para cumplir la certificación ISO 27001.

Como Prestador de Servicios de Valor añadido - SVA, LLEIDANET PKI S.L. provee servicios través de la implementación de soluciones que utilizan los certificados digitales para asegurar las transacciones documentarias y de negocio de las organizaciones tanto en el sector privado como en el gubernamental los cuales se podrían agrupar en dos servicios principales:

- La creación de firmas mediante sistemas de firma centralizada, en el cual LLEIDANET PKI S.L. gestiona en nombre del firmante su dispositivo de creación de firma permitiéndole generar firmas electrónicas cualificadas asegurando el control exclusivo del firmante sobre sus claves de firma, ya sea mediante mecanismos de autenticación (usuario y password), huella dactilar o mediante el uso de la APP móvil Lleida.net Wallet.

La validación de firmas electrónicas y custodia de dichos documentos en el servicio eSignaBox, permitiendo asegurar la validación a largo plazo de las firmas electrónicas incrustadas en el documento.

4.1 VISIÓN GENERAL

El alcance de la acreditación cubre la infraestructura, sistemas y procesos de los servicios de certificación que utiliza LLEIDANET PKI S.L. en la entrega de sus servicios, y que son proporcionados por la Entidad de Certificación LLEIDANET PKI S.L.

La Declaración de Practicas de Certificación (más adelante DPC), tiene como objeto la descripción de las operaciones y prácticas que utiliza LLEIDANET PKI S.L. para la administración de sus servicios como Prestador de Servicios de Confianza, en el marco del cumplimiento de los requerimientos del "Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014" o también como es conocido "Reglamento eIDAS" establecida por el Parlamento Europeo.

4.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre del documento	Declaración de Prácticas Certificación de Lleidanet PKI S.L.
Descripción del documento	Este documento se describe las operaciones y prácticas que utiliza LLEIDANET PKI S.L. para la administración de sus servicios como Prestador de Servicios de Confianza.
Versión	18
OID	1.3.6.1.4.1.49959.1.2.1
Localización	https://www.indenova.com/acreditaciones/eidas/

4.3 PARTES INTERVINIENTES

Las partes que intervienen en la gestión y uso de los Servicios de Confianza descritos en la presente DPC son las siguientes:

1. Autoridad de Certificación
2. Autoridad de Registro
3. Suscriptores o Titulares de los Certificados
4. Partes que confían
5. Otros participantes

4.3.1 Autoridad de Certificación

LLEIDANET PKI S.L., 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.

4.3.1.1 Certificados de Prueba

LLEIDANET PKI S.L., en su papel de Entidad de Certificación, puede emitir certificados de pruebas con datos ficticios. LLEIDANET PKI S.L. incluye en estos certificados solo la parte pública esto quiere decir que la parte privada no se comparte al solicitante, para que el solicitante pueda ver claramente que se trata de un certificado de pruebas sin garantía, los certificados de pruebas se generan con la siguiente información:

Número de Documento Nacional de Identidad (DNI): 00000000T

Número de Identidad de Extranjero (NIE): X0000000T, Y0000000R, Z0000000W

Nombre: Nombre

Primer apellido: Apellido1

Segundo apellido: Apellido2

4.3.2 Autoridad de Registro

LLEIDANET PKI S.L., 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.

Las funciones de ER podrán ser tercerizadas. En este caso la ER de LLEIDANET PKI S.L. evaluará el cumplimiento de sus políticas realizando evaluaciones internas que determinen su cumplimiento a dicho tercero.

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. Sin embargo, la responsabilidad legal frente al Organismo de supervisión, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro. El tercero 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 el Organismo de supervisión el responsable ante terceros es la ER.

Cabe indicar que LLEIDANET PKI S.L. 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 eSignaPKI con el certificado digital del operador.

En este siguiente enlace: https://www.indenova.com/acreditaciones/eidas/ se encuentran los perfiles de los certificados.

4.3.2.1 Certificados emitidos por la Autoridad de Registro

A continuación, se indican los certificados que son emitidos por la autoridad de Registro de LLEIDANET PKI S.L.

Nombre del certificado	OID	OID QCP	QCP
Políticas de Certificación Certificados de Persona Natural	1.3.6.1.4.1.49959.1.1.1		

Persona Natural Software	1.3.6.1.4.1.49959.1.1.1.1.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Persona Natural Hardware (qscd)	1.3.6.1.4.1.49959.1.1.1.2.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.1.3.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.1.3.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.1.3.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificados de Pertenencia a Empresa	1.3.6.1.4.1.49959.1.1.2		
Pertenencia a Empresa Software	1.3.6.1.4.1.49959.1.1.2.1.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Pertenencia a Empresa Hardware (qscd)	1.3.6.1.4.1.49959.1.1.2.2.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)

Pertenencia a Empresa Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.2.3.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Pertenencia a Empresa Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.2.3.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Pertenencia a Empresa Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.2.3.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificados Representante Legal	1.3.6.1.4.1.49959.1.1.3		
Persona Natural Representante Legal Software	1.3.6.1.4.1.49959.1.1.3.1.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Persona Natural Representante Legal Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.2.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Representante Legal Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.3.3.1	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Persona Natural Representante Legal	1.3.6.1.4.1.49959.1.1.3.3.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova

Centralizado UP (qscd)			SUB CA 003)
Persona Natural Representante Legal Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.3.3.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Sello Electrónico	1.3.6.1.4.1.49959.1.1.3.4		
Sello Electrónico Software	1.3.6.1.4.1.49959.1.1.3.4.1	0.4.0.194112.1.1	QCP-l-(inDenova SUB CA 003)
Sello Electrónico Hardware	1.3.6.1.4.1.49959.1.1.3.4.2	0.4.0.194112.1.3	QCP-l-qscd (inDenova SUB CA 003)
Sello Electrónico Lleida.net Wallet	1.3.6.1.4.1.49959.1.1.3.4.3	0.4.0.194112.1.3	QCP-l-qscd (inDenova SUB CA 003)
Sello Electrónico Centralizado UP	1.3.6.1.4.1.49959.1.1.3.4.4	0.4.0.194112.1.3	QCP-l-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Empleado Público	1.3.6.1.4.1.49959.1.1.3.5		
Empleado Público Software	1.3.6.1.4.1.49959.1.1.3.5.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)

Empleado Público Hardware	1.3.6.1.4.1.49959.1.1.3.5.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público Lleida.net Wallet	1.3.6.1.4.1.49959.1.1.3.5.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público Centralizado UP	1.3.6.1.4.1.49959.1.1.3.5.4	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público Centralizado Huella dactilar	1.3.6.1.4.1.49959.1.1.3.5.5	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Representante Legal Sin Personalidad Jurídica	1.3.6.1.4.1.49959.1.1.3.6		
Representante Legal Sin Personalidad Jurídica Software	1.3.6.1.4.1.49959.1.1.3.6.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Representante Legal Sin Personalidad Jurídica Hardware	1.3.6.1.4.1.49959.1.1.3.6.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Representante Legal Sin Personalidad	1.3.6.1.4.1.49959.1.1.3.6.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova

Jurídica Lleida.net Wallet			SUB CA 003)
Representante Legal Sin Personalidad Jurídica Centralizado UP	1.3.6.1.4.1.49959.1.1.3.6.4	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Representante Legal Sin Personalidad Jurídica Centralizado Huella dactilar	1.3.6.1.4.1.49959.1.1.3.6.5	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Políticas de Certificación Certificado de Empleado Público con Seudónimo	1.3.6.1.4.1.49959.1.1.3.7		
Empleado Público con Seudónimo Software	1.3.6.1.4.1.49959.1.1.3.7.1	0.4.0.194112.1.0	QCP-n (inDenova SUB CA 003)
Empleado Público con Seudónimo Hardware	1.3.6.1.4.1.49959.1.1.3.7.2	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público con Seudónimo Lleida.net Wallet	1.3.6.1.4.1.49959.1.1.3.7.3	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)
Empleado Público con Seudónimo Centralizado UP	1.3.6.1.4.1.49959.1.1.3.7.4	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)

Empleado Público con Seudónimo Centralizado Huella dactilar	1.3.6.1.4.1.49959.1.1.3.7.5	0.4.0.194112.1.2	QCP-n-qscd (inDenova SUB CA 003)

4.3.2.2 Descripción de los Certificados emitidos por la Autoridad de Registro

Nombre	OID	Descripción
Persona Natural		
Persona Natural Software	1.3.6.1.4.1.49959.1.1.1.1.1	Certificado que permite que una persona natural disponga de un certificado digital emitido en su ordenador y podrá utilizarlo con cualquier aplicación, entidad y administración pública de España, evitando así desplazamientos y esperas innecesarias. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con plenas garantías legales, es igual, en cuanto a validez, que tu firma manuscrita. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Hardware (qscd)	1.3.6.1.4.1.49959.1.1.1.2.1	Certificado que permite que una persona natural disponga de un certificado digital emitido en un dispositivo criptográfico cualificado (token o tarjeta criptográfica), lo que da mayor seguridad al uso y custodia del certificado, este dispositivo

		necesitará un dispositivo externo que permitirá hacerlo funcionar en el ordenador, con ello podrá acceder a cualquier entidad y administración pública de España, evitando así desplazamientos y esperas innecesarias. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con plenas garantías legales, es igual, en cuanto a validez, que tu firma manuscrita. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.1.3.1	Certificado que permite que una persona natural disponga de un certificado digital cualificado emitido en su teléfono móvil, para su uso desde las aplicaciones eSigna de LLEIDANET PKI S.L., tales como eSignaBox. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con plenas garantías legales, es igual, en cuanto a validez, que tu firma manuscrita. El certificado digital de Persona Natural Lleida.net Wallet (qscd) será emitido en el teléfono móvil del suscriptor del certificado y será este quien tenga uso exclusivo y acceso a las claves privadas del mismo. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados

		aspectos de los servicios electrónicos de confianza.
Persona Natural Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.1.3.2	Certificado que permite que una persona natural disponga de un certificado digital cualificado de firma centralizada con acceso al mismo mediante credenciales (usuario y contraseña) y un PIN que solo conoce el suscriptor. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con plenas garantías legales, es igual, en cuanto a validez, que tu firma manuscrita. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.1.3.3	Certificado que permite que una persona natural disponga de un certificado digital cualificado de firma centralizada con acceso al mismo mediante su huella dactilar y un PIN que solo conoce el suscriptor. Mediante dicho certificado podrá realizar operaciones de autenticación y firmar digitalmente documentos con plenas garantías legales, es igual, en cuanto a validez, que tu firma manuscrita. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Perteneciente a Empresa		

Pertenencia a Empresa Software	1.3.6.1.4.1.49959.1.1.2.1.1	Es un certificado que identifica digitalmente a una persona física y la vincula a una organización o entidad informando el cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación. El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación. El certificado digital será emitido en el ordenador del suscriptor, con lo que podrá utilizarlo con cualquier aplicación, entidad y administración pública de España, evitando así desplazamientos y esperas innecesarias. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Pertenencia a Empresa Hardware (qscd)	1.3.6.1.4.1.49959.1.1.2.2.1	Es un certificado cualificado que identifica digitalmente a una persona física y la vincula a una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación.

		El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación. El certificado digital será emitido en un dispositivo criptográfico cualificado (token o tarjeta criptográfica), lo que da mayor seguridad al uso y custodia del certificado, este dispositivo necesitará un dispositivo externo que permitirá hacerlo funcionar en el ordenador, con lo que podrá utilizarlo con cualquier aplicación, entidad y administración pública de España, evitando así desplazamientos y esperas innecesarias. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Pertenencia a Empresa Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.2.3.1	Es un certificado cualificado que identifica digitalmente a una persona física y la vincula a una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su

		actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación. El certificado digital será emitido en el smartphone del suscriptor del certificado y será este quien tenga uso exclusivo y acceso a las claves privadas del mismo. Pueden obtener más información de la aplicación eSigna ID (disponible para iOS y Android) en https://www.esignaid.com/ USABILIDAD Lleida.net Wallet facilita el proceso de identificación y firma mediante el uso del teléfono móvil, eliminando las complicaciones de los certificados digitales. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Pertenencia a Empresa Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.2.3.2	Es un certificado cualificado que identifica digitalmente a una persona física y la vincula a una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación. El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales,

		ya que no informa de la existencia de poderes de representación. El certificado digital será de firma centralizada con acceso al mismo mediante credenciales (usuario y contraseña) y un PIN que solo conoce el suscriptor. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza
Pertenencia a Empresa Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.2.3.3	Es un certificado cualificado que identifica digitalmente a una persona física y la vincula a una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación. El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación. El certificado digital será de firma centralizada con acceso al mismo mediante su huella dactilar y un PIN que solo conoce el suscriptor. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley

		Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Representante Legal		
Persona Natural Representante Legal Software	1.3.6.1.4.1.49959.1.1.3.1.1	Certificado que permite que una persona natural ostente la condición de representante legal con poderes generales, de una organización y disponga de un certificado digital emitido para instalarlo en su computador y que pueda utilizarlo en cualquier aplicación o entidad de la UE. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Representante Legal Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.2.1	Certificado cualificado que permite que una persona jurídica ostente la condición de representante legal con poderes generales sin limitaciones, de una organización y disponga de un certificado digital emitido en un dispositivo criptográfico cualificado (token o tarjeta criptográfica) lo que da mayor seguridad al uso y custodia del certificado, este dispositivo necesitará un dispositivo externo que permitirá hacerlo funcionar en el ordenador. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Representante Legal	1.3.6.1.4.1.49959.1.1.3.3.1	Certificado cualificado que permite que una persona jurídica ostente la condición

Lleida.net Wallet (qscd)		de representante legal con poderes generales sin limitaciones, de una organización y disponga de un certificado digital emitido en su smartphone para su uso desde las aplicaciones eSigna de LLEIDANET PKI S.L., como eSignaBox. El certificado digital de Persona Jurídica Representante Legal (Lleida.net Wallet) será emitido en el smartphone del suscriptor del certificado y será este quien tenga uso exclusivo y acceso a las claves privadas del mismo. Pueden obtener más información de la aplicación eSigna ID (disponible para iOS y Android) en Más información de Lleida.net Wallet. USABILIDAD Lleida.net Wallet facilita el proceso de identificación y firma mediante el uso del smartphone, eliminando las complicaciones de los certificados digitales. SEGURIDAD La tecnología de Lleida.net Wallet ofrece una alta seguridad en todo el proceso, empleando mecanismos de autenticación de doble factor, protegiendo las comunicaciones mediante SSL y encriptado de información a nivel de aplicación y servidor. GARANTÍAS LEGALES La identidad digital y los procesos realizados con Lleida.net Wallet cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Persona Natural Representante Legal	1.3.6.1.4.1.49959.1.1.3.3.2	Certificado cualificado que permite que una persona jurídica ostente la condición de representante legal con poderes generales sin limitaciones, de una

Centralizado UP (qscd)		organización y disponga de un certificado digital de firma centralizada. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza
Persona Natural Representante Legal Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.3.3.3	Certificado cualificado que permite que una persona jurídica ostente la condición de representante legal con poderes generales sin limitaciones, de una organización y disponga de un certificado digital de firma centralizada. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Sello Electrónico		
Sello Electrónico Software	1.3.6.1.4.1.49959.1.1.3.4.1	Este certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas sin que sea necesario la incorporación de los datos de un representante. Representa inequívocamente a la entidad a la que se ha expedido el certificado, incluyendo su denominación, localidad y número de identificación fiscal – N.I.F. El certificado de sello tiene una configuración flexible que permite diferentes usos: Sellos electrónicos para garantizar, mediante firma electrónica, la autenticidad e integridad de los

		documentos electrónicos a los que están vinculados. Autenticación de componentes informáticos de una entidad en su acceso a servicios informáticos o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Sello Electrónico Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.4.2	Este certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas Representa inequívocamente a la entidad a la que se ha expedido el certificado, incluyendo su denominación, localidad y número de identificación fiscal – N.I.F. El certificado de sello tiene una configuración flexible que permite diferentes usos: Sellos electrónicos para garantizar, mediante firma electrónica, la autenticidad e integridad de los documentos electrónicos a los que están vinculados Autenticación de componentes informáticos de una entidad en su acceso a servicios informáticos o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente

		GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Sello Electrónico Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.3.4.3	Este certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas Representa inequívocamente a la entidad a la que se ha expedido el certificado, incluyendo su denominación, localidad y número de identificación fiscal – N.I.F. El certificado de sello tiene una configuración flexible que permite diferentes usos: Sellos electrónicos para garantizar, mediante firma electrónica, la autenticidad e integridad de los documentos electrónicos a los que están vinculados Autenticación de componentes informáticos de una entidad en su acceso a servicios informáticos o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.

Sello Electrónico Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.3.4.4	Este certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas Representa inequívocamente a la entidad a la que se ha expedido el certificado, incluyendo su denominación, localidad y número de identificación fiscal – N.I.F. El certificado de sello tiene una configuración flexible que permite diferentes usos: Sellos electrónicos para garantizar, mediante firma electrónica, la autenticidad e integridad de los documentos electrónicos a los que están vinculados Autenticación de componentes informáticos de una entidad en su acceso a servicios informáticos o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Empleado Público		
Empleado Público Software	1.3.6.1.4.1.49959.1.1.3.5.1	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor.

		Firma digital sin poderes de representación El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Empleado Público Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.5.2	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones

		del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Empleado Público Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.3.5.3	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación El certificado digital será emitido en el smartphone del suscriptor del certificado y será este quien tenga uso exclusivo y acceso a las claves privadas del mismo. Pueden obtener más información de la aplicación eSigna ID (disponible para iOS y Android) en Más información de Lleida.net Wallet USABILIDAD Lleida.net Wallet facilita el proceso de identificación y firma mediante el uso del smartphone, eliminando las complicaciones de los certificados digitales

		SEGURIDAD La tecnología de Lleida.net Wallet ofrece una alta seguridad en todo el proceso, empleando mecanismos de autenticación de doble factor, protegiendo las comunicaciones mediante SSL y encriptado de información a nivel de aplicación y servidor GARANTÍAS LEGALES La identidad digital y los procesos realizados con Lleida.net Wallet cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española en materia de firma electrónica
Empleado Público Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.3.5.4	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley

		Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Empleado Público Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.3.5.5	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella, ya sea empleado, asociado, colaborador, cliente o proveedor. Firma digital sin poderes de representación El certificado permite a su titular realizar comunicaciones firmadas digitalmente acreditando su pertenencia a una determinada organización, pero no le otorgan ningún poder superior al que tiene por el desempeño habitual de su actividad. No está indicado para apoderados ni representantes generales, ya que no informa de la existencia de poderes de representación GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Representante Legal Sin Personalidad Jurídica		
Representante Legal Sin Personalidad Jurídica Software	1.3.6.1.4.1.49959.1.1.3.6.1	Certificado que permite que una persona natural ostente la condición de representante legal sin personalidad jurídica de una organización y disponga de un certificado digital emitido para instalarlo en su computador y que pueda

		utilizarlo en cualquier aplicación o entidad de la UE. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Representante Legal Sin Personalidad Jurídica Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.6.2	Certificado que permite que una persona natural ostente la condición de representante legal sin personalidad jurídica de una organización y disponga de un certificado digital emitido en un token o tarjeta criptográfica. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española en materia de firma electrónica
Representante Legal Sin Personalidad Jurídica Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.3.6.3	Certificado que permite que una persona natural ostente la condición de representante legal sin personalidad jurídica de una organización y disponga de un certificado digital emitido en su smartphone para su uso desde las aplicaciones eSigna de LLEIDANET PKI S.L., como eSignaBox. El certificado digital de Persona Jurídica Representante Legal sin personalidad jurídica (Lleida.net Wallet) será emitido en el smartphone del suscriptor del certificado y será este quien tenga uso exclusivo y acceso a las claves privadas del mismo. Pueden obtener más información de la aplicación eSigna ID

		(disponible para iOS y Android) en Más información de Lleida.net Wallet USABILIDAD Lleida.net Wallet facilita el proceso de identificación y firma mediante el uso del smartphone, eliminando las complicaciones de los certificados digitales SEGURIDAD La tecnología de Lleida.net Wallet ofrece una alta seguridad en todo el proceso, empleando mecanismos de autenticación de doble factor, protegiendo las comunicaciones mediante SSL y encriptado de información a nivel de aplicación y servidor GARANTÍAS LEGALES La identidad digital y los procesos realizados con Lleida.net Wallet cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española en materia de firma electrónica
Representante Legal Sin Personalidad Jurídica Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.3.6.4	Certificado que permite que una persona natural ostente la condición de representante legal sin personalidad jurídica de una organización y disponga de un certificado digital de firma centralizada. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española en materia de firma electrónica

Representante Legal Sin Personalidad Jurídica Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.3.6.5	Certificado que permite que una persona natural ostente la condición de representante legal sin personalidad jurídica de una organización y disponga de un certificado digital de firma centralizada. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española en materia de firma electrónica
Empleado Público con Seudónimo		
Empleado Público con Seudónimo Software	1.3.6.1.4.1.49959.1.1.3.7.1	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella ocultando tras un alias la identidad real. El certificado permite a su titular firmar digitalmente sin mostrar datos como su NIF, o su nombre y apellidos. Cuidado porque el correo electrónico sí es un dato público en el certificado y, en consecuencia, es necesario facilitar una cuenta que no dé pistas de los datos personales de su propietario. Se trata de una acreditación digital que protege la identidad real del titular cuando es necesario (policías, inspectores de sanidad, etc). No pudiendo ser utilizado cuando realmente la identidad real debe conocerse. Por ejemplo, cuando el empleado se relaciona internamente con otra Administración. Para esos casos se utilizará un certificado de Empleado público convencional.

		GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.
Empleado Público con Seudónimo Hardware (qscd)	1.3.6.1.4.1.49959.1.1.3.7.2	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella ocultando tras un alias la identidad real. El certificado permite a su titular firmar digitalmente sin mostrar datos como su NIF, o su nombre y apellidos. Cuidado porque el correo electrónico sí es un dato público en el certificado y, en consecuencia, es necesario facilitar una cuenta que no dé pistas de los datos personales de su propietario. Se trata de una acreditación digital que protege la identidad real del titular cuando es necesario (policías, inspectores de sanidad, etc). No pudiendo ser utilizado cuando realmente la identidad real debe conocerse. Por ejemplo, cuando el empleado se relaciona internamente con otra Administración. Para esos casos se utilizará un certificado de Empleado público convencional. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.

Empleado Público con Seudónimo Lleida.net Wallet (qscd)	1.3.6.1.4.1.49959.1.1.3.7.3	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella ocultando tras un alias la identidad real. El certificado permite a su titular firmar digitalmente sin mostrar datos como su NIF, o su nombre y apellidos. Cuidado porque el correo electrónico sí es un dato público en el certificado y, en consecuencia, es necesario facilitar una cuenta que no dé pistas de los datos personales de su propietario. Se trata de una acreditación digital que protege la identidad real del titular cuando es necesario (policías, inspectores de sanidad, etc). No pudiendo ser utilizado cuando realmente la identidad real debe conocerse. Por ejemplo, cuando el empleado se relaciona internamente con otra Administración. Para esos casos se utilizará un certificado de Empleado público convencional. USABILIDAD Lleida.net Wallet facilita el proceso de identificación y firma mediante el uso del smartphone, eliminando las complicaciones de los certificados digitales SEGURIDAD La tecnología de Lleida.net Wallet ofrece una alta seguridad en todo el proceso, empleando mecanismos de autenticación de doble factor, protegiendo las comunicaciones mediante SSL y encriptado de

		información a nivel de aplicación y servidor GARANTÍAS LEGALES La identidad digital y los procesos realizados con Lleida.net Wallet cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española en materia de firma electrónica
Empleado Público con Seudónimo Centralizado UP (qscd)	1.3.6.1.4.1.49959.1.1.3.7.4	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella ocultando tras un alias la identidad real. El certificado permite a su titular firmar digitalmente sin mostrar datos como su NIF, o su nombre y apellidos. Cuidado porque el correo electrónico sí es un dato público en el certificado y, en consecuencia, es necesario facilitar una cuenta que no dé pistas de los datos personales de su propietario. Se trata de una acreditación digital que protege la identidad real del titular cuando es necesario (policías, inspectores de sanidad, etc). No pudiendo ser utilizado cuando realmente la identidad real debe conocerse. Por ejemplo, cuando el empleado se relaciona internamente con otra Administración. Para esos casos se utilizará un certificado de Empleado público convencional. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados

		aspectos de los servicios electrónicos de confianza.
Empleado Público con Seudónimo Centralizado Huella dactilar (qscd)	1.3.6.1.4.1.49959.1.1.3.7.5	Es un certificado que identifica digitalmente a una persona física y la vincula una organización o entidad informando del cargo que desempeña en ella ocultando tras un alias la identidad real. El certificado permite a su titular firmar digitalmente sin mostrar datos como su NIF, o su nombre y apellidos. Cuidado porque el correo electrónico sí es un dato público en el certificado y, en consecuencia, es necesario facilitar una cuenta que no dé pistas de los datos personales de su propietario. Se trata de una acreditación digital que protege la identidad real del titular cuando es necesario (policías, inspectores de sanidad, etc). No pudiendo ser utilizado cuando realmente la identidad real debe conocerse. Por ejemplo, cuando el empleado se relaciona internamente con otra Administración. Para esos casos se utilizará un certificado de Empleado público convencional. GARANTÍAS LEGALES La identidad digital y los procesos realizados cumplen con las disposiciones del reglamento eIDAS, así como la Ley Española reguladora de determinados aspectos de los servicios electrónicos de confianza.

4.3.3 Suscriptores o Titulares de los Certificados

El Suscriptor o el titular del certificado es la persona natural a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos publicados en la DPC de LLEIDANET PKI S.L.

Es el 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.

4.3.4 Partes que confían

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la EC LLEIDANET PKI S.L. a un titular. El Tercero que confía, a su vez puede ser o no titular.

4.3.5 Otros participantes

4.3.5.1 Autoridad de sellado de tiempo

LLEIDANET PKI S.L., en su papel de Autoridad de Sellado de Tiempo, es la persona jurídica privada que presta indistintamente servicios de emisión de sellados de tiempo.

4.3.5.2 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación LLEIDANET PKI S.L., 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 S.L.son provistos por la Entidad de Certificación LLEIDANET PKI S.L.

4.3.5.3 PROVEEDOR DE SERVICIOS DE FIRMA CENTRALIZADA Y SERVICIO CUALIFICADO DE VALIDACIÓN DE FIRMAS Y SELLOS (LLEIDANET PKI S.L.)

LLEIDANET PKI S.L. actúa como proveedor del servicio de aplicación de firma centralizada (SSASP) y del servicio de validación de firmas y sellos electrónicos y no delega ninguna parte del servicio a entidades terceras.

4.3.5.4 COMITÉ DE SEGURIDAD

El comité de seguridad es un organismo interno de la Entidad de Certificación LLEIDANET PKI S.L., conformado por el Director de Nuevos Productos, el Administrador del Sistema, Director Técnico y el Responsable del SGSI y tiene entre otras funciones la aprobación de la DPC como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la DPC aprobada y autorizar su publicación. El Comité de Seguridad es el responsable de integrar la DPC, a la DPC de terceros prestadores de servicios de certificación.

4.4 USO DE LOS CERTIFICADOS

4.4.1 Usos adecuados del certificado

Los usos adecuados de los Certificados emitidos se encuentran especificado en la Política de Certificación de LLEIDANET PKI S.L.

Los Certificados emitidos indicados en el apartado 4.3.2.1 Certificados emitidos por la Autoridad de Registro bajo esta DPC 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 ser 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.
- Cifrado asimétrico o mixto, basado en certificados X.509v3

4.4.2 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 DPC y concretamente en las Políticas de Certificación.

Se consideran indebidos aquellos usos que no están definidos en esta DPC y en consecuencia para efectos legales, LLEIDANET PKI S.L. 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 DPC.

No se podrán emplear los Certificados de entidad final expedidos por LLEIDANET PKI S.L. para:

- Firmar o sellar otro Certificado, salvo supuestos expresamente autorizados previamente.
- Firmar o sellar software o componentes a excepción de los Certificados de componente de firma de código
- Generar sellos de tiempo para procedimientos de Fechado electrónico a excepción de los Certificados expedidos por LLEIDANET PKI S.L. para Unidades de Sellado de Tiempo.

4.5 ADMINISTRACIÓN DE LAS POLÍTICAS

4.5.1 Entidad responsable

LLEIDANET PKI S.L., con CIF B97458996, es la Autoridad de Certificación que expide los certificados a los que aplica esta DPC.

4.5.2 Datos de contacto

Los datos de contacto de LLEIDANET PKI S.L., como Prestador de Servicios de Confianza es la siguiente:

Dirección: Carrer Dels Traginers, 14 - 2° B C.P 46014, Valencia, España
Tel: (+34) 96 381 99 47
Correo electrónico: consultas@indenova.com
Página Web: www.indenova.com

Para informar problemas de seguridad, tales como sospecha de compromiso clave, uso indebido de certificados, fraude u otros asuntos, comuníquese con consultas@indenova.com

4.5.3 Responsables de adecuación de la DPC

La Comisión de Seguridad de LLEIDANET PKI S.L. dispone, dentro de sus competencias, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento, tanto para la presente

Declaración de Prácticas de Certificación, como para las Prácticas de Certificación Particulares y la Política de Certificación correspondiente.

4.5.4 Procedimiento de gestión del documento

La publicación de las revisiones de esta DPC deberá estar aprobada por la Comisión de Seguridad.

LLEIDANET PKI S.L. publica en su página web https://www.indenova.com/acreditaciones/eidas/ cada nueva versión de la DPC la cual se encuentra en formato PDF.

4.6 DEFINICIONES Y ACRÓNIMOS

4.6.1 Definiciones

Entidad de Certificación - EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la legislación vigente.
Entidad de Registro - ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y registro de los solicitantes del certificado.
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 S.L. y que está de acuerdo con los términos y condiciones publicados en la https://www.indenova.com/acreditaciones/eidas/ de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

4.6.2 Acrónimos

EC	Entidad de Certificación

ER	Entidad de Registro
TSA	Autoridad de Sellado de Tiempo
DPC	Declaración de Practicas de Certificación
OID	Identificador de Objeto
RRHH	Recursos Humanos
SGSI	Sistema de Gestión de Seguridad de la Información
QSCD	Qualified (electronic) Signature Creation Device - Dispositivo Cualificado de Creación de Firma

5 PUBLICACIÓN Y REPOSITORIO

5.1 REPOSITORIO

Los servicios de consulta están diseñados para garantizar una disponibilidad de 24 horas por día y durante los 7 días a la semana.

Certificado Raíz de servicios de LLEIDANET PKI S.L.

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

Certificado Subordinada LLEIDANET PKI S.L.

http://certs.esigna.es/ca/indenova_pki_003.crt

Lista de Certificados Revocados (CRL)

http://crl1.esigna.es/sub/indenova_pki_003.crl

http://crl.esigna.es/sub/indenova_pki_003.crl

Declaración de Prácticas de Certificación (DPC)

http://cps.esigna.es/sub/cps_sub003_ca.pdf

https://www.indenova.com/acreditaciones/eidas/

Validación de Certificados

http://ocsp2.esigna.es

5.2 PUBLICACIÓN DE INFORMACIÓN DEL CERTIFICADO

El Responsable de la EC de LLEIDANET PKI S.L. es el encargado de la publicación de la DPC y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web: https://www.indenova.com/acreditaciones/eidas/

La Lista de Certificados Revocados es publicada en la página web https://www.indenova.com/acreditaciones/eidas/ y está firmada digitalmente por la Entidad de Certificación LLEIDANET PKI S.L.

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

5.3 FRECUENCIA DE PUBLICACIÓN

Certificado Raíz

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

Certificado Subordinada

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

Lista de Certificados Revocados (CRL)

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

Declaración de Prácticas de Certificación (DPC)

Con autorización de la Comisión de seguridad de la Entidad de Certificación de LLEIDANET PKI S.L., se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán publicados en la página Web de La Entidad de Certificación LLEIDANET PKI S.L. junto con la nueva versión. La Auditoria anual validará estos cambios y emitirá el informe de cumplimiento.

Validación de Certificados

La Entidad de Certificación LLEIDANET PKI S.L. publicará los certificados emitidos en un repositorio en formato X.509 V3 los cuales podrán ser consultados en la dirección: http://ocsp2.esigna.es

5.4 CONTROL DE ACCESO A LOS REPOSITORIOS

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

6 IDENTIFICACIÓN Y AUTENTICACIÓN

6.1 NOMBRES

6.1.1 Tipos de nombres

El documento guía que LLEIDANET PKI S.L. 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 9594 (X.500).

Los certificados emitidos por LLEIDANET PKI S.L. 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.

6.1.1.1 Certificado raíz de LLEIDANET PKI S.L.

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

CN = Certification Authority Root Indenova SL
O = Indenova SL
SERIALNUMBER = B97458996
OU = Certification Authority Indenova SL
L = Valencia
C = ES

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

CN = Certification Authority Root Indenova SL
O = Indenova SL
SERIALNUMBER = B97458996
OU = Certification Authority Indenova SL
L = Valencia
C = ES

Número de serie = 1A 7D 8F CD 5A 36

Huella digital = 10 38 27 02 08 75 F6 49 87 10 4A 55 A4 66 C4 5F E6 F6 B9 E4

SHA-256 = 148D7812AB418CC6D14D8CA9F36F89DFCCA09D8D77A2412E23EF85F6A5B594A1

6.1.1.2 Certificados de las Subordinadas DE LLEIDANET PKI S.L.

El DN del 'issuer name' de los certificados de las subordinadas de LLEIDANET PKI S.L., tiene las siguientes características:

CN = Certification Authority Root Indenova SL
O = Indenova SL
SERIALNUMBER = B97458996
OU = Certification Authority Indenova SL
L = Valencia
C = ES

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

Description = inDenova Subordinate CA 003
CN = inDenova SUB CA 003
O = inDenova SL
2.5.4.97 = VATES-B97458996
SERIALNUMBER = B97458996
OU = Certification Authority inDenova SL
T = Subordinate Certificate Authority inDenova SL
L = VALENCIA
C = ES

Número de serie = 10 F6 92 0D 39 D8

Huella digital = 71 CB FC 67 33 EA C7 01 CC 74 A5 42 54 81 68 BF 30 AD FB A4

SHA-256 = FA9E1D4C06906C436FA790F03E684258C74D7987B59F94133788E138AEF0D91A

6.1.1.3 CERTIFICADOS DE TITULAR DE LLEIDANET PKI S.L.

El DN del 'issuer name' de los certificados de titular de LLEIDANET PKI S.L., tiene las siguientes características generales:

Description = inDenova Subordinate CA 003
CN = inDenova SUB CA 003
O = inDenova SL
2.5.4.97 = VATES-B97458996
SERIALNUMBER = B97458996
OU = Certification Authority inDenova SL
T = Subordinate Certificate Authority inDenova SL
L = VALENCIA
C = ES

La descripción y los campos en el DN del 'subject name', para cada tipo de certificado cubiertos por esta DPC, están detallados en el documento DOC-200216.2093009 - Perfiles Certificados.pdf.

6.1.2 Significado de los NOMBRES

Todos los Nombres Distinguidos son significativos, y la identificación de los atributos asociados al suscriptor debe ser en una forma legible por humanos. Ver 7.1.4 Formato de Nombres y documento de Política de Certificación.

6.1.3 Anonimato o pseudónimos de suscriptores

LLEIDANET PKI S.L. utilizará el Seudónimo en el atributo CN del nombre del Sujeto/Firmante guardando confidencialmente la identidad real del Sujeto/Firmante. El cálculo del seudónimo en aquellos certificados donde se permita se realiza de manera que se identifica unívocamente al titular real del certificado.

6.1.4 Reglas utilizadas para interpretar varios formatos de nombres

LLEIDANET PKI S.L. 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 9594.

6.1.5 Unicidad de los NOMBRES

Dentro de una misma AC no se puede volver a asignar un nombre de sujeto/Firmante que ya haya sido ocupado, a un sujeto/Firmante diferente, esto se consigue incorporando el identificador fiscal único a la cadena del nombre que distingue al titular del certificado.

Bajo esta CPS un Firmante persona física puede pedir más de un certificado siempre que la combinación de los siguientes valores en la solicitud sea diferente:

- CIF
- DNI-Tarjeta de residente.
- Tipo de certificado: Identificador de política.
- También puede considerarse un certificado diferente cuando la posición, atributo título (title) o departamento, en el campo titular del certificado sea diferente.

6.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos

LLEIDANET PKI S.L.no asume compromisos en la emisión de certificados respecto al uso de marcas y otros signos distintivos.

LLEIDANET PKI S.L.no permite deliberadamente el uso de un signo distintivo sobre el Sujeto/Firmante que no ostente derechos de uso.

Sin embargo, LLEIDANET PKI S.L.no está obligada a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados, por lo que puede negarse a generar o solicitar la revocación de cualquier certificado involucrado en una disputa

6.1.7 Procedimiento de resolución de disputas de nombres

LLEIDANET PKI S.L. no tiene responsabilidad en el caso de resolución de disputas de nombres. En todo caso, la asignación de nombres se realizará basándose en su orden de entrada. LLEIDANET PKI S.L. no arbitra este tipo de disputas que deberán ser resueltas directamente por las partes

6.2 VALIDACIÓN INICIAL DE LA IDENTIDAD

6.2.1 Método para demostrar la posesión de la clave privada

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

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

6.2.2 Autenticación de la identidad de una organización (persona jurídica)

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.[1]

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:

De manera presencial:

- En el caso de empresas con domicilio en España, la existencia y vigencia de la persona jurídica deberá acreditarse con el certificado[2] o consulta electrónica de vigencia emitidos por los Registros Públicos, la citada verificación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.
- En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado[3] de vigencia de la sociedad u otro instrumento equivalente o consulta en línea expedida por la autoridad competente en su país de origen.

De manera telemática:

- Según lo indicado en el artículo 5.4 de la "Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados", se podrá, a partir de la fecha de notificación de la

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

[2] La vigencia del certificado presentado no debe ser mayor de 15 días.

[3] La vigencia del certificado no debe ser mayor de 15 días.

resolución favorable por parte del Organismo de supervisión, realizar la acreditación del solicitante de manera telemática mediante el sistema de video identificación o verificación biométrica facial utilizado por LLEIDANET PKI S.L. de acuerdo a los métodos de identificación reconocidos a escala nacional para la expedición de certificados cualificados, de conformidad con el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, mientras no exista resolución favorable los certificados que sean emitidos por esta vía no serán cualificados.

- Se verificará la acreditación del representante legal con la solicitud de los instrumentos públicos indicados para cuando se realiza de manera presencial.

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 o consulta a la base de datos respectiva.

6.2.3 Autenticación de la identidad de la persona física solicitante

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

De manera presencial:

- Se acreditará mediante el documento nacional de identidad, pasaporte, tarjeta de residencia, TIE u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

De manera telemática:

- El Solicitante puede optar alternativamente por personarse ante un Notario y aportar la solicitud de expedición del certificado con su firma legitimada en presencia notarial.
- Por medio de otro certificado cualificado expedido por la CA de LLEIDANET PKI S.L. o por otra CA, para el cual se hubiese empleado la personación física o un medio de identificación electrónica notificado, para la identificación del Solicitante, siempre y cuando conste al Prestador que la personación se produjo hace menos de cinco años.
- Utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad.
- Según lo indicado en el artículo 5.4 de la “Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados”, se podrá, a partir de la fecha de notificación de la resolución favorable por parte del Organismo de supervisión, realizar la acreditación del solicitante de manera telemática mediante el sistema de video identificación o verificación biométrica facial utilizado por Indenova de acuerdo a los métodos de identificación reconocidos a escala nacional para la expedición de certificados cualificados, de

conformidad con el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, mientras no exista resolución favorable los certificados que sean emitidos por esta vía no serán cualificados

- Se verificará la acreditación del solicitante con los documentos indicados para cuando se realiza de manera presencial.

LLEIDANET PKI S.L. dispone de un método de Video Identificación (videofirma de eSignaBox integrado con el producto que se encuentra publicado en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (Guía de Seguridad de las TIC CCN-STIC-105) publicado por el Centro Criptológico Nacional).

Breve descripción de la videofirma:

- Requiere que los Solicitantes estén equipados con un dispositivo con acceso a internet (PC, Tablet, smartphone, etc.), una cámara y un sistema de sonido.

- El Operador envía al solicitante un enlace para que éste acceda a que se le grabe su imagen durante la sesión e indique un código de operación único que vincula de forma única la solicitud de certificado que está realizando, además de mostrar su documento de identidad.

- El Operador procederá a la validación de la prueba de vida del Solicitante y el reconocimiento facial coincidiendo con el Documento de identidad, realizando las siguientes revisiones:

  - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
  - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota
  - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
  - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
  - Documentación que acredite su representación.

- Todo el proceso se graba para poder ser auditado.

- Los datos de registro, es decir los archivos de audio y video y metadatos estructurados en formato electrónico, se almacenan de forma protegida y de acuerdo con la norma europea sobre protección de datos personales.

La recopilación y validación del titular se realizará por la misma persona, con perfil de Operador ER que emitirá el certificado posteriormente.

6.2.4 Información no verificada del Suscriptor

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

6.2.5 Validación de la Autoridad

La documentación requerida de acuerdo al tipo de certificado se encuentra en el siguiente documento: DOC-201112.24A2415_Documentos_solicitados_a_usuarios.pdf al cual se puede acceder a través del siguiente enlace:

https://descargas.indenova.net/calidad/www.indenova.com/eIDAS/DOC-201112.24A2415_Documentos_solicitados_a_usuarios.pdf

De acuerdo al artículo 27.1 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos establece que "Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca."

NOTA: Aquellos perfiles de certificados que no contengan al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal no podrán ser utilizados para la identificación y firma de las personas interesadas ante las Administraciones Públicas[4]

6.2.6 Criterios para la Interoperabilidad

LLEIDANET PKI S.L. puede proporcionar servicios que permitan que otra CA opere dentro de, o interopere con, su PKI. Dicha interoperación puede incluir certificación cruzada, certificación unilateral u otras formas de operación. LLEIDANET PKI S.L. se reserva el derecho de proporcionar servicios de interoperación e interoperar con otras CA; los términos y criterios de los cuales deben establecerse contractualmente.

[4] Administraciones Públicas en el ámbito subjetivo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

6.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES

6.3.1 Identificación y autenticación de las solicitudes rutinarias de renovación

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

Los procedimientos de autenticación son descritos en el apartado 6.2 Validación inicial de la identidad de este mismo documento.

6.3.2 Identificación y autenticación de la solicitud de renovación tras una revocación

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

Los procedimientos de autenticación son descritos en el apartado 6.2 Validación inicial de la identidad de este mismo documento.

6.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Tras la solicitud de revocación debe autenticarse la identidad a los solicitantes.

Para los suscriptores deben presentar en la ER el documento nacional de identidad, pasaporte, tarjeta de residencia, TIE u otros medios admitidos en derecho.

El representante asignado por la persona jurídica debe presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica para lo cual deberá acreditarse con el certificado[5] o consulta electrónica de vigencia emitidos por los Registros Públicos, la citada verificación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos

[5] La vigencia del certificado presentado no debe ser mayor de 15 días.

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.

7 REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

7.1 SOLICITUD DE CERTIFICADOS

LLEIDANET PKI S.L. emplea para la gestión del ciclo de vida de los certificados su Plataforma. Esta Plataforma permite la solicitud, registro, publicación, revocación de todos los certificados emitidos.

7.1.1 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 S.L.
- De manera presencial en las instalaciones del cliente, o un lugar asignado por este en presencia de un representante de la ER.
- Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial
- Según lo indicado en el artículo 5.4 de la "Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados", se podrá, a partir de la fecha de notificación de la resolución favorable por parte del Organismo de supervisión, realizar la acreditación del solicitante de manera telemática mediante el sistema de video identificación o verificación biométrica facial utilizado por LLEIDANET PKI S.L. de acuerdo a los métodos de identificación reconocidos a escala nacional para la expedición de certificados cualificados, de conformidad con el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, mientras no exista resolución favorable los certificados que sean emitidos por esta vía no serán cualificados

7.1.2 Quién puede solicitar el certificado

Cualquier persona física o jurídica que cumpla los requisitos necesarios para el registro inicial indicados en el apartado 6.2 Validación inicial de la identidad de este documento y cuya solicitud se adapte a las políticas de certificados cubiertas por esta DPC.

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

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder. En este caso, el titular del certificado será el poderdante y corresponderá al apoderado la condición de suscriptor. El ámbito de utilización del certificado digital en este supuesto se encontrará circunscrito y limitado a las facultades expresamente conferidas en el poder.

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

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

Los procedimientos de solicitud según el tipo de titular son descritos en el apartado 6.2 Validación inicial de la identidad de este mismo documento.

7.1.3 Proceso de Registro y Responsabilidades

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

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

7.2 PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

La Entidad de Registro de LLEIDANET PKI S.L. puede emitir los siguientes certificados:

- Certificado de Persona Física en Software: Cuando el certificado digital se emite en un fichero p12 o pfx.
- Certificado de Persona Física en Hardware: Cuando la ER proporciona el módulo criptográfico.
- Certificado de Persona Física en Mobile: Cuando el certificado digital se emite en dispositivo móvil.
- Certificado de Persona Física en Servicio Centralizado con acceso mediante credenciales (usuario y contraseña): Cuando el certificado digital se emite sobre el servicio de firma

centralizada de la EC de LLEIDANET PKI S.L. y se generan unas credenciales de acceso al certificado para su uso.

- Certificado de Persona Física en Servicio Centralizado con acceso mediante datos biométricos (huella digital): Cuando el certificado digital se emite sobre el servicio de firma centralizada de la EC de LLEIDANET PKI S.L. y se genera el acceso al certificado mediante la huella digital del solicitante.

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/o telemática siempre y cuando cumpla con las condiciones y requisitos técnicos aplicables según lo indicado en el artículo 5.4 de la "Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados", se podrá, a partir de la fecha de notificación de la resolución favorable por parte del Organismo de supervisión, realizar la acreditación del solicitante de manera telemática mediante el sistema de video identificación o verificación biométrica facial utilizado por LLEIDANET PKI S.L. de acuerdo a los métodos de identificación reconocidos a escala nacional para la expedición de certificados cualificados, de conformidad con el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, mientras no exista resolución favorable los certificados que sean emitidos por esta vía no serán cualificados
- 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[6] y que tenga la certificación FIPS 140-2 nivel 3 o Common Criterial EAL 4+[7].
- 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.

[6] La plataforma de Registro solo reconoce los módulos con FIPS 140-2 nivel 3 mínimo o Common Criterial EAL 4+, de no ser así se detiene el proceso se informa al titular.

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

Para la emisión de certificados de forma 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 el envío 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[8] y que tenga la certificación FIPS 140-2 nivel 3 o Common Criterial EAL 4+[9].
- 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 del servicio.

7.2.1 Ejecución de las funciones de identificación y autenticación

La ejecución de las funciones de Identificación y autenticación están indicadas en el apartado 6.2 Validación inicial de la identidad.

7.2.2 Aprobación o rechazo de la solicitud del certificado

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

Igualmente, LLEIDANET PKI S.L. se reserva el derecho de no emitir certificados a pesar de que la identificación del solicitante y/o la información suministrada por este haya sido plenamente autenticada, cuando la emisión de un certificado en particular por razones de orden legal y/o de conveniencia comercial,

[8] La plataforma de Registro solo reconoce los módulos con FIPS 140-2 nivel 3 mínimo o Common Criterial EAL 4+, de no ser así se detiene el proceso se informa al titular.

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

buen nombre o reputación de EC de LLEIDANET PKI S.L. pueda poner en peligro el sistema de certificación digital.

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

- Se comunicará a la EC su aprobación para la emisión del certificado. Para ello se deben implementar los mecanismos de seguridad necesarios para establecer una comunicación segura entre la EC y la ER durante el proceso de emisión del certificado y generación del par de claves.

La ER de LLEIDANET PKI S.L. requerirá al suscriptor la firma de un contrato de conformidad personal de dichas responsabilidades, así como de conformidad por parte de los titulares en cuyo nombre actúa el suscriptor.

7.2.2.1 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 S.L., 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 suscriptor.

f) 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 S.L. 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 tiempo máximo de respuesta para la emisión del certificado será de cinco (5) días, luego de haber sido aprobada la validación de identidad el suscriptor tiene 15 días para realizar la instalación del certificado de lo contrario el suscriptor deberá enviar una nueva solicitud de certificado.

7.2.2.2 Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento y cuyo motivo del rechazo quedará registrada en la herramienta.

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

7.2.3 Tiempo para procesar la solicitud del certificado

Las solicitudes presentadas por la plataforma PKI de LLEIDANET PKI S.L. se validan una vez comprobada la documentación acreditativa asociado al perfil del certificado.

7.2.4 Coexistencia de dos certificados del mismo tipo y para el mismo usuario

LLEIDANET PKI S.L. permite coexistir dos certificados del mismo tipo para el mismo suscriptor, para lo cual, el certificado anterior tendrá una vigencia de 30 días.

7.3 EMISIÓN DEL CERTIFICADO

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

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

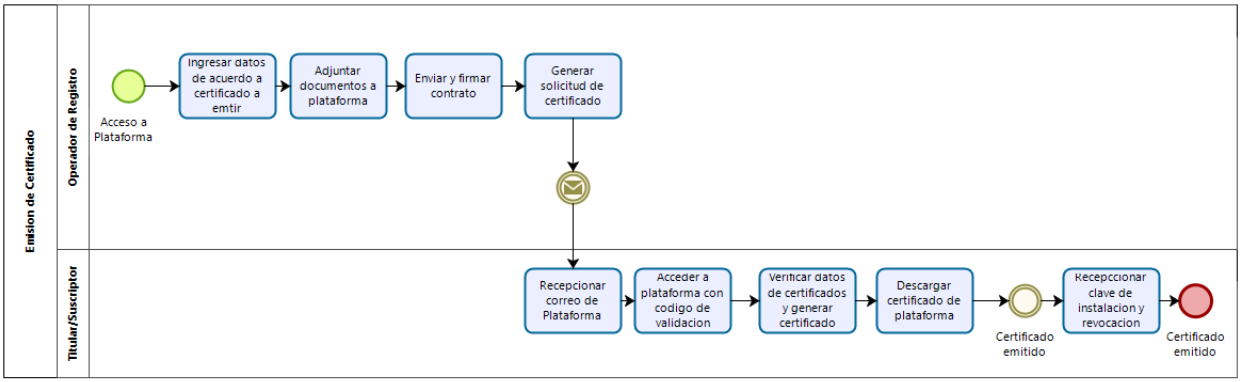
El certificado emitido se encuentra firmado digitalmente por el proveedor de servicios de certificación digital que lo emitió.

7.3.1 Acciones de la AC durante la emisión

La emisión del certificado será realizada según el medio seleccionado: software, hardware, mediante Lleida.net Wallet o en el servicio de firma centralizada.

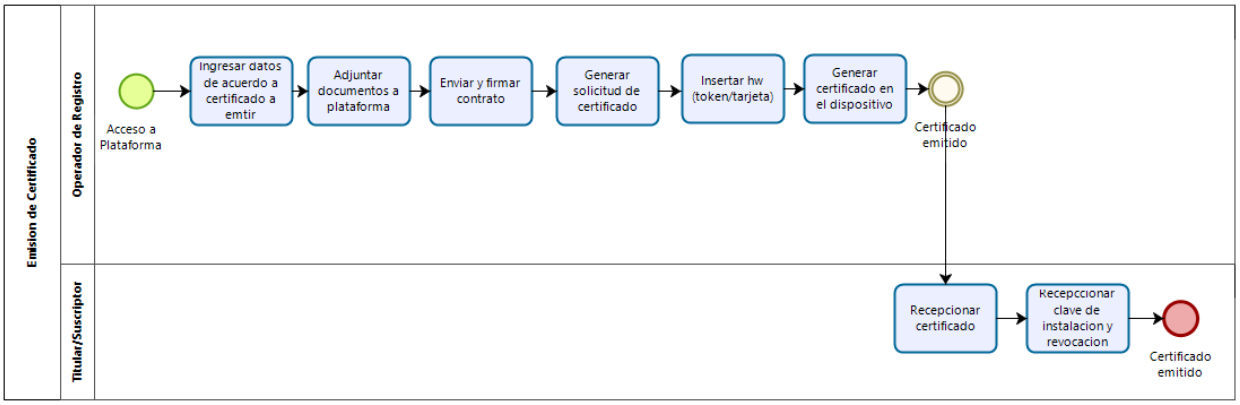
La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor. La petición segura del certificado a la EC LLEIDANET PKI S.L. se realizará en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

A. En el caso de que la emisión del certificado se haga en software, el proceso es el siguiente:



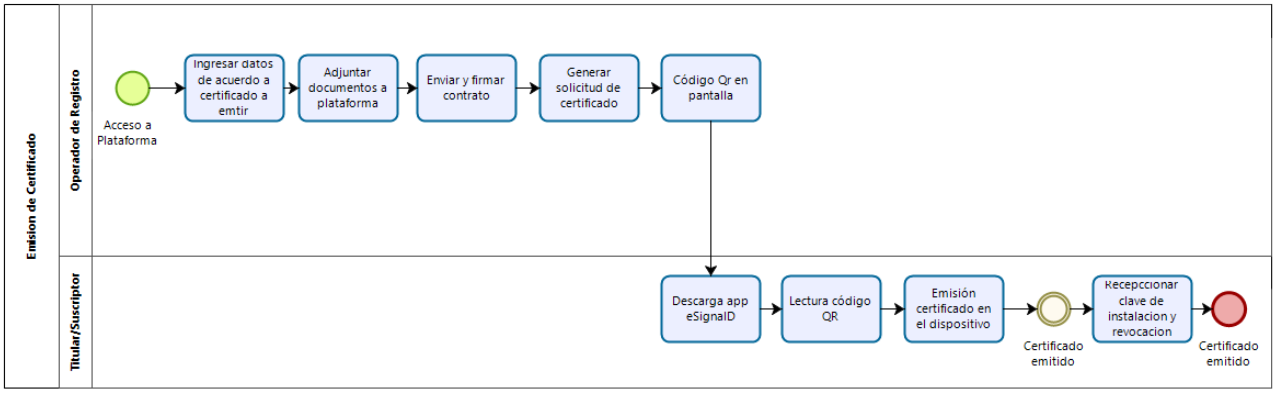
Se realizará el envío de un enlace al usuario por correo que incluye un código de validación. Una vez se acceda y se verifiquen los datos, se generará el certificado que se podrá descargar e instalar el certificado a través de un archivo p12 o pfx.

B. 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 3 o Common Criterial EAL 4+.

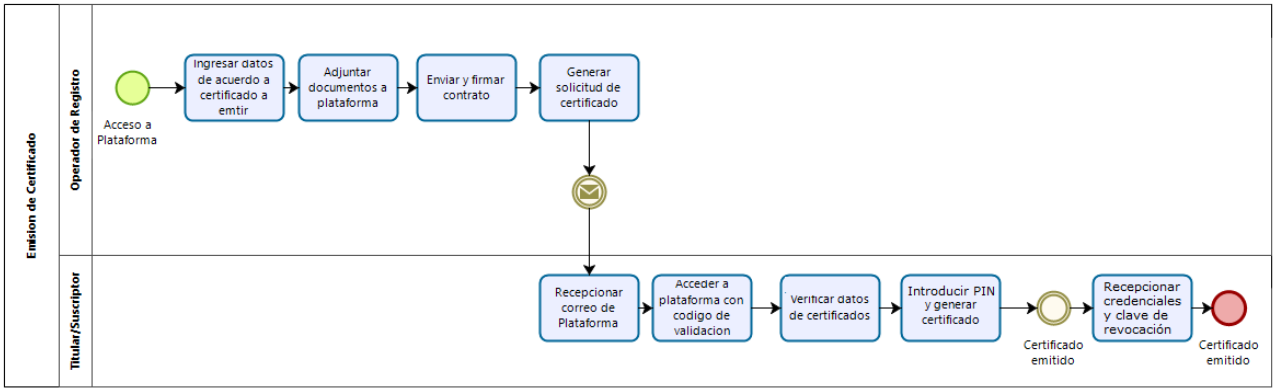
C. En el caso de que la emisión del certificado se haga usando la aplicación Lleida.net Wallet el proceso es el siguiente:



En el caso de Lleida.net Wallet, se generará un código QR en la pantalla del Operador de Registro. En este caso, el solicitante se instala el aplicativo Lleida.net 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.

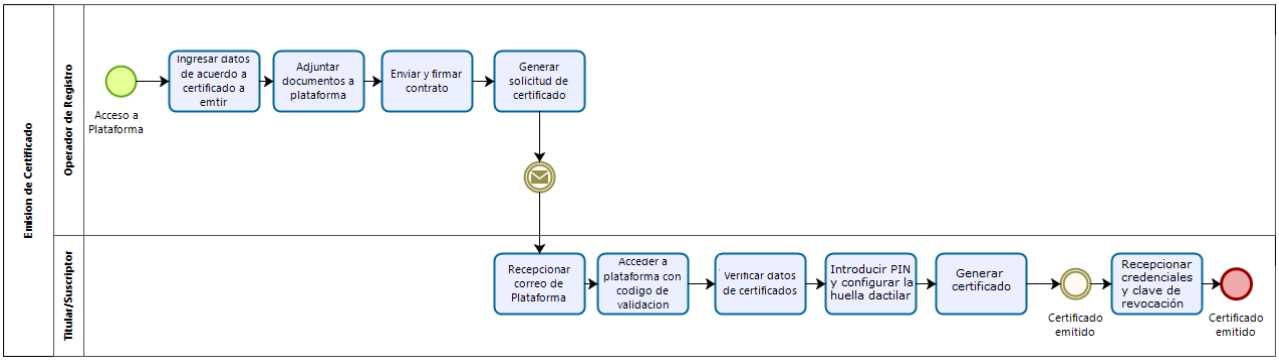
D. En el caso de que la emisión del certificado se haga en el servicio de firma centralizada con acceso mediante credenciales, el proceso es el siguiente:



En este caso del servicio de firma centralizada mediante credenciales, al solicitante le llegará un correo electrónico con un enlace para continuar el proceso de emisión del certificado, en el que deberá introducir un PIN que tendrá que recordar ya que será necesario posteriormente para el uso del certificado generado. Además, recibirá otros correos de activación del certificado y con las credenciales generadas para el acceso al certificado mediante el servicio de firma centralizada.

En este caso la ER no administra ningún módulo criptográfico ya que el certificado es generado en el servicio de firma centralizada de la EC de LLEIDANET PKI S.L.

E. En el caso de que la emisión del certificado se haga en el servicio de firma centralizada con acceso mediante huella dactilar, el proceso es el siguiente:



En este caso del servicio de firma centralizada mediante huella dactilar, al solicitante le llegará un correo electrónico con un enlace para continuar el proceso de emisión del certificado, en el que deberá introducir un PIN que tendrá que recordar ya que será necesario posteriormente para el uso del certificado generado. Posteriormente se configurará la huella dactilar para el acceso al certificado mediante el servicio de firma centralizada.

En este caso la ER no administra ningún módulo criptográfico ya que el certificado es generado en el servicio de firma centralizada de la EC de LLEIDANET PKI S.L.

7.3.2 Notificación al Suscriptor

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

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

7.4 ACEPTACIÓN DEL CERTIFICADO

7.4.1 Conducta que constituye aceptación del certificado

Se considera que un certificado es aceptado por el titular, desde el momento que realiza la descarga o generación de su certificado desde los medios ofrecidos por la AC, por ello, si la información contenida en el certificado expedido no corresponde al estado actual de la misma o no fue suministrada correctamente, se debe solicitar su revocación por parte del solicitante y éste así lo acepta, según

procedimiento descrito en el apartado 7.9.4 Procedimiento de solicitud de la revocación del certificado de este mismo documento.

7.4.2 Publicación del certificado por la AC

LLEIDANET PKI S.L. publica los certificados emitidos en un repositorio en formato X.509 V3 y puede ser consultado en la página Web https://www.indenova.com/acreditaciones/eidas/ donde podemos acceder al repositorio de certificados.

7.4.3 Notificación de la emisión a otras entidades

LLEIDANET PKI S.L. ofrece un sistema de consulta del estado de los certificados emitidos, en su página web https://www.indenova.com/acreditaciones/eidas/. El acceso a esta página es libre y gratuito.

7.5 USO DEL PAR DE CLAVES Y LOS CERTIFICADOS

7.5.1 Uso del certificado y la clave privada del suscriptor

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

El titular o suscriptor deberá notificar a la EC o ER de LLEIDANET PKI S.L. los siguientes casos:

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

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

7.5.2 Uso del certificado y la clave pública por terceros que confían

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

En este sentido deberá comprobar que:

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

El tercero que confía deberá cumplir lo siguiente:

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de LLEIDANET PKI S.L., sin permiso previo por escrito de la EC.
- No comprometer intencionadamente la seguridad de la Jerarquía de LLEIDANET PKI S.L.
- Aplicar los criterios de verificación adecuados para la validación de un certificado durante su uso en las transacciones electrónicas.

Denunciar cualquier situación en la que la EC deba revocar el certificado de un titular, siempre y cuando se tengan pruebas fehacientes del compromiso de la clave privada o de un uso ilegal del manejo de la misma. Por ejemplo, debe denunciar la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena una clave privada que no le pertenece (computador, token criptográfico o tarjeta inteligente).

7.6 RENOVACIÓN DEL CERTIFICADO

7.6.1 Circunstancias para la renovación del certificado

Para la Entidad de Certificación LLEIDANET PKI S.L., un requerimiento de renovación de un certificado es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante.

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

7.6.2 Quién puede solicitar la renovación del certificado

Sólo los titulares de certificados (de persona física o de persona jurídica) pueden solicitar la renovación de certificados:

De persona física:

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

De persona jurídica:

- 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 S.L., 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 nacional de identidad.

7.6.3 Procesamiento de solicitudes de renovación de certificados

7.6.3.1 Solicitud de renovación de certificados

De persona física:

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

De persona jurídica:

- Solicitud de renovación 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.

- Solicitud de renovación 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.

7.6.3.2 Identificación y autenticación de solicitantes de renovación de certificados

De Persona física:

- Se producirá tal como se describe en el apartado 6.2.3 Autenticación de la identidad de la persona física solicitante de este documento.

De persona jurídica:

- Se producirá tal como se describe en el apartado 6.2.2 Autenticación de la identidad de una organización (persona jurídica) de este documento.

7.6.3.3 Aprobación o rechazo de la solicitud de renovación de certificado

Se producirá tal como se describe en el apartado 7.2.2 Aprobación o rechazo de la solicitud del certificado de este documento.

7.6.4 Notificación de la renovación del certificado

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

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

7.6.5 Conducta que constituye la aceptación de la renovación con generación de claves

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

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

7.6.6 Publicación del certificado renovado

Al igual que los certificados nuevos, la Entidad de Certificación LLEIDANET PKI S.L. publica los certificados renovados en un repositorio en formato X.509 V3 y pueden ser consultados en la dirección https://www.indenova.com/acreditaciones/eidas/.

7.6.7 Notificación de la renovación del certificado a otras entidades

LLEIDANET PKI S.L. notifica la renovación del certificado a otras entidades según apartado 7.4.3 Notificación de la emisión a otras entidades.

7.7 RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

Para la Entidad de Certificación LLEIDANET PKI S.L., un requerimiento de renovación de un certificado con regeneración de claves, es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante.

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

7.7.1 Circunstancias para la renovación con regeneración de claves

Las circunstancias para la renovación de certificados con regeneración de claves se realiza del mismo modo explicado en el apartado 7.6.1 Circunstancias para la renovación del certificado.

7.7.2 Quién puede solicitar la renovación con regeneración de claves

Se realiza del mismo modo explicado en el apartado 7.6.2 Quién puede solicitar la renovación del certificado.

7.7.3 Procesamiento de solicitudes de renovación con regeneración de claves

Se realiza del mismo modo explicado en el apartado 7.6.3 Procesamiento de solicitudes de renovación de certificados

7.7.4 Notificación de la renovación con regeneración de claves

Se realiza del mismo modo explicado en el apartado 7.6.4 Notificación de la renovación del certificado.

7.7.5 Conducta que constituye la aceptación de la renovación con regeneración de claves

Se realiza del mismo modo explicado en el apartado 7.6.5 Conducta que constituye la aceptación de la renovación con generación de claves.

7.7.6 Publicación del certificado renovado

Se realiza del mismo modo explicado en el apartado 7.6.6 Publicación del certificado renovado.

7.7.7 Notificación de la renovación con regeneración de claves a otras entidades

Se realiza del mismo modo explicado en el apartado 7.6.7 Notificación de la renovación del certificado a otras entidades.

7.8 MODIFICACIÓN DEL CERTIFICADO

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

7.8.1 Circunstancias para la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.8.2 Quién puede solicitar la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.8.4 Notificación de la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.8.5 Conducta que constituye la aceptación de la modificación del certificado

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.8.6 Publicación del certificado modificado

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.8.7 Notificación de la modificación del certificado modificado a otras entidades

No aplica ya que los certificados digitales emitidos por LLEIDANET PKI S.L. no pueden ser modificados.

7.9 REVOCACIÓN DEL CERTIFICADO

7.9.1 Circunstancias para la revocación del certificado

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

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

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

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

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

7.9.2 Quién puede solicitar la revocación del certificado

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

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

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

7.9.3 NOTIFICACIÓN AL SUSCRIPTOR

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

7.9.4 Procedimiento de solicitud de la revocación del certificado

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

- Servicio de Revocación en línea. A través de la página Web de LLEIDANET PKI S.L., ingresando al servicio de revocación de certificados digitales y mediante la autenticación

del PIN de revocación (CRIN), asignado durante el proceso de solicitud del certificado digital.

- En las oficinas de LLEIDANET PKI S.L. En horario de atención al público se reciben las solicitudes escritas de revocación de certificados digitales firmadas por los titulares.

Los procedimientos de solicitud de revocación según el tipo de solicitante:

De persona física:

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

De persona jurídica:

- 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.

7.9.5 Periodo de gracia de la solicitud de revocación del certificado

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

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

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

7.9.6 Plazo de tiempo para procesar la solicitud de revocación del certificado

La solicitud de revocación de un certificado digital será atendida de manera inmediata a partir del procedimiento descrito en el apartado 7.9.4 Procedimiento de solicitud de la revocación del certificado, de este documento, lo que implica que se realizará en menos de 60 minutos.

7.9.7 Obligación de verificar las revocaciones por las partes que confían

Es responsabilidad del titular de un certificado digital y éste así lo acepta y reconoce, informar a los Terceros que confían de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado. Informará igualmente el titular al Tercero que confía que, para realizar dicha consulta, dispone de la lista de certificados revocados DPC, publicada de manera de periódica por LLEIDANET PKI S.L. en https://www.indenova.com/acreditaciones/eidas/

7.9.8 Frecuencia de generación de las CRLs

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

7.9.9 Periodo máximo de latencia de las CRLs

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática, menor a 24 horas.

7.9.10 Disponibilidad del sistema de verificación online del estado de los certificados

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

7.9.11 Requisitos de comprobación en línea de la revocación del certificado

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

7.9.12 Otras formas de aviso de revocación de claves comprometidas

Los mecanismos que LLEIDANET PKI S.L. pone a disposición de los usuarios del sistema, estarán publicados en su página Web https://www.indenova.com/acreditaciones/eidas/

7.9.13 Requisitos especiales de revocación de claves comprometidas

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

7.9.14 Circunstancias para la suspensión

Cuando se produce una suspensión, LLEIDANET PKI S.L. tendrá una semana para decidir el estado definitivo del certificado: (revocado o activo). En caso de no tener en este plazo toda la información necesaria para la verificación de su estado definitivo, LLEIDANET PKI S.L. revocará el certificado.

En el caso de producirse una suspensión del certificado, se envía un comunicado mediante email al Firmante/Suscriptor comunicando la hora de suspensión y la causa de la misma.

Si finalmente la suspensión no da lugar a la revocación definitiva y el certificado tiene que ser de nuevo activado, el Firmante/Suscriptor recibirá un correo indicando el nuevo estado del certificado.

El proceso de suspensión no se aplica a certificados

• De TSU

• De CA

• De Operador de ER.

• De OCSP

7.9.15 Quién puede solicitar la suspensión

Ver apartado 7.9.2 Quién puede solicitar la revocación del certificado

7.9.16 Procedimiento para la petición de la suspensión

La solicitud de suspensión se realizará según mediante el acceso a la página correspondiente de la web de LLEIDANET PKI S.L. o mediante comunicación oral o escrita previamente autenticada. El suscriptor debe poseer el código de revocación para proceder a la suspensión del certificado.

7.9.17 Límites sobre el periodo de suspensión

Un certificado no permanecerá suspendido más de 7 días.

LLEIDANET PKI S.L. supervisará mediante un sistema de alertas de la plataforma de gestión de certificados que el periodo de suspensión marcado por las Políticas correspondientes y esta DPC no se sobrepasa.

7.10 SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS

La información sobre el estado de revocación de los Certificados permite a los usuarios conocer el estado del Certificado, no solo hasta que éste expire, sino más allá de dicha fecha, dado que no se eliminan los certificados revocados de la correspondiente CRL después de que hayan expirado. En caso de cese de la actividad y/o compromiso de claves de la CA, se generará una última CRL que se mantendrá íntegra y disponible para su consulta garantizando la disponibilidad del servicio de información sobre el estado de los certificados, durante al menos 15 años desde su publicación. En la web: https://www.indenova.com/acreditaciones/eidas/ se indicará el HASH del fichero resultante de la CRL, para su verificación cuando sea necesaria.

La provisión de la información sobre el estado de revocación de los Certificados, en caso de cese de actividad de LLEIDANET PKI S.L. como Prestador de Servicios de Confianza, queda garantizada mediante la transferencia, al organismo supervisor o a otro Prestador con el que se llegue al correspondiente acuerdo, de toda la información relativa a los Certificados y, especialmente, de los datos de su estado de revocación.

Cuando la infraestructura realiza la revocación de un Certificado, el sistema refleja este hecho en la base de datos consultada por el Servicio de información y consulta del estado de los Certificados mediante el protocolo OCSP, al tiempo que genera una nueva CRL y la publica en el repositorio. La citada base de datos cuenta con una copia de respaldo. En caso de ocurrir algún fallo en la secuencia descrita, se produce una alarma al objeto de subsanar el posible error. De esta forma se garantiza la consistencia de la información suministrada por estos dos métodos (OCSP y consulta de CRL). Adicionalmente se realiza la monitorización periódica del repositorio como mantenimiento preventivo.

La información relativa a la verificación del estado de revocación de los Certificados electrónicos expedidos por LLEIDANET PKI S.L. puede ser consultada mediante CRLs y/o el Servicio de información y consulta del estado de los Certificados mediante el protocolo OCSP.

7.10.1 Características operacionales

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

7.10.2 Disponibilidad del servicio

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

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

7.10.3 Características opcionales

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

7.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

La Entidad de Certificación LLEIDANET PKI S.L. da por finalizada la vigencia de un certificado digital emitido ante las siguientes circunstancias:

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

7.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

7.12.1 Prácticas y Políticas de custodia y recuperación de claves

La generación de la clave privada es responsabilidad del titular y es generada directamente sobre un dispositivo controlado por el usuario ya sea en formato hardware o software o con mecanismos de autenticación sólo disponibles para el usuario en el caso de firma centralizada, del cual no se puede exportar. En consecuencia, no es posible la recuperación de la clave privada del titular debido a que no existe copia alguna. La responsabilidad de la custodia de la clave privada es del titular y éste así lo acepta y reconoce.

Para el caso de firma centralizada, LLEIDANET PKI S.L. realiza la custodia de las claves en dispositivos seguros de creación de firma HSM. Las claves almacenadas por LLEIDANET PKI S.L. en sus instalaciones cuentan con mecanismos de encriptación que sólo el usuario conoce o tiene. LLEIDANET PKI S.L. no recuperará las Claves privadas asociadas a los Certificados de Firma Centralizada. En el caso de pérdida del PIN que protege el acceso a dicha Clave por parte del Firmante, se deberá revocar dicho Certificado y solicitar la emisión de uno nuevo.

7.12.2 Prácticas y Políticas de protección y recuperación de la clave de sesión

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

8 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIÓN

8.1 CONTROLES DE SEGURIDAD FÍSICA

8.1.1 Ubicación de las instalaciones

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

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

Esta área restringida cumple con los siguientes requisitos:

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

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

8.1.1.1 Situación del Centro de Proceso de Datos

Se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

8.1.2 Acceso Físico

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

8.1.2.1 Perímetro de seguridad física

Se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

8.1.2.2 Controles físicos de entrada

Se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

8.1.2.3 El trabajo en áreas seguras

Se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

8.1.2.4 Visitas

Se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

8.1.2.5 Áreas aisladas de carga y descarga

Se encuentra especificado en el documento: DOC-1792117 - Dossier Técnico CPD Indenova.

8.1.3 Electricidad y Aire Acondicionado

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

8.1.4 Exposición al agua

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

8.1.5 Prevención y Protección contra incendios

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

8.1.6 Almacenamiento de Soportes

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

8.1.7 Eliminación de residuos

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

8.1.8 Copia de seguridad fuera del sitio

LLEIDANET PKI S.L. mantendrá una copia de respaldo de las bases de datos en custodia fuera de las instalaciones.

8.2 CONTROLES DE PROCEDIMIENTO

8.2.1 Roles de confianza

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

- **Administrador del Sistema**: Responsable de actividades relacionadas con la instalación, configuración y mantenimiento de la infraestructura de hardware, software.
- **Administrador del Servicio**: Responsable de monitorizar la disponibilidad, el estado de salud y gestionar los accesos a los servicios ofrecidos por la plataforma PKI, entre sus funciones está la revisión periódica de los logs de auditoria.
- **Auditor Interno**: Encargado de auditar los procesos del ciclo de emisión de certificados digitales y garantizar el cumplimiento de los procedimientos y políticas de seguridad de la información.
- **Operador ER**: Es el responsable de verificar que la información suministrada por los solicitantes de certificados digitales sea auténtica e integra. Es el responsable de solicitar en nombre de los titulares la emisión o revocación de certificados digitales.
- **Responsable del SGSI**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de LLEIDANET PKI S.L. Debe encargarse aspecto relacionado con la seguridad de la información: lógica, física, redes, organizativa, etc.
- **Proveedor CPD**: Responsable del Centro de Datos y manos remotas[10] a los sistemas de la CA.
- **Responsable de la Información**: Es el máximo responsable del uso que se haga de la información.
- **Responsable de la Red**: Es el responsable de garantizar que las redes y sistemas funcionen de manera ininterrumpida, supervisando infraestructuras complejas,

[10] Este servicio se utilizará en caso excepcional y bajo autorización del responsable de la PKI.

resolviendo incidentes técnicos y previniendo fallos que podrían impactar operaciones clave

Documento de referencia: DOC-200216.20B1609 Organigrama y Roles

8.2.2 Número de personas por tarea

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

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

8.2.3 Identificación y autenticación para cada rol

El Administrador de Sistema, Administrador del Servicio, el Auditor Interno, Operador ER y Responsable del SGSI se autentican mediante certificados digitales emitidos por LLEIDANET PKI S.L. o por login/password.

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

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

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

Documento de referencia: DOC-200216.20B1609 Organigrama y Roles

8.2.4 Roles que requieren segregación de funciones

Los roles de Responsable del SGSI y Auditor Interno son incompatible con cualquier otro rol. El rol de Administrador del Sistema, Administrado del Servicio y el rol de Operador ER son incompatibles entre ellos.

8.3 CONTROLES DEL PERSONAL

8.3.1 Calificaciones, experiencias y requisitos de autorización

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

8.3.2 Procedimientos de verificación de antecedentes

Los términos y condiciones de la relación laboral se integran, además de en el contrato correspondiente, en el Convenio Laboral que regula las relaciones de trabajo entre LLEIDANET PKI S.L. y su personal laboral, así como en la diversa normativa que le es de aplicación en virtud del mencionado Estatuto.

8.3.3 Requisitos de formación

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

- Conocimiento de la Declaración de Prácticas de Certificación.
- Conocimiento de la normatividad vigente y relacionada con las entidades de certificación abierta y los servicios que presta.
- Conocimiento de las Políticas de Seguridad y la aceptación de un acuerdo de confidencialidad sobre la información que se maneja en virtud del cargo.
- Conocimiento de la operación del software y hardware para cada papel específico.
- Conocimiento de los procedimientos de seguridad para cada rol específico.
- Conocimiento de los procedimientos de operación y administración para cada rol específico.
- Conocimiento de los Procedimientos de Contingencia.
- Conocimiento del Documento de Segregación de Funciones.

8.3.4 Requisitos y frecuencia de actualización formativa

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

8.3.5 Secuencia y frecuencia de rotación laboral

No existe rotación de tareas en los cargos mencionados.

8.3.6 Sanciones por acciones no autorizadas

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

8.3.7 Requisitos de contratación de personal

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por LLEIDANET PKI S.L.. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

8.3.7.1 Requisitos de contratación de terceros

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

8.3.8 Suministro de documentación al personal

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

8.4 PROCEDIMIENTO DE REGISTRO DE EVENTOS

LLEIDANET PKI S.L. está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001:2014 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

8.4.1 Tipos de eventos registrados

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

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

Se registran los siguientes eventos:

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

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

8.4.2 Frecuencia de procesamiento de registro

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

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

8.4.3 Periodo de conservación de los registros

LLEIDANET PKI S.L. almacena la información de los registros de auditoría durante al menos quince (15) años.

8.4.4 Protección de los registros

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

8.4.5 Procedimientos de copias de seguridad de los registros auditados

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

8.4.6 Sistema de recolección de registros

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

8.4.7 Notificación al sujeto causante de los eventos

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

8.4.8 Análisis de vulnerabilidades

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

8.5 ARCHIVO DE LOS REGISTROS

8.5.1 Tipos de registros archivados

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

8.5.2 Periodo de retención del archivo

El periodo de conservación de este tipo de documentación es de quince 15 años.

8.5.3 Protección del archivo

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

8.5.4 Procedimientos de copia de respaldo del archivo

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

8.5.5 Requisitos para el sellado de tiempo de los registros

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

8.5.6 Sistema de archivo

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

8.5.7 Procedimientos para obtener y verificar la información archivada

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

8.6 CAMBIO DE CLAVES

8.7 CAMBIO DE CLAVES DE LA RAÍZ

El procedimiento de cambio de claves de la Raíz es el equivalente a generar un nuevo certificado digital. Los certificados emitidos por las EC subordinadas con la clave anterior deben ser revocados o se

debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el titular.

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

8.8 CAMBIO DE CLAVES DE UNA EC SUBORDINADA

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

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

8.9 COMPROMISO Y RECUPERACIÓN ANTE DESASTRES

8.9.1 Gestión de incidentes y vulnerabilidades

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

Documentos de referencia:

- PR-035.110616_-_Gestion_de_incidentes_de_SI
- DOC-110616.17101117 - Plan de continuidad de negocio PKI

8.9.2 Actuación ante datos y software corruptos

Ante una sospecha de alteración de los recursos hardware, software, y/o datos se detendrá el funcionamiento de la EC hasta que se restablezca la seguridad del entorno. Para evitar que se repita el incidente se debe identificar la causa de la alteración.

8.9.3 Procedimiento ante compromiso de la clave privada de la entidad

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

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

- Informará a todos los Titulares, Tercero que confía y otras EC's con los cuales tenga acuerdos u otro tipo de relación del compromiso.

Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

8.9.4 Continuidad de negocio después de un desastre

LLEIDANET PKI S.L. ante un desastre natural u otro tipo de catástrofe, está en capacidad de recuperar los servicios más críticos del negocio, en los tiempos descritos en el documento **Plan de Continuidad de Negocio**.

8.10 CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CONFIANZA

En caso de terminación de la actividad de la EC y ER, LLEIDANET PKI S.L. se regirá por lo dispuesto en la normativa vigente sobre firma electrónica.

LLEIDANET PKI S.L. Informará debidamente a los Suscriptores y Titulares de los Certificados, así como a los Usuarios de los servicios afectados, sobre sus intenciones de terminar su actividad como Prestador de Servicios de Confianza al menos con dos (2) meses de antelación al cese de esta actividad

Terminará cualquier subcontratación que tenga al objeto de la prestación de funciones en nombre de la LLEIDANET PKI S.L. del servicio a cesar.

Podrá transferir, una vez acreditada la ausencia de oposición de los Suscriptores, aquellos Certificados que sigan siendo válidos en la fecha efectiva de cese de actividad a otro Prestador de Servicios de Confianza que los asuma. De no ser posible esta transferencia los Certificados se extinguirán.

Sea cual fuere el servicio en cese, LLEIDANET PKI S.L. transferirá a un tercero los registros de eventos, la información de registro, la información de estado de revocación y auditoría, así como los Certificados empleados en la prestación del servicio, por un periodo suficiente a los efectos que dictamine la legislación vigente.

Comunicará al Organismo de supervisión el cese de su actividad y el destino que vaya a dar a los Certificados, especificando en su caso: si los va a transferir, a quién, o si los dejará sin efecto. La notificación a dicho organismo se realizará con al menos dos (2) meses de antelación, en documento firmado

manuscrita o electrónicamente. Además, se remitirá a dicho organismo la información relativa a los Certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos pertinentes.

Se transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios

Se destruirán las Claves privadas, de forma que no puedan recuperarse.

Todas estas actividades estarán recogidas en el documento interno: DOC-200216.20B2309 Plan de Cese de los Servicios de Certificación

9 CONTROLES DE SEGURIDAD TÉCNICA

9.1 GENERACIÓN E INSTALACIÓN DE LAS CLAVES

9.1.1 Generación del par de claves

9.1.1.1 Generación del par de claves de la CA

La generación del par de claves de la EC Raíz, se realizó dentro de la sala criptográfica del proveedor de servicios de plataforma de la EC/ER con las más estrictas medidas de seguridad y bajo el protocolo de ceremonia de generación de claves establecido para este tipo de eventos y en presencia del representante legal de la Entidad de Certificación LLEIDANET PKI S.L.. Para el almacenamiento de la clave privada se utilizó un dispositivo criptográfico homologado FIPS 140-1 nivel 3 o Common Criteria EAL 4+ con control dual.

9.1.1.2 Generación del par de claves de la RA

La generación del par de claves de las EC subordinadas de LLEIDANET PKI S.L., se realiza dentro de la sala criptográfica del proveedor de servicios de LLEIDANET PKI S.L. bajo el protocolo de ceremonia de generación de claves. Para el almacenamiento de la clave privada subordinada se utiliza un dispositivo criptográfico homologado FIPS 140-1 nivel 3 o Common Criteria EAL 4+ con control dual.

9.1.1.3 Generación del par de claves de los suscriptores

La generación del par de claves, es generada directamente por parte del suscriptor, utilizando un dispositivo criptográfico seguro *"Hardware Security Module (HSM)"*, de generación segura de claves y transmitida mediante un canal seguro; o mediante archivo protegido utilizando el estándar PKCS#12.

9.1.2 Envío de la clave privada al suscriptor

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

9.1.3 Envío de la clave pública al emisor del certificado

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

9.1.4 Distribución de la clave pública de la AC a las partes que confían

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

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

El certificado de la EC Subordinada puede ser consultado por los terceros de confianza en la dirección http://certs.esigna.es/ca/indenova_pki_003.crt

9.1.5 Tamaños de claves y algoritmos utilizados

El tamaño de las claves de la EC Raíz de LLEIDANET PKI S.L. es de 4096 bits.

El tamaño de las claves de las Subordinadas de LLEIDANET PKI S.L. es de 4096 bits.

El tamaño de las claves de los certificados emitidos por LLEIDANET PKI S.L. a usuarios finales es de 2048 bits.

Al intentar derivar la clave privada, a partir de la clave pública de 2048 bits contenida en los certificados de usuarios finales, el problema radica, en encontrar los factores primos de dos números grandes, ya que se tendrían 2^{2047} posibilidades por cada número. En la actualidad resulta

computacionalmente imposible factorizar estos números en un tiempo razonable. Se estima que descifrar una clave pública de 2048 bits requeriría un trabajo de procesamiento del orden de 3 x10^{20} MIPS-10*.

9.1.6 Parámetros de generación de la clave pública y verificación de la calidad

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

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

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

9.1.7 Usos admitidos de las claves

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

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

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

9.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

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

9.2.1 Estándares para los módulos criptográficos

Los módulos criptográficos utilizados en la creación de claves utilizadas por EC Raíz de Entidad de Certificación LLEIDANET PKI S.L. cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria EAL 4+ o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

9.2.2 Control multi-persona (n de m) de la clave privada

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

9.2.3 Custodia de la clave privada

Las claves privadas de la Entidad de Certificación LLEIDANET PKI S.L. se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos de seguridad, Common Criteria EAL 4+ o FIPS 140-2 Nivel 3 o superior.

La clave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del titular. Bajo ninguna circunstancia LLEIDANET PKI S.L. guarda copia de la clave privada del titular ya que esta es generada por el mismo titular y no es posible tener acceso a ella por LLEIDANET PKI S.L.

Los dispositivos utilizados son catalogados como cualificados incluidos en la lista publicada por los estados miembros de la Comisión Europea.

Y ante cualquier cambio de modelo o adquisición de un nuevo dispositivo se realiza una verificación de que este sea cualificado y esté incluido en la lista publicada por los estados miembros de la Comisión Europea.

En caso de pérdida de la certificación QSCD de alguno de los dispositivos cualificados de creación de firma / sello de los que estuviera utilizando LLEIDANET PKI S.L. en calidad de Prestador Cualificado de Servicios de Confianza, se tomarán las medidas oportunas para reducir al mínimo el posible impacto, informando de las mismas al organismo supervisor y paralizando la expedición de certificados sobre dichos dispositivos. Además notificar a los suscriptores de la revocación del certificado indicando el motivo de la pérdida de la certificación QSCD y se le indicará la posibilidad de volver a emitir el certificado en un dispositivo que cumpla con la certificación QSCD.

9.2.4 Copia de seguridad de la clave privada

Las claves privadas de la Entidad de Certificación LLEIDANET PKI S.L. se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria EAL 4+ o FIPS 140-1 Nivel 3 o superior nivel de seguridad. (ver Custodia de la clave privada).

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

9.2.5 Archivado de la clave privada

Las claves privadas de la Entidad de Certificación LLEIDANET PKI S.L. se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria EAL 4+ o FIPS 140-1 Nivel 3 o superior nivel de seguridad. (ver Custodia de la clave privada).

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

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

9.2.6 Transferencia de la clave privada al módulo criptográfico

Las claves privadas de la Entidad de Certificación LLEIDANET PKI S.L. se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria EAL 4+ o FIPS 140-1 Nivel 3 o superior nivel de seguridad. (Ver Custodia de la clave privada).

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

9.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de la Entidad de Certificación LLEIDANET PKI S.L. son generadas y almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria EAL 4+ o FIPS 140-1 Nivel 3 o superior nivel de seguridad. (Ver Custodia de la clave privada).

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

9.2.8 Método de activación de la clave privada

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

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

9.2.9 Método de desactivación de la clave privada

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

9.2.10 Método de destrucción de la clave privada

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

9.2.11 Clasificación de los módulos criptográficos

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

9.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

9.3.1 Archivo de la clave pública

La AC LLEIDANET PKI S.L., en cumplimiento de lo establecido por el artículo 20 f) de la LFE 59/2003 mantendrá sus archivos por un periodo mínimo de quince (15) años siempre y cuando la tecnología de cada momento lo permita. Dentro de la documentación a custodiar se encuentran los certificados de clave pública emitidos a sus suscriptores y los certificados de clave pública propios.

9.3.2 Periodo de uso para las claves públicas y privadas

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

El periodo de validez del certificado digital y el par de claves de EC Raíz de la Entidad de Certificación y de las EC Subordinadas de LLEIDANET PKI S.L. es de treinta (30) años.

9.4 DATOS DE ACTIVACIÓN

9.4.1 Generación e instalación de datos de activación

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

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

9.4.2 Protección de datos de activación

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

9.4.3 Otros aspectos de los datos de activación

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

9.5 CONTROLES DE SEGURIDAD INFORMÁTICA

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

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

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

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

9.5.1 Requisitos técnicos específicos de seguridad informática

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

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

9.5.2 Evaluación del nivel de seguridad informática

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

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

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

9.6 CONTROLES SEGURIDAD DEL CICLO DE VIDA

9.6.1 Controles de desarrollo del sistema

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

9.6.2 Controles de gestión de la seguridad

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

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

9.6.3 Controles de seguridad del ciclo de vida

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

9.7 CONTROLES DE SEGURIDAD DE LA RED

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

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

9.8 FUENTE DE TIEMPO

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

10 PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

10.1 PERFIL DE CERTIFICADO

Los certificados cumplen con el estándar X.509 versión 3 y para la infraestructura de autenticación se basa en el RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

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

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

- Para el caso de personas naturales

La identificación del titular implica el número de documento de identidad y el tipo de documento más el nombre y apellidos

- Para el caso de certificados de personas naturales vinculadas con una persona jurídica (certificados de representante legal, pertenencia a empresa o sello electrónico)

El nombre y la identificación del titular implica lo siguiente número de identificación fiscal de la organización, nombre de la razón social y nombre y apellidos del suscriptor.

De acuerdo al artículo 27.1 del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos establece que "Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca."

NOTA: Aquellos perfiles de certificados que no contengan al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal no podrán ser utilizados para la identificación y firma de las personas interesadas ante las Administraciones Públicas[11]

Descripción del contenido de los certificados

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por LLEIDANET PKI S.L.
Algoritmo de Firma	SHA1RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para LLEIDANET PKI S.L. como emisor se especifica: Description = inDenova Subordinate CA 003 CN = inDenova SUB CA 003

[11] Administraciones Públicas en el ámbito subjetivo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

	O = inDenova SL 2.5.4.97 = VATES-B97458996 SERIALNUMBER = B97458996 OU = Certification Authority inDenova SL T = Subordinate Certificate Authority inDenova SL L = VALENCIA C = ES
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido. Se encuentra sincronizado con el servicio de tiempo UTC-5.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Se encuentra sincronizado con el servicio de tiempo UTC-5.
Sujeto	Ver sección "Reglas para la interpretación de varias formas de nombre".
Clave pública del Sujeto	Codificado de acuerdo con el RFC 5280. La longitud mínima de la clave es de 1024 bits y algoritmo RSA. Los certificados emitidos por LLEIDANET PKI S.L. tienen una longitud de 2048 bits y algoritmo RSA.
Identificador de clave de la autoridad	Es utilizado para identificar el certificado raíz en la jerarquía de certificación. Normalmente referencia el campo "Subject Key Identifier" de LLEIDANET PKI S.L. como entidad emisora de certificación digital.
Identificador de la clave del sujeto	Es usado para identificar un certificado que contiene una determinada clave pública.
Política de certificado	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible las políticas de certificación.
Uso de la clave	Especifica los usos permitidos de la clave. Es un CAMPO CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de LLEIDANET PKI S.L. En el certificado de la EC Raíz, este atributo no se especifica.
Acceso a la información de la Autoridad	Es usado para indicar las direcciones donde se encuentra el certificado raíz de LLEIDANET PKI S.L.. Además, para indicar la dirección para acceder al servicio de OCSP. En el certificado raíz de LLEIDANET PKI S.L., este atributo no se especifica.

Usos extendidos de la clave	Se especifican otros propósitos adicionales al uso de la clave.
Restricciones básicas	La extensión "PathLenConstraint" indica el número de sub-niveles que se admiten en la ruta del certificado. No existe restricción para LLEIDANET PKI S.L. por tanto, es cero.

10.1.1 Numero de versión

Los certificados emitidos por la Entidad de Certificación LLEIDANET PKI S.L. cumplen con el estándar X.509 Versión 3.

10.1.2 Extensiones del certificado

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

10.1.3 Identificadores del objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma puede ser:

• 1.2.840.113549.1.1.11 - sha256WithRSAEncryption

• 1.2.840.113549.1.1.13 – sha512WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es 1.2.840.113549.1.1.1 rsaEncryption

10.1.4 Formato de nombres

El documento guía que LLEIDANET PKI S.L. 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 9594 (X.500).

Los certificados emitidos por LLEIDANET PKI S.L. 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.

10.1.4.1 CERTIFICADO RAÍZ DE LLEIDANET PKI S.L.

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

CN = Certification Authority Root Indenova SL

O = Indenova SL

SERIALNUMBER = B97458996

OU = Certification Authority Indenova SL

L = Valencia

C = ES

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

CN = Certification Authority Root Indenova SL

O = Indenova SL

SERIALNUMBER = B97458996

OU = Certification Authority Indenova SL

L = Valencia

C = ES

10.1.4.2 Certificados de las subordinadas de LLEIDANET PKI S.L.

El DN del 'issuer name' de los certificados de las subordinadas de LLEIDANET PKI S.L., tiene las siguientes características:

CN = Certification Authority Root Indenova SL

O = Indenova SL

SERIALNUMBER = B97458996

OU = Certification Authority Indenova SL

L = Valencia

C = ES

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

Description = inDenova Subordinate CA 003

CN = inDenova SUB CA 003

O = inDenova SL

2.5.4.97 = VATES-B97458996

SERIALNUMBER = B97458996

OU = Certification Authority inDenova SL

T = Subordinate Certificate Authority inDenova SL

L = VALENCIA

C = ES

10.1.4.3 CERTIFICADOS DE TITULAR DE LLEIDANET PKI S.L.

El DN del 'issuer name' de los certificados de titular de LLEIDANET PKI S.L., tiene las siguientes características generales:

Description = inDenova Subordinate CA 003

CN = inDenova SUB CA 003

O = inDenova SL

2.5.4.97 = VATES-B97458996

SERIALNUMBER = B97458996

OU = Certification Authority inDenova SL

T = Subordinate Certificate Authority inDenova SL

L = VALENCIA

C = ES

La descripción y los campos en el DN del 'subject name', para cada tipo de certificado cubiertos por esta DPC, están detallados en el documento DOC-200216.2093009 - Perfiles Certificados.pdf.

10.1.5 Restricciones de los nombres

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

El código del país se asigna de acuerdo al estándar ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”.

10.1.6 Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto de la Política de certificado se indica en el apartado 4.2 Nombre del documento e Identificación.

10.1.7 Uso de la extensión “Policy Constraints”

No se estipula.

10.1.8 Sintaxis y semántica de los calificadores de política

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

10.1.9 Tratamiento semántico para la extensión “certificate policy”

No se estipula.

10.2 PERFIL DE LA CRL

Las CRL´s emitidas por la Entidad de Certificación LLEIDANET PKI S.L. cumplen con el RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2” y contienen los siguientes elementos básicos:

10.2.1 Número de versión

Las CRL´s emitidas por LLEIDANET PKI S.L. cumplen con el estándar X.509 versión 2.

10.2.2 CRL y extensiones

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

10.3 PERFIL DE LA OCSP

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

10.3.1 Número de versión

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

10.3.2 Extensiones del OCSP

No aplica.

11 AUDITORÍAS DE CUMPLIMIENTO

11.1 FRECUENCIA DE LAS AUDITORÍAS

La infraestructura y procedimientos de LLEIDANET PKI S.L. será evaluado al menos anualmente por un organismo de evaluación de la conformidad.

Acreditación del cumplimiento como Prestador de Servicios de Confianza, en aplicación del Reglamento UE nº 910/2014 (Reglamento eIDAS), ETSI EN 319 401 “General Policy Requirements for Trust Service Providers” y ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates”:

- La frecuencia de la auditoría es bienal (al menos cada dos años), con auditorías de seguimiento anuales.

Los Certificados que tienen la consideración de cualificados, son sometidos a la auditoría anual que garantiza el cumplimiento con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”

Sistema de Gestión de Seguridad de la Información según la Norma UNE-ISO/IEC 27001:2014:

- Renovación cada 3 años con auditorías de seguimiento anuales.

Sistema de Gestión de la Calidad conforme con la Norma ISO 9001:2015:

- Renovación cada 3 años con auditorías de seguimiento anuales.

Madurez de los procesos del ciclo de vida de software conforme con la Norma ISO/IEC 33000 e ISO/IEC 12207, nivel alcanzado 3:

- Renovación cada 3 años con auditorías de seguimiento anuales.

11.2 CUALIFICACIÓN DEL AUDITOR

El auditor será seleccionado en el momento de la realización de cada auditoría, será independiente externo, el cual tendrá que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y/o en auditorías de conformidad de Autoridades de Certificación y los elementos relacionados.

11.3 RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

11.4 ELEMENTOS OBJETOS DE AUDITORIA

Los elementos cubiertos por la auditoría son la implementación de las prácticas de certificación, personal, procedimientos y técnicas, descritos en el Reglamento vigente.

11.5 TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

11.6 COMUNICACIÓN DE LOS RESULTADOS

Una vez terminada la Auditoria, la firma Auditora debe presentar el Informe de Auditoria a LLEIDANET PKI S.L. y si se requiere LLEIDANET PKI S.L. debe establecer un Plan de Acciones Correctivas.

11.7 AUTOEVALUACIÓN

Adicionalmente, LLEIDANET PKI S.L. realiza auditorías internas para autoevaluar el cumplimiento de sus Políticas de Certificación, Declaración de Prácticas de Certificación, normativa aplicable, para controlar la calidad en la prestación de los servicios. Estas auditorías internas se llevan a cabo anualmente, tomando una muestra seleccionada al azar.

12 OTROS ASUNTOS LEGALES Y COMERCIALES

12.1 TARIFAS

12.1.1 Tarifas de emisión o renovación de certificados

Las tarifas serán definidas por LLEIDANET PKI S.L. de acuerdo a los contratos celebrados con sus clientes.

12.1.2 Tarifas de acceso a los certificados

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

12.1.3 Tarifas de acceso a la información de estado o revocación

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

12.1.4 Tarifas para otros servicios

Una vez se ofrezcan otros servicios por parte de LLEIDANET PKI S.L., se publicarán en la dirección https://www.indenova.com/acreditaciones/eidas/

12.1.5 Política de reembolso

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

12.2 RESPONSABILIDAD FINANCIERA

12.2.1 Seguro de Responsabilidad Civil

La EC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente, por un importe de 4.000.000 de euros.

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

Las responsabilidades de la EC incluyen las establecidas por la presente DPC, así como las que resulten de aplicación como consecuencia de la normativa vigente.

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

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

12.2.2 Otros activos

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

12.2.3 Seguro de cobertura o garantía para entidades finales

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

12.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

12.3.1 Alcance de la información confidencial

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

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

12.3.2 Información no incluida en el alcance

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

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

12.3.3 Responsabilidad para proteger la información confidencial

LLEIDANET PKI S.L. mantiene medidas de seguridad para proteger toda la información confidencial suministrada a ella directamente o a través de los canales establecidos para ello desde su recibo hasta su almacenamiento y custodia en el archivo central donde reposarán por el tiempo indicado en la normativa vigente. LLEIDANET PKI S.L. cuenta con un procedimiento de Seguridad para el manejo y custodia de la

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

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

12.4 PROTECCIÓN DE DATOS PERSONALES

12.4.1 Plan de privacidad

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

12.4.2 Información tratada como privada

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

12.4.3 Información no considerada privada

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

12.4.4 Responsabilidad de proteger la información privada

La Entidad de Certificación LLEIDANET PKI S.L. es responsable y cuenta con los adecuados mecanismos de seguridad y control para garantizar la protección, confidencialidad y debido al uso de la información suministrada por el titular, para ello, LLEIDANET PKI S.L. se rige de acuerdo al Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

12.4.4.1 Delegado de Protección de Datos

El RGPD establece la obligación de designar un Delegado de Protección de Datos (DPD) a toda autoridad u organismo del sector público que lleve a cabo tratamiento de datos personales. Los datos de contacto del DPD de LLEIDANET PKI S.L. están publicados en el sitio web https://www.indenova.com/acreditaciones/eidas/.

12.4.4.2 Registro de actividades de tratamiento

LLEIDANET PKI S.L. cuenta con un registro de las actividades de tratamiento que realiza bajo su responsabilidad, entre los que se encuentra el de "Datos para la solicitud y emisión de certificados digitales asociados a la infraestructura de pki" relativo a la actividad que realiza esta Entidad como Prestador de Servicios de Confianza. Dicho registro incluye, para cada tratamiento identificado, la siguiente información:

- Nombre del fichero o tratamiento
- Unidad/es con acceso al fichero o tratamiento
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos
- Nivel de medidas de seguridad a adoptar
- Administrador
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento
- Código Tipo Aplicable
- Estructura del fichero principal
- Información sobre el fichero o tratamiento
    - Finalidad y usos previstos
    - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos
    - Procedimiento de recogida
    - Cesiones previstas
    - Transferencias Internacionales
    - Sistema de tratamiento
    - Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición
    - Descripción detallada de las copias de respaldo y de los procedimientos de recuperación
    - Información sobre conexión con otros sistemas

- Funciones del personal con acceso a los datos personales
- Descripción de los procedimientos de control de acceso e identificación
- Relación actualizada de usuarios con acceso autorizado

Documento de referencia: DOC-220100.2233115 - Registro de las Actividades de Tratamiento.pdf

12.4.4.3 Derechos de los interesados

Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del RGPD, dirigiéndose al responsable del tratamiento por vía electrónica, a través de la sede electrónica de LLEIDANET PKI S.L., o presencialmente en la dirección indicada en el apartado 4.5.2 Datos de contacto.

12.4.4.4 Cooperación con las autoridades

LLEIDANET PKI S.L. cooperará con la Agencia Española de Protección de Datos cuando sea requerida.

12.4.4.5 Notificación de violaciones de seguridad

LLEIDANET PKI S.L. notificará a la Agencia Española de Protección de Datos (AEPD) cualquier violación de seguridad[12] en materia de datos personales, sin dilación posible y, en todo caso, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella, siempre que esta sea susceptible de constituir un riesgo para los derechos las libertades de las personas físicas afectadas.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la AEPD se complementará con una notificación dirigida a estos últimos, al objeto de permitirles la adopción de medidas para protegerse de sus consecuencias.

12.4.5 Aviso y consentimiento para usar información privada

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

[12] Según el RGPD, violación de seguridad de los datos personales incluye todo incidente que ocasione la destrucción, pérdida, o alteración , divulgación no autorizada o acceso accidental o ilegal de accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a de dichos datos.

12.4.6 Divulgación conforme al proceso judicial o administrativo

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

12.4.7 Otras circunstancias de divulgación de información

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

12.5 DERECHOS DE PROPIEDAD INTELECTUAL

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

12.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL

12.6.1 Obligaciones de la EC

LLEIDANET PKI S.L. está obligada según normativa vigente y en lo dispuesto en las Políticas de Certificación y en esta DPC a:

1. Respetar lo dispuesto en la normatividad vigente, en esta DPC y en las Políticas de Certificación PC.
2. Publicar esta DPC y cada una de las Políticas de Certificación en la página Web de LLEIDANET PKI S.L..
3. Mantener publicada en la página Web la última versión de la DPC y las Políticas de Certificación de LLEIDANET PKI S.L.
4. Proteger y custodiar de manera segura y responsable su clave privada.
5. Emitir certificados conforme a las Políticas de Certificación y a los estándares definidos en la presente DPC.
6. Generar certificados consistentes con la información suministrada por el solicitante o titular.

7. Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.
8. Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
9. Publicar el estado de los certificados emitidos en un repositorio de acceso libre.
10. No mantener copia de la clave privada del solicitante o titular.
11. Revocar los certificados según lo dispuesto en la Política de revocación de certificados digitales.
12. Actualizar y publicar la lista de certificados revocados CRL con los últimos certificados revocados.
13. Notificar al Solicitante o Titular la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con la política de revocación de certificados digitales.

12.6.2 Obligaciones de la ER

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

1. Conocer y dar cumplimiento a lo dispuesto en la presente DPC y en la Política de Certificación correspondiente a cada tipo de certificado.
2. Custodiar y proteger su clave privada.
3. Comprobar la identidad de los Solicitantes y Titulares de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
5. Archivar y custodiar la documentación suministrada por el solicitante o titular, durante el tiempo establecido por la legislación vigente.
6. Respetar lo dispuesto en los contratos firmados entre LLEIDANET PKI S.L. y el titular.
7. Identificar e informar a la EC las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

12.6.3 Obligación de los titulares

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

1. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados digitales para facilitar su oportuna y plena identificación.
2. Cumplir con lo aceptado y firmado en el Formulario de Solicitud de certificado digital.
3. Proporcionar con exactitud y veracidad la información requerida.
4. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
5. Custodiar y proteger de manera responsable su clave privada.

6. Dar uso al certificado de conformidad con las Políticas de Certificación establecidos en la presente DPC para cada uno de los tipos de certificado.
7. Solicitar como titular de manera inmediata la revocación de su certificado digital cuando tenga conocimiento que existe una causal definida en numeral *Circunstancias para la revocación de un certificado* de la presente DPC.
8. No hacer uso de la clave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
9. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
10. Informar al Tercero que confía para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera de periódica por LLEIDANET PKI S.L.

12.6.4 Obligación de las partes de confían

Los Terceros que confían en su calidad de parte que confía en los certificados digitales emitidos por la Entidad de Certificación LLEIDANET PKI S.L. está en la obligación de:

1. Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
2. Conocer lo dispuesto en la Declaración de Prácticas de Certificación.
3. Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
4. Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
5. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.
6. Verificar la validez de los certificados en el momento de realizar cualquier operación basado en los mismos. En ese sentido, los terceros que confíen comprobarán que el certificado es cualificado consultando a la Lista de Confianza de la Unión Europea (TSL), con el fin de determinar si puede ser considerado como un certificado cualificado.

12.6.5 Obligaciones de otros participantes

El Comité de Seguridad como organismo interno de la Entidad de Certificación LLEIDANET PKI S.L. está en la obligación de:

1. Revisar la consistencia de DPC con la normatividad vigente.
2. Autorizar los cambios o modificaciones requeridas sobre la DPC.
3. Autorizar la publicación de la DPC en la página Web de LLEIDANET PKI S.L..
4. Integrar la DPC, a la DPC de terceros proveedores de servicios de certificación.
5. Aprobar los cambios o modificaciones a las Políticas de Seguridad de LLEIDANET PKI S.L..
6. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la Entidad de Certificación LLEIDANET PKI S.L..

7. Asegurar la existencia de controles sobre la infraestructura tecnológica de la Entidad de Certificación LLEIDANET PKI S.L.
8. Solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la clave privada del subscriptor o cualquier otro hecho que tienda al uso indebido de clave privada del titular o de la Entidad de Certificación.
9. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.

12.7 RENUNCIA DE GARANTÍAS

LLEIDANET PKI S.L. puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la legislación vigente, reguladora de determinados aspectos de los servicios electrónicos de confianza, especialmente aquellas garantías de adaptación para un propósito particular del certificado.

12.8 LIMITACIONES DE RESPONSABILIDAD

Según la legislación vigente, la responsabilidad de LLEIDANET PKI S.L. no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Sujeto, y a la Parte Usuaria por:

- No haber proporcionado información adecuada, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación;
- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad;
- No haber solicitado la suspensión o revocación de los datos del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad;
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico;
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables a la Parte Usuaria si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado
- De los daños ocasionados al Sujeto o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible.

- Un uso inadecuado o fraudulento del certificado en caso de que el Sujeto/Titular lo haya cedido o haya autorizado su uso a favor de una tercera persona en virtud de un negocio jurídico como el mandato o apoderamiento, siendo exclusiva responsabilidad del Sujeto /Titular el control de las claves asociadas a su certificado.

LLEIDANET PKI S.L. tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en las Políticas de Certificación
- Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la AC
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Sujeto.

12.9 INDEMNIZACIONES

Revisar apartado 12.2 Responsabilidad financiera

12.9.1 Indemnizaciones de la CA

Revisar apartado 12.2 Responsabilidad financiera

12.9.2 Indemnizaciones de los suscriptores

Revisar apartado 12.2 Responsabilidad financiera

12.9.3 Indemnizaciones de las partes de confían

Revisar apartado 12.2 Responsabilidad financiera

12.10 PERIODO DE VALIDEZ DE ESTE DOCUMENTO

12.10.1 Plazo

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

12.10.2 Terminación

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

12.10.3 Efectos de la finalización

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

12.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

Cualquier notificación referente a la presente DPC se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto 4.5.2 Datos de contacto

12.12 MODIFICACIONES DE ESTE DOCUMENTO

12.12.1 Procedimiento para las modificaciones

Esta DPC se modificará cuando se produzcan cambios relevantes en la gestión de cualquier tipo de certificados sujetos a ella. Se producirán al menos revisiones anuales en caso de que no se produzcan cambios en este tiempo.

12.12.2 Periodo y mecanismo de notificación

Esta DPC se revisará anualmente y, en cualquier caso, cada vez que deba llevarse a cabo alguna modificación de la misma.

Cualquier modificación en la presente DPC será publicada de forma inmediata en la URL https://www.indenova.com/acreditaciones/eidas/.

Si las modificaciones a realizar no conllevan cambios significativos en cuanto al régimen de obligaciones y responsabilidades de las partes o relativos a una modificación de las políticas de prestación

de los servicios, LLEIDANET PKI S.L. no informará previamente a los usuarios, limitándose a publicar una nueva versión de la declaración afectada en su página web. Si las modificaciones a realizar conllevan cambios significativos en cuanto al régimen de obligaciones y responsabilidades de las partes o relativos a una modificación de las políticas de prestación de los servicios, LLEIDANET PKI S.L. informará a las partes involucradas en el cambio.

12.12.3 Circunstancias bajo las cuales debe cambiarse un OID

No estipulado.

12.13 RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

LLEIDANET PKI S.L. atenderá cualquier solicitud, queja o reclamación por parte de sus clientes o terceros que confían en sus servicios de confianza, de conformidad con los protocolos aprobados por dicha Entidad mediante el procedimiento interno PR-005-110616.1170608 v.1.0 - Reclamaciones de clientes. Los datos de contacto para remitir dichas sugerencias, quejas o reclamaciones son los consignados en el apartado 4.5.2 Datos de contacto del presente documento.

12.14 NORMATIVA DE APLICACIÓN

Las operaciones y funcionamiento, así como la presente DPC, estarán sujetas a la legislación vigente. Explícitamente se asumen como de aplicación las siguientes leyes y reglamentos:

Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Real Decreto 505/2007, de 20 de abril, por el que se aprueban las condiciones básicas de accesibilidad y no discriminación de las personas con discapacidad para el acceso y utilización de los espacios públicos urbanizados y edificaciones.

Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

Adicionalmente, las prácticas de los servicios de confianza provistos por LLEIDANET PKI S.L. siguen los siguientes estándares o las modificaciones realizadas en su caso:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.

12.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE

El cumplimiento se encuentra consignado en el apartado 12.14 Normativa de aplicación

12.16 OTRAS DISPOSICIONES

12.16.1 Acuerdo integro

Sin estipulación.

12.16.2 Asignación

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

12.16.3 Severabilidad

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

12.16.4 Cumplimiento (honorarios de abogados y exención de derechos)

LLEIDANET PKI S.L. puede solicitar una indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de dicha parte. El hecho de que LLEIDANET PKI S.L. no haga cumplir una disposición de esta DPC no elimina el derecho de LLEIDANET PKI S.L. de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de esta DPC. Para ser efectiva, cualquier renuncia debe estar por escrito y firmada por LLEIDANET PKI S.L.

12.16.5 Fuerza mayor

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

12.17 OTRAS PROVISIONES

Sin estipulación.

13 ANEXOS

DOC-1792117 - Dossier Técnico CPD Indenova.pdf

DOC-200216.20B1609 Organigrama y Roles.pdf

PR-035.110616 - Gestión de incidentes de SI.pdf

DOC-110616.17101117 - Plan de continuidad de negocio PKI.pdf

DOC-200216.20B2309 Plan de Cese de los Servicios de Certificación.pdf

PR-005.110616.1170608 Reclamaciones de clientes

DOC-200216.2093009 - Perfiles Certificados.pdf